

**КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА**

**Костюк Ю.В., Складанний П.М., Гулак Г.М.
Бєбешко Б.Т., Хорольська К.В., Рзаєва С.Л.**

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ
Підручник

Київ 2025

УДК 004.056.5

*Рекомендовано Вченою радою Факультету інформаційних технологій та математики
(протокол №3 від 19 березня 2025 року)*

Автори:

**Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т.,
Хорольська К.В., Рзаєва С.Л.**

Рецензенти: В. Л. Шевченко, д-р техн. наук, професор, заступник директора з наукової роботи Інституту програмних систем Національної академії наук України;
О. А. Смірнов, д-р техн. наук, професор, професор кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Костюк Ю. В.

Системи захисту інформації : підручник / Ю.В. Костюк, П.М. Складанний, Г.М. Гулак, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва. – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 887 с.

У підручнику розглянуто широкий спектр питань, що стосуються забезпечення безпеки інформаційно-комунікаційних систем, з особливим акцентом на системах захисту інформації. Аналізуються різні аспекти нормативно-правового забезпечення безпеки, адміністративного та організаційного управління, а також інженерно-технічного захисту ІКС. Окрема увага приділяється сучасним і методам захисту інформації, включаючи програмно-апаратні комплекси, криптографічні методи, технології міжмережевих екранів і системи виявлення атак. Підручник описує принципи технічної та економічної розвідки, що є важливими для запобігання кіберзагрозам, а також стратегії захисту інформації від реалізації цих загроз. Автори також висвітлюють роль комплексних систем захисту, технологій управління доступом і проведення аудиту ІКС, що дозволяють забезпечити максимальний рівень безпеки на всіх етапах функціонування ІКС. Важливим розділом є стратегія відновлення функціонування ІКС після кіберзламів, збоїв або інших загроз, що забезпечує безперервність роботи систем.

Підручник стане корисним для фахівців з кібербезпеки, студентів і всіх, хто цікавиться питаннями захисту інформації в умовах сучасних технологічних викликів.

УДК 004.056.5

ISBN

© Костюк Ю. В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. 2025
© Київський столичний університет імені Бориса Грінченка, 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	9
ВСТУП.....	10
ТЕМА 1. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІКС	13
РОЗДІЛ 1 ЗАКони, НОРМАТИВНІ ДОКУМЕНТИ І СТАНДАРТИ.....	13
1.1. Законодавство України по забезпеченню кібербезпеки	15
1.2. Нормативні документи системи технічного захисту інформації.....	33
1.3. Стандарти інформаційної безпеки. Стандарт TCSEC	38
1.4. Поняття кіберзлочинності. Класифікація кіберзлочинів	54
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 1	63
РОЗДІЛ 2 МІЖНАРОДНІ СТАНДАРТИ	67
2.1. Класи безпеки комп'ютерних систем	68
2.2. Міжнародні стандарти серії ISO 27000.....	76
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 2	88
Контрольні питання	90
ТЕМА 2. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ УПРАВЛІННЯ БЕЗПЕКОЮ ІКС	92
РОЗДІЛ 3 ПОЛІТИКА БЕЗПЕКИ.....	92
3.1. Організаційний захист	94
3.2. Склад і структура політики безпеки.....	110
3.3. Зразок спеціалізованої політики безпеки допустимого використання	128
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 3	132
РОЗДІЛ 4 ПРОЦЕДУРИ ВПРОВАДЖЕННЯ ТА РЕАЛІЗАЦІЇ ПОЛІТИКИ БЕЗПЕКИ.....	135
4.1. Процедури реалізації політики безпеки.....	135
4.2. Оновлення ПЗ та зниження привілеїв	145
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 4	156
РОЗДІЛ 5 УПРАВЛІННЯ РИЗИКАМИ	159
5.1. Підходи до аналізу ризиків безпеки ІКС	159
5.2. Реалізація змішаного підходу до аналізу ризиків	173
5.3. Оцінювання ризиків	179
5.4. Типові витрати на забезпечення безпеки ІКС	181
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 5	189
Контрольні питання	191
ТЕМА 3. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІКС.....	193
РОЗДІЛ 6 МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ	193

6.1. Загальна характеристика інженерно-технічних засобів безпеки.....	194
6.2. Методи фізичного захисту інформації.....	204
6.3. Характеристика технічних каналів витоку інформації	209
6.4. Захист інформації від витоку електричними та електромагнітними каналами.....	239
6.5. Методи захисту від витоку інформації за рахунок акустичних та оптичних каналів	244
6.6. Технічні канали витоку інформації на основі закладних пристроїв	249
6.7. Заходи захисту інформації від витоку каналами на основі закладних пристроїв.....	257
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 6	260
РОЗДІЛ 7 ПРИНЦИПИ ТЕХНІЧНОЇ РОЗВІДКИ	263
7.1. Поняття та принципи технічної розвідки	264
7.2. Основні задачі, органи та види технічної розвідки	269
7.3. Поняття промислового шпигунства	278
7.4. Принципи захисту від технічної розвідки	283
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 7	284
РОЗДІЛ 8 ЕКОНОМІЧНА РОЗВІДКА І ПРИНЦИПИ ЗАХИСТУ ВІД НЕЇ.....	287
8.1. Технічні засоби економічної розвідки	288
8.2. Принципи захисту від економічної розвідки	301
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 8	312
Контрольні питання	314
ТЕМА 4. ПРОГРАМНО-АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІКС	316
РОЗДІЛ 9 ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ	316
9.1. Загальна характеристика програмних засобів безпеки ІКС	317
9.2. Ідентифікація, аутентифікація та авторизація в ІКС	325
9.3. Види аутентифікації суб'єктів в ІКС	333
9.4. Парольна аутентифікація.....	338
9.5. Аутентифікація на основі PIN-коду	341
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 9	345
РОЗДІЛ 10 ВИДИ АУТЕНТИФІКАЦІЇ	348
10.1. Апаратна аутентифікація.....	348
10.2. Аутентифікація за допомогою біометричних даних	360
10.3. Аутентифікація на основі цифрових сертифікатів	367
10.4. Централізовані системи аутентифікації. Концепція єдиного логічного входу.....	370
10.5. Система Kerberos.....	376
10.6. Централізований контроль віддаленого доступу.....	382

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 10	393
РОЗДІЛ 11 ВИКОРИСТАННЯ СПИСКІВ КОНТРОЛЮ ДОСТУПУ	396
11.1. Типи і використання списків контролю доступу.....	396
11.2. Використання шаблонних масок	400
11.3. Стандартні списки контролю доступу	402
11.4. Розширені списки контролю доступу	405
11.5. Іменовані списки контролю доступу.....	407
11.6. Розміщення стандартних і розширених списків контролю доступу	409
11.7. Перевірка списків контролю доступу	412
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 11	415
РОЗДІЛ 12 ТЕХНОЛОГІЯ МІЖМЕРЕЖЕВИХ ЕКРАНІВ ТА СИСТЕМ ВИЯВЛЕННЯ АТАК.....	417
12.1. Класифікація та архітектура міжмережевих екранів.....	417
12.2. Міжмережіві екран прикладного рівня. Проксі-сервери.....	439
12.3. Проксі-сервер Squid	453
12.4. Системи виявлення атак	454
12.5. Системи виявлення та запобігання вторгнень	462
12.6. Системи контролю та управління доступом у мережі (Active Directory, ACL)	466
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 12	469
РОЗДІЛ 13 МОНІТОРИНГ ПРОЦЕСІВ ФУНКЦІОНУВАННЯ ІКС	472
13.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторингу	472
13.2. Система візуалізації та управління подіями (SIEM)	474
13.3. Аналіз подій SIEM	478
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 13	481
РОЗДІЛ 14 МЕХАНІЗМИ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ.....	484
14.1. Віртуальні приватні мережі (VPN).....	484
14.2. Протоколи аутентифікації RADIUS	488
14.3. Протоколи SSL/TLS	492
14.4. Захищений протокол віддаленого доступу SSH	509
14.5. Протоколи IPSec	515
14.6. PGP (Pretty Good Privacy)	525
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 14	528
Контрольні питання	530
ТЕМА 5. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.....	532
РОЗДІЛ 15 ОСНОВНІ ПОНЯТТЯ І ЗАДАЧІ КРИПТОЛОГІЇ	532
15.1. Симетричні та асиметричні криптосистеми.....	533
15.2. Основи криптоаналізу.....	552
15.3. Методи стеганографії	558
15.4. Модель стеганосистеми.....	566

15.5. Поняття ЦВЗ та їх класифікація	571
15.6. Метод модифікації найменшого значущого біта	572
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 15	573
РОЗДІЛ 16 МОДЕЛІ ЗАГРОЗ БЕЗПЕКИ КРИПТОСИСТЕМ	576
16.1. Формальна модель загроз криптосистем	576
16.2. Атаки на симетричні і асиметричні шифрсистеми	580
16.3. Властивості елементарних шифрів	588
16.4. Теоретична та практична стійкість, абсолютно стійкий шифр	593
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 16	598
РОЗДІЛ 17 ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ І МЕТОДИ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ _	601
17.1. Дані для формування ключової інформації	601
17.2. Статистичне тестування псевдовипадкових послідовностей	605
17.3. Генератори псевдовипадкових послідовностей	606
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 17	610
РОЗДІЛ 18 КЛАСИЧНІ МЕТОДИ СИМЕТРИЧНОГО ШИФРУВАННЯ	613
18.1. Шифри перестановок	613
18.2. Шифри підстановок	618
18.3. Гамування	623
18.4. Аналітичні методи	625
18.5. Поточкові шифри	626
18.6. Блокові складені шифри	631
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 18	638
РОЗДІЛ 19 СИМЕТРИЧНІ КРИПТОАЛГОРИТМИ	641
19.1. Алгоритм DES	641
19.2. Основні режими роботи алгоритму DES	648
19.3. Стійкість та модифікація DES	653
19.4. Алгоритм шифрування IDEA	656
19.5. Алгоритм AES	659
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 19	661
РОЗДІЛ 20 АСИМЕТРИЧНІ КРИПТОСИСТЕМИ	664
20.1. Основні поняття	664
20.2. Криптосистема RSA	667
20.3. Криптосистема Ель-Гамала	670
20.4. Криптосистеми на основі еліптичних кривих	672
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 20	680
РОЗДІЛ 21 ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС	683
21.1. Проблема аутентифікації даних і електронний цифровий підпис	683
21.2. Хеш-функція	687

21.3. Алгоритми електронного цифрового підпису.....	696
21.4. Стандарти алгоритмів формування і перевірки ЕЦП.....	699
21.5. Протоколи взаємодії і сертифікати в стандарті X.509	700
21.6. Структура сертифіката відкритих ключів	702
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 21	704
РОЗДІЛ 22 КРИПТОГРАФІЧНІ ПРОТОКОЛИ	
22.1. Поняття криптографічного протоколу.....	707
22.2. Розподіл ключів і аутентифікація.....	712
22.3. Протоколи розподілу секрету	714
22.4. Стандарти криптопротоколів.....	715
22.5. Формальний аналіз криптографічних протоколів	717
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 22	719
РОЗДІЛ 23 АРХІТЕКТУРА СИСТЕМИ ЕЦП	
23.1. Основні характеристики архітектури системи ЕЦП	722
23.2. Управління сертифікатами і ключами	727
23.3. Управління інфраструктурою відкритих ключів (РКІ).....	731
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 23	737
Контрольні питання	739
ТЕМА 6. ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ І АУДИТ ІКС	
РОЗДІЛ 24 УПРАВЛІННЯ ДОСТУПОМ.....	
24.1. Поняття і технології управління доступом	741
24.2. Форми подання обмежень доступу	746
24.3. Дискреційна модель розмежування доступу.....	749
24.4. Мандатна модель розмежування доступу	752
24.5. Рольова модель розмежування доступу.....	757
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 24	762
РОЗДІЛ 25 РЕЄСТРАЦІЯ ПОДІЙ В СИСТЕМІ І АУДИТ	
25.1. Реєстрація подій	765
25.2. Протоколювання й аудит.....	774
25.3. Функціональні компоненти й архітектура	
аудиту	781
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 25	783
Контрольні питання	785
ТЕМА 7. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ.....	
РОЗДІЛ 26 СТВОРЕННЯ ТА ОЦІНКА КОМПЛЕКСНИХ.....	
СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ.....	
26.1. Сутність та задачі комплексної системи захисту інформації.....	788
26.2. Суб'єкти та об'єкти захисту КСЗІ	794
26.3. Основні вимоги, завдання та принципи організації КСЗІ	799
26.4. Концепція створення захищених КСЗІ	805
26.5. Етапи створення комплексної системи захисту інформації	807
26.6. Моделювання КСЗІ	809

26.7. Вибір показників ефективності і критеріїв оптимальності	
КСЗІ	812
26.8. Підходи до оцінки ефективності КСЗІ.....	813
26.9. Концептуальні підходи до проектування систем захисту	816
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 26	817
Контрольні питання	819
ТЕМА 8. ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ ІКС ПІСЛЯ РЕАЛІЗАЦІЇ ЗАГРОЗ, ЗДІЙСНЕННЯ КІБЕРАТАК, ЗБОЇВ	821
РОЗДІЛ 27 ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ ІКС	821
27.1. Організаційно-технічні заходи відновлення функціонування ІКС	821
27.2. Журнал аудиту подій.....	829
27.3. Політики резервного копіювання	834
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 27	839
Контрольні питання	841
ТЕМА 9. СУЧАСНІ ТА ПЕРСПЕКТИВНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ.....	843
РОЗДІЛ 28 СУЧАСНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІКС	843
28.1. Технології виявлення та блокування кібератак на кінцевих пристроях (EDR, UBA, UEBA)	844
28.2. Технології протидії витокам інформації (DLP)	847
28.3. Технології механізму безпечного виконання програм (Sandbox)	852
28.4. Стек ELK як система централізованого зберігання журналів	857
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 28	861
Контрольні питання	862
СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ	865

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС	– інформаційна система
ІТ	– інформаційні технології
ІКС	– інформаційно-комунікаційна система
ЦОД	– центр обробки даних
ПЗ	– програмне забезпечення
ІоТ	– інтернет речей
ІоЕ	– інтернет всього
НСД	– несанкціонований доступ
КЦД	– конфіденційність, цілісність, доступність
КСЗІ	– комплексна система захисту інформації
ПБ	– політика безпеки
ІБ	– інформаційна безпека
ЕМВ	– електромагнітне випромінювання
ПЕМВ	– побічне електромагнітне випромінювання
ТЗР	– технічні засоби розвідки побічних електромагнітних
ПЕМВН	випромінювань і наведень
ОС	– операційна система
ЕОМ	– електронна обчислювальна машина
ПК	– персональний комп'ютер
LAN	– локальна комп'ютерна мережа
WAN	– глобальна мережа
UNIX	– сімейство операційних систем
НТТР	– протокол передачі гіпертексту та інших типів даних
MAC	– унікальний ідентифікатор обладнання для комп'ютерних мереж

ВСТУП

У сучасному світі інформаційно-комунікаційні системи стали основою для функціонування практично всіх сфер діяльності. Від ефективності їх роботи залежить безпека економічних, наукових, освітніх та державних процесів. Однак, разом з ростом значущості ІКС, збільшується й кількість загроз, що можуть вплинути на їхнє функціонування. Кіберзагрози, кібератаки, збої в роботі систем і порушення безпеки інформації є реальними проблемами, які потребують комплексного підходу до захисту.

Підручник "Системи захисту інформації" присвячений вивченню основних аспектів забезпечення безпеки ІКС і систем захисту інформації. У ньому детально розглядаються нормативно-правові аспекти забезпечення безпеки, які визначають правила та вимоги для захисту інформації, а також адміністративне та організаційне управління безпекою, яке гарантує ефективне виконання політик захисту на різних рівнях управлінської структури. Особлива увага приділяється інженерно-технічному захисту ІКС, що включає в себе захист від фізичних та технічних загроз, а також програмно-апаратному забезпеченню, яке забезпечує надійний рівень захисту інформації від несанкціонованого доступу. Окремо розглядаються технології міжмережевих екранів і систем виявлення атак, а також криптографічні методи захисту інформації, що є основою для забезпечення конфіденційності, цілісності та доступності даних. У підручнику також розглядаються принципи технічної та економічної розвідки, які дозволяють виявляти і прогнозувати потенційні загрози для ІКС. Окремі розділи присвячено технологіям управління доступом, а також аудиту ІКС, що є важливим інструментом для моніторингу і оцінки ефективності заходів безпеки. Крім того, посібник охоплює комплексні системи захисту інформації, що поєднують різні засоби для створення багаторівневого захисту інформаційних ресурсів, а також питання відновлення функціонування ІКС після реалізації загроз, кібернападів або збоїв. Сучасні та перспективні технології захисту інформації, такі як штучний інтелект і машинне навчання, розглядаються як важливі інструменти для підвищення рівня безпеки і ефективного управління захистом в умовах швидко змінюваного кіберпростору.

Підручник «Системи захисту інформації» містить основні положення теорії, які викладаються студентам спеціальностей 125 «Кібербезпека та захист інформації» освітньої програми «Безпека інформаційних і комунікаційних систем» та 123 «Комп'ютерна інженерія» освітньої

програми «Комп'ютерна інженерія», галузь знань 12 «Інформаційні технології». У кожній темі представлено стислі теоретичні положення та контрольні питання для оцінки рівня засвоєння матеріалу.

Матеріали посібника будуть корисними не лише для студентів зазначених спеціальностей, а й для здобувачів інших спеціальностей, таких як «Комп'ютерна інженерія», «Інженерія програмного забезпечення», «Системний аналіз», «Комп'ютерні науки» та ін. Крім того, посібник стане у пригоді аспірантам і здобувачам ступеня доктор філософії з технічних наук, які досліджують методи захисту інформації, що базуються на аналізі ризиків, управлінні безпекою інформаційних, комунікаційних та комп'ютерних систем, а також комп'ютерних мереж.

Головною метою посібника є надання студентам базових теоретичних знань для засвоєння курсу з управління інформаційною безпекою та кіберзахистом. Здобуті знання дозволять майбутнім фахівцям розробляти, впроваджувати та підтримувати комплексні системи захисту інформації, а також забезпечувати відновлення функціонування систем після атак, збоїв чи інших інцидентів.

Для зміцнення національної безпеки України важливим є систематичний розвиток кіберінфраструктури та посилення заходів безпеки, зокрема захисту критично важливих об'єктів. У сучасних умовах, коли інформаційна війна стає невід'ємною частиною глобальних геополітичних процесів, наша держава повинна розуміти важливість інтеграції сучасних технологій для забезпечення надійного захисту національних інформаційних ресурсів. Окрему увагу слід приділити захисту стратегічно важливих інфраструктурних об'єктів, таких як енергетика, транспорт, фінансові установи та державні органи, оскільки вони є основою для функціонування економіки та забезпечення державної безпеки. В умовах постійних кіберзагроз та зростаючої кількості кібератак з боку як державних, так і недержавних акторів, наша держава повинна продовжувати вдосконалювати законодавство у сфері кібербезпеки, адаптуючи його до сучасних вимог та міжнародних стандартів. Необхідно забезпечити чітку регламентацію відповідальності за порушення кібербезпеки, створення ефективних механізмів для боротьби з кіберзлочинністю, а також визначення чітких процедур реагування на інциденти в кіберпросторі. Окрім законодавчого вдосконалення, важливим є розвиток технічних рішень для забезпечення кіберзахисту. Це включає впровадження інноваційних технологій, таких як штучний інтелект для автоматичного виявлення та нейтралізації загроз, удосконалення систем виявлення та реагування на кібератаки, розробка нових криптографічних методів для захисту даних, а також забезпечення стійкості критично

важливих інфраструктур до кіберзагроз. Технічні засоби повинні бути здатні функціонувати в умовах складних і динамічних кіберзагроз, зокрема при здійсненні масштабних атак на національні або міжнародні інформаційні ресурси.

Міжнародна співпраця також відіграє ключову роль у забезпеченні кібербезпеки України. Враховуючи глобальність кіберзагроз, країни повинні об'єднувати свої зусилля для розробки та реалізації спільних стандартів безпеки, обміну інформацією про кіберзагрози та координації дій у разі інцидентів у кіберпросторі. Це включає участь у міжнародних організаціях, таких як Європейський Союз, НАТО, та інших платформ, де країни можуть обмінюватися досвідом та підтримувати колективну безпеку в кіберпросторі.

Завдяки цим крокам Україна зможе не лише зміцнити свою національну кібербезпеку, а й ефективно реагувати на виклики сучасного інформаційного середовища, забезпечуючи стійкість національних інфраструктур і створення умов для стабільного розвитку країни в умовах глобальної цифровізації.

ТЕМА 1. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІКС

РОЗДІЛ 1 ЗАКОНИ, НОРМАТИВНІ ДОКУМЕНТИ І СТАНДАРТИ



- 1.1. Законодавство України по забезпеченню кібербезпеки**
- 1.2. Нормативні документи системи технічного захисту інформації**
- 1.3. Стандарти інформаційної безпеки. Стандарт TCSEC**
- 1.4. Поняття кіберзлочинності. Класифікація кіберзлочинів**

"Право — це не тільки закони, а й культура їхнього застосування, без якої забезпечення безпеки в інформаційних системах неможливе."

Річард Кларк, американський експерт з кібербезпеки та колишній радник президента США з питань безпеки.

Нормативно-правове забезпечення безпеки інформаційно-комунікаційних систем (ІКС) є ключовим елементом захисту інформаційних активів підприємств і державних установ, враховуючи сучасні виклики кібербезпеки. Воно охоплює міжнародні стандарти, національне законодавство, внутрішні нормативні документи та галузеві рекомендації, які разом створюють комплексну основу для забезпечення інформаційної безпеки.

Одним із важливих компонентів є міжнародні стандарти, серед яких виділяються ISO/IEC 27001, що регулює впровадження системи управління інформаційною безпекою (СУІБ), та ISO/IEC 27002, який містить рекомендації з управління ризиками та передових практик у сфері захисту даних. Важливим інструментом для структуризації процесів кіберзахисту є рамковий документ NIST Cybersecurity Framework, що широко використовується в міжнародній практиці. Крім того, для підприємств, які працюють із персональними даними громадян ЄС, ключовим залишається дотримання регламенту GDPR, який визначає жорсткі вимоги до захисту та обробки персональної інформації.

На національному рівні нормативно-правова база України включає кілька фундаментальних документів. Зокрема, Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" визначає основні принципи забезпечення безпеки інформації в ІКС, а Закон України "Про кібербезпеку" регламентує правові відносини у сфері кіберзахисту, створюючи основи для формування національної системи кібербезпеки. Важливу роль також відіграє Закон України "Про захист персональних даних", який встановлює правила обробки, зберігання та передачі даних із метою забезпечення конфіденційності та недоторканності інформації.

Підприємства доповнюють це законодавство внутрішніми нормативними актами, які деталізують специфічні аспекти безпеки. Серед них ключовими є політики інформаційної безпеки, що регламентують правила роботи з інформацією, регламенти доступу для співробітників і плани реагування на інциденти. Такі документи дозволяють структурувати управління безпекою на рівні підприємства, забезпечуючи узгодженість дій під час виявлення та усунення загроз.

Галузеві рекомендації, такі як CIS Controls та методології ENISA (Європейського агентства з кібербезпеки), надають підприємствам передові практики, які дозволяють знижувати ризики, запобігати атакам і впроваджувати сучасні технічні рішення.

Таким чином, нормативно-правове забезпечення безпеки ІКС, що інтегрує міжнародні стандарти, національне законодавство та внутрішні документи підприємств, формує надійний фундамент для протидії кіберзагрозам. В умовах стрімкого розвитку технологій та збільшення кількості кіберінцидентів дотримання цих норм є ключовим фактором захисту інформаційних активів і забезпечення сталого розвитку підприємств.

1.1. Законодавство України по забезпеченню кібербезпеки

Правове забезпечення безпеки інформаційно-комунікаційних систем (ІКС) в Україні є критично важливим для гарантування цілісності, конфіденційності та доступності інформації в умовах цифровізації економіки та суспільства. Законодавчі акти, що регулюють сферу кібербезпеки та захисту інформації, мають на меті створення правового середовища для забезпечення ефективного захисту від кіберзагроз, попередження інцидентів та визначення відповідальності за порушення вимог безпеки.

Законодавство України по забезпеченню кібербезпеки — це система нормативно-правових актів, яка регулює питання захисту інформаційних систем, мереж, даних та інфраструктури від кіберзагроз. Цей комплекс законів та інших правових документів визначає принципи, правила, права та обов'язки суб'єктів, що займаються забезпеченням кібербезпеки на всіх рівнях державної та приватної діяльності.

Основною метою законодавства є захист інформаційних ресурсів, забезпечення безпеки цифрових платформ і технологій, а також створення умов для мінімізації кіберзагроз. Воно охоплює питання, пов'язані з обробкою даних, інформаційною безпекою в різних сферах, а також правилами взаємодії організацій та установ щодо кібербезпеки. З 2025 року законодавство буде зосереджено на створенні правових механізмів для забезпечення кіберстійкості новітніх технологій, таких як Інтернет речей та блокчейн, а також на адаптації нормативно-правової бази до вимог міжнародних стандартів кібербезпеки. Очікується введення нових нормативів для захисту цифрових платформ, що обробляють великі обсяги даних, а також для інтеграції технологій штучного інтелекту у сферу кібербезпеки. Крім того, важливим напрямом буде регулювання взаємодії між державними, приватними та міжнародними структурами для створення ефективних систем захисту від кіберзагроз на глобальному рівні.

Законодавче забезпечення кібербезпеки є важливим, тому що мета законодавчих заходів — попередження і стримування потенційних порушників (*більшість людей не здійснюють протиправних дій в цій сфері, так як це засуджується і карається, а не тому, що це технічно неможливо*). Законодавчі заходи щодо захисту інформації полягають у виконанні документів, що регулюють юридичну відповідальність персоналу організації за витік, втрату або модифікацію інформації, що підлягає захисту. Сюди ж відноситься і відповідальність сторонніх осіб за спробу несанкціонованого доступу до апаратури і конфіденційної інформації.

Законодавство України у сфері кібербезпеки постійно адаптується до нових викликів та технологічних змін. У 2024–2025 роках було прийнято та оновлено низку нормативно-правових актів, спрямованих на посилення

кіберзахисту держави. З 2025 року очікується подальша адаптація законодавства України до вимог ЄС, зокрема у сфері сертифікації кібербезпеки для критичних секторів та розширення механізмів моніторингу кіберзагроз. Крім того, буде посилено правову відповідальність за порушення у сфері кібербезпеки, зокрема за несанкціоновану обробку персональних даних та використання застарілих технологій безпеки. Очікується також розробка нових ініціатив для захисту інтелектуальної власності в умовах стрімкого розвитку технологій штучного інтелекту та автоматизації кіберзахисту.

1. План заходів на 2023—2024 роки з реалізації Стратегії кібербезпеки України

У грудні 2023 року Кабінет Міністрів України затвердив план заходів на 2023—2024 роки з реалізації Стратегії кібербезпеки України. Цей документ визначає конкретні кроки для досягнення цілей стратегії, включаючи модернізацію системи виявлення уразливостей та реагування на кіберінциденти. З 2025 року лановано подальшу імплементацію механізмів штучного інтелекту для аналізу кіберзагроз та автоматизації управління інцидентами. Крім того, передбачено розширення співпраці з міжнародними партнерами для обміну даними про кіберзагрози та впровадження найкращих практик у сфері кібербезпеки.

2. Законопроект № 12207 щодо удосконалення процедур нагляду за кібербезпекою

У листопаді 2024 року у Верховній Раді України був зареєстрований законопроект № 12207, який передбачає удосконалення процедур нагляду за кібербезпекою та запровадження європейських схем сертифікації кібербезпеки. Проект визначає правові та організаційні засади створення та функціонування національної системи кібербезпеки відповідно до Директиви (ЄС) 2022/2555. З 2025 року планується ухвалення законопроекту та поступове впровадження європейських стандартів сертифікації для критичної інформаційної інфраструктури. Особливий акцент буде зроблено на забезпеченні прозорості наглядових процедур і створенні механізмів оцінки відповідності кібербезпекових рішень.

3. Розпорядження Кабінету Міністрів України від 18.10.2024 № 1021-р

Це розпорядження визначає заходи щодо забезпечення кібербезпеки на 2024—2025 роки, зокрема модернізацію системи виявлення уразливостей і реагування на кіберінциденти та кібератаки. А також на 2025—2026 роки заплановано розширення функціоналу державних платформ моніторингу кіберзагроз і інтеграцію їх із міжнародними

системами обміну даними. Також передбачено впровадження нових навчальних програм з кібергігієни та підвищення кваліфікації фахівців із кібербезпеки.

4. Внесення змін до Закону України "Про національну безпеку України"

У 2024 році були внесені зміни до цього закону, які стосуються стратегічних основ інтегрованого управління державним кордоном, зокрема в частині кібербезпеки. З 2025 року передбачено створення єдиної національної системи кіберзахисту критичної прикордонної інфраструктури, що об'єднує державні та приватні ресурси. Планується впровадження автоматизованих систем аналізу даних для виявлення аномалій у прикордонному інформаційному просторі. Крім того, законодавчо закріплюється обов'язкове проведення регулярних аудитів кібербезпеки на об'єктах державного кордону.

5. Розробка стандартів вищої освіти у сфері кібербезпеки

Міністерство освіти і науки України затвердило стандарт вищої освіти за спеціальністю "Кібербезпека", який вводиться в дію з 2024/2025 навчального року. Цей стандарт визначає вимоги до підготовки фахівців у галузі кібербезпеки. З 2025 року планується оновлення стандартів для врахування швидкого розвитку технологій штучного інтелекту та їхнього застосування у сфері кібербезпеки. Передбачено впровадження практичних курсів із використанням сучасних платформ для моделювання кіберзагроз і тестування систем захисту. Крім того, у стандартах буде акцентовано увагу на міждисциплінарному підході, що охоплює кібергігієну, правові аспекти та управління ризиками.

6. Наказ № НОД/830/24 від 06.11.2024 "Про мінімізацію кіберзагроз"

Цей наказ встановлює вимоги щодо мінімізації кіберзагроз в організаціях, зокрема забороняє передавання інформації, що використовується у роботі, та здійснення комунікацій зі службовою метою з використанням ненадійних каналів зв'язку. З 2025 року наказ доповнюється вимогами щодо обов'язкового використання багатофакторної аутентифікації та засобів шифрування під час передачі чутливої інформації. Передбачено регулярне навчання співробітників організацій щодо протидії фішинговим атакам та інших соціально-інженерних загроз. Також планується створення централізованої платформи для моніторингу та аналізу інцидентів кібербезпеки в

організаціях, що працюють із критичною інформаційною інфраструктурою.

7. Закон України "Про основні засади забезпечення кібербезпеки України"

Цей закон визначає правові основи забезпечення кібербезпеки в Україні, встановлюючи обов'язки органів державної влади, підприємств та організацій щодо захисту інформаційних систем та даних. Він також передбачає відповідальність за порушення законодавства у сфері кібербезпеки. З 2025 року очікується внесення змін до цього закону, спрямованих на адаптацію до європейських стандартів кіберзахисту, зокрема в частині сертифікації кібербезпекових рішень. Планується запровадження вимог до обов'язкових аудитів кібербезпеки для державних установ та підприємств критичної інфраструктури. Крім того, буде передбачено створення національної бази даних про кіберінциденти для оперативного обміну інформацією та аналізу загроз.

8. Закон України "Про захист персональних даних" (2010 р.)

Цей закон регулює обробку персональних даних в Україні та встановлює вимоги до їх захисту, що є важливим аспектом кібербезпеки. З 2025 року очікується оновлення закону для врахування нових технологій, таких як штучний інтелект та блокчейн, які використовуються для обробки персональних даних. Крім того, планується посилення вимог щодо транскордонної передачі персональних даних та адаптація до стандартів Європейського Союзу, зокрема, GDPR. Також буде введена обов'язковість проведення регулярних перевірок відповідності підприємств та організацій вимогам законодавства щодо захисту персональних даних.

9. Закон України "Про критичну інфраструктуру" (2021 р.)

Цей закон стосується захисту об'єктів критичної інфраструктури, до яких відносяться енергетика, транспорт, інформаційні технології, охорона здоров'я та інші важливі сектори. Він визначає необхідність захисту від кіберзагроз, що можуть становити загрозу національній безпеці. З 2025 року закон буде доповнений вимогами щодо інтеграції новітніх технологій кібербезпеки, таких як штучний інтелект і машинне навчання, для автоматизованого моніторингу та реагування на кіберзагрози в критичній інфраструктурі. Планується також створення спеціалізованих національних центрів кіберзахисту для оперативної підтримки підприємств, що працюють у критичних секторах. Крім того, очікується посилення вимог до взаємодії між державними органами та приватними

компаніями для забезпечення безпеки критичних об'єктів в умовах зростаючих кіберзагроз.

10. Закон України "Про основи національної безпеки України"

Цей закон визначає стратегічні напрямки забезпечення національної безпеки в Україні, включаючи кібербезпеку. Закон встановлює основи політики щодо захисту державних і приватних інформаційних ресурсів, а також визначає обов'язки органів державної влади щодо боротьби з кіберзагрозами. Закон України "Про основи національної безпеки України" також регулює питання координації дій державних органів і національних компаній для забезпечення кіберзахисту та безпеки критичної інформаційної інфраструктури. Він визначає роль кібербезпеки як одного з ключових елементів національної безпеки, що має стратегічне значення для економічної та оборонної спроможності держави. З прийняттям нових викликів в кіберпросторі, цей закон буде актуальним для впровадження механізмів захисту від сучасних кіберзагроз і атак на національну інфраструктуру.

11. Закон України "Про кібербезпеку України"

Основний закон, що регулює всі питання кібербезпеки в Україні. Він охоплює питання захисту інформаційних систем, кіберінцидентів, заходів, що мають бути вжиті для забезпечення безпеки державних та приватних інформаційних ресурсів, а також відповідальність за порушення вимог кібербезпеки. Включає вимоги до кіберзахисту, а також описує співпрацю між державою і приватними підприємствами в сфері кібербезпеки. Закон України "Про кібербезпеку України" також встановлює вимоги до організації інфраструктури кіберзахисту на національному рівні, включаючи створення та підтримку національних центрів кіберзахисту, а також механізми координації дій з міжнародними партнерами в разі кіберінцидентів. Він передбачає розробку та впровадження стандартів і процедур для реагування на кіберзагрози та інциденти в реальному часі. Крім того, закон визначає роль державних органів у забезпеченні постійного моніторингу кіберзагроз і розробці політик для підвищення рівня кіберзахисту в усіх секторах економіки та критичній інфраструктурі.

12. Закон України "Про захист інформації в інформаційно-комунікаційних системах"

Цей закон визначає вимоги до захисту інформації в ІКС (інформаційно-комунікаційних системах), встановлює правила організації захисту від несанкціонованого доступу, а також забезпечення кібербезпеки для запобігання кіберзагрозам. Окрему увагу приділено організаційним і

технічним аспектам захисту. Закон також визначає обов'язки власників інформаційно-комунікаційних систем щодо забезпечення їх безпеки та регулярного моніторингу стану захисту. Він передбачає обов'язкове проведення оцінки ризиків та впровадження необхідних заходів для мінімізації загроз, пов'язаних з обробкою, зберіганням та передачею даних. Крім того, закон встановлює санкції за порушення вимог захисту інформації, що сприяє підвищенню відповідальності підприємств та організацій за належне забезпечення кібербезпеки.

13. Закон України "Про державну таємницю"

Цей закон регулює порядок захисту державної таємниці, що включає важливі для національної безпеки інформаційні ресурси. Враховуючи, що інформація, пов'язана з державною таємницею, є мішенню для кіберзлочинців, цей закон визначає правила обробки, зберігання і доступу до таких даних. Закон також встановлює вимоги до створення захищених інформаційних систем для обробки державної таємниці, зокрема щодо криптографічного захисту та фізичної безпеки. Він передбачає обов'язкову перевірку осіб, які мають доступ до секретних даних, та встановлює механізми контролю за їх використанням. Крім того, закон передбачає відповідальність за порушення норм щодо захисту державної таємниці, включаючи заходи, спрямовані на попередження витоків і несанкціонованого доступу до конфіденційної інформації.

14. Закон України "Про електронний цифровий підпис"

Цей закон встановлює правила використання електронного підпису, що є основою для безпечного електронного документообігу, а також для забезпечення автентичності та цілісності інформації, яка передається в електронному вигляді. Кібербезпека в цій сфері включає криптографічний захист даних і документів, що використовуються в комунікаціях між організаціями та громадянами. Закон також визначає вимоги до провайдерів послуг електронного підпису, які повинні забезпечити належний рівень захисту даних і запобігати можливим загрозам, пов'язаним із використанням підроблених підписів. Важливими аспектами є регулювання процедур реєстрації та верифікації користувачів, а також збереження та обробка електронних підписів у відповідності до встановлених стандартів. Закон також визначає правові наслідки використання електронного підпису для підтвердження угод і контрактів, забезпечуючи юридичну силу електронних документів.

15. Закон України "Про телекомунікації"

Цей закон визначає правові основи для діяльності в сфері телекомунікацій, зокрема питання захисту інформації в телекомунікаційних мережах. Він забезпечує правове регулювання функціонування телекомунікаційної інфраструктури та встановлює вимоги до безпеки обробки інформації, що передається через такі мережі. Закон також визначає обов'язки операторів телекомунікацій щодо захисту від кіберзагроз, таких як несанкціонований доступ та втручання в мережі, що можуть поставити під загрозу конфіденційність і цілісність інформації. Враховуючи зростаючу роль цифрових технологій, цей закон сприяє розвитку інфраструктури, здатної ефективно протидіяти новим типам кіберзагроз у майбутньому. Окрім того, закон встановлює вимоги щодо моніторингу та контролю за мережами для своєчасного виявлення та реагування на кіберінциденти.

16. Закон України "Про інформацію"

Цей закон визначає правовий статус інформації, регулює права громадян на доступ до неї та відповідальність за порушення цих прав. Кібербезпека в цьому контексті включає захист інформації від несанкціонованого доступу, витоку даних, а також захист прав на персональні дані та комунікації. Закон також встановлює вимоги до організацій, які зберігають або обробляють інформацію, щодо її захисту та обробки відповідно до міжнародних стандартів кібербезпеки. Важливим аспектом є забезпечення прозорості процесів обробки даних та захисту прав користувачів на всіх етапах використання інформації. У майбутньому, з урахуванням розвитку цифрових технологій, цей закон продовжить відігравати ключову роль у встановленні балансу між правами громадян та необхідністю забезпечення кібербезпеки.

17. Закон України "Про електронні документи і електронний документообіг"

Закон, який регулює використання електронних документів і процеси їх обробки. Він є частиною більш широкої нормативної бази щодо забезпечення кібербезпеки, оскільки електронні документи повинні бути захищені від підробок, несанкціонованого доступу та зловживань. Закон також встановлює вимоги до автентифікації документів, що включає застосування електронного цифрового підпису та інших криптографічних методів для забезпечення їх цілісності та законності. Він визначає правила обміну електронними документами між органами влади, підприємствами та громадянами, що сприяє забезпеченню надійного і безпечного документообігу. У майбутньому, з розвитком електронних сервісів, ці

норми стануть основою для безпечного функціонування цифрової економіки та захисту інформації в усіх сферах діяльності.

18. Розробка правових аспектів забезпечення кібербезпеки

У 2024 році було опубліковано дослідження, яке аналізує правові аспекти забезпечення кібербезпеки в Україні, зокрема ефективність механізмів реагування на кіберзагрози та кіберінциденти. Ці ініціативи свідчать про прагнення України посилити правову основу кібербезпеки, адаптуючи її до сучасних викликів та міжнародних стандартів. З 2025 року буде продовжено роботу над вдосконаленням правових механізмів, зокрема розробкою законодавчих ініціатив для регулювання використання штучного інтелекту та інших передових технологій у кібербезпеці. Очікується створення спеціалізованих нормативних актів для забезпечення безпеки національних цифрових платформ та інфраструктур. Крім того, буде активізовано співробітництво з міжнародними організаціями для узгодження українського законодавства з європейськими та світовими стандартами кібербезпеки.

Документи, що визначають правову відповідальність:

- Кримінальний кодекс України встановлює відповідальність за кіберзлочини, зокрема, за несанкціоноване втручання в роботу інформаційних систем, їхнє пошкодження або викрадення даних. Порушення можуть каратися як штрафами, так і позбавленням волі.
- Кодекс України про адміністративні правопорушення передбачає штрафи за порушення вимог до захисту інформації та доступу до неї без відповідних дозволів.

З 2025 року передбачається вдосконалення кримінального кодексу для врахування нових видів кіберзлочинів, зокрема, злочинів, пов'язаних із використанням штучного інтелекту та кіберзлочинними групами. У Кодексі про адміністративні правопорушення також планується введення додаткових санкцій для осіб та організацій, що порушують вимоги щодо захисту персональних даних та конфіденційної інформації. Крім того, буде розширено правову відповідальність для підприємств, що не забезпечують належний рівень кібербезпеки в умовах постійного зростання кіберзагроз.

Роль державних органів:

✳ Державна служба спеціального зв'язку та захисту інформації України — основний орган, що відповідає за національну політику в сфері кібербезпеки та захисту державних інформаційних ресурсів. Державна служба спеціального зв'язку та захисту інформації України розробляє та впроваджує стандарти і вимоги до захисту інформації в державних та

приватних інформаційних системах, здійснюючи контроль за їх виконанням. Вона також координує діяльність органів державної влади та приватних підприємств щодо кіберзахисту, веде роботу з підвищення кіберсвідомості та навичок у сфері безпеки. У майбутньому, з огляду на розвиток кіберзагроз та новітніх технологій, роль служби буде ще важливішою для забезпечення національної кібербезпеки.

• **Центр кіберзахисту** — орган, що надає консультації та методичну допомогу державним і приватним організаціям щодо запобігання та реагування на кіберінциденти. Центр кіберзахисту також здійснює моніторинг та аналіз кіберзагроз, розробляє рекомендації щодо захисту інформаційних систем та проводить навчання для фахівців у галузі кібербезпеки. Важливим напрямком його роботи є розробка стандартів і протоколів реагування на кіберінциденти, що дозволяє ефективно мінімізувати шкоду від атак. Враховуючи швидкий розвиток технологій та зростання кількості кіберзагроз, Центр буде відігравати ключову роль у забезпеченні безпеки інформаційних систем в Україні.

• **Державна регуляторна служба** — відповідає за виконання заходів щодо сертифікації систем захисту інформації та інфраструктур. Державна регуляторна служба також здійснює контроль за дотриманням стандартів захисту інформації та забезпечує відповідність технологічних рішень вимогам законодавства. Вона працює над удосконаленням нормативної бази для сертифікації та ліцензування програмних і апаратних засобів захисту інформації, що має важливе значення для кібербезпеки на державному рівні. З огляду на постійну еволюцію кіберзагроз, роль цієї служби буде залишатися критично важливою для забезпечення безпеки державних та приватних інформаційних систем в Україні.

З 2025 року очікується розширення повноважень Державної служби спеціального зв'язку для координації національних заходів з кіберзахисту на стратегічному рівні та інтеграції з міжнародними кібербезпековими ініціативами. Центр кіберзахисту буде активно взаємодіяти з приватним сектором для створення єдиних стандартів реагування на кіберінциденти та розвитку аналітичних платформ для прогнозування кіберзагроз. Державна регуляторна служба також працюватиме над створенням системи сертифікації для нових технологій кіберзахисту, таких як системи на базі штучного інтелекту.

Міжнародні угоди і стандарти:

- Україна активно впроваджує міжнародні стандарти кібербезпеки, зокрема **Директиву ЄС NIS (Network and Information Systems Directive)**, що регламентує заходи щодо безпеки

мереж та інформаційних систем. Україна співпрацює з міжнародними партнерами для адаптації національних стандартів до вимог цієї директиви, забезпечуючи високий рівень кіберзахисту в критичних галузях економіки та інфраструктури. Впровадження Директиви NIS передбачає створення механізмів для виявлення, реагування та відновлення після кіберінцидентів, що стає важливим елементом національної кіберстратегії. Ці заходи не тільки покращують захист інформаційних систем в Україні, а й забезпечують інтеграцію країни в європейське кіберпростір, підвищуючи її кіберстійкість.

- Україна є учасником міжнародних угод, що стосуються захисту інформаційних ресурсів, таких як **Конвенція про кіберзлочинність**. Ці угоди сприяють посиленню співпраці між Україною та іншими країнами у боротьбі з кіберзлочинністю, дозволяючи оперативно обмінюватися інформацією та ресурсами для ефективного реагування на кіберзагрози. Вони також допомагають впроваджувати єдині міжнародні стандарти в сфері кібербезпеки та правового захисту інформації. Участь у таких угодах підвищує рівень довіри до української кіберінфраструктури та сприяє розвитку міжнародної співпраці у сфері кібербезпеки.

З 2025 року Україна планує поглибити співпрацю з ЄС у рамках кібербезпекових ініціатив, адаптуючи національне законодавство до нових вимог ЄС, зокрема щодо кіберстійкості критичної інфраструктури. Участь України в міжнародних угодах також включатиме підписання нових протоколів щодо боротьби з транснаціональними кіберзагрозами та обміну інформацією між державами для підвищення глобальної кібербезпеки. Крім того, буде розроблено механізм взаємодії з міжнародними організаціями для впровадження передових технологій захисту інформаційних систем та запобігання кіберзлочинам.

Структура законодавства щодо захисту інформації

Структура державного законодавства України є багаторівневою. Законодавство України щодо захисту інформації є багаторівневим і охоплює широкий спектр нормативних актів, які забезпечують правовий захист інформаційних ресурсів та кібербезпеку. Кожен рівень законодавства має своє призначення і спрямований на врегулювання різних аспектів інформаційної безпеки.

Перший рівень – конституційний. На найвищому рівні перебувають норми Конституції України, які визначають основні принципи

національної безпеки, зокрема в частині інформаційної безпеки. Конституція України закріплює права громадян на захист інформації та доступ до неї, а також формулює основи для прийняття законодавчих актів, що регулюють питання національної та кібербезпеки.

Крім того, важливу роль відіграють стратегічні документи:

- **Стратегія національної безпеки України** — документ, що окреслює основні напрямки державної політики щодо захисту національних інтересів, включаючи інформаційну безпеку. З 2025 року Стратегія національної безпеки України буде активно адаптована до нових глобальних загроз, зокрема кіберзлочинності, яка має все більший вплив на національну безпеку. Очікується посилення інтеграції стратегічних ініціатив з міжнародними партнерами для забезпечення спільного реагування на кіберзагрози. Крім того, буде акцент на розвитку технологій і методів для захисту критичної інфраструктури, що сприятиме досягненню високої рівня кіберстійкості в усіх секторах економіки.

- **Воєнна доктрина України** — визначає основні завдання захисту держави, у тому числі в кіберпросторі. З 2025 року Воєнна доктрина України буде акцентувати увагу на посиленні кіберзахисту у відповідь на зростаючі загрози з боку державних і недержавних акторів у кіберпросторі. Доктрина передбачатиме інтеграцію передових технологій кібероборони та розвиток національних спроможностей для захисту критичної інфраструктури в умовах війни та криз. Крім того, стратегічна роль кіберзахисту буде визнана як невід'ємна частина загальної оборонної стратегії країни, з фокусом на розвиток міжурядових та міжнародних співпраць у галузі кібербезпеки.

- **Закон України "Про основи національної безпеки України"** — встановлює основні засади забезпечення національної безпеки в Україні, враховуючи ризики в інформаційній сфері. З 2025 року Закон України "Про основи національної безпеки України" буде оновлюватися з урахуванням нових викликів, зокрема загроз в кіберпросторі та захисту критичної інфраструктури від кібернападів. Особлива увага буде приділятися інтеграції національних систем кібербезпеки з міжнародними стандартами та співпраці з глобальними партнерами для боротьби з кіберзлочинністю. Крім того, законодавство буде зосереджено на розширенні правових інструментів для швидкого реагування на кіберінциденти, зокрема у випадках великих масштабних кіберзагроз.

Ці документи базуються на міжнародних договорах і угодах, ратифікованих Україною, що стосуються її національної безпеки, зокрема в інформаційній сфері.

Другий рівень — загальні закони (про землю, про громадянство, про власність і т. п.), які включають норми з питань інформаційної безпеки та кібербезпеки. Цей рівень охоплює загальні закони, які стосуються багатьох аспектів правового регулювання, в тому числі і безпеки інформації. Закони, що мають відношення до кібербезпеки та захисту інформації:

- **Закон України "Про громадянство"** — встановлює правила обробки особистих даних, що також стосується питань кібербезпеки. З 2025 року Закон України "Про громадянство" буде враховувати нові аспекти кібербезпеки, зокрема, питання захисту особистих даних у цифровому середовищі та впровадження сучасних технологій для їхнього захисту. Оновлені положення будуть регламентувати обробку даних громадян, зокрема в контексті використання біометричних даних та інших чутливих інформаційних ресурсів у рамках кібербезпеки. Крім того, закон сприятиме посиленню співпраці з міжнародними партнерами щодо захисту персональних даних та боротьби з кіберзлочинністю, яка може впливати на громадянство та ідентифікаційні процеси.

- **Закон України "Про власність"** — включає норми, які регулюють права на інформаційні ресурси. З 2025 року Закон України "Про власність" буде доповнений новими положеннями, що стосуються прав на цифрові активи та інформаційні ресурси в умовах розвитку технологій блокчейн та криптовалют. Закон також передбачатиме уточнення щодо захисту прав власників інформаційних ресурсів від кіберзагроз, зокрема щодо доступу та зловживань персональними даними. Крім того, оновлені норми сприятимуть розвитку правового регулювання інтелектуальної власності в цифровому середовищі, зокрема захисту авторських прав на програмне забезпечення та інші цифрові продукти.

- **Закон України "Про землю"** — має вплив на регулювання безпеки інформації в контексті кадастрових та земельних даних. З 2025 року Закон України "Про землю" буде оновлено з урахуванням нових вимог до захисту кадастрових та земельних даних, які зберігаються та обробляються в електронному вигляді. В оновлених нормах буде передбачено посилення заходів безпеки для запобігання несанкціонованому доступу до інформації про земельні ділянки, що є критичним для забезпечення національної безпеки. Крім того, законодавство зосередиться на інтеграції технологій цифровізації та кібербезпеки для захисту даних у сфері земельних відносин та кадастрових реєстрів від можливих кіберзагроз.

Третій рівень – спеціальні закони по інформатизації і захисту інформації. На цьому рівні знаходяться закони, які безпосередньо регулюють питання захисту інформації, кібербезпеки та інформатизації:

- **Закон України "Про основні засади забезпечення кібербезпеки України"** — визначає правові основи кібербезпеки в країні, встановлює обов'язки органів державної влади та приватних організацій щодо захисту інформаційних систем. З 2025 року Закон України "Про основні засади забезпечення кібербезпеки України" буде доповнений новими вимогами щодо захисту критичної інфраструктури та національних інформаційних ресурсів, зокрема в умовах зростаючих кіберзагроз. Закон передбачатиме більш суворі вимоги до організацій в частині звітності та моніторингу уразливостей у їхніх інформаційних системах, а також нові механізми для співпраці між державним сектором та приватними компаніями в боротьбі з кіберзлочинністю. Крім того, на базі цього законодавства буде розвиватися система сертифікації кібербезпеки, що відповідатиме міжнародним стандартам та вимогам ЄС щодо забезпечення кіберзахисту.

- **Закон України "Про інформацію"** — регулює правовий статус інформації, права громадян на доступ до неї та відповідальність за порушення цих прав. З 2025 року Закон України "Про інформацію" буде доповнено новими нормами, що стосуються захисту персональних даних та забезпечення конфіденційності в умовах зростаючого цифрового середовища. Зокрема, будуть уточнені правила щодо обробки та зберігання інформації, що стосується критичних даних, а також впроваджено більш жорсткі вимоги до організацій щодо забезпечення безпеки інформації. Закон також стане основою для розвитку нових механізмів контролю та нагляду за дотриманням прав громадян на доступ до інформації, враховуючи нові виклики кібербезпеки.

- **Закон України "Про захист інформації в інформаційно-комунікаційних системах"** — встановлює вимоги до захисту інформації в ІКС, зокрема щодо організації захисту від несанкціонованого доступу та кіберзагроз. З 2025 року Закон України "Про захист інформації в інформаційно-комунікаційних системах" буде адаптовано до нових міжнародних стандартів кібербезпеки, зокрема щодо захисту даних у хмарних технологіях та Інтернеті речей. Закон передбачатиме вдосконалення процедур сертифікації систем захисту інформації та посилення вимог до захисту персональних даних у реальному часі. Крім того, буде введено нові механізми контролю за виконанням вимог кібербезпеки, зокрема для критичних інфраструктур, що потребують особливого рівня захисту від кіберзагроз.

- **Закон України "Про державну таємницю"** — регулює питання захисту секретної інформації, важливої для національної безпеки. З 2025 року Закон України "Про державну таємницю" буде враховувати нові кіберзагрози та загрози з боку державних акторів, що зможуть впливати на захист секретної інформації. Закон також зосередиться на інтеграції новітніх технологій для забезпечення більш ефективного захисту інформації на всіх етапах її обробки та передачі, зокрема у цифрових платформах. Оновлення вимог до доступу та обробки державної таємниці враховуватиме глобальні тенденції у кіберзахисті та міжнародних угодах щодо безпеки інформації.

- **Закон України "Про електронні документи і електронний документообіг"** — визначає правові аспекти використання електронних документів в Україні. З 2025 року Закон України "Про електронні документи і електронний документообіг" буде адаптований до новітніх стандартів кібербезпеки, враховуючи підвищення вимог до захисту електронних даних у зв'язку з ростом кібератак. Оновлені норми будуть включати посилені заходи для запобігання несанкціонованому доступу до електронних документів, а також стандарти для їх автентифікації та криптографічного захисту. Закон також передбачатиме інтеграцію з міжнародними стандартами щодо безпечного обміну електронними документами в умовах глобалізації та цифрової трансформації.

- **Закон України "Про електронний цифровий підпис"** — встановлює правила використання електронного підпису, що є основою для безпечного електронного документообігу. З 2025 року Закон України "Про електронний цифровий підпис" буде доповнений новими вимогами щодо посилення безпеки використання електронних підписів, зокрема через впровадження технологій блокчейн для забезпечення їх цілісності та достовірності. Також закон буде адаптований до європейських стандартів eIDAS, що дозволить українським підприємствам та державним органам забезпечити взаємодію з іншими країнами в рамках електронного документообігу. Крім того, посилиться контроль за використанням електронних підписів для запобігання шахрайству та зловживанням в цифрових операціях.

- **Закон України "Про телекомунікації"** — регулює питання захисту інформації в телекомунікаційних системах та забезпечення безпеки телекомунікаційної інфраструктури. Він визначає правові засади функціонування телекомунікаційної галузі, включаючи питання захисту інформації та забезпечення безпеки телекомунікаційних мереж. З 2025 року Закон буде оновлений із урахуванням новітніх загроз у сфері кібербезпеки, зокрема підвищення вимог до захисту даних в умовах 5G

технологій. Крім того, очікується введення нових норм щодо захисту критичної телекомунікаційної інфраструктури та вдосконалення співпраці з міжнародними органами для боротьби з кіберзагрозами на глобальному рівні.



Рис. 1.1. Структура схеми законів 3-го рівня

Джерело: [1-6]

Четвертий рівень — підзаконні нормативні акти (укази, постанови, рішення, державні стандарти та ін.), відомчі накази, інструкції, керівництва. Цей рівень включає підзаконні акти, які детально регулюють застосування законів на практиці:

- **Укази, постанови, рішення** — нормативно-правові акти, які конкретизують вимоги законів, наприклад, щодо стандартів безпеки інформаційних систем та їх сертифікації.

- **Державні стандарти і технічні регламенти** — документи, що визначають вимоги до безпеки інформаційних систем та їх компонентів, а також методи оцінки їх захищеності.

- **Відомчі накази, інструкції та керівництва** — регулюють питання захисту інформації у конкретних галузях або на підприємствах, визначаючи внутрішні політики безпеки.

Держстандарт

Держстандарт (ДСТУ) — це національний стандарт, розроблений і затверджений органами державної влади України, що регулює вимоги до певних видів продукції, послуг, технологій або процесів у різних сферах

діяльності. Стандарти є нормативними документами, які встановлюють правила, норми і вимоги для забезпечення якості, безпеки та ефективності у виробництві, обігу товарів, наданні послуг і виконанні робіт. З 2025 року в Україні продовжиться інтеграція міжнародних стандартів у сфері кібербезпеки, зокрема в частині захисту інформаційних систем та даних. Держстандарти будуть переглянуті та адаптовані до нових викликів, пов'язаних з технологіями 5G, штучним інтелектом та Інтернетом речей. Очікується, що стандарт ДСТУ в галузі кібербезпеки надасть чіткі вказівки для організацій щодо захисту критичних інфраструктур і впровадження новітніх методів запобігання кіберзагрозам.

Зокрема, в контексті захисту інформації та кібербезпеки, Держстандарти визначають технічні, організаційні та процедурні вимоги для забезпечення належного рівня захисту даних і інформаційних систем. Вони охоплюють аспекти, як-от технічний захист інформації, криптографічний захист, цифрові підписи, процеси управління безпекою, а також встановлюють вимоги до апаратних і програмних засобів захисту інформаційних технологій. З 2025 року, з огляду на швидкий розвиток новітніх технологій, Держстандарти будуть адаптовані до вимог забезпечення кібербезпеки в умовах глобальних цифрових загроз, зокрема для забезпечення захисту інформаційної інфраструктури від атак. Буде особлива увага приділена стандартизації безпеки в умовах використання штучного інтелекту та машинного навчання для аналізу та запобігання кіберзагрозам. Крім того, оновлені стандарти сприятимуть вдосконаленню процедур сертифікації та аудиту безпеки для підприємств і державних установ, зокрема в критичних сферах інфраструктури.

Держстандарти виконують кілька функцій:

- Встановлення єдиних вимог для виробників і споживачів в різних галузях.
- Забезпечення сумісності, безпеки та якості продукції та послуг.
- Підтримка економічної і технологічної інтеграції в рамках національних і міжнародних ринків.
- Сприяння розвитку інновацій та підвищення ефективності діяльності організацій через стандартизацію процесів і технологій.

Таким чином, Держстандарти є важливим інструментом для регулювання безпеки та якості в різних сферах, включаючи кібербезпеку та захист інформації.

В Україні продовжує застосовуватися ряд державних стандартів, що регулюють технічний захист інформації, зокрема криптографічні методи захисту та правила проведення робіт із захисту інформації. Ці стандарти

забезпечують основи для належного рівня безпеки інформаційних систем в Україні, дотримуючись вимог національної та міжнародної практики.

1. ДСТУ 3396.0-96 – Захист інформації. Технічний захист інформації. Основні положення

Цей стандарт визначає основні принципи технічного захисту інформації та є базовим документом для створення захищених інформаційних систем. Він охоплює такі питання, як методи і засоби технічного захисту, вимоги до апаратних і програмних засобів захисту інформації, а також організаційні заходи для мінімізації ризиків інформаційних порушень.

2. ДСТУ 3396.1-96 – Захист інформації. Технічний захист інформації. Порядок проведення робіт

Цей стандарт регулює порядок проведення робіт із технічного захисту інформації. Він охоплює етапи проектування, впровадження та тестування засобів захисту, а також перевірку їх ефективності. Стандарт забезпечує єдині вимоги до процедур щодо встановлення і підтримки захищених систем, а також описує технічні засоби для забезпечення безпеки передачі та зберігання даних.

3. ДСТУ 3396.2-97 – Захист інформації. Технічний захист інформації. Терміни і визначення

Цей стандарт є необхідним для формулювання єдиного розуміння технічних аспектів захисту інформації в Україні. В ньому визначені терміни і поняття, що використовуються у сфері технічного захисту інформації, включаючи захист даних, шифрування, аутентифікацію, цифровий підпис і багато інших критичних аспектів для кібербезпеки.

4. ДСТУ 4145-2002 – Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння

Цей стандарт описує застосування криптографічних методів для забезпечення захисту інформації, зокрема цифрового підпису, який базується на еліптичних кривих. Криптографія на основі еліптичних кривих дозволяє створювати більш ефективні і надійні криптографічні алгоритми з меншою довжиною ключів, що забезпечує високу швидкість обробки даних при збереженні високого рівня безпеки.

5. ДСТУ 3420-2017 – Інформаційні технології. Захист інформації. Вимоги до засобів криптографічного захисту даних

Цей стандарт встановлює вимоги до засобів криптографічного захисту інформації, що використовуються для шифрування, підпису та автентифікації даних. Він визначає основні принципи і методи, що забезпечують надійність криптографічного захисту в інформаційних

системах, а також встановлює критерії безпеки для криптографічних алгоритмів.

6. ДСТУ ISO/IEC 27001:2015 – Інформаційні технології. Техніки захисту інформації. Системи управління безпекою інформації. Вимоги

Цей міжнародний стандарт, який використовується в Україні, визначає вимоги до системи управління безпекою інформації (СУБІ), що включають процеси та методи для управління інформаційними ризиками. Відповідно до стандарту, організації повинні встановити та підтримувати систему управління для захисту конфіденційності, цілісності та доступності інформації, а також реагувати на кіберзагрози та інциденти безпеки.

7. ДСТУ ISO/IEC 27002:2015 – Інформаційні технології. Техніки захисту інформації. Кодекс практики для управління безпекою інформації

Цей стандарт є доповненням до ISO/IEC 27001 і містить детальні рекомендації щодо впровадження заходів безпеки для захисту інформації в організаціях. Він описує кращі практики, політики, методи та інструменти для захисту даних, включаючи управління доступом, захист від кіберзагроз і заходи щодо забезпечення фізичної та логічної безпеки.

8. ДСТУ 3165-2011 – Інформаційні технології. Програмні засоби для криптографічного захисту інформації. Основні вимоги до безпеки

Цей стандарт встановлює вимоги до програмних засобів, які використовуються для криптографічного захисту інформації, а також критерії їх безпеки. Він охоплює питання використання криптографічних алгоритмів, перевірки їх відповідності стандартам безпеки та забезпечення надійності програмного забезпечення при реалізації криптографічного захисту.

9. ДСТУ 3444-96 – Захист інформації. Стандарти захисту інформації. Загальні вимоги

Цей стандарт визначає загальні вимоги до систем захисту інформації, які можуть бути використані для створення безпечних інформаційних систем на підприємствах, в установах і організаціях. Він описує методи, засоби і заходи, що забезпечують цілісність і конфіденційність інформації, а також запобігають несанкціонованому доступу до даних.

10. ДСТУ 4135-2002 – Інформаційні технології. Криптографічний захист інформації. Основні положення щодо криптографічної стійкості

Цей стандарт регулює основні принципи криптографічного захисту, визначаючи вимоги до криптографічних алгоритмів і засобів, що використовуються для захисту інформації від несанкціонованого доступу.

Він зокрема надає рекомендації щодо вибору криптографічних методів для різних рівнів безпеки.

11. ДСТУ ISO/IEC 15408:2008 – Інформаційні технології. Оцінка безпеки ІТ-систем. Оцінка захисту інформаційних технологій

Цей стандарт встановлює вимоги для оцінки безпеки інформаційних технологій, надаючи структуру для визначення вимог до захисту ІТ-систем. Він базується на принципах оцінки захисту, тестуванні систем безпеки та встановленні відповідності міжнародним стандартам безпеки.

12. ДСТУ 3962-2000 – Інформаційні технології. Програмні засоби для забезпечення безпеки інформації. Вимоги до програмних засобів для захисту від несанкціонованого доступу

Цей стандарт визначає вимоги до програмного забезпечення, що використовується для захисту інформації від несанкціонованого доступу, у тому числі засобів шифрування, аутентифікації та контролю доступу. Він включає в себе також методи оцінки ефективності таких програмних засобів.

13. ДСТУ 4343-2005 – Інформаційні технології. Прогнозування і моніторинг загроз безпеці інформації в інформаційно-комунікаційних системах

Цей стандарт визначає методи прогнозування, моніторингу та аналізу загроз безпеці інформаційних систем, що дозволяє своєчасно виявляти та реагувати на можливі кіберзагрози. Він також надає вимоги до систем моніторингу безпеки та інструментів для захисту від нових типів атак.

Ці стандарти залишаються важливими для розвитку інформаційної безпеки в Україні, адже вони забезпечують відповідність національних вимог до міжнародних стандартів безпеки. З огляду на постійне зростання загроз у сфері кібербезпеки, особливо у світлі зростаючої цифрової трансформації та впровадження новітніх технологій, ці стандарти відіграють ключову роль у забезпеченні належного захисту даних та інформаційних систем. Технічні стандарти та криптографічні вимоги, прописані в цих ДСТУ, допомагають визначити ефективні стратегії для захисту від різних типів кіберзагроз, що є критично важливим для підтримки національної безпеки.

1.2. НОРМАТИВНІ ДОКУМЕНТИ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Нормативні документи системи технічного захисту інформації — це комплекс правових, організаційних та технічних стандартів, правил і

вимог, що регулюють питання захисту інформації за допомогою технічних засобів. Ці документи встановлюють обов'язки організацій, підприємств, установ і державних органів у забезпеченні конфіденційності, цілісності та доступності інформаційних систем та даних, а також визначають технічні вимоги до засобів, які застосовуються для їхнього захисту. Крім законів і підзаконних актів, впроваджено багато нормативних документів, які регламентують певні аспекти діяльності у сфері захисту інформації. Ці документи створюють нормативно-правову базу для впровадження ефективних заходів із технічного захисту інформації, таких як криптографія, системи моніторингу безпеки, засоби аутентифікації, захист мереж, а також методики управління ризиками та збереження конфіденційності інформації. Вони також регулюють використання технічних засобів, що забезпечують безпеку інфраструктури на всіх рівнях організаційної діяльності.

Нормативні документи системи технічного захисту інформації, які безпосередньо стосуються питань захисту інформації у комп'ютерних системах

Нормативні документи системи технічного захисту інформації, що безпосередньо стосуються питань захисту інформації у комп'ютерних системах включають в себе серію стандартів та методичних вказівок, що регулюють захист інформації від несанкціонованого доступу, а також створення, впровадження та супроводження систем технічного захисту інформації в автоматизованих системах. На 2024-2025 роки важливими нормативними документами є:

НД ТЗІ 1.1-002-99: *Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу.* Цей документ визначає базові принципи захисту інформації в комп'ютерних системах від несанкціонованого доступу, акцентуючи увагу на важливості комплексного підходу до забезпечення конфіденційності та цілісності даних. Застосування цього документу допомагає знижувати ймовірність витоків інформації та несанкціонованого втручання в системи. Це залишатиметься актуальним в умовах зростаючих кіберзагроз.

НД ТЗІ 1.1-003-99: *Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.* Окреслює основні терміни і поняття, що використовуються в області захисту інформації в комп'ютерних системах, і є основою для подальшого правильного розуміння та застосування технологій захисту.

НД ТЗІ 2.5-004-99: *Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу.*

Визначає методи оцінювання рівня захищеності інформації від загроз несанкціонованого доступу, що дозволяє здійснювати регулярні перевірки та аудит систем безпеки.

НД ТЗІ 2.5-005-99: *Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.* Містить класифікацію автоматизованих систем за рівнем захисту та визначає стандартні функціональні профілі для різних типів інформації, що обробляється в таких системах.

НД ТЗІ 3.7-001-99: *Методичні вказівки з розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.* Цей документ надає методичні рекомендації з розробки технічних завдань для створення комплексних систем захисту інформації в автоматизованих системах, що важливо для проектування та впровадження ефективних засобів захисту.

НД ТЗІ 1.4-001-2000: *Типове положення про службу захисту інформації в автоматизованій системі.* Визначає вимоги та функції служби захисту інформації в автоматизованій системі, що є відповідальною за забезпечення безпеки та інтеграцію технічних засобів захисту в організаційні структури.

НД ТЗІ 3.6-001-2000: *Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.* Регулює процеси створення, впровадження та модернізації засобів захисту інформації, охоплюючи не лише технічні аспекти, а й процедури супроводження системи безпеки протягом її експлуатації.

НД ТЗІ 2.5-008-02: *Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.* Встановлює вимоги до захисту конфіденційної інформації в автоматизованих системах класу 2, які обробляють інформацію середнього рівня важливості, забезпечуючи її належну безпеку.

НД ТЗІ 2.5-010-03: *Вимоги до захисту інформації вебсторінки від несанкціонованого доступу.* Окреслює стандарти та вимоги до захисту вебсторінок від зовнішніх загроз і несанкціонованого доступу, що є важливою складовою частиною захисту в сучасних інформаційних системах.

НД ТЗІ 3.7-003-05: *Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.* Регламентує порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, визначаючи етапи проектування та впровадження ефективних засобів захисту на всіх рівнях.

НД ТЗІ 2.5-014-04: *Вимоги до захисту інформації в хмарних обчислювальних системах.* Оскільки хмарні технології стають все більш популярними, цей стандарт регламентує вимоги захисту даних, що зберігаються та обробляються в хмарних середовищах.

НД ТЗІ 1.5-017-06: *Стандарти безпеки при використанні технологій блокчейн для захисту інформації.* Зважаючи на зростаючий інтерес до технологій блокчейн, цей документ стане важливим для регулювання аспектів захисту інформації за допомогою цієї технології.

НД ТЗІ 2.5-020-07: *Вимоги до захисту інформації в інтернеті речей (IoT).* У зв'язку з розвитком Інтернету речей, цей стандарт описує заходи безпеки для таких систем і пристроїв, що забезпечують взаємодію між фізичними об'єктами та інформаційними системами.

Ці нормативні документи складають основу для створення та підтримки надійної системи технічного захисту інформації в Україні, а також сприяють інтеграції міжнародних стандартів в процеси захисту інформаційних систем.

Нормативні документи організації

Нормативні документи організації для забезпечення безпеки ІКС є важливим інструментом для належного регулювання внутрішніх процесів підприємства, що стосуються захисту інформації. Вони сприяють створенню структур і процедур, які забезпечують надійний захист конфіденційної інформації та належне реагування на можливі загрози. Основними документами, що повинні бути розроблені в організації, є:

1. Положення про збереження конфіденційної інформації – цей документ визначає основні принципи та заходи, які застосовуються для захисту інформації, що має конфіденційний характер. В ньому детально прописані заходи для збереження таких відомостей на всіх етапах їх обробки та передачі.

2. Перелік відомостей, що становлять конфіденційну інформацію – визначає конкретний список відомостей та даних, які є конфіденційними для організації, та повинні оброблятися з підвищеними заходами безпеки.

Це може включати комерційну таємницю, персональні дані, технічні розробки тощо.

3.Інструкція про порядок допуску працівників до відомостей, що становлять конфіденційну інформацію – документ, який регламентує правила та процедури для допуску співробітників до конфіденційної інформації в залежності від їх посадових обов'язків. Визначає вимоги щодо підготовки співробітників, необхідних допусків та нагляд за їх діяльністю.

4.Положення про роботу з іноземними фірмами і їх представниками – визначає правила взаємодії з зовнішніми партнерами, особливо в частині передачі конфіденційної інформації. Такий документ є необхідним для забезпечення належного рівня захисту під час співпраці з міжнародними контрагентами.

Належне правове забезпечення безпеки ІКС має критичне значення для ефективної роботи будь-якої організації. Якщо внутрішні нормативно-правові документи не визначають чітко перелік конфіденційної інформації, порядок її обробки та відповідальність за порушення, то будь-які претензії у разі несанкціонованого доступу до таких відомостей можуть бути визнані безпідставними. Це може призвести до відсутності юридичної підтримки в разі конфлікту.

Вимоги забезпечення безпеки і захисту інформації мають бути відображені також у **Статуті організації**. Це дає право адміністрації підприємства:

- **Створювати організаційні структури** для забезпечення захисту конфіденційної інформації, включаючи розробку політик, процедур і виділення відповідальних осіб.
- **Включати вимоги щодо захисту інформації в договори з постачальниками, контрагентами та іншими зовнішніми партнерами**, що гарантує відповідальність за недотримання вимог безпеки.
- **Вимагати захисту інтересів підприємства з боку державних органів і судових інстанцій у разі порушення умов безпеки інформації.**

Таким чином, правове забезпечення безпеки ІКС є ключовим елементом у забезпеченні належного рівня захисту інформації на підприємстві та дозволяє ефективно управляти потенційними ризиками, що пов'язані з її обробкою та збереженням.



При укладанні трудового договору та оформленні наказу про прийом на роботу нового співробітника важливо передбачити відмітку про його ознайомленість з порядком захисту інформації підприємства. Така відмітка є важливою правовою процедурою, яка підтверджує, що співробітник усвідомлює важливість збереження конфіденційної

інформації та правила її обробки в рамках компанії. Це є частиною політики безпеки підприємства, що визначає основи для ефективного захисту чутливих відомостей.

Однак, не слід думати, що підписання трудового договору та ознайомлення співробітника з політикою безпеки забезпечує безумовну надійність збереження конфіденційної інформації. Така угода є лише першим кроком у забезпеченні безпеки, адже саме після її підписання активується система заходів щодо захисту інформації. Це означає, що підприємство застосовує ряд організаційних, технічних і правових заходів для моніторингу та контролю дій співробітника в разі порушення встановлених норм.

Правова основа, що лежить в основі цієї політики, дає змогу у разі необхідності:

- ✱ **Юридично реагувати** на можливі порушення правил доступу або збереження конфіденційної інформації, включаючи відповідальність за розголошення або несанкціоноване використання даних.

- ✱ **Припиняти протиправні дії** співробітника на основі документально зафіксованих порушень, що забезпечує захист інтересів підприємства на всіх рівнях.

Такий підхід допомагає зміцнити загальну правову безпеку в організації та запобігти витоку важливої інформації або іншим порушенням, що можуть зашкодити репутації чи фінансовому стану компанії.

1.3. СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. СТАНДАРТ TCSEC

Безпека системи — це складна характеристика, яка не піддається прямому вимірюванню. Різні фахівці мають свої підходи до підвищення захищеності системи та оцінки її рівня безпеки. Для того, щоб досягти єдиного підходу до оцінювання та покращення безпеки інформаційних систем, необхідно розробити стандарти безпеки, які визначають вимоги до систем та шляхи їх реалізації. Важливим аспектом є створення критеріїв оцінки захищеності та розробка процедур, які дозволяють оцінити систему за цими критеріями.

Історично перші вимоги до стандартів безпеки виходили від військових. Інформація, якою володіють державні структури, є надзвичайно важливою для національної безпеки. Будь-яке порушення безпеки інформації (особливо її розголошення) може мати серйозні наслідки: від втрати міжнародного престижу країни до значних економічних, політичних і фінансових втрат. У найгіршому випадку це

може призвести до зниження обороноздатності, економічних санкцій, відставки урядів, змін у державному устрої і навіть до втрати суверенітету.

Зважаючи на це, держави, для забезпечення захисту такої інформації, впроваджують спеціальні режими безпеки, які регулюються законодавчими актами та державними стандартами. Такі норми визначають, які дані вважаються конфіденційними, як їх обробляти та зберігати, а також яких стандартів мають дотримуватись установи для запобігання витоків важливої інформації. Цей процес включає розробку детальних національних стандартів з кібербезпеки, що визначають порядок захисту даних, процедур контролю доступу, вимог до технологій шифрування та інші критичні аспекти безпеки.

У наш час впровадження та дотримання стандартів безпеки є необхідною умовою для забезпечення надійного захисту інформаційних систем не тільки в секторі національної оборони, але й у багатьох інших сферах діяльності — від державного управління до комерційних підприємств, що мають доступ до чутливих даних, включаючи фінансову та персональну інформацію.

Стандарти інформаційної безпеки — це набори вимог і рекомендацій, розроблених для забезпечення належного рівня захисту інформації в організаціях, компаніях і національних структурах. Вони охоплюють всі аспекти захисту інформації, включаючи її конфіденційність, цілісність і доступність, а також порядок реагування на інциденти безпеки. На основі таких стандартів розробляються організаційні і технічні заходи для забезпечення безпеки інформаційних систем.

На сьогоднішній день існує кілька основних **міжнародних і національних стандартів**, що регулюють інформаційну безпеку.

Національні стандарти, які регулюють інформаційну безпеку в Україні охоплюють широкий спектр аспектів захисту інформації в інформаційно-комунікаційних системах, комп'ютерних мережах та автоматизованих системах:

1. ДСТУ 27001:2015. Системи управління інформаційною безпекою. Вимоги

Цей стандарт є національним еквівалентом міжнародного стандарту ISO/IEC 27001. Він визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) на основі оцінки ризиків та забезпечення належного рівня захисту інформації. Стандарт вимагає від організацій

належного управління безпекою інформації, що включає як технічні, так і організаційні заходи.

2. ДСТУ ISO/IEC 27002:2015. *Практики управління інформаційною безпекою. Кодекс практики*

Цей стандарт визначає основні практики та рекомендації щодо управління безпекою інформації в організаціях. Він охоплює широкий спектр питань, включаючи фізичну безпеку, управління доступом, контроль за операціями та збереженням даних, а також управління інцидентами безпеки. Це допоміжний стандарт до ДСТУ 27001, зосереджуючи увагу на конкретних практиках, які повинні бути застосовані для ефективного управління безпекою.

3. ДСТУ 27005:2015. *Оцінка ризиків у сфері інформаційної безпеки*

Цей стандарт описує методології та підходи до оцінки ризиків, пов'язаних з інформаційною безпекою. Він дає рекомендації щодо ідентифікації, аналізу, оцінки та управління ризиками в контексті систем управління інформаційною безпекою. Використовується в організаціях для розробки планів з управління ризиками та вживання заходів для мінімізації можливих загроз.

4. ДСТУ 3191:2016. *Захист інформації. Основні терміни та визначення*

Цей стандарт містить термінологію, яка використовується в сфері захисту інформації в інформаційно-комунікаційних системах та комп'ютерних мережах. Він є основою для всіх інших нормативних документів у цій галузі, допомагаючи створити єдину мову та розуміння термінів у галузі інформаційної безпеки.

5. ДСТУ 3832:2021. *Технічний захист інформації. Засоби захисту інформації в комп'ютерних системах. Вимоги*

Цей стандарт визначає вимоги до технічних засобів, які використовуються для захисту інформації в комп'ютерних системах. Включає в себе стандарти для програмних і апаратних засобів захисту, що забезпечують конфіденційність, цілісність та доступність інформації від несанкціонованого доступу.

6. ДСТУ 3500:2019. *Інформаційна безпека. Методи та засоби захисту інформації в автоматизованих системах. Оцінка ефективності засобів захисту*

Цей стандарт описує методи та засоби захисту інформації в автоматизованих системах, а також надає критерії оцінки ефективності цих

засобів. Він використовується для перевірки ефективності впроваджених засобів захисту та визначення, чи відповідають вони необхідним вимогам.

7. ДСТУ 4200:2020. *Захист інформації в інформаційно-телекомунікаційних системах. Загальні положення*

Цей стандарт визначає основні принципи та підходи до захисту інформації в інформаційно-телекомунікаційних системах. Включає в себе вимоги щодо захисту від несанкціонованого доступу, а також методи для запобігання інформаційним витокам.

8. ДСТУ 4270:2022. *Вимоги до інформаційної безпеки в електронних платіжних системах*

Цей стандарт є важливим для забезпечення безпеки в електронних платіжних системах. Він включає вимоги щодо захисту інформації від несанкціонованого доступу, шахрайства та інших загроз в онлайн-транзакціях.

9. ДСТУ 4527:2021. *Захист інформації в системах критичної інфраструктури*

Цей стандарт регламентує вимоги до захисту інформації, що обробляється в системах критичної інфраструктури, таких як енергетика, водопостачання, транспорт. Він включає в себе методи і заходи для запобігання впливу кіберзагроз на важливі об'єкти національної безпеки.

10. ДСТУ 4741:2021. *Заходи з технічного захисту інформації в хмарних обчислювальних середовищах*

Стандарт описує вимоги до захисту інформації в хмарних середовищах, включаючи аспекти безпеки при зберіганні та обробці даних у хмарі. Це стає все більш актуальним через популярність хмарних технологій в різних сферах економіки.

Додаткові стандартні документи, які залишатимуться актуальними:

- **ДСТУ 5114:2020. *Керівництво з оцінки ефективності засобів захисту інформації в організаціях***
- **ДСТУ ISO/IEC 27034-1:2016. *Безпека програмного забезпечення. Загальні принципи***
- **ДСТУ ISO/IEC 27018:2019. *Захист особистих даних у хмарних обчислювальних середовищах.***

Однак існують й інші нормативні документи, які стосуються різних аспектів інформаційної безпеки, зокрема:

1. ДСТУ 3440:2013. *Інформаційна безпека. Стандарти захисту інформації від несанкціонованого доступу в інформаційно-комунікаційних системах*

Визначає стандартні вимоги щодо захисту інформації від несанкціонованого доступу в різних типах інформаційно-комунікаційних системах.

2. ДСТУ 4530:2021. *Інформаційна безпека. Засоби криптографічного захисту інформації. Вимоги до засобів шифрування*

Охоплює вимоги до засобів криптографічного захисту інформації, зокрема використання шифрування для забезпечення конфіденційності та цілісності даних.

3. ДСТУ 3543:2022. *Керування інцидентами інформаційної безпеки*

Визначає вимоги щодо управління інцидентами інформаційної безпеки в організаціях, процеси і процедури для реагування на кіберінциденти.

4. ДСТУ 4760:2021. *Захист інформації в критичних інформаційних інфраструктурах*

Розглядає особливості забезпечення інформаційної безпеки в системах критичної інфраструктури, таких як енергетика, водопостачання, транспорт та ін.

5. ДСТУ 3200:2020. *Захист інформації в автоматизованих системах управління*

Стандарт для захисту інформації в автоматизованих системах управління, включаючи промислові та інші технологічні процеси, які використовують автоматизовані системи.

6. ДСТУ 5154:2020. *Захист інформації в мобільних пристроях*

Охоплює захист інформації, що зберігається та обробляється на мобільних пристроях, включаючи смартфони та планшети, з акцентом на безпеку даних при їх передачі та зберіганні.

7. ДСТУ 4701:2021. *Безпека інформаційних технологій для телекомунікацій*

Описує вимоги до безпеки телекомунікаційних технологій, забезпечуючи захист інформації, що передається через телекомунікаційні мережі.

8. ДСТУ ISO/IEC 15408:2019. *Оцінка безпеки інформаційних технологій. Критерії оцінки*

Стандарт для оцінки безпеки програмних і апаратних засобів, що використовується для виявлення уразливостей і оцінки рівня захисту в системах.

Ці стандарти та нормативні документи є основою для створення ефективної системи захисту інформації в Україні, що дозволяє забезпечити належний рівень безпеки у різних сферах використання інформаційних технологій.

Основні міжнародні стандарти, які регулюють інформаційну безпеку:

1. ISO/IEC 27001:2013 — Системи управління інформаційною безпекою (ISMS)

Один із найважливіших міжнародних стандартів для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS). Стандарт встановлює вимоги до процесів і контролів безпеки, включаючи управління ризиками та захист інформаційних активів. Це основа для управління інформаційною безпекою в організаціях по всьому світу. ISO/IEC 27001 залишається актуальним стандартом для сертифікації організацій з точки зору їх здатності захищати інформацію.

2. ISO/IEC 27002:2022 — Практичні рекомендації для реалізації заходів інформаційної безпеки

Цей стандарт надає керівництво щодо впровадження і підтримки практичних заходів для захисту інформаційних активів. Він містить список контролів безпеки, які можна застосувати в межах ISMS, для забезпечення конфіденційності, цілісності та доступності інформації. Це супутній стандарт до ISO/IEC 27001, що надає інструкції щодо реалізації заходів безпеки. Використовується як допоміжний стандарт для впровадження та підтримки політик безпеки в організаціях.

3. ISO/IEC 27005:2018 — Управління ризиками в інформаційній безпеці

Стандарт описує процеси оцінки та управління ризиками в інформаційній безпеці. Стандарт допомагає організаціям оцінювати ризики для інформаційної безпеки, а також визначати заходи для їх зниження та управління ними. Ключовий стандарт для організацій, що прагнуть систематично і зважено підходити до управління ризиками в сфері інформаційної безпеки.

4. ISO/IEC 27032:2012 - Кібербезпека. Керівництво з кіберзахисту

Стандарт визначає найкращі практики для забезпечення кібербезпеки, зокрема на рівні організацій та держав. Охоплює захист від кіберзагроз і спрямований на захист інфраструктури в мережах, а також на забезпечення захисту інформації в процесах електронної комунікації. Потрібен для організацій, що працюють в умовах високих кіберзагроз і займаються захистом від кібератак.

5. ISO/IEC 22301:2019 – *Системи управління безпекою та неперервністю бізнесу*

Стандарт для управління бізнес-неперервністю, що включає питання захисту інформації в рамках неперервності бізнесу. Він допомагає організаціям забезпечити свою здатність до відновлення після інцидентів, зокрема, в разі кіберзагроз або катастроф. Залишається актуальним для організацій, що хочуть мінімізувати збитки та час простою в разі порушення їхніх систем інформаційної безпеки.

6. ISO/IEC 27018:2019 – *Захист персональних даних в хмарних обчисленнях*

Стандарт, орієнтований на забезпечення конфіденційності та захисту персональних даних при використанні хмарних обчислень. Охоплює конкретні аспекти безпеки персональних даних в хмарних інфраструктурах, що є важливим у світлі росту популярності хмарних технологій. Особливо важливий для хмарних провайдерів та компаній, які обробляють персональні дані в хмарних середовищах.

7. ISO/IEC 29100:2011 – *Захист конфіденційності інформації. Рамки для захисту конфіденційності*

Надає рамки для організацій щодо забезпечення конфіденційності інформації. Визначає принципи та заходи для управління конфіденційністю інформації на всіх етапах її обробки. Це важливий стандарт для організацій, що працюють з конфіденційною інформацією і хочуть забезпечити належний рівень захисту.

8. ISO/IEC 20000-1:2018 – *Системи управління інформаційними технологіями. Вимоги*

Стандарт для управління послугами ІТ, включаючи аспекти, пов'язані з інформаційною безпекою та управлінням ризиками. Він визначає вимоги до інтеграції заходів безпеки в процеси управління інформаційними технологіями. Потрібен для організацій, що надають ІТ-послуги або взаємодіють із зовнішніми постачальниками ІТ-послуг.

9. ISO/IEC 27035:2016 – *Управління інцидентами інформаційної безпеки*

Цей стандарт визначає процеси для ідентифікації, реагування та відновлення після інцидентів інформаційної безпеки. Окреслює кроки, необхідні для розв'язання інцидентів, що виникають у процесі роботи з інформаційними системами. Незамінний для організацій, що мають чітку стратегію з реагування на інциденти інформаційної безпеки.

10. NIST SP 800-53 – Безпека та конфіденційність інформаційних систем

Цей стандарт був розроблений Національним інститутом стандартів і технологій США (NIST) і є універсальним інструментом для організацій, що прагнуть досягти високого рівня кібербезпеки. Він описує чотири основні функції управління кібербезпекою: ідентифікація, захист, виявлення і реагування, відновлення. Широко використовується в усьому світі, зокрема в міжнародних корпораціях, для підвищення рівня безпеки інформаційних систем.

11. GDPR (General Data Protection Regulation) – Регламент захисту персональних даних ЄС

Хоча це і не стандарт інформаційної безпеки у вузькому сенсі, GDPR регулює захист персональних даних у Європейському Союзі і вимагає від організацій вжиття заходів для забезпечення безпеки таких даних. У ньому визначено, як інформація має оброблятися, зберігатися, і як повинна захищатися від несанкціонованого доступу або витоку.

Ці міжнародні стандарти є основою для організацій, які хочуть забезпечити високий рівень інформаційної безпеки, управляти ризиками, реагувати на інциденти, захищати дані та забезпечити бізнес-неперервність в умовах глобальних кіберзагроз. Вони залишатимуться актуальними й надалі для всіх, хто займається інформаційною безпекою на міжнародному рівні.

Актуальні національні стандарти

Україна розробила низку стандартів, спрямованих на забезпечення інформаційної безпеки, адаптуючи міжнародні норми та створюючи власні нормативні документи. Актуальні стандарти інформаційної безпеки в Україні охоплюють всі аспекти захисту інформації: від управління ризиками до технічного захисту даних. Розробка та впровадження цих стандартів забезпечують сумісність із міжнародними практиками та відповідають сучасним викликам кібербезпеки.

1. ДСТУ 3396.0-96 — Захист інформації. Технічний захист інформації. Основні положення

Цей стандарт закладає базові принципи технічного захисту інформації, визначає основні поняття, терміни та загальні вимоги. Використовується для створення загальної концепції технічного захисту інформації.

2. ДСТУ 3396.1-96 — Захист інформації. Технічний захист інформації. Порядок проведення робіт

Регламентує порядок виконання робіт із технічного захисту інформації, від розробки заходів до впровадження технічних рішень. Забезпечує методологічну основу для виконання робіт на всіх етапах захисту.

3. Закон України "Про основні засади забезпечення кібербезпеки України" (2018)

Цей закон визначає основні принципи, суб'єкти та завдання забезпечення кібербезпеки, а також взаємодію державних органів, бізнесу та громадян. Регулює сферу кібербезпеки та формує правову основу для захисту кіберпростору.

4. ДСТУ ISO/IEC 27001:2015 — Системи управління інформаційною безпекою

Адаптований міжнародний стандарт ISO/IEC 27001:2013. Він встановлює вимоги до впровадження систем управління інформаційною безпекою. Визначає структуру для забезпечення конфіденційності, цілісності та доступності інформації.

5. ДСТУ ISO/IEC 27002:2015 — Керівництво з інформаційної безпеки

Стандарт, який надає рекомендації щодо вибору, впровадження та управління заходами безпеки. Використовується для розробки заходів інформаційної безпеки відповідно до вимог ДСТУ ISO/IEC 27001.

6. НД ТЗІ 1.1-003-99 — Технічний захист інформації. Основні положення

Документ, який визначає основні положення та принципи технічного захисту інформації від несанкціонованого доступу. Використовується для створення систем технічного захисту.

Україна активно адаптує міжнародні стандарти та інтегрує їх у національну практику. Додаткові сучасні документи:

7. ДСТУ ISO/IEC 27005:2018 — Управління ризиками інформаційної безпеки

Стандарт описує процеси ідентифікації, оцінки, управління та моніторингу ризиків інформаційної безпеки. Використовується організаціями для визначення заходів захисту на основі оцінки ризиків.

8. ДСТУ ISO/IEC 27701:2021 — Захист персональних даних

Розширення ISO/IEC 27001 для управління персональними даними відповідно до вимог GDPR та інших міжнародних регуляторів. Актуальний для компаній, які обробляють персональні дані, зокрема в хмарних середовищах.

9. ДСТУ ISO/IEC 27017:2016 — Інформаційна безпека у хмарних середовищах

Рекомендації щодо безпеки хмарних сервісів, включаючи права і обов'язки провайдерів та користувачів. Забезпечує захист інформації у хмарних інфраструктурах.

10. НД ТЗІ 2.5-004-2014 — Захист інформації. Вимоги до організації захисту

Документ визначає вимоги до організації технічного захисту інформації в державних органах та підприємствах. Застосовується для побудови захищених інформаційних систем.

Система національних стандартів України щодо захисту інформації

1. Загальні положення щодо технічного захисту інформації

- ❖ **ДСТУ 3396.0-96 — «Захист інформації. Технічний захист інформації. Основні положення»**

Визначає загальні принципи організації технічного захисту інформації, базові поняття і термінологію.

- ❖ **ДСТУ 3396.1-96 — «Захист інформації. Технічний захист інформації. Порядок проведення робіт»**

Регламентує методику і порядок виконання робіт із технічного захисту інформації (ТЗІ).

2. Управління інформаційною безпекою

- ❖ **ДСТУ ISO/IEC 27001:2015 — «Системи управління інформаційною безпекою. Вимоги»**

Адаптований міжнародний стандарт, який визначає структуру для впровадження систем управління інформаційною безпекою (СУІБ).

- ❖ **ДСТУ ISO/IEC 27002:2015 — «Керівництво з інформаційної безпеки»**

Містить рекомендації для впровадження практичних заходів захисту інформації.

3. Оцінка ризиків інформаційної безпеки

- ❖ **ДСТУ ISO/IEC 27005:2018 — «Управління ризиками інформаційної безпеки»**

Визначає процеси ідентифікації, оцінки та управління ризиками, пов'язаними з інформаційною безпекою.

4. Захист персональних даних

- ❖ **ДСТУ ISO/IEC 27701:2021** — *«Розширення до СУІБ для управління персональними даними»*

Розроблений на основі GDPR, регулює управління персональними даними в системах обробки інформації.

5. Специфічні аспекти захисту інформації

- ❖ **НД ТЗІ 1.1-003-99** — *«Технічний захист інформації. Основні положення»*

Базовий документ, який окреслює принципи створення та підтримання систем ТЗІ.

- ❖ **НД ТЗІ 2.5-004-2014** — *«Вимоги до організації захисту інформації»*

Описує підходи до організації ТЗІ на державному та корпоративному рівнях.

6. Захист інформації у хмарних середовищах

- ❖ **ДСТУ ISO/IEC 27017:2016** — *«Керівництво з безпеки хмарних обчислень»*

Надає рекомендації щодо безпеки для хмарних сервісів та їх користувачів.

7. Інтеграція з міжнародними стандартами

Україна активно адаптує міжнародні стандарти до національних умов, забезпечуючи сумісність із такими документами, як:

- ❖ ISO/IEC 27003, 27004 (планування та моніторинг СУІБ);
- ❖ ISO/IEC 27018 (захист персональних даних у хмарах);
- ❖ ISO/IEC 22301 (управління безперервністю бізнесу).

Особливості системи національних стандартів

▲ Охоплюють технічні, організаційні та методологічні аспекти.

▲ Україна активно впроваджує міжнародні стандарти (ISO, IEC) у національну практику.

▲ Стандарти базуються на чинному законодавстві, зокрема Законах України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», а також «Про кібербезпеку».

▲ Регулярне оновлення стандартів відповідно до розвитку технологій і міжнародних вимог.

В Україні також розробляються національні стандарти щодо захисту інформації, зокрема для конкретних галузей і типів інформаційних систем. Вони охоплюють вимоги до захисту інформаційних систем на всіх етапах: від розробки і впровадження до експлуатації і обслуговування. Система національних стандартів України щодо захисту інформації забезпечує комплексну основу для впровадження, моніторингу та вдосконалення

заходів інформаційної безпеки. Вона гармонізована з міжнародними стандартами, що дозволяє українським підприємствам і державним органам інтегруватися в глобальні інформаційні та кібербезпекові системи.

Стандарти інформаційної безпеки допомагають організаціям:

- Забезпечити відповідність вимогам національного законодавства та міжнародним стандартам.
- Визначити чіткі процеси для управління інформаційними активами та кіберзагрозами.
- Підвищити довіру до своїх систем серед партнерів і клієнтів, оскільки дотримання міжнародних стандартів є ознакою надійності та безпеки.
- Мінімізувати ризики втрати або розголошення конфіденційної інформації.

Таким чином, відповідність стандартам забезпечує організаціям надійний механізм для захисту своїх інформаційних ресурсів від численних кіберзагроз, одночасно створюючи умови для сталого розвитку і підвищення ефективності.

TCSEC (Trusted Computer System Evaluation Criteria), або "Критерії оцінки довірених комп'ютерних систем", був одним із перших стандартів, який встановлював вимоги до безпеки комп'ютерних систем і мав значний вплив на формування міжнародної практики в області інформаційної безпеки. Цей стандарт був розроблений Міністерством оборони США (DoD) в середині 1980-х років і став основою для формалізації критеріїв безпеки в комп'ютерних системах, що обробляють конфіденційну інформацію. Основною метою TCSEC є визначення характеристик безпечних комп'ютерних систем для захисту від несанкціонованого доступу та забезпечення надійності обробки конфіденційної інформації. Хоча TCSEC вже є застарілим стандартом, його принципи заклали основу для більш сучасних нормативних документів, таких як **Common Criteria (ISO/IEC 15408)**, які є міжнародним стандартом для сертифікації безпеки інформаційних систем.

Стандарт визначав кілька рівнів довіри, від яких залежала безпека системи: від найнижчого рівня D до найвищого рівня A. Для систем з рівнем D вимоги до безпеки були мінімальними, тоді як рівень A вимагав найвищого рівня довіри, включаючи використання апаратних засобів для забезпечення безпеки та криптографічних методів захисту даних.

ОСНОВНІ ХАРАКТЕРИСТИКИ TCSEC:

1. Сертифікація систем безпеки

TCSEC вводить поняття сертифікації комп'ютерних систем за рівнями безпеки. Всі комп'ютерні системи повинні оцінюватися за конкретними критеріями на основі їхніх функціональних можливостей і властивостей безпеки.

2. Класифікація безпеки

Стандарт TCSEC визначає різні рівні захищеності комп'ютерних систем, які дозволяють класифікувати системи на основі рівня безпеки:

▲ A (Verified Protection) — найвищий рівень, який забезпечує найбільш суворий контроль доступу, захист від атак та інші заходи для збереження безпеки.

▲ B (Mandatory Protection) — системи з обов'язковим контролем доступу, які надають захист від несанкціонованого доступу.

▲ C (Discretionary Protection) — системи з дискреційним контролем доступу, що забезпечують базову безпеку, але без суворих вимог до захисту.

▲ D (Minimal Protection) — системи з мінімальним захистом.

TCSEC мав значний вплив на подальший розвиток міжнародних стандартів, таких як **ISO/IEC 15408**, що отримав назву **Common Criteria**, який встановлює спільні критерії для оцінки безпеки інформаційних технологій. Цей стандарт надає можливість сертифікувати системи безпеки на основі чітко визначених вимог та оцінки за різними рівнями безпеки (Evaluation Assurance Levels — EAL). Завдяки цьому TCSEC став основою для формування єдиної глобальної практики у сфері сертифікації безпеки інформаційних технологій.

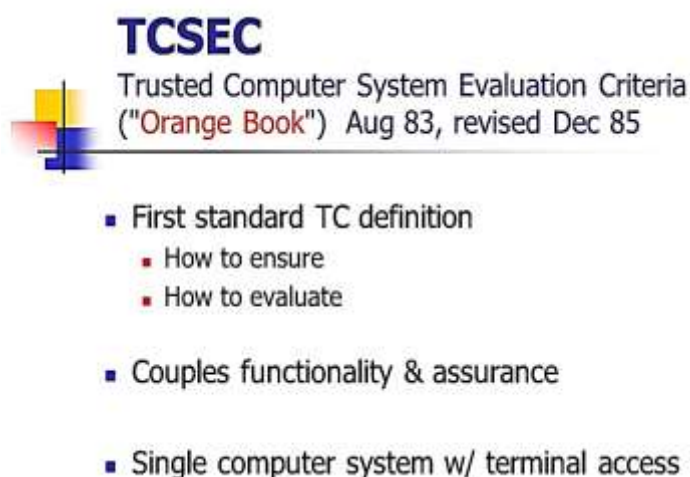


Рис. 1.2. Стандарт TCSEC ((Trusted Computer System Evaluation Criteria)
Джерело: URL: <https://slideplayer.com/slide/5168978/>

Принципи, закладені в TCSEC, також лягли в основу національних стандартів у різних країнах. Наприклад, в Україні було розроблено **ДСТУ 3396.0-96**, який визначає основні положення технічного захисту інформації, враховуючи підходи до оцінки безпеки, подібні до тих, що були впроваджені в TCSEC. Таким чином, цей стандарт забезпечив уніфікацію вимог до безпеки та визначення рівнів довіри для інформаційних систем, що є важливим інструментом у забезпеченні їх захищеності в різних секторах.

Незважаючи на те, що TCSEC був розроблений для потреб оборони, його вплив на стандартизацію безпеки інформаційних систем зберігається й сьогодні, оскільки основні принципи цього стандарту використовуються для створення, оцінки та сертифікації інформаційних систем, що обробляють важливі дані. Враховуючи сучасні загрози в сфері кібербезпеки, ці стандарти залишаються актуальними для визначення найкращих практик і вимог до безпеки в різних організаціях, зокрема урядових структурах, військових установах і корпораціях, що мають високі вимоги до захисту інформації. Такими стандартами є, зокрема, ISO/IEC 27001 для управління інформаційною безпекою, NIST Cybersecurity Framework, а також інші специфічні стандарти для окремих галузей, які охоплюють всі аспекти кібербезпеки — від політик доступу і шифрування до моніторингу і реагування на інциденти.

Ці стандарти допомагають створити ефективну стратегію захисту даних і знизити ризики від кібератак, адже вони включають комплексний підхід до управління безпекою, що охоплює не тільки технічні заходи, але й організаційні та правові аспекти. Вони дозволяють забезпечити сталий рівень безпеки, адаптуючись до постійно змінюваного ландшафту кіберзагроз, і гарантують, що організації можуть відповідати на нові виклики в галузі безпеки.

Документ *TCSEC* було розроблено і опубліковано з метою визначення вимог безпеки, що висуваються до апаратного, програмного і спеціального програмного й інформаційного забезпечення:

- ➔ безпечна система має бути здатною розрізняти користувачів;
- ➔ кожний процес у системі має діяти від імені певного користувача;
- ➔ система має підтримувати розмежування доступу суб'єктів до об'єктів, які містять інформацію;
- ➔ до об'єктів системи можна застосовувати такі дії читання, записування, створення і видалення.

В оригінальному документі Міністерства оборони США, що став основою для багатьох міжнародних стандартів з безпеки, вперше було використано термін “Trusted”, який в контексті безпеки комп’ютерних систем тепер часто перекладається як «захищений» або «безпечний». Цей термін використовувався для опису систем, які були здатні забезпечувати належний рівень захисту інформації від несанкціонованого доступу, порушення цілісності чи розголошення, зокрема в контексті військових та урядових інформаційних технологій. Поширення цього терміну в подальшому стало основою для формулювання багатьох критеріїв безпеки інформаційних систем, як у США, так і в інших країнах.

Документ, на основі якого цей термін був введений, здебільшого відомий як **“Помаранчева книга”** через колір обкладинки оригінального видання. Назва стала популярною внаслідок характерного кольору, яким була оформлена перша публікація. Помаранчева книга містить основні критерії та рекомендації щодо безпеки комп’ютерних систем, а також вимоги до оцінки їхнього захисту. Вона справила значний вплив на розвиток стандартів і практик у галузі інформаційної безпеки в багатьох країнах і міжнародних організаціях.

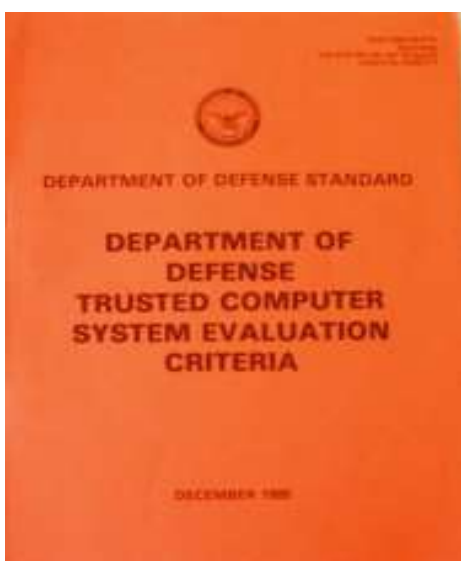


Рис. 1.3. Фотографія документа «Помаранчева книга»
Джерело: URL: <https://slideplayer.com/slide/3386657/>

У 2024-2025 роках, хоча сам TCSEC вже не є актуальним стандартом для сертифікації сучасних систем, принципи, закладені в ньому, і досі активно використовуються для розробки нових стандартів, зокрема в рамках **ISO/IEC 15408** (Common Criteria), який продовжує розвивати ідеї та підходи до оцінки безпеки систем, закладені в **Помаранчевій книзі**.

Цей підхід дозволяє створювати чіткі вимоги до захищеності інформаційних систем і дає можливість проводити сертифікацію, що є важливим для забезпечення відповідності сучасним вимогам безпеки в умовах зростаючих кіберзагроз.

TCSEC був важливим кроком у розвитку інформаційної безпеки і привернув увагу урядів та підприємств до важливості створення безпечних комп'ютерних систем. Його вимоги та класифікація залишаються важливими до сьогодні, хоча з часом були розроблені більш сучасні стандарти для оцінки і сертифікації безпеки.

«Помаранчева книга» (Trusted Computer System Evaluation Criteria, TCSEC) визначає шість основних фундаментальних вимог до безпечних систем, яким повинні відповідати комп'ютерні системи для проходження сертифікації на відповідність стандартам безпеки. Ці вимоги стали основою для оцінки довіри до інформаційних систем, що обробляють конфіденційну або важливу інформацію. Вони визначають рівень захищеності системи від несанкціонованого доступу, порушення цілісності інформації та інших загроз, яким повинні задовольняти такі системи, щоб пройти сертифікацію:

- ✱ **Безпека доступу (Access Control)** – Система повинна мати механізми, які забезпечують контроль за доступом до ресурсів на основі прав доступу користувачів і процесів. Це включає в себе аутентифікацію, авторизацію і моніторинг активності користувачів.

- ✱ **Цілісність інформації (Information Integrity)** – Забезпечення того, щоб інформація не була змінена без дозволу. Система повинна запобігати несанкціонованим змінам даних і дозволяти виявлення будь-яких змін, що відбулися.

- ✱ **Конфіденційність (Confidentiality)** – Інформація повинна бути доступною лише тим особам, які мають відповідні права на її перегляд або обробку. Необхідно забезпечити ізоляцію конфіденційних даних від сторонніх осіб або процесів.

- ✱ **Доступність (Availability)** – Система повинна забезпечувати своєчасний доступ до інформації та ресурсів для авторизованих користувачів, навіть у разі відмови частини системи або виникнення атак.

- ✱ **Аудит (Accountability)** – Система повинна мати можливість реєстрації і перевірки всіх дій користувачів та системних подій. Це необхідно для виявлення порушень безпеки та для доведення відповідальності в разі несанкціонованих дій.

- ✱ **Захист від небажаних дій (Assurance)** – Система повинна мати документи, що підтверджують її здатність забезпечити безпеку згідно з вимогами стандарту. Це включає тестування, перевірку та сертифікацію

системи для виявлення слабких місць і підтвердження відповідності всім вимогам безпеки.

Ці шість вимог допомагають створити цілісну систему безпеки, яка може забезпечити необхідний рівень захисту інформації в будь-якому середовищі. У 2024-2025 роках, хоча TCSEC вже є застарілим стандартом, його принципи і далі застосовуються в сучасних вимогах і стандартах безпеки, таких як **Common Criteria (ISO/IEC 15408)**.

1.4. ПОНЯТТЯ КІБЕРЗЛОЧИННОСТІ. КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ

Кіберзлочинність та комп'ютерна злочинність — це терміни, які часто використовуються як синоніми, але вони мають різні значення, що важливо для точного розуміння цих явищ у контексті сучасної інформаційної безпеки.

1. **Кіберзлочинність (англ. *cybercrime*)** — це більш широкий термін, який включає в себе будь-які злочини, скоєні з використанням комп'ютерних технологій або в кіберпросторі. Це може включати незаконні дії, що пов'язані з комп'ютерними мережами, Інтернетом, програмним забезпеченням, хмарними сервісами, криптовалютами тощо. Кіберзлочинність включає злочини, як-от:

- ▲ **Фінансові шахрайства** (наприклад, крадіжка грошей через онлайн-банкінг або банківські картки);

- ▲ **Крадіжка персональних даних** (збір і використання конфіденційної інформації для цілей шахрайства);

- ▲ **Атаки на інфраструктуру** (хакерські атаки на системи критичної інфраструктури, такі як енергетика, транспорт, державні служби);

- ▲ **Розповсюдження вірусів і шкідливого програмного забезпечення** (malware, ransomware);

- ▲ **Торгівля незаконними матеріалами** (наприклад, дитячою порнографією або наркотиками через онлайн-платформи);

- ▲ **Кібертероризм** (здійснення атак, що ставлять під загрозу національну безпеку).

Кіберзлочинність охоплює не тільки злочини, здійснені безпосередньо за допомогою комп'ютерів, а й ті, які використовують Інтернет для організації, поширення або зберігання злочинної діяльності.

2. **Комп'ютерна злочинність (англ. *computer crime*)** — це більш вузьке поняття, яке стосується злочинів, скоєних через пряме використання комп'ютерних систем і програм. Тобто це

категорія злочинів, вчинених за допомогою комп'ютерного обладнання, таких як:

- ▲ Неавторизований доступ до комп'ютерних систем (хакерство);
- ▲ Злом паролів і неправомірне використання програмного забезпечення;
- ▲ Крадіжка чи підробка електронних даних (наприклад, змінювання фінансових записів або крадіжка інтелектуальної власності).

Таким чином, **кіберзлочинність** є більш всеохоплюючим терміном, оскільки вона включає не тільки злочини, здійснені за допомогою комп'ютерних систем, а й злочини, пов'язані з використанням Інтернету, мереж та онлайн-платформ. Зокрема, це включає в себе новітні злочини, як-от **кібертероризм** чи **онлайн-шахрайства**, які мають значні соціальні та економічні наслідки для держав та бізнесу.

На сучасному етапі, з урахуванням розвитку технологій, кіберзлочинність стала серйозною загрозою для глобальної економіки і безпеки, що вимагає створення нових міжнародних стандартів, політик і технологій для боротьби з такими злочинами. Важливими залишаються питання координації зусиль міжнародних організацій, державних установ і приватного сектору для ефективної протидії кіберзлочинності.

*Термін «**cybercrime**» (кіберзлочинність) став широко використовуваним у сучасній правовій та технологічній практиці, і він описує злочини, пов'язані з використанням комп'ютерних технологій, Інтернету та глобальних мереж. Як зазначено в Оксфордському та Кембриджському тлумачних словниках, приставка «**cyber-**» вказує на зв'язок із інформаційними технологіями, віртуальними середовищами та Інтернетом. Таким чином, **cybercrime** охоплює різноманітні види злочинів, що здійснюються за допомогою або в контексті технологій і глобальних мереж. Це можуть бути як фінансові злочини (наприклад, онлайн-шахрайства, крадіжка кредитних карток, фішинг), так і кібертероризм, інтернет-торгівля незаконними матеріалами, атаки на інформаційні системи, а також незаконне використання даних.*

*Натомість, «**computer crime**» (комп'ютерна злочинність) є більш вузьким і спеціалізованим терміном, який зосереджується на злочинах, що безпосередньо*

спрямовані проти комп'ютерних систем, апаратного забезпечення або даних, які зберігаються в цих системах. Це можуть бути злочини, такі як несанкціонований доступ до комп'ютерних мереж, злом паролів, крадіжка чи підробка електронних даних, порушення авторських прав в цифровому середовищі.

У зв'язку з постійним розвитком технологій та цифровізації бізнесу і повсякденного життя, термін **«cybercrime»** все більше втілює концепцію злочинів, скоєних не лише проти комп'ютерів, але й у контексті більш широкого застосування інформаційних технологій, в тому числі через Інтернет і інші віртуальні простори. Зокрема, сучасні кіберзлочини включають в себе такі явища, як кібербулінг, хактивізм, атаки на критичні інфраструктури, та інші форми онлайн-злочинів, що можуть мати серйозні наслідки для глобальної економіки і безпеки.

Таким чином, хоча терміни **«cybercrime»** і **«computer crime»** схожі, вони мають різний контекст: перший є більш широким і описує злочини, що мають справу з глобальними мережами, а другий більше фокусується на технічних аспектах злочинів, спрямованих на комп'ютерні системи та їх компоненти.

Кіберзлочинність залишається однією з найшвидше зростаючих сфер злочинності у світі. Згідно з прогнозами, до 2025 року глобальні збитки від кіберзлочинності можуть досягти 10,5 трильйонів доларів США на рік.

У Європейському Союзі ситуація також викликає серйозне занепокоєння. У першій половині 2024 року в Польщі було зареєстровано понад 400 тисяч кібератак, що свідчить про високий рівень кіберзагроз у регіоні.

В Україні кіберзлочинність також є актуальною проблемою. У 2023 році кіберполіція виявила понад 3 600 кіберзлочинів, що на 59% більше порівняно з попереднім роком.

З огляду на ці тенденції, важливою є розробка та впровадження ефективних стандартів і заходів з кібербезпеки, щоб протистояти зростаючим кіберзагрозам та забезпечити захист інформаційних систем і даних.

В Україні на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини в цій сфері. Законодавча база України у сфері кібербезпеки значно розширилася та вдосконалилася.

ОСНОВНІ НОРМАТИВНО-ПРАВОВІ АКТИ:

- ✱ **Конституція України:** визначає основні принципи та права громадян, включаючи право на інформацію та її захист.
 - ✓ **Стаття 32.** *Заборона втручання в особисте та сімейне життя, захист персональних даних.*
 - ✓ **Стаття 34.** *Право на свободу інформації.*
- ✱ **Кримінальний кодекс України:** встановлює відповідальність за злочини, пов'язані з інформаційними технологіями та кіберзлочинністю.
 - ✓ Кібератаки (Ст. 361–363-1).
 - ✓ Неправомірний доступ до інформаційних систем.
 - ✓ Порушення законодавства у сфері захисту інформації.
- ✱ **Закон України «Про основні засади забезпечення кібербезпеки України» (2017):** регулює питання забезпечення кібербезпеки на державному рівні. Передбачає створення *Національного координаційного центру кібербезпеки* та взаємодію з CERT-UA.
- ✱ **Закон України «Про інформацію» (оновлена редакція 2021 року):** визначає правові основи доступу до інформації та її захисту. Регламентує права та обов'язки власників і користувачів інформації.
- ✱ **Закон України «Про захист інформації в інформаційно-комунікаційних системах»:** регулює питання захисту інформації в ІТ-системах. Включає положення щодо аудиту, сертифікації систем захисту та застосування криптографії.
- ✱ **Закон України «Про основи національної безпеки» (2018):** визначає захист інформації та кібербезпеку як складові національної безпеки. Затверджує положення щодо протидії гібридним загрозам.
- ✱ **Доктрина інформаційної безпеки України (затверджена у 2017 році):** визначає стратегічні напрямки забезпечення інформаційної безпеки.
 - ✓ Протидія інформаційним впливам та дезінформації.
 - ✓ Захист критичної інформаційної інфраструктури.
 - ✓ Розвиток кібербезпеки у державному секторі.
- ✱ **Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція):** міжнародний договір, що регулює боротьбу з кіберзлочинністю. Визначає правові механізми для боротьби з кіберзлочинами, зокрема щодо транскордонного співробітництва.

- **Закон України «Про захист персональних даних» (оновлений у 2021 році).** Гармонізований із Загальним регламентом ЄС щодо захисту даних (GDPR). Регулює обробку, зберігання та передачу персональних даних.
- **Інші нормативно-правові акти.**
 - ✓ **Закон України «Про електронні довірчі послуги» (2017).** Регулює цифрові підписи, електронні печатки та сертифікацію.
 - ✓ **Стандарти та положення Державної служби спеціального зв'язку та захисту інформації України (ДССЗІ).** Включають технічні вимоги до захисту інформації та криптографії.
 - ✓ **Постанова Кабінету Міністрів України № 518 (2019).** Визначає порядок обміну інформацією у разі кіберінцидентів.

Оновлення та нові ініціативи:

- **План заходів на 2023—2024 роки з реалізації Стратегії кібербезпеки України:** затверджений Кабінетом Міністрів України, цей план визначає конкретні кроки для посилення кібербезпеки в країні.
- **Законопроект № 12207:** зареєстрований у Верховній Раді України, цей законопроект спрямований на удосконалення процедур нагляду за кібербезпекою та впровадження європейських схем сертифікації кібербезпеки.
- **Розпорядження Кабінету Міністрів України від 18.10.2024 № 1021-р:** передбачає заходи з модернізації системи виявлення уразливостей та реагування на кіберінциденти протягом 2024—2025 років.
- **Наказ № НОД/830/24 від 06.11.2024:** встановлює вимоги щодо мінімізації кіберзагроз у державних органах.
- **Стандарт вищої освіти «Кібербезпека»:** затверджений Міністерством освіти і науки України, цей стандарт вводиться в дію з 2024/2025 навчального року, що свідчить про підвищену увагу до підготовки фахівців у сфері кібербезпеки.

Ці ініціативи свідчать про системний підхід України до забезпечення кібербезпеки та інтеграції європейських стандартів у національне законодавство.

*Згідно з українським законодавством, **кібербезпека** — це процес забезпечення захищеності життєво важливих інтересів людини, громадянина, суспільства та держави в*

умовах використання кіберпростору. Вона спрямована на забезпечення сталого розвитку інформаційного суспільства та цифрового комунікативного середовища, а також на своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України в кіберпросторі. Це визначено в ст. 5 ч. 1 ст. 1 **Закону України «Про основні засади забезпечення кібербезпеки України»**.

В контексті глобальної безпеки, **кібербезпека** охоплює заходи, спрямовані на захист мереж, програмного забезпечення та інформаційних систем від кіберзагроз, зокрема, від атак, що можуть призвести до порушень в функціонуванні критичних інфраструктур або витоку важливої інформації.

Таким чином, кібербезпека є не лише технічним питанням, а й ключовим компонентом національної безпеки, оскільки в умовах цифровізації більшість критичних і стратегічних функцій держави та суспільства здійснюється через інформаційно-комунікаційні технології.

Згідно з Конвенцією про кіберзлочинність, яка є частиною українського законодавства з 11 жовтня 2005 року, кіберзлочинність умовно поділяється на чотири основні види. Цей поділ допомагає чітко класифікувати злочини в кіберпросторі та відповідно регулювати заходи боротьби з ними.

До першого виду належать злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Цей вид кіберзлочинів включає злочини, спрямовані на порушення роботи комп'ютерних систем або їх даних. Наприклад:

- Несанкціонований доступ до комп'ютерних систем або їх частин.
- Навмисне пошкодження, знищення, зміна або приховування інформації.
- Незаконне виготовлення, продаж, придбання або розповсюдження програмного забезпечення, яке може призвести до порушення безпеки системи або даних.

До другого виду належать злочини, пов'язані з комп'ютерами, що ведуть до втрати майна

Цей вид включає злочини, які спричиняють економічні збитки, через втручання в комп'ютерні системи або дані. Це може бути:

- Введення, зміна чи знищення комп'ютерних даних з шахрайською метою.
- Втручання у функціонування комп'ютерних систем з метою здобуття незаконної економічної вигоди.

кіберзлочинів належать правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, не маючи на це права, економічних переваг для себе чи іншої особи.

Третій вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі.

Четвертим видом є порушення авторських прав і суміжних прав, умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди ВОІВ про авторське право, а також національного законодавства України.

Конвенції про кіберзлочинність, що набрала чинність від 01.07.2006

В Конвенції про кіберзлочинність є важливим міжнародним правовим документом, що встановлює загальні стандарти боротьби з кіберзлочинністю та сприяє міжнародному співробітництву в цьому напрямі. Вона була розроблена в рамках Ради Європи і з того часу стала основою для розробки національних законодавств, у тому числі в Україні. Представлена класифікація кіберзлочинів, які характеризуються наявністю наміру як елемента суб'єктивної сторони. Всього – три категорії кіберзлочинів:

1. Злочини проти конфіденційності, цілісності і працездатності комп'ютерних даних і систем – незаконний доступ, незаконне перехоплення, створення перешкод для обміну даними, створення перешкод для функціонування систем, неправомірне використання апаратних пристроїв. Зокрема:

- **Незаконний доступ** до комп'ютерних систем або даних.
- **Незаконне перехоплення** інформації, що передається через комп'ютерні мережі.
- Створення **перешкод для обміну даними** або для **функціонування систем**.
- **Неправомірне використання апаратних пристроїв**, що веде до порушення безпеки інформаційних систем.

2. Комп'ютерні злочини – фальсифікація і підробка, що здійснюються з використанням комп'ютерної техніки. Це злочини, що вчиняються з використанням комп'ютерної техніки для фальсифікації або підробки даних, документів або інформації. Це може включати:

- **Фальшування даних** для шахрайських цілей.
- **Підробка фінансових документів** або інших записів за допомогою комп'ютерних програм.

3. Злочини, пов'язані з контентом – виготовлення, поширення і зберігання дитячої порнографії. Ці правопорушення стосуються незаконного створення, поширення та зберігання шкідливого або незаконного контенту в інтернеті, зокрема:

- **Виготовлення, поширення та зберігання дитячої порнографії.**

Визначення та класифікація кіберзлочинів у Конвенції допомагає краще розуміти природу кіберзлочинності та сприяє формуванню єдиної міжнародної правової бази для боротьби з цими правопорушеннями. Україна, як член міжнародного співтовариства, також інтегрує положення цієї Конвенції в національне законодавство для посилення кібербезпеки та ефективної боротьби з кіберзлочинністю.

Схема Конвенції Ради Європи

У схемі, що запропонована *Конвенцією Ради Європи (Будапештська конвенція)* включає чотири основні категорії кіберзлочинів, що описуються через різні типи інцидентів, які можуть бути пов'язані з порушенням кібербезпеки. Спрямована на боротьбу з кіберзлочинністю, йдеться про чотири можливі групи таких дій:

1. Інциденти, що мають на меті завдати шкоди конфіденційності, цілісності й доступності комп'ютерних даних та систем і реалізуються через:

- ➔ **несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або**

її частини, а також до IP проти борчої сторони, здійснений в обхід систем безпеки);

- ➔ втручання в дані (протиправна зміна, ушкодження, вилучення, перекручування або блокування комп'ютерних даних і керуючих команд за допомогою кібератак на інформаційні системи, ресурси та мережі державного і військового управління);
- ➔ втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розробку та поширення вірусного ПЗ, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікацій і зв'язку, на обробку та передачу інформації, на системи захисту IP, систем і мереж, програмно-математичне забезпечення, протоколи передачі даних, алгоритми адресації та маршрутизації);
- ➔ незаконне перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних, переданих ІКС в обхід заходів безпеки);
- ➔ незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

2. Шахрайство та підробка, пов'язані з використанням комп'ютерних систем:

- ➔ підробка документів із застосуванням комп'ютерних засобів (протиправне навмисне внесення, змінювання, вилучення або блокування комп'ютерних даних, що призводить до зниження вірогідності документів);
- ➔ шахрайство із застосуванням комп'ютерних засобів (втручання у функціонування комп'ютерної системи з метою навмисного протиправного одержання економічної вигоди).

3. Інциденти, пов'язані з розміщенням у мережах протиправної інформації (наприклад, поширення дитячої порнографії, продаж зброї, наркотичних речовин тощо).

4. Інциденти, що порушують авторські та суміжні права

Це включає порушення прав інтелектуальної власності, зокрема:

- ➔ Незаконне розповсюдження авторських творів через Інтернет;
- ➔ Піратство у цифровому середовищі, включаючи несанкціоноване копіювання та поширення програмного забезпечення, музики, фільмів та інших захищених творів.

Ці інциденти справді залишаються актуальними, оскільки технології продовжують удосконалюватися, а кіберзлочинність зростає в умовах

швидкої цифровізації та глобалізації. Враховуючи ці фактори, законодавства різних країн, зокрема України, активно адаптуються до нових кіберзагроз, запроваджуючи відповідні норми і стратегії для боротьби з кіберзлочинністю. Важливою складовою цього є участь у міжнародних угодах, таких як Будапештська конвенція, яка має на меті гармонізацію правових підходів до кіберзлочинів та покращення співпраці між державами для ефективної боротьби з кіберзлочинністю. Крім того, країни активно розвивають механізми для захисту інформаційної безпеки, інтегруючи технології обміну даними, розробляючи національні програми з кіберзахисту та створюючи спеціалізовані органи для моніторингу та реагування на кіберзагрози.



Наприклад:

Міжнародна організація кримінальної поліції (Інтерпол) використовує спеціальну систему ідентифікації інцидентів кіберзлочинності, де кожен тип злочину має унікальний код, що починається з літери "Q".

1. **QA** – несанкціонований доступ або перехоплення;
2. **QD** – зміна комп'ютерних даних;
3. **QF** – комп'ютерне шахрайство;
4. **QR** – незаконне копіювання (піратство).

Ця система кодування дійсно є важливим інструментом для класифікації та відслідковування різних видів кіберзлочинів на міжнародному рівні. Вона дозволяє уніфікувати підхід до визначення типів кіберзлочинної діяльності та спрощує обмін інформацією між країнами, сприяючи більш ефективному розслідуванню та виявленню кіберзлочинців. Проте слід зазначити, що така інформація є загальною і може не охоплювати всі специфічні аспекти окремих випадків. Для отримання більш детальних відомостей щодо конкретних кримінальних справ або практик, що застосовуються в різних країнах, рекомендується звертатися до офіційних джерел Інтерполу або відповідних національних правоохоронних органів, які займаються розслідуванням кіберзлочинності.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 1

1. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.
2. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.

3. Жданова, Ю., Шевченко, С., Спасітелева, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки.

4. Закон України «Про стандартизацію», від 05.06.2014 № 1315-VII, <https://zakon.rada.gov.ua/laws/show/1315-18#Text>

5. Закон України «Про технічні регламенти та оцінку відповідності» від 15.01.2015 № 124-VIII, <https://zakon.rada.gov.ua/laws/show/124-19#Text>

6. Закон України «Про захист інформації в інформаційно-комунікаційних системах», <http://zakon.rada.gov.ua/>

7. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

8. Закон України «Про електронні довірчі послуги», <http://zakon.rada.gov.ua/>

9. Закон України «Про Державну службу спеціального зв'язку та захисту інформації», <http://zakon.rada.gov.ua/>

10. Указ Президента України від 22.05.1998 №505 «Про затвердження Положення про порядок криптографічного захисту інформації в Україні», <http://zakon.rada.gov.ua/>

11. Указ Президента України від 27.09.1999 № 1229 «Про затвердження Положення про технічний захист інформації в Україні», <http://zakon.rada.gov.ua/>

12. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" <http://zakon.rada.gov.ua/> 1

13. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, цифрових комунікаційних та інформаційно-комунікаційних системах», <http://zakon.rada.gov.ua/>

14. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», https://tzi.ua/ua/nd_tz_1.1-003-99.html

15. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі. Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 № 125 https://tzi.ua/ua/nd_tz_3.7-003_-2005.html

16. Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 468–486.

17. I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27.

18. Шевченко, С., Жданова, Ю., Спасітелєва, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

19. Z. Hu, et al., Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range, DataCentric Business and Applications 48 (2020) 675–709.

20. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18.

21. V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

22. H. Hulak, et al., Dynamic model of guarantee capacity and cyber security management in the critical automated systems, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2022) 102–111.

23. Машталяр, Я., Козачок, В., Бржевська, З., Богданов, О., Оксанич, І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 156–167.

24. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.

25. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 99–120.

26. Shevchenko, S., Zhdanova Y., Skladannyi, P., & Boiko, S. (2022). Інсайтери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 175–185.

27. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT) "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги"
28. ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою".
29. ДСТУ ISO/IEC 27005:2022 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки".
30. ДСТУ ISO/IEC 27701:2022 "Розширення для управління конфіденційністю в системах управління інформаційною безпекою".
31. ДСТУ ISO/IEC 15408:2020 "Критерії оцінювання безпеки інформаційних технологій".
32. ДСТУ ISO/IEC 24762:2015 "Інформаційні технології. Методи захисту. Рекомендації з відновлення інформаційно-комунікаційних технологій після інцидентів".

РОЗДІЛ 2

МІЖНАРОДНІ СТАНДАРТИ



International
Organization for
Standardization



International
Electrotechnical
Commission



2.1. Класи безпеки комп'ютерних систем

2.2. Міжнародні стандарти серії ISO 27000

Міжнародні стандарти у сфері кібербезпеки є важливими інструментами для визначення найкращих практик захисту інформації та інформаційних систем на глобальному рівні. Вони допомагають забезпечити гармонізацію підходів до безпеки та підтримують міжнародне співробітництво у боротьбі з кіберзлочинністю. Основні міжнародні стандартів у сфері кібербезпеки:

ISO/IEC 27001 — міжнародний стандарт для систем управління інформаційною безпекою (ISMS). Він визначає вимоги до створення, впровадження, підтримки та постійного покращення системи управління безпекою інформації в організаціях будь-яких розмірів і сфер діяльності.

ISO/IEC 27002 — цей стандарт надає рекомендації щодо найкращих практик управління безпекою інформації, включаючи заходи, що забезпечують конфіденційність, цілісність та доступність інформації.

NIST Cybersecurity Framework (CSF) — створений Національним інститутом стандартів і технологій США (NIST), цей стандарт надає практичні рекомендації для організацій щодо управління кібербезпекою та зменшення ризиків кіберзагроз. Він складається з п'яти основних функцій: Ідентифікація, Захист, Виявлення, Реагування та Відновлення.

General Data Protection Regulation (GDPR) — це регламент Європейського Союзу, що визначає правила захисту персональних даних. Він має глобальне значення, оскільки охоплює всі організації, що обробляють дані громадян ЄС, і встановлює строгі вимоги щодо безпеки даних.

Payment Card Industry Data Security Standard (PCI DSS) — набір стандартів для захисту даних платіжних карт, розроблений міжнародними фінансовими організаціями. Він визначає вимоги до зберігання, обробки та передачі інформації про платіжні картки.

Cybersecurity Act of the European Union — акт ЄС, який створює загальні рамки для кібербезпеки в Європі, включаючи сертифікацію продуктів і послуг у сфері кібербезпеки та сприяє розвитку національних інфраструктур з кібербезпеки в країнах ЄС.

BudaPest Convention (Convention on Cybercrime) — міжнародна угода, спрямована на боротьбу з кіберзлочинністю. Вона визначає стандарти для криміналізації діяльності, пов'язаної з комп'ютерними злочинами, та забезпечує міжнародне співробітництво в розслідуванні таких злочинів. Ці стандарти сприяють забезпеченню кібербезпеки як на національному, так і на міжнародному рівнях, встановлюючи єдині вимоги до захисту інформаційних ресурсів, що дозволяє знижувати ризики для організацій, зокрема у випадках кіберзлочинності та інцидентів з безпекою даних.

2.1. Класи безпеки комп'ютерних систем

Класифікація безпеки комп'ютерних систем на основі різних аспектів захисту, таких як конфіденційність, цілісність, доступність та інші, є важливою частиною управління інформаційною безпекою. У сучасній практиці виділяються кілька основних класів безпеки комп'ютерних систем, що використовуються для класифікації рівня їх захищеності.

Основні класи безпеки комп'ютерних систем:

- ✿ **Клас конфіденційності:**
 - ✓ Забезпечує захист від несанкціонованого доступу до інформації. Цей клас гарантує, що тільки авторизовані користувачі можуть отримувати доступ до чутливої інформації.
 - ✓ Методи забезпечення: шифрування даних, контроль доступу, багаторівневі системи аутентифікації.
- ✿ **Клас цілісності:**
 - ✓ Охоплює захист інформації від несанкціонованих змін. Гарантує, що дані не були змінені або знищені без відома користувача або адміністратора.
 - ✓ Методи забезпечення: контроль цілісності через хешування, цифрові підписи, використання контрольних сум для перевірки даних.
- ✿ **Клас доступності:**

- ✓ Гарантує, що інформація та ресурси доступні в потрібний час і не піддаються збоїв у роботі. Важливим є забезпечення надійності роботи системи, навіть у разі атак або технічних неполадок.
- ✓ Методи забезпечення: резервне копіювання даних, відновлення після аварій, забезпечення безперервної роботи системи.
- ✱ **Клас аутентифікації та авторизації:**
 - ✓ Аутентифікація визначає, чи є користувач тим, за кого себе видає. Авторизація визначає, які дії дозволено виконувати конкретному користувачеві.
 - ✓ Методи забезпечення: двофакторна аутентифікація, контроль доступу на основі ролей (RBAC), використання біометричних даних.
- ✱ **Клас аудиту та моніторингу:**
 - ✓ Забезпечує моніторинг активності в системі для виявлення аномалій або спроб несанкціонованого доступу. Ведення журналів безпеки дозволяє здійснювати аудит і аналіз інцидентів.
 - ✓ Методи забезпечення: системи моніторингу подій безпеки (SIEM), ведення журналів доступу і змін, інтеграція з системами виявлення вторгнень (IDS/IPS).
- ✱ **Клас захисту від вірусів і шкідливих програм:**
 - ✓ Орієнтований на захист від вірусів, троянських програм, шпигунських і рекламних програм.
 - ✓ Методи забезпечення: антивірусне програмне забезпечення, брандмауери, системи запобігання вторгненням (IPS).
- ✱ **Клас фізичної безпеки:**
 - ✓ Охоплює захист від несанкціонованого фізичного доступу до комп'ютерних систем і пристроїв.
 - ✓ Методи забезпечення: контроль доступу до приміщень, відеоспостереження, замки, обмеження фізичного доступу до серверів.
- ✱ **Клас відновлення після катастроф:**
 - ✓ Забезпечує можливість відновлення роботи систем після аварії або катастрофи.
 - ✓ Методи забезпечення: резервні копії, географічно розподілені дата-центри, використання хмарних рішень для відновлення даних.

Класифікація за моделями безпеки:

➤ Модель Бела – ЛаПадулі (Bell-LaPadula Model):

Орієнтована на забезпечення конфіденційності інформації. У моделі використовуються правила "не читай вище" (no read up, NRU) і "не пиши нижче" (no write down, NWD), що забезпечує захист від несанкціонованого доступу до інформації з високим рівнем конфіденційності. Модель Бела –

ЛаПадулі (Bell-LaPadula Model) є однією з основних моделей контролю доступу, що застосовується для захисту інформації в системах з різними рівнями конфіденційності. Вона була розроблена в 1970-х роках і спрямована на збереження конфіденційності даних, забезпечуючи запобігання несанкціонованому доступу до чутливої інформації. Правило "не читай вище" (no read up, NRU) забороняє користувачеві доступ до інформації на вищому рівні конфіденційності, ніж у нього є дозвіл. Це означає, що користувач з обмеженими правами не може читати документи, які мають більш високий рівень захисту, ніж його власний. У свою чергу, правило "не пиши нижче" (no write down, NWD) обмежує користувача в можливості запису інформації на нижчий рівень конфіденційності. Таким чином, навіть якщо користувач має дозвіл на доступ до висококонфіденційних даних, він не може випадково або навмисно передавати їх на нижчий рівень, де доступ до цих даних мають менш авторизовані користувачі. Модель забезпечує важливий захист від витоків інформації та можливих атак, коли висококонфіденційні дані можуть бути випадково чи навмисно передані на менш захищені рівні. Модель Бела – ЛаПадулі є дуже корисною для організацій, які працюють з інформацією різних рівнів секретності, таких як урядові установи, військові організації та інші корпоративні структури, що потребують захисту конфіденційних даних. Однак модель має певні обмеження, оскільки вона не враховує цілісність даних або доступ до інформації для її модифікації. Тому для комплексного забезпечення безпеки інформаційних систем можуть застосовуватися інші моделі, такі як модель Биби (Biba Model) або модель Лінуца (Lattice-Based Model).

➤ **Модель Биба – Мандела (Biba Model):**

Орієнтована на забезпечення цілісності даних. Модель визначає принципи, які забороняють зміну даних користувачем з нижчим рівнем привілеїв. Модель Биба – Мандела (Biba Model) фокусується на забезпеченні цілісності даних, запобігаючи несанкціонованим змінам або пошкодженням інформації. Вона розроблена для забезпечення того, щоб користувачі з меншими правами доступу не могли змінювати дані, що належать користувачам з більш високим рівнем доступу, таким чином забезпечуючи захист від навмисних або випадкових змін. Основними принципами цієї моделі є правила "не читай нижче" (no read down, NRD) і "не пиши вище" (no write up, NWU). Правило "не читай нижче" забороняє користувачеві доступ до інформації на нижчому рівні цілісності, ніж у нього є дозвіл, щоб запобігти можливості зчитування або використання застарілої або неперевіреної інформації. Правило "не пиши вище" забороняє користувачу з низьким рівнем привілеїв змінювати дані на більш високому рівні, що захищає їх від неконтрольованих змін. Модель Биба є важливою в контексті критичних інформаційних систем, де точність і достовірність даних є першочерговими. Вона широко застосовується в таких

сферах, як фінансові та медичні інформаційні системи, де цілісність даних має вирішальне значення для прийняття правильних рішень і забезпечення безпеки. Однак модель Биба не вирішує питання конфіденційності даних, оскільки її основний фокус – це саме цілісність. Вона може використовуватися в поєднанні з іншими моделями, наприклад, з моделлю Бела – ЛаПадулі, щоб забезпечити більш комплексний захист як конфіденційності, так і цілісності. Таким чином, застосування моделі Биба допомагає створити більш стійку інформаційну систему, яка не лише зберігає конфіденційність, але й гарантує, що дані не будуть пошкоджені або змінені несанкціонованими особами.

➤ Модель лінійної безпеки:

Включає концепцію збереження балансу між доступністю, цілісністю та конфіденційністю даних. Ця модель застосовується для забезпечення захисту на різних рівнях комп'ютерних систем, при цьому кожен рівень має свої стандарти і критерії безпеки. Модель лінійної безпеки зосереджується на балансуванні трьох ключових аспектів: доступності, цілісності та конфіденційності даних, що забезпечує цілісну систему захисту. Вона дозволяє організаціям визначати, як різні рівні безпеки взаємодіють між собою та як кожен з них впливає на інші аспекти захисту інформації. Основною метою цієї моделі є забезпечення того, щоб зміни в одному рівні безпеки не порушували інші, створюючи тим самим цілісну і ефективну систему. Модель лінійної безпеки застосовується на всіх етапах життєвого циклу інформаційних систем, від проектування до експлуатації. Вона може бути адаптована до конкретних потреб організацій, враховуючи специфіку їхніх інфраструктур і вимоги до безпеки. У цій моделі для кожного рівня безпеки визначаються чіткі стандарти, що дозволяє адаптувати систему до змінюваних загроз. Крім того, модель дозволяє створювати гнучкі механізми захисту, які здатні швидко реагувати на нові виклики та уразливості. Лінійна модель безпеки також враховує не лише технічні, а й організаційні аспекти захисту інформації. Наприклад, на рівні доступу до інформації можуть бути застосовані специфічні протоколи аутентифікації, а на рівні передачі даних — методи шифрування. У результаті, модель лінійної безпеки дозволяє досягти більш високого рівня захисту та зниження ймовірності порушень цілісності або витоку даних у складних інформаційних середовищах.

➤ Модель доступу на основі ролей (RBAC – Role-Based Access Control):

Модель доступу на основі ролей (RBAC – Role-Based Access Control) є однією з найбільш поширених і ефективних моделей безпеки, що використовується для управління доступом до ресурсів в інформаційних системах. Вона передбачає, що доступ до ресурсів системи надається користувачам не безпосередньо, а через ролі, які їм призначаються відповідно

до їхніх функціональних обов'язків у межах організації. Кожен користувач має бути призначений одній або кільком ролям, які визначають його рівень доступу до різних ресурсів системи. Ролі можуть бути узагальнені (наприклад, "менеджер", "адміністратор") або специфічні для певних функцій (наприклад, "технічний спеціаліст"). Кожна роль має певний набір прав доступу до ресурсів. Це можуть бути права на читання, запис, модифікацію або видалення даних, виконання операцій тощо. Користувачі отримують доступ до ресурсів шляхом призначення їм ролей, відповідно до їхніх обов'язків у організації. Наприклад, адміністратору можуть бути надані права для конфігурації серверів, а рядовим співробітникам — лише на доступ до певних баз даних. Важливим принципом моделі RBAC є принцип мінімальних прав, згідно з яким користувачам надаються лише ті права доступу, які необхідні для виконання їхніх конкретних завдань. Це знижує ймовірність несанкціонованого доступу до чутливих даних і критичних систем. Модель також підтримує ієрархічні ролі, де одна роль може успадковувати права іншої. Наприклад, роль "менеджер" може мати всі права доступу "співробітника", а також додаткові права, що дозволяють керувати іншими користувачами чи доступом до специфічних даних. Модель RBAC дозволяє зручно здійснювати моніторинг доступу користувачів до системи, оскільки зміни в ролях автоматично оновлюють права доступу для всіх користувачів, які мають ці ролі. Це значно полегшує адміністрацію та аудит доступу. Вона також дозволяє швидко і ефективно налаштувати необхідний рівень доступу при зміні ролі користувача або при переході на нову посаду. Призначення прав доступу на основі ролей знижує складність адміністрування, оскільки зміни прав доступу здійснюються через зміни ролей, а не через зміни прав конкретних користувачів. Це зменшує ймовірність помилок у призначенні доступу і дає змогу краще контролювати доступ до важливих ресурсів. Модель RBAC є надзвичайно корисною для організацій, що мають велику кількість співробітників, оскільки забезпечує централізоване та зручне управління доступом, що сприяє підтримці високого рівня безпеки інформаційних систем.

Класи безпеки комп'ютерних систем визначають рівень захисту різних аспектів системи і служать основою для розробки заходів безпеки, що відповідають потребам користувачів та організацій. Управління безпекою є багатогранним процесом, який включає застосування різних методів захисту, моніторингу і відновлення після атак або катастроф.

Єдина ієрархічна шкала класів безпеки наведена в стандарті **TCSEC** (англ. *Trusted Computer System Evaluation Criteria*). Вона дає змогу оцінити загальну захищеність системи. Система належить до певного класу, якщо вона задовольняє всі вимоги, які висувають до систем цього класу. Кожний наступний клас, окрім вимог попереднього класу, містить кілька додаткових вимог.

Залежно від конкретних значень цих вимог, інформаційні системи поділяють на групи А, В, С і D:

Група D – мінімальний захист (вимоги з безпеки системи не визначені);

Група C (дискреційний захист). Характеризується наявністю дискреційного керування доступом і реєстрації дій суб'єктів. Група розрахована на багатокористувацькі системи, в яких здійснюється спільне оброблення даних одного рівня конфіденційності. Цей рівень ділиться на два підрівня:

▲ **Системи класу C1** містять засоби контролю і керування доступом, які дають змогу визначати обмеження для користувачів, що надає їм можливість захищати свою приватну інформацію від інших користувачів;

▲ **Системи класу C2** застосовують засоби індивідуального контролю за діями користувачів, реєстрацію і облік подій (аудит). Саме вимогам цього класу відповідають різні операційні системи універсального призначення. Серед операційних систем можна назвати **Windows, HP-UX, Solaris**. Серед СКБД – **Oracle, Informix** і деякі інші.

Група B (мандатний захист). Основні вимоги цієї групи нормативне (мандатне) керування доступом із використанням міток безпеки, підтримка політики безпеки. У число цього рівня входять три підрівня:

▲ **B1** – системи, що підтримують мандатне управління доступом і взаємну ізоляцію процесів шляхом поділу їх адресних просторів;

▲ **B2** – система цього класу має здійснювати контроль прихованих каналів витоку інформації. Керування безпекою здійснюють адміністратори системи. Передбачені засоби керування конфігурацією. Механізми аутентифікації посилені;

▲ **B3** – у цих системах передбачається введення адміністратора безпеки, а механізми контролю розширені так, щоб забезпечити обов'язкову сигналізацію про всі події, пов'язані з можливим порушенням встановлених в системі правил безпеки.

Група A (перевірений захист). Ця група характеризується застосуванням формальних методів верифікації коректності роботи механізмів керування доступом. Група має один клас – **A1**. Системи цього класу еквівалентні системам класу **B3**, до них не висувають додаткових функціональних вимог.

«Помаранчева книга» передбачає чотири групи, що відповідають різному ступеню захищеності: від мінімальної (**група D**) до формально доведеної (**група A**). Кожна група включає один чи кілька класів. **Групи D і A** містять по одному класу (**класи D1 і A1**, відповідно), **група C** – **класи C1, C2**, а **група B** три класи – **B1, B2, B3**, що характеризуються різними наборами вимог безпеки. Рівень безпеки зростає при русі від **групи D** до **групи A**, а всередині групи – зі зростанням номера класу.

Групи	Класи			
A	A1			Верифікований захист
B	B1	B2	B3	Мандатний захист
C	C1	C2		Дискреційний захист
D	D1			Мінімальний захист

Рис. 2.1. Розподіл захисту на чотири групи, які передбачає «Помаранчева книга»

Джерело: [1-6]



У «Помаранчевій книзі» не розглядалися проблеми, що виникають при об'єднанні комп'ютерів у загальну мережу. Сформоване становище таке, що наявність мережі позбавляє законної сили сертифікат «Помаранчевої книги». Тому слідом за критеріями безпеки для комп'ютерних систем з'явилися критерії і для комп'ютерних мереж («Червона книга»). У «Червону книгу» збережені всі вимоги до безпеки з «Помаранчевої книги», зроблена спроба адресації мережевого простору і створення концепції безпеки мережі. У наші дні проблеми стали ще серйозніше. Організації стали використовувати бездротові мережі, появи яких «Червона книга» не могла передбачити. Для бездротових мереж сертифікат «Червоної книги» вважається застарілим. Запропоновані в цьому документі концепції захисту і набір функціональних вимог було покладено в основу створення всіх стандартів безпеки, що з'явилися згодом.

Від «Помаранчевої книги» до «Червоної книги»

1. «Помаранчева книга» — це перший серйозний документ, який визначав критерії безпеки для комп'ютерних систем. Проте в ньому не враховувалися проблеми, пов'язані з об'єднанням комп'ютерів у мережу, що з часом стало важливою проблемою для багатьох

організацій, адже мережі стали основним середовищем для обміну даними та інформацією.

2. «Червона книга» — це наступний етап розвитку критеріїв безпеки, що враховує проблеми мережевої безпеки, зокрема питання захисту інформації при її передачі по мережах. У «Червоній книзі» також були збережені вимоги з «Помаранчевої книги», але додано нові критерії для мережевого простору, і представлено концепцію мережевої безпеки.
3. Бездротові мережі — у 2024-2025 роках бездротові мережі (Wi-Fi, 5G, LTE) стали основною частиною інфраструктури багатьох підприємств та організацій. Проблеми, пов'язані з безпекою бездротових мереж, не могли бути передбачені у «Червоній книзі», що робить її сертифікат застарілим для сучасних вимог.

Застарілість «Червоної книги» і нові виклики:

- Захист бездротових мереж - безпека бездротових мереж вимагає нових підходів до шифрування і аутентифікації. Протоколи безпеки, які застосовуються для дротових мереж, часто не підходять для бездротових мереж, де існують проблеми з охороною каналу передачі і зменшенням ризику несанкціонованого доступу через ефір.
- Мобільні пристрої та IoT - поява мобільних пристроїв і Інтернету речей (IoT) створює нові загрози, оскільки ці пристрої часто підключаються до корпоративних мереж без належної безпеки. Для цього потрібні нові стандарти та критерії, що дозволяють забезпечити безпеку даних на кожному етапі їх передачі та зберігання.
- Сучасні мережеві атаки - з розвитком технологій і збільшенням обсягів даних, використовуваних у мережах, зростає кількість атак, таких як DDoS-атаки, атак на слабкі точки безпеки бездротових мереж, інсайдерські атаки, фішинг, а також використання соціальної інженерії для проникнення в мережі.

Сучасні стандарти безпеки:

Наразі для комп'ютерних мереж розроблено безліч стандартів, що допомагають забезпечити необхідний рівень захисту. Деякі з них включають:

- ISO/IEC 27001 — міжнародний стандарт, який описує вимоги до системи управління інформаційною безпекою.
- NIST Cybersecurity Framework — набір стандартів, керівництв і найкращих практик для керування кіберризиками.
- Wi-Fi Alliance WPA3 — протокол безпеки для захисту бездротових мереж.

Хоча «Помаранчева книга» і «Червона книга» внесли значний вклад у розвиток концепцій безпеки комп'ютерних систем та мереж, їхня актуальність зменшилася в умовах швидкого розвитку нових технологій. Бездротові мережі,

мобільні пристрої, IoT і нові типи кіберзагроз вимагають розробки нових стандартів і концепцій захисту. На основі цих вимог вже створено ряд сучасних стандартів, що мають на меті забезпечити комплексний захист корпоративних та приватних мереж в умовах динамічного розвитку технологій.

2.2. Міжнародні стандарти серії ISO 27000

ISO (Міжнародна організація стандартизації) і **IEC** (Міжнародна електротехнічна комісія) формують спеціалізовану систему всесвітньої стандартизації, яка охоплює широкий спектр технічних і організаційних напрямків, включаючи інформаційні технології, електроніку, енергетику та інші ключові сфери економіки та промисловості. Міжнародні стандарти, розроблені в рамках ISO і IEC, є важливими для забезпечення високої якості продукції, безпеки, а також для сприяння зниженню бар'єрів у міжнародній торгівлі та забезпечення взаємодії різних технологій.

Національні органи, які є членами ISO або IEC, беруть участь у розробці Міжнародних Стандартів через технічні комітети, створені відповідними організаціями з метою роботи зі специфічними областями технічної діяльності. Технічні комітети ISO й IEC працюють на основі технічних експертів, що представляють інтереси промисловості, урядів, наукових організацій та інших установ. Ці комітети аналізують наявні технології, передові практики та нові тенденції, щоб визначити найкращі підходи до стандартів у відповідних сферах.

Крім того, технічні комітети ISO й IEC співпрацюють в областях взаємного інтересу, що дозволяє створювати стандарти, що охоплюють різні аспекти міжнародної діяльності, наприклад, у сфері кібербезпеки, інформаційних технологій, енергетичних систем тощо. Ця співпраця між організаціями забезпечує узгодженість і взаємодію між стандартами, розробленими різними технічними комітетами.

Інші урядові й неурядові міжнародні організації, пов'язані з ISO й IEC, також беруть участь у цій роботі. Це включає організації, такі як Міжнародний союз електрозв'язку (ITU), Міжнародна організація праці (ILO), а також різні спеціалізовані наукові та технічні асоціації, що сприяють створенню і впровадженню стандартів у своїх сферах діяльності. Участь таких організацій дозволяє врахувати інтереси всіх зацікавлених сторін і забезпечити високу якість міжнародних стандартів.

У результаті, стандарти ISO і IEC мають вирішальне значення для забезпечення ефективної глобальної економічної діяльності, зокрема в сфері

технологій та інновацій, допомагаючи країнам і компаніям орієнтуватися на єдині міжнародні вимоги та практики.

У цей час сформовано цілий ряд стандартів **ISO/IEC** з урахуванням їх впровадження у галузь «Інформаційної безпеки»: **стандарт серії 27000**. Основними завданнями цього проекту були:

- ➔ уніфікація національних стандартів у сфері оцінювання безпеки ІТ;
- ➔ підвищення рівня довіри до оцінювання безпеки ІТ;
- ➔ скорочення витрат на оцінювання рівня безпеки ІТ на основі взаємною визнання сертифікатів.

Розробники стандартів серії **ISO/IEC 27000** зазначають, що основоположний стандарт серії **ISO/IEC 27001** постійно вдосконалюється, що дає можливість постійно оновлюватися у боротьбі з кіберзлочинністю. Завдяки впровадженню стандарту **ISO/IEC 27001** організація може оцінювати свої ризики, впроваджувати засоби контролю щодо їх пом'якшення, а потім контролювати та переглядати свої ризики та контроль за ними, покращуючи, за необхідності, захист. Таким чином, вона завжди готова до атак.

Таким чином, стандарти серії **ISO/IEC 27000** дійсно допомагають зробити безпечнішими усі сфери інформаційного життя, при цьому постійно розвиваючись і вдосконалюючись.

За десятиліття розробки стандарти цієї серії неодноразово редагувалися кращими фахівцями світу. Найсучасніша версія стандарту відображається в його назві як рік прийняття стандарту.

Сімейство стандартів ISO 27000

Сімейство стандартів включає в себе наступні документи, що стосуються систем менеджменту ІБ:

ISO/IEC 27000:2023 «*Information security management systems. Overview and vocabulary – Системи менеджменту інформаційної безпеки. Огляд і термінологія*».

ISO/IEC 27001:2022 «*Information security management systems. Requirements – Системи менеджменту інформаційною безпекою. Вимоги*». Ця версія замінила попередню 2015 року, уточнивши вимоги до управління інформаційною безпекою.

ISO/IEC 27002:2022 «*Information security controls*» (Контрольні заходи інформаційної безпеки). Стандарт допомагає в розробці та впровадженні заходів безпеки.

ISO/IEC 27003:2017 «*Information Security Management Systems. Guidance – Системи менеджменту інформаційної безпеки. Керівництво*». Остання версія 2017 року, актуальна для впровадження системи.

ISO/IEC 27004:2022 «*Information security management. Monitoring, measurement, analysis, and evaluation*» (Моніторинг, вимірювання, аналіз і оцінка інформаційної безпеки). Оновлена версія стандарту.

ISO/IEC 27005:2022 «*Information security risk management*» (Управління ризиками інформаційної безпеки). Остання версія стандарту для управління ризиками.

ISO/IEC 27006:2021 «*Requirements for bodies providing audit and certification of information security management systems – Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційною безпекою*».

ISO/IEC 27007:2020 «*Guidelines for Information Security Management Systems auditing (FCD) – Керівництво для аудиту систем менеджменту інформаційної безпеки*».

ISO/IEC 27017:2015 «*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*» (Рекомендації щодо заходів безпеки для хмарних послуг). Стандарт актуальний для хмарної безпеки.

ISO/IEC 27018:2019 «*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*» (Захист персональних даних у хмарних середовищах). Дієвий і важливий для конфіденційності даних.

Додаток А ISO/IEC 27001:2022 Містить оновлений перелік контрольних заходів безпеки, пов'язаний з ISO/IEC 27002:2022.

Ключові елементи політик та практик, що стосуються управління інформаційною безпекою в організаціях

Політики інформаційної безпеки (А. 5) — розробка політик безпеки, визначення їхніх вимог та методів перевірки ефективності.

Політики формуються для забезпечення захисту інформації та повинні регулярно перевірятися на відповідність стандартам та актуальним загрозам.

Організація інформаційної безпеки (А. 6) — ефективне розподілення обов'язків між членами організації щодо забезпечення інформаційної безпеки. Це включає визначення відповідальних за різні аспекти безпеки і встановлення процедур для забезпечення захисту.



Рис. 2.2. Стандарт ISO/IEC 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник»

Джерело: [1-6]

Безпека людських ресурсів (А. 7) — забезпечення безпеки через управління людськими ресурсами, зокрема шляхом навчання персоналу, перевірки кандидатів на відповідність вимогам безпеки, а також управління доступом співробітників до чутливої інформації.

Управління активами (А. 8) — інвентаризація активів (включаючи інформаційні, програмні та апаратні ресурси) та забезпечення їхнього правильного використання. Це включає класифікацію інформації і безпечну обробку носіїв даних.

Контроль доступу (А. 9) — встановлення політики контролю доступу для користувачів, управління правами доступу до систем, додатків і даних, а також моніторинг відповідності вимогам безпеки.

Криптографія (А. 10) — застосування методів шифрування та управління криптографічними ключами для захисту конфіденційності і цілісності інформації.

Фізична і екологічна безпека (А. 11) — заходи для захисту фізичних об'єктів (обладнання, сервери тощо) та навколишнього середовища (контроль температури, вологість, безпека приміщень).

Операційна безпека (А. 12) — контроль над операціями, що включають управління змінами в системах, моніторинг діяльності, захист від шкідливих програм, резервне копіювання і ведення журналів.

Безпека зв'язку (А. 13) — засоби захисту даних при їх передачі через мережі, включаючи використання захищених каналів і методів криптографії для забезпечення конфіденційності та цілісності комунікацій.

Придбання, розробка і супровід системи (А. 14) — вимоги безпеки під час розробки та підтримки інформаційних систем, що включає оцінку потенційних загроз і впровадження заходів для їхнього мінімізації на всіх етапах життєвого циклу системи.

Відносини з постачальниками (А. 15) — визначення вимог до постачальників і контроль за виконанням угод з метою забезпечення відповідності стандартам безпеки.

Управління інцидентами інформаційної безпеки (А. 16) — процес виявлення, реагування і документування інцидентів, пов'язаних з безпекою, а також заходи для збору доказів та визначення процедур для мінімізації наслідків.

Аспекти інформаційної безпеки управління безперервністю бізнесу (А. 17) — планування заходів, що забезпечують безперервність бізнесу в разі критичних інцидентів, включаючи відновлення ІТ-ресурсів, перевірки та аналіз безперервності процесів.

ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки».

ISO/IEC 27002:2015 — це міжнародний стандарт, який надає керівництво щодо методів захисту та кращих практик для забезпечення інформаційної безпеки в організаціях. Він є частиною серії стандартів ISO/IEC 27000, які спрямовані на управління інформаційною безпекою. Стандарт ISO/IEC 27002:2015 є актуальним документом, що містить

рекомендації по реалізації контрольних заходів для досягнення ефективної інформаційної безпеки в організаціях.

Основна мета стандарту — надання рекомендацій з управління заходами безпеки, які сприяють захисту конфіденційності, цілісності та доступності інформації. Стандарт описує різноманітні практики, які організації можуть застосовувати для управління інформаційною безпекою, зокрема в таких сферах як управління доступом, фізична та екологічна безпека, криптографія, безпека при розробці програмного забезпечення, управління інцидентами безпеки, моніторинг, аудит та управління ризиками.

ISO/IEC 27002:2015 містить 14 розділів, в яких описуються найбільш важливі аспекти інформаційної безпеки, включаючи:

1. Політика інформаційної безпеки.
2. Організаційні заходи та управління безпекою.
3. Управління доступом до інформаційних ресурсів.
4. Безпека персоналу.
5. Управління інцидентами безпеки інформації.
6. Оцінка та управління ризиками.

Стандарт надає практичні поради для організацій у розробці політик безпеки, визначенні та реалізації контрольних заходів, а також у забезпеченні постійного вдосконалення системи управління інформаційною безпекою.

Однією з ключових переваг ISO/IEC 27002:2015 є її універсальність: вона застосовна для організацій будь-якого розміру та типу діяльності, незалежно від галузі. Крім того, дотримання стандарту може бути корисним при отриманні сертифікації ISO/IEC 27001, що є міжнародним стандартом для систем управління інформаційною безпекою (ISMS).

Структура стандарту

Структура стандарту дозволяє вибрати засоби управління, які мають відношення до конкретної організації або сфери відповідальності у середині організації. Зміст стандарту має такі розділи:

- ➔ основні поняття і визначення інформаційної безпеки;
- ➔ політика безпеки [*security policy*];
- ➔ організація захисту [*organizational security*];
- ➔ класифікація та управління ресурсами [*asset classification and control*];
- ➔ безпека персоналу [*personnel security*];

- фізична безпека та безпека навколишнього середовища [*physical and environmental security*];
- адміністрування комп'ютерних систем та обчислювальних мереж [*computer and network management*];
- управління доступом до системи [*system access control*];
- управління комунікаціями і захист комп'ютерів від шкідливих програм;
- виконання вимог (відповідність законодавству) [*compliance*].



DSTU ISO/IEC 27002:2015

Information Technology. Methods of protection. Code of practice for information security measures

ДСТУ ISO/IEC 27002:2015

Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки

PLEASE CONTACT WWW.UKRAINELAWS.COM

TO REQUEST YOUR COPY IN RUSSIAN, ENGLISH, GERMAN, ITALIAN, FRENCH, SPANISH, CHINESE, JAPANESE AND OTHER LANGUAGES.



UKRAINELAWS
ALL CODES. ONE DATABASE



Electronic Adobe Acrobat PDF, Microsoft Word DOCX versions. Hardcopy editions. Immediate download. Download here. On sale. ISBN, SKU, RGTT | Immediate PDF Download. Russian regulations (GOST, SNiP) norms (PB, NPB, RD, SP, OST, STO) and laws in English. | UKRAINELAWS.com; Codes, Letters, NP, POT, RTM, TOI, DBN, MDK, OND, PPB, SanPiN, TR TS, Decisions, MDS, ONTP, PR, SN, TSN, Decrees, MGSN, Orders, PUE, SNiP, TU, DSTU, MI, OST, R, SNiP RK, VNTP, GN, MR, Other norms, RD, SO, VPPB, GOST, MU, PB, RDS, SP, VRD, Instructions, ND, PNAE, Resolutions, STO, VSN, Laws, NPB, PND, RMU, TI, Construction, Engineering, Environment, Government, Health and Safety, Human Resources, Imports and Customs, Mining, Oil and Gas, Real Estate, Taxes, Transport and Logistics, railroad, railway, nuclear, atomic.

Рис. 2.3. Стандарт ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки»
Джерело: [1-6]

ISO/IEC 27002:2022 *"Information security, cybersecurity and privacy protection — Information security controls"* (Інформаційна безпека, кібербезпека та захист персональних даних — Контролі інформаційної безпеки) - це оновлена версія стандарту, що надає рекомендації щодо заходів безпеки, які допомагають організаціям захищати інформаційні активи. Цей стандарт є частиною серії ISO/IEC 27000, яка фокусується на управлінні інформаційною безпекою та ризиками, пов'язаними з інформаційними технологіями. Стандарт містить рекомендації щодо реалізації контрольних заходів для захисту інформаційних активів, забезпечення кібербезпеки та захисту персональних даних, зокрема в контексті сучасних технологій та кіберзагроз.

Основні моменти **ISO/IEC 27002:2022**:

1. Оновлена структура контрольних заходів

У версії 2022 року було переглянуто структуру контрольних заходів. Було зроблено акцент на **14 категорій безпеки**, які зосереджуються на всіх аспектах управління інформаційною безпекою в організації. Ці категорії включають управління активами, фізичну безпеку, криптографію, безпеку людських ресурсів, контролі доступу, управління інцидентами, безпеку зв'язку та інші.

2. Зміни в категоріях і контрольних заходах

Стандарт 2022 року включає нові підходи, пов'язані з останніми тенденціями в кібербезпеці та розвитку технологій, таких як хмарні сервіси, кіберзагрози, шкідливе програмне забезпечення, інтернет речей (IoT), цифрова трансформація і нові вимоги до управління ризиками. Кілька контрольних заходів було оновлено для забезпечення більш ефективного захисту від сучасних загроз.

3. Акцент на управлінні ризиками

У порівнянні з попередньою версією, ISO/IEC 27002:2022 більше фокусується на управлінні ризиками в умовах динамічного технологічного середовища, що дає організаціям можливість швидше адаптувати свої політики і стратегії до нових загроз і ситуацій.

4. Інтеграція з іншими стандартами

ISO/IEC 27002:2022 розроблений для більш зручної інтеграції з іншими стандартами ISO/IEC, такими як **ISO/IEC 27001**, що визначає вимоги до системи управління інформаційною безпекою (ISMS), а також іншими стандартами в області управління бізнес-ризиками та забезпечення безпеки.

5. Участь персоналу та культура безпеки

У новій версії стандарту значно більше уваги приділено важливості **освіти і навчання персоналу** з питань інформаційної безпеки, а також створенню **організаційної культури безпеки**, що є ключовим елементом для ефективного захисту інформації.

ISO/IEC 27002:2022 є важливим інструментом для організацій, які прагнуть ефективно впроваджувати політики та практики управління інформаційною безпекою і відповідати новим викликам в області кіберзахисту.

Загалом, Стандарт **ISO/IEC 27002:2022** є важливим інструментом для розробки програм безпеки, оскільки надає детальні рекомендації щодо реалізації та управління заходами безпеки в організації. На практиці він часто використовується при проведенні аудиту безпеки інформаційно-комунікаційних систем (ІКС), допомагаючи оцінити ефективність існуючих контрольних заходів. Аудит за стандартом включає не лише перевірку документації з системи менеджменту безпеки, а й вибіркового контроль процесів і процедур в організації, щоб переконатися, що вони відповідають встановленим вимогам. Завдяки цьому, організації можуть виявляти слабкі місця в системах безпеки та вживати необхідних заходів для їх виправлення.

Основні етапи аудиту безпеки

Аудит безпеки є важливою частиною управління інформаційною безпекою в організації, що дозволяє оцінити ефективність заходів захисту інформаційних активів та виявити потенційні уразливості в системах безпеки. Він включає комплексний аналіз політик, процедур і практик, що стосуються захисту інформації, а також перевірку відповідності встановленим стандартам і нормативам, таким як ISO/IEC 27002. Аудит здійснюється через перевірку документації системи менеджменту безпеки інформаційно-комунікаційних систем (ІКС), що дозволяє оцінити наявність необхідних заходів безпеки, відповідність їх вимогам та виявлення можливих невідповідностей між задекларованою політикою безпеки і фактичним станом справ. Крім того, важливим етапом аудиту є вибіркового контроль практичних заходів у самій організації, включаючи інтерв'ю з персоналом, перевірку фізичної безпеки та тестування систем для визначення, наскільки насправді реалізовані заходи відповідають стандартам безпеки та чи ефективно вони захищають від загроз. Завдяки такому підходу аудит безпеки дозволяє виявити слабкі місця в системах безпеки, що дає можливість організаціям своєчасно впроваджувати

коригувальні заходи, зменшувати ризики та підвищувати рівень захисту даних.

Роботи з аудиту безпеки ІС включають ряд послідовних етапів, які в цілому відповідають етапам проведення комплексного ІТ-аудиту автоматизованої системи, а саме:

- ➔ ініціювання процедури аудиту;
- ➔ збір інформації аудиту;
- ➔ аналіз даних аудиту;
- ➔ вироблення рекомендацій;
- ➔ підготовку аудиторського звіту.

Аудиторський звіт є основним результатом проведення аудиту. Його якість характеризує якість роботи аудитора. Він повинен, принаймні, містити опис цілей проведення аудиту, характеристику обстежуваної ІС, вказівку меж проведення аудиту і використовуваних методів, результати аналізу даних аудиту, висновки, що узагальнюють ці результати та містять оцінку рівня захищеності системи або відповідність її вимогам стандартів, і, звичайно, рекомендації аудитора по усуненню наявних недоліків і вдосконалення системи захисту.



Аудитор безпеки по стандарту 27000 – одна із найбільш затребуваних професій. Аудит безпеки, особливо за стандартами серії ISO/IEC 27000, є важливим елементом забезпечення кібербезпеки та захисту інформаційних активів. З ростом кіберзагроз і посиленням вимог до захисту персональних та корпоративних даних, роль **аудитора безпеки** стає дедалі важливішою. Професії в сфері кібербезпеки, зокрема аудитори, які працюють згідно з міжнародними стандартами, такими як ISO/IEC 27001 та ISO/IEC 27002, користуються високим попитом у багатьох сферах, включаючи фінансові установи, технологічні компанії та організації, що працюють з великими даними. Професійний аудит безпеки дозволяє організаціям не тільки перевірити свою відповідність вимогам стандартів, але й виявити слабкі місця в системах захисту, що допомагає підвищити загальний рівень кіберзахисту.

Рекомендації, що видаються аудитором за результатами аналізу стану ІС, визначаються використанням підходом, особливостями обстежуваної ІС, станом справ з безпекою і ступенем деталізації, що використовується при проведенні аудиту. У будь-якому випадку, рекомендації аудитора повинні бути конкретними і застосовними до даної ІС, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізу) і відсортованими за ступенем важливості. При

цьому заходи щодо забезпечення захисту організаційного рівня практично завжди мають пріоритет над конкретними програмно-технічними методами захисту. У той же час не варто чекати від аудитора, як результату проведення аудиту, видачі технічного проєкту підсистеми інформаційної безпеки або детальних рекомендацій щодо впровадження конкретних програмно-технічних засобів захисту інформації. Це вимагає детальнішого опрацювання конкретних питань організації захисту, хоча внутрішні аудитори можуть брати в цих роботах найактивнішу участь.

Міжнародні стандарти серії **ISO/IEC 27000** є одним із основних наборів стандартів для забезпечення безпеки інформаційних систем та управління інформаційною безпекою. Ці стандарти визначають вимоги та надають рекомендації щодо процесів і процедур, що допомагають організаціям захищати свої інформаційні активи, зокрема від кіберзагроз, втрати даних та несанкціонованого доступу.

Основні стандарти серії ISO/IEC 27000 на 2024-2025

роки:

1. ISO/IEC 27000:2018 – Основи і словник

- ✓ Цей стандарт є основним у серії ISO/IEC 27000 і містить загальні визначення, терміни та концепції, пов'язані з управлінням інформаційною безпекою. Він також дає загальну картину для інших стандартів серії.

2. ISO/IEC 27001:2022 – Системи управління інформаційною безпекою (ISMS)

- ✓ ISO/IEC 27001 є основним стандартом для створення, реалізації, підтримки та постійного поліпшення системи управління інформаційною безпекою (ISMS). Стандарт визначає вимоги до управління безпекою інформації та є обов'язковим для сертифікації організацій, які хочуть підтвердити свої зусилля у забезпеченні захисту інформації.
- ✓ Включає вимоги до оцінки та управління ризиками, впровадження політик та заходів для забезпечення конфіденційності, цілісності та доступності інформації.

3. ISO/IEC 27002:2022 – Керівництво щодо практик управління безпекою інформації

- ✓ Цей стандарт надає рекомендації щодо найкращих практик для впровадження заходів безпеки у межах ISMS. Він доповнює ISO/IEC 27001, надаючи конкретні заходи та практики, які організації можуть застосовувати для захисту своїх інформаційних активів.

4. ISO/IEC 27005:2018 – Оцінка ризиків у сфері інформаційної безпеки

- ✓ Стандарт визначає настанови щодо процесу оцінки та управління ризиками в інформаційних системах. Це важлива частина стандартів серії, оскільки забезпечує розуміння того, як визначати і зменшувати ризики, пов'язані з безпекою інформації.

5. ISO/IEC 27017:2015 – Керівництво щодо безпеки інформаційних систем у хмарних обчисленнях

- ✓ Цей стандарт дає настанови щодо практик безпеки для забезпечення захисту даних у хмарних середовищах. Ураховує специфіку управління безпекою даних та сервісів у хмарних технологіях.

6. ISO/IEC 27018:2019 – Захист персональних даних у хмарних обчисленнях

- ✓ Стандарт забезпечує настанови щодо захисту персональних даних у хмарних сервісах, що особливо важливо в умовах зростання кількості даних, які обробляються у хмарах.

7. ISO/IEC 27031:2011 – Підготовка до непередбачених ситуацій і відновлення після аварій в сфері ІТ

- ✓ Цей стандарт визначає вимоги щодо планування відновлення діяльності після аварій в ІТ-системах. Він допомагає організаціям створювати плани з відновлення та забезпечення безперервності бізнес-процесів у випадку виникнення надзвичайних ситуацій.

8. ISO/IEC 27032:2012 – Кібербезпека

- ✓ ISO/IEC 27032 визначає настанови щодо кібербезпеки, надаючи організаціям інструменти для захисту від кіберзагроз, таких як кібер-атаки, інсайдерські загрози, фішинг, зловмисне програмне забезпечення та інші.

9. ISO/IEC 27035:2016 – Управління інцидентами з інформаційною безпекою

- ✓ Цей стандарт визначає настанови щодо управління інцидентами інформаційної безпеки, зокрема як виявляти, розслідувати і реагувати на інциденти безпеки. Він надає практичні кроки для розробки ефективних процедур реагування на інциденти.

10. ISO/IEC 27036:2014 – Безпека постачальників

- ✓ Стандарт описує підходи до забезпечення безпеки інформації під час роботи з постачальниками та партнерами. Він визначає вимоги до управління ризиками, що виникають при взаємодії з іншими організаціями.

Загалом, ці стандарти залишаються актуальними у 2024-2025 роках, оскільки вони охоплюють ключові аспекти інформаційної безпеки та кібербезпеки, які необхідні для забезпечення належного захисту в умовах швидко змінюваного технологічного середовища. Вони допомагають організаціям не лише виконувати вимоги національних і міжнародних нормативів, а й реалізувати комплексний підхід до управління безпекою.

Актуальність стандартів ISO/IEC 27000 у 2024-2025 роках:

- **Зростання кіберзагроз**

З кожним роком збільшується кількість кіберзлочинів, таких як атаки на дані, зловмисне програмне забезпечення, фішинг і шахрайство. Стандарти ISO/IEC 27000 дозволяють організаціям розробити систему управління безпекою інформації, яка є важливою для захисту від таких загроз.

- **Інтеграція хмарних технологій і IoT**

Перехід до хмарних обчислень і використання Інтернету речей вимагає нових підходів до забезпечення безпеки даних, тому стандарти, такі як ISO/IEC 27017 та ISO/IEC 27018, набувають особливої значущості.

- **Захист персональних даних**

У зв'язку з посиленням законодавства щодо захисту персональних даних, таких як GDPR в Європейському Союзі, відповідні стандарти серії ISO/IEC 27000 допомагають організаціям відповідати вимогам щодо обробки та захисту персональних даних.

Таким чином, серія ISO/IEC 27000 є актуальним інструментом для організацій, які прагнуть забезпечити належний рівень захисту своїх інформаційних систем, зокрема для підприємств, що працюють з великими обсягами даних або з високими вимогами до безпеки інформації.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 2

1. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

2. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.

3. H. Hulak, et al., Dynamic model of guarantee capacity and cyber security management in the critical automated systems, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2022) 102-111. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.

4. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.

5. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Порівняльний аналіз рішень для забезпечення контролю та управління привілейованим доступом в іт-середовищі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 98–112.

6. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

7. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.

8. V. Astapenya, et al., Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems, in: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021).

9. V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master's Program on Cybersecurity, Advances in Computer Science for Engineering and Education II, vol. 938 (2020) 610-624.

10. Костюк Ю.В., Рзаєва С.Л. Стратегічні рішення SOC для забезпечення інформаційної безпеки в умовах сучасних кіберзагроз (2024) Сучасні вектори розвитку України: забезпечення сталості та безпеки. Збірник матеріалів II Міжнародної науково-практичної конференції (м. Київ, 28 жовтня 2024 року). Чернігів: ГО «Науково-освітній інноваційний центр суспільних трансформацій».

11. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233.

12. H. Shevchenko, et al., Information Security Risk Analysis SWOT, Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021) 309-317.
13. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.
14. N. Dovzhenko, et al., Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes, in: Cybersecurity Providing in Information and Telecommunication Systems vol. 3421 (2023) 278–283.
15. Жданова, Ю., Шевченко, С., Спасітелева, С., & Сокульский, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.
16. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
17. Cisco -Україна. URL: <https://www.cisco.com>
18. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.
19. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.
20. P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 97–106.

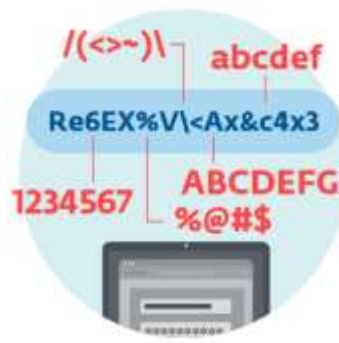
КОНТРОЛЬНІ ПИТАННЯ

1. Поясніть структуру законодавства по забезпеченню кібербезпеки.
2. Назвіть основні закони України з кібербезпеки.
3. Що таке ДСТУ і які стандарти з захисту інформації ви знаєте?
4. Що таке НД ТЗІ і назвіть основні документи.
5. Які документи мають бути в організації з захисту інформації?
6. Що входить до «Помаранчевої книги»?
7. Дайте поняття кіберзлочинності.
8. Як класифікується кіберзлочини?

9. Що таке серія стандартів ISO 27000 і в чому полягає її основна мета?
10. Які основні стандарти входять до серії ISO 27000 і які їхні основні принципи?
11. Як стандарт ISO/IEC 27001 допомагає організаціям у забезпеченні інформаційної безпеки?
12. У чому полягає різниця між ISO/IEC 27001 і ISO/IEC 27002?
13. Яка роль ISO/IEC 27005 у процесі управління ризиками в сфері інформаційної безпеки?
14. Які вимоги висуває ISO/IEC 27018 щодо захисту персональних даних у хмарних обчисленнях?
15. Які основні напрямки науково-дослідної роботи в галузі технологій захисту інформації (НД ТЗІ)?
16. Як оцінюється ефективність технологій захисту інформації в рамках НД ТЗІ?
17. Які ключові проблеми та виклики стоять перед дослідниками при розробці нових технологій для захисту інформації?
18. Як результативність НД ТЗІ впливає на розвиток національних стандартів і нормативних актів у сфері інформаційної безпеки?
19. Як впровадження стандартів науково-дослідної та технічної діяльності у сфері захисту інформації може впливати на ефективність управління ризиками інформаційної безпеки на підприємстві?
20. Як стандарт ISO/IEC 27032 пов'язаний з безпекою в Інтернеті і захистом від кіберзагроз?
21. Чому важливо інтегрувати стандарти ISO 27000 у систему управління інформаційною безпекою підприємства?
22. Як серія стандартів ISO 27000 сприяє забезпеченню довіри клієнтів і партнерів?
23. Які ключові процеси і методи визначаються в ISO/IEC 27001 для підтримки і поліпшення системи управління інформаційною безпекою?
24. Назвіть класи безпеки комп'ютерних систем.

ТЕМА 2. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ УПРАВЛІННЯ БЕЗПЕКОЮ ІКС

РОЗДІЛ 3 ПОЛІТИКА БЕЗПЕКИ



3.1. Організаційний захист

3.2. Склад і структура політики безпеки

3.3. Зразок спеціалізованої політики безпеки допустимого використання

"Безпека — це не продукт, а процес. Вона починається з політики, яка визначає, як ми підходимо до захисту інформації."

Брюс Шнайєр, експерт із кібербезпеки.

Адміністративне та організаційне забезпечення безпеки інформаційно-комунікаційної системи (ІКС) є ключовим компонентом комплексного підходу до захисту інформації. Воно включає розробку політик і процедур безпеки, що охоплюють формування політики інформаційної безпеки підприємства, встановлення регламентів доступу до інформаційних ресурсів та опис процедур реагування на інциденти безпеки.

Важливим елементом є організаційна структура безпеки, яка передбачає призначення відповідальних осіб за інформаційну безпеку (наприклад, CISO), формування команди із захисту інформації та розподіл зон відповідальності серед працівників. Контроль доступу реалізується через впровадження систем аутентифікації та авторизації користувачів,

регулярний перегляд прав доступу та ведення журналів дій користувачів у системі.

Особлива увага приділяється навчанню персоналу, зокрема проведенню регулярних тренінгів із кібергігієни, ознайомленню співробітників із ризиками соціальної інженерії та розробці інструкцій щодо безпечного використання робочих пристроїв. Управління ризиками включає ідентифікацію загроз та уразливостей, оцінку ризиків, визначення пріоритетів їх усунення, а також розробку та реалізацію планів зниження ризиків.

Моніторинг і аудит відіграють ключову роль у постійному відстеженні роботи ІКС, проведенні регулярних аудитів безпеки та аналізі ефективності впроваджених заходів. Управління інцидентами передбачає створення плану реагування на інциденти, розробку процесів комунікації під час кризових ситуацій, проведення розслідувань і впровадження коригуючих дій. Усі ці заходи забезпечують системний підхід до захисту інформації в ІКС, підвищуючи її стійкість до внутрішніх і зовнішніх загроз.

Політика безпеки є центральним елементом адміністративного та організаційного забезпечення безпеки інформаційно-комунікаційної системи (ІКС) і виконує роль регулятивного документа, що встановлює основні принципи, стандарти та процедури для захисту інформаційних активів підприємства. Вона формує базові принципи безпеки, визначаючи загальні підходи до управління ризиками, розподілу доступу, захисту даних і реагування на інциденти. У політиці чітко регламентуються обов'язки та відповідальність усіх учасників процесу безпеки: керівників, адміністраторів ІКС, служби інформаційної безпеки та кінцевих користувачів, що сприяє розумінню кожним працівником свого внеску в забезпечення захисту.

Політика встановлює правила керування доступом до інформаційних ресурсів, зокрема процедури аутентифікації, авторизації, реєстрації дій користувачів і управління обліковими записами. Вона також слугує основою для створення детальних стандартів і процедур, таких як резервне копіювання, оновлення програмного забезпечення, шифрування даних і управління конфігурацією систем. Особлива увага приділяється підвищенню рівня обізнаності персоналу: політика визначає вимоги до навчання співробітників, регулярного проведення тренінгів із кібергігієни, протидії соціальній інженерії та підготовки до реагування на кіберзагрози.

Політика безпеки також встановлює норми для інтеграції механізмів моніторингу та контролю, зокрема проведення аудиту безпеки, моніторингу роботи ІКС, виявлення аномалій і оцінки ефективності

впроваджених заходів. У ній передбачено чіткий план дій у разі інцидентів, що включає фіксацію подій, аналіз причин, повідомлення відповідальних осіб і розробку коригуючих заходів. Важливою характеристикою політики є її гнучкість і актуальність: вона передбачає регулярний перегляд і оновлення відповідно до змін у законодавстві, бізнес-процесах, технологіях чи загрозах.

Таким чином, політика безпеки виконує функцію стратегічного інструменту, що забезпечує узгодженість дій усіх учасників, формує єдині стандарти безпеки та дозволяє ефективно управляти ризиками, створюючи основу для адміністративного та організаційного забезпечення безпеки ІКС.

3.1. ОРГАНІЗАЦІЙНИЙ ЗАХИСТ

Організаційний захист ІКС передбачає впровадження заходів, спрямованих на забезпечення безпеки ІКС шляхом управлінських і організаційних рішень. Основними аспектами організаційного захисту є розробка політики безпеки, яка формулює чіткі правила та процедури для захисту інформаційних активів, включаючи обов'язки співробітників, правила доступу до даних і використання ресурсів. Організаційна структура безпеки визначає ролі і відповідальності усіх учасників процесу безпеки, створюючи спеціальні підрозділи або призначаючи відповідальних осіб, таких як керівник служби безпеки інформації (CISO). Важливим аспектом є управління доступом, яке встановлює чіткі правила доступу до ІКС для різних категорій користувачів, визначаючи права доступу на основі ролей, а також впроваджує засоби аутентифікації та авторизації для контролю доступу до системи.

Окрім того, необхідно здійснювати регулярне навчання персоналу, підвищуючи обізнаність співробітників щодо загроз інформаційній безпеці, принципів кібергігієни та реагування на інциденти безпеки. Реагування на інциденти включає розробку чітких планів дій у разі виникнення інцидентів безпеки, таких як виток інформації або кібератаки, включаючи фіксацію інцидентів, розслідування та запобігання повторенню.

Моніторинг та аудит є невід'ємними елементами організаційного захисту, адже вони дозволяють здійснювати постійний моніторинг системи для виявлення аномалій або порушень безпеки, а також проводити регулярні аудити для оцінки ефективності впроваджених заходів.

Керування ризиками включає ідентифікацію потенційних загроз і уразливостей ІКС, оцінку їхніх можливих наслідків та розробку заходів для мінімізації ризиків. Нарешті, планування безперервності бізнесу

передбачає розробку планів відновлення після інцидентів, що включають процедури для збереження працездатності ІКС у разі надзвичайних ситуацій або аварій. Організаційний захист ІКС дозволяє створити системний підхід до безпеки, забезпечити відповідальність за дотримання стандартів безпеки та гарантувати стійкість системи до можливих загроз та атак.

Головна мета організаційного захисту – сформувати програму робіт у галузі безпеки ІКС і забезпечити її виконання, виділяючи необхідні кошти і контролюючи стан справ. Водночас важливим аспектом є дотримання правил економічної ефективності, оскільки вартість реалізації програми захисту повинна бути менше можливого збитку від інцидентів безпеки. Це означає, що заходи безпеки повинні бути пропорційні рівню потенційного ризику, а інвестиції в безпеку повинні забезпечувати збереження цінних інформаційних активів підприємства, мінімізуючи можливі фінансові та репутаційні втрати.

Сучасний організаційний захист також передбачає інтеграцію інноваційних підходів і технологій для підвищення ефективності захисту. Це включає використання автоматизованих систем моніторингу та виявлення загроз, аналітичних інструментів для оцінки ризиків, а також застосування методів машинного навчання для передбачення нових загроз і аномалій. Наприклад, сучасні інструменти на основі штучного інтелекту можуть автоматично виявляти незвичну активність в ІКС, що дозволяє оперативно реагувати на потенційні інциденти безпеки. Також важливим є використання технологій блокчейн для забезпечення прозорості та незмінності логів безпеки, що підвищує довіру до системи.

Окрім технологічних аспектів, організаційний захист повинен включати адаптацію до змінюваного законодавчого та нормативного середовища. Постійне оновлення стандартів і вимог, таких як загальний регламент захисту даних (GDPR) або рекомендації NIST, вимагає від організацій постійного моніторингу змін у законодавстві та оперативного реагування на нові вимоги. Це забезпечує не лише належний рівень безпеки, а й захист юридичних та фінансових інтересів організації.

Наразі важливим елементом є також розвиток корпоративної культури безпеки, що включає регулярне навчання і підвищення обізнаності співробітників, особливо в умовах постійно зростаючих кіберзагроз. Створення середовища, де всі працівники організації усвідомлюють свою роль у захисті інформації, є критично важливим для забезпечення ефективного організаційного захисту.

Таким чином, сучасний організаційний захист ІКС – це комплексний підхід, що включає не лише технічні засоби, а й ефективне управління

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

ресурсами, постійний моніторинг змін у зовнішньому середовищі, а також розвиток культури безпеки серед співробітників.

Організаційний захист – це регламентація діяльності і взаємовідносин виконавців, що виключає або суттєво ускладнює неправомірне використання інформації та інформаційних ресурсів. Для цього передбачені відповідні організаційні та адміністративні заходи.

Організаційні заходи включають:

- ❖ організацію режиму охорони;
- ❖ організацію роботи з персоналом;
- ❖ організацію роботи з інформаційними ресурсами.

Організація режиму охорони є ключовим елементом у забезпеченні фізичної безпеки інформаційно-комунікаційних систем (ІКС) та інших важливих активів підприємства. Вона дозволяє виключити можливість таємного проникнення сторонніх осіб на територію, що охороняється, а також здійснювати контроль за дотриманням співробітниками посадових інструкцій і режимних заходів. Це включає контроль доступу до певних приміщень, зон із високою інформаційною цінністю, а також доступ до обладнання, систем та документів, що містять чутливу інформацію.

Режим охорони передбачає впровадження багаторівневих систем безпеки, таких як система контролю доступу, відеоспостереження, фізична охорона і моніторинг. За допомогою технологій контролю доступу можна обмежити вхід до критичних зон лише авторизованими особами, що знижує ризик несанкціонованого доступу та крадіжки інформації або обладнання. Відеоспостереження дає змогу контролювати рух співробітників і відвідувачів в межах організації, а також записувати події для подальшого аналізу у разі виникнення інцидентів.

Додатково, організація режиму охорони включає постійний моніторинг виконання режимних заходів і посадових інструкцій співробітниками, що дозволяє вчасно виявляти порушення і вживати необхідних заходів для їх виправлення. Це може включати перевірки на відповідність стандартам поведінки, виявлення аномальної активності або неправильного використання доступу до ресурсів. Режим охорони також передбачає навчання персоналу щодо важливості дотримання правил безпеки, що дозволяє запобігти можливим загрозам безпеці, зокрема

соціальній інженерії або іншим видам маніпуляцій з боку внутрішніх або зовнішніх осіб.

Таким чином, організація режиму охорони сприяє не тільки забезпеченню фізичної безпеки, а й підтримці внутрішнього порядку, що є невід'ємною частиною комплексної системи захисту інформаційно-комунікаційних систем підприємства.

Організація роботи з персоналом є важливим аспектом у забезпеченні інформаційної безпеки організації. Вона включає кілька ключових етапів, що сприяють надійному захисту конфіденційної інформації та запобіганню можливим загрозам з боку працівників. Першим етапом є відбір персоналу, що передбачає ретельний процес вибору кандидатів, орієнтуючись на їх професійні навички, досвід, а також здатність дотримуватись норм безпеки. Відбір повинен включати перевірку репутації кандидатів та їхньої історії безпеки, що дозволяє знизити ризики, пов'язані з соціальною інженерією або іншими видами зловживань з боку нових працівників. Після прийому на роботу кожен співробітник повинен пройти ознайомлення з політикою безпеки організації, яка визначає правила роботи з конфіденційною інформацією, обов'язки та обмеження, що застосовуються до персоналу. Це також включає ознайомлення з процедурою доступу до різних рівнів інформації та засобами захисту даних. Важливо, щоб працівники усвідомлювали свою відповідальність за безпеку інформації та наслідки її порушення. Регулярне навчання співробітників є ключовим елементом організації роботи з персоналом. Це може включати тренінги з основ безпеки, захисту даних, управління ризиками та реагування на інциденти безпеки. Навчання повинно також включати вивчення новітніх загроз, таких як фішинг, соціальна інженерія, та методи їх запобігання. Залучення спеціалістів для проведення таких тренінгів допоможе підтримувати високий рівень обізнаності працівників. Після відбору та навчання необхідно забезпечити правильну розстановку персоналу в організації. Це включає призначення відповідальних осіб за інформаційну безпеку, визначення ролей і прав доступу до інформації в залежності від рівня відповідальності кожного працівника. Розстановка персоналу повинна відповідати принципам мінімальних прав доступу (працівники повинні мати доступ лише до тієї інформації, яка необхідна для виконання їхніх обов'язків). Після впровадження всіх заходів важливо постійно моніторити діяльність персоналу і оцінювати ефективність існуючих процедур безпеки. Це може включати перевірки на дотримання політики безпеки, а також використання систем аудиту та моніторингу доступу до конфіденційної інформації.

Таким чином, організація роботи з персоналом сприяє не тільки забезпеченню захисту інформаційних ресурсів організації, але й створенню атмосфери довіри та відповідальності серед співробітників, що є основою для підтримки надійної системи інформаційної безпеки.

Організація роботи з інформаційними ресурсами передбачає є важливою складовою частиною забезпечення інформаційної безпеки в організації. Вона передбачає контроль за розробкою, обліком, зберіганням та знищенням документів, а також за роботами з налаштування, конфігурацією та утилізацією інших (непаперових) інформаційних ресурсів. Це включає кілька ключових аспектів, спрямованих на забезпечення належного рівня захисту інформації та запобігання витоку чутливих даних.

Перш за все, організація контролю за розробкою документів передбачає чітке визначення процесів створення та обробки інформаційних матеріалів, а також забезпечення того, щоб кожен документ був створений, схвалений та збережений відповідно до встановлених норм і процедур безпеки. Це включає ведення обліку документів, що дозволяє контролювати їх життєвий цикл і вчасно виявляти порушення політики безпеки.

Зберігання документів та інших інформаційних ресурсів повинно здійснюватися відповідно до стандартів безпеки, зокрема, в умовах захищених серверів або за допомогою зашифрованих носіїв, що унеможливорює несанкціонований доступ до чутливої інформації. Для цього можуть використовуватися різноманітні технології, включаючи захищене зберігання в хмарних сховищах або локальних серверах з високим рівнем шифрування та доступу на основі ролей.

Знищення документів та інформаційних ресурсів є не менш важливим етапом у роботі з інформацією. Всі документи, які більше не використовуються, повинні бути знищені таким чином, щоб відновити їх було неможливо. Для паперових документів це можуть бути спеціальні shredderi, а для цифрових — використання програмного забезпечення для безпечного видалення файлів. Важливо також документувати процес знищення, щоб у разі перевірки можна було підтвердити виконання відповідних процедур.

Роботи з налаштування та конфігурації інформаційних ресурсів включають контроль за правильним налаштуванням апаратного та програмного забезпечення, що використовуються для зберігання та обробки інформації. Це включає налаштування систем доступу, а також забезпечення того, щоб усі налаштування відповідали вимогам безпеки.

Утилізація інформаційних ресурсів, таких як старі сервери, жорсткі диски та інші носії, також має бути організована згідно з протоколами безпеки. Перед їх утилізацією важливо виконати процедури безпечного стирання або знищення даних, щоб уникнути можливості відновлення конфіденційної інформації.

Таким чином, організація роботи з інформаційними ресурсами включає комплекс заходів, спрямованих на забезпечення цілісності, конфіденційності та доступності інформації протягом всього її життєвого циклу, а також на запобігання витоку або несанкціонованого доступу до інформаційних матеріалів.

Адміністративні заходи забезпечення безпеки є важливою складовою частиною загальної системи захисту інформаційних ресурсів організації. Вони включають в себе комплекс організаційних і управлінських процедур, які спрямовані на регулювання діяльності співробітників, організацію доступу до інформаційних ресурсів і забезпечення належного рівня захисту від різноманітних загроз. Одним з перших кроків є розробка детальних політик і процедур безпеки, що визначають правила доступу до інформаційних ресурсів, порядок їх обробки, зберігання, а також процедури реагування на інциденти безпеки. Такі політики мають відповідати вимогам законодавства та міжнародним стандартам.

Управління доступом є ключовим елементом адміністративних заходів. Встановлення чітких правил доступу до інформаційних ресурсів на основі ролей і обов'язків співробітників дозволяє забезпечити належний рівень захисту, застосовуючи принцип мінімальних прав доступу, коли працівники мають доступ лише до тієї інформації, яка необхідна для виконання їхніх обов'язків. Це також включає визначення прав доступу та призначення відповідальних осіб, що дозволяє централізовано контролювати доступ до критичних даних.

Підбір і навчання персоналу є наступним важливим етапом. Усі співробітники повинні бути не лише ознайомлені з політиками безпеки, але й пройти відповідне навчання, що включає питання інформаційної безпеки, управління ризиками та виявлення загроз. Це дозволяє знизити ризики, пов'язані з людським фактором, який часто є найслабшою ланкою в системі безпеки.

Для забезпечення належного рівня захисту необхідно також впровадити систему моніторингу і аудиту, яка дозволяє регулярно перевіряти дотримання політик безпеки, контролювати діяльність співробітників і виявляти порушення або несанкціоновані доступи. Аудити

повинні охоплювати перевірки доступу до даних, використання технічних засобів безпеки і виявлення потенційних уразливостей.

Інциденти безпеки вимагають чітко визначених процедур реагування. Підготовлені плани і інструкції для оперативного реагування дозволяють швидко нейтралізувати загрози, мінімізуючи можливі збитки. Реагування на інциденти включає визначення конкретних дій, які мають бути виконані, якщо виникає загроза або вже відбувся інцидент.

Регулярна оцінка та управління ризиками є необхідними для виявлення нових загроз та уразливостей в інформаційних системах організації. Це дозволяє своєчасно впроваджувати заходи для зниження або усунення цих ризиків, а також коригувати існуючі процедури безпеки.

Також важливо мати розроблені плани безперервності бізнесу, що включають процедури відновлення критичних інформаційних ресурсів після надзвичайних ситуацій. Це дозволяє організації швидко відновити свою діяльність після інцидентів, таких як кібератаки або технічні збої.

Окрему увагу слід приділяти організації фізичної безпеки, яка включає встановлення систем контролю доступу до приміщень з інформаційними ресурсами, а також встановлення відеоспостереження та інших засобів захисту.

Адміністративні заходи повинні бути гнучкими та регулярно оновлюватися відповідно до нових технологій і змін у законодавстві. Тільки комплексний підхід до забезпечення безпеки, який включає всі ці елементи, дозволяє організації ефективно захищати свої інформаційні ресурси від потенційних загроз.

Адміністративні заходи забезпечення безпеки включають в себе:

- ➔ розробку і публікацію політик безпеки, інструкцій, процедур та настанов, що пов'язані з безпекою ІКС;
- ➔ класифікацію всієї інформації, що використовується в ІКС;
- ➔ конфігурування, тестування та контроль за системою безпеки ІКС;
- ➔ підбір персоналу, проведення тренінгів та навчань з питань безпеки;
- ➔ управління ризиками.

Ці ключові аспекти організації роботи з інформаційними ресурсами є основою програми безпеки організації чи підприємства. Вони сприяють створенню комплексної системи захисту, яка охоплює всі етапи життєвого циклу інформації — від її розробки та зберігання до знищення та утилізації. Програма безпеки повинна включати чітко визначені політики

та процедури, що регламентують роботу з документацією та іншими інформаційними ресурсами, зокрема, забезпечення належного контролю доступу, шифрування даних, а також методи безпечного знищення або утилізації чутливої інформації. Важливими елементами програми безпеки є також регулярні аудити та перевірки дотримання встановлених норм, що дозволяють своєчасно виявляти та усувати потенційні уразливості. Програма повинна бути гнучкою, здатною адаптуватися до нових загроз і технологічних змін, а також регулярно оновлюватися відповідно до змін законодавчих вимог і стандартів безпеки. Забезпечення безпеки інформаційних ресурсів включає не лише технічні засоби, а й навчання та підвищення обізнаності співробітників щодо важливості дотримання безпекових процедур. Це дозволяє знижувати ризики, пов'язані з людським фактором, який часто є найслабшим ланкою в системі безпеки. Програма безпеки має бути інтегрована в загальну стратегію управління підприємством і сприяти не лише захисту інформації, але й підтримці довіри з боку клієнтів і партнерів організації.

Адміністративно-організаційні заходи безпеки є важливою складовою частиною загальної стратегії забезпечення інформаційної безпеки в організації, що охоплюють організаційні та управлінські процеси, спрямовані на захист інформаційних ресурсів від різноманітних загроз. Основною метою цих заходів є розробка та реалізація політик і процедур, які забезпечують ефективний контроль за обробкою та захистом інформації на всіх етапах її життєвого циклу.

Ключовим етапом є розробка політик безпеки, що регулюють доступ до інформаційних ресурсів, їх обробку, зберігання та знищення. Важливою складовою є встановлення чітких правил доступу до конфіденційних даних на основі принципу найменших прав, коли кожен співробітник має доступ лише до тієї інформації, яка необхідна для виконання його службових обов'язків. Ці політики повинні бути інтегровані з існуючими корпоративними стандартами та відповідати вимогам чинного законодавства та міжнародних норм.

Невід'ємною частиною адміністративно-організаційних заходів є управління персоналом, що включає відбір співробітників, їх навчання і ознайомлення з політиками безпеки. Важливо забезпечити регулярне підвищення кваліфікації працівників з питань інформаційної безпеки, навчити їх ідентифікувати загрози та реагувати на інциденти безпеки. Це дозволяє значно знизити ризики, пов'язані з людським фактором, який часто є однією з основних причин порушень безпеки.

Не менш важливим аспектом є контроль за доступом до інформаційних ресурсів та інфраструктури. Для цього необхідно

впроваджувати систему моніторингу доступу, що дозволяє своєчасно виявляти несанкціоновані дії та порушення. Для здійснення цього ефективно використовуються технічні засоби контролю доступу, такі як біометрія, електронні картки, паролі та інші засоби аутентифікації.

Ще одним важливим аспектом є оцінка і управління ризиками для інформаційної безпеки. Регулярна оцінка ризиків дозволяє виявляти потенційні загрози для інформаційних систем і вжити відповідні заходи для їх мінімізації. Це також включає розробку сценаріїв на випадок надзвичайних ситуацій та визначення дій для відновлення нормальної роботи систем у разі інциденту.

Також необхідно забезпечити належний рівень фізичної безпеки для захисту інформаційних ресурсів. Це включає в себе впровадження систем контролю доступу до приміщень, де зберігаються важливі дані або обладнання, установку відеоспостереження, а також забезпечення охорони приміщень з високим рівнем безпеки.

Моніторинг, аудит і регулярна перевірка відповідності політик безпеки вимогам організації та стандартам є важливою складовою для забезпечення належного рівня безпеки інформаційних ресурсів. Регулярні аудити дозволяють виявити можливі уразливості в системах та вчасно коригувати політики і процедури для підвищення рівня захисту.

У разі виникнення інцидентів безпеки організація повинна мати чітко визначені процедури реагування, що дозволяють мінімізувати збитки та швидко відновити нормальну роботу. Це включає створення планів реагування на інциденти, визначення ролей і відповідальностей співробітників, а також забезпечення швидкої комунікації та координації дій у випадку загрози.

Важливу роль у забезпеченні безпеки інформаційних ресурсів відіграє адаптація адміністративно-організаційних заходів до нових технологічних реалій і зміни в зовнішньому середовищі. Оскільки загрози та технології безпеки постійно змінюються, організація повинна регулярно переглядати та оновлювати політики безпеки для забезпечення максимальної ефективності захисту.

Таким чином, адміністративно-організаційні заходи безпеки є фундаментальним елементом стратегії захисту інформаційних ресурсів організації. Вони сприяють не лише запобіганню інцидентів безпеки, а й забезпечують постійне вдосконалення системи захисту інформації, адаптуючи її до нових викликів і загроз.

Основою адміністративного захисту є **політика безпеки (ПБ)**, яка визначає ставлення організації до забезпечення безпеки та необхідні дії для захисту її ресурсів і активів. Політика безпеки служить основою для

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

створення стратегій і процедур, спрямованих на зменшення ризиків та забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів. Вона охоплює широкий спектр аспектів, починаючи від управління доступом до інформації та визначення прав і обов'язків співробітників, до процедур реагування на інциденти безпеки та управління ризиками.



Рис. 3.1. Адміністративно-організаційні заходи безпеки організації
Джерело: побудовано автором

Розробка політики безпеки є важливим етапом у створенні ефективної системи захисту інформації, оскільки вона визначає основні принципи безпеки, які повинні бути дотримані на всіх рівнях організації. Це включає визначення загроз та уразливостей, встановлення вимог до безпеки даних, а також визначення ролей та відповідальностей співробітників у процесах захисту інформації.

ПБ має забезпечити не тільки технічні, але й організаційні та адміністративні заходи для досягнення максимального рівня безпеки.

Політика безпеки також служить основою для навчання персоналу, визначає вимоги до фізичної безпеки, а також сприяє створенню культури безпеки в організації. Вона повинна регулярно переглядатися і оновлюватися відповідно до змін у зовнішньому середовищі, технологіях та нормативних вимогах, що дозволяє організації своєчасно реагувати на нові загрози та виклики.

Забезпечення належного адміністративного захисту вимагає від організації не лише визначення політики безпеки, але й постійного моніторингу її виконання, аудиту та аналізу ефективності застосовуваних заходів, що дозволяє вчасно виявляти недоліки та вносити корективи в стратегію захисту інформаційних активів.

Рівні політики безпеки

Рівні політики безпеки організації визначають комплексний підхід до забезпечення захисту інформаційних ресурсів, що охоплює стратегію, тактику та операційні заходи. Кожен рівень має свою специфіку та призначення, проте всі вони тісно взаємопов'язані й сприяють досягненню загальної мети — забезпечення надійної безпеки інформації.

На стратегічному рівні політика безпеки визначає основні напрями та цілі забезпечення безпеки на довгострокову перспективу. Це включає формулювання загальних принципів, пріоритетів і завдань для всієї організації, а також розподіл ресурсів для їх досягнення. Стратегічна політика фокусується на розробці основних напрямів розвитку безпеки, що відповідають зовнішнім загрозам і вимогам законодавства. Вона є основою для розробки більш детальних планів на наступних рівнях.

Тактичний рівень політики безпеки є більш конкретизованим і орієнтований на середньострокову перспективу. Тут детально розробляються політики, процедури та інструкції для забезпечення безпеки інформаційних систем. Тактична політика забезпечує виконання стратегічних цілей і встановлює конкретні методи для захисту даних: це включає контроль доступу, заходи для запобігання інцидентам безпеки, процеси реагування на загрози та виявлення порушень, а також організацію фізичної та технічної безпеки в межах підприємства.

Операційний рівень політики безпеки стосується повсякденних операцій з інформаційними ресурсами організації. Це найнижчий рівень, на якому здійснюються конкретні заходи для забезпечення безпеки в реальному часі. Операційна політика включає в себе контроль доступу, управління пароллями, аутентифікацію користувачів, моніторинг діяльності, реагування на інциденти безпеки та технічне обслуговування систем. На цьому рівні важливо забезпечити виконання процедур безпеки

кожним співробітником, що дозволяє оперативно реагувати на загрози та ефективно управляти системами безпеки.

Нормативно-правовий рівень політики безпеки охоплює всі юридичні та нормативні вимоги, що регулюють інформаційну безпеку на національному та міжнародному рівнях. Це включає виконання вимог законодавства щодо захисту персональних даних, конфіденційності та приватності, а також дотримання міжнародних стандартів, таких як ISO/IEC 27001 або GDPR. Нормативно-правова політика є важливим елементом забезпечення безпеки, оскільки вона встановлює правові основи для управління інформаційними активами та регулює відповідальність організації в разі порушення безпеки.

Тактичний рівень політики безпеки для технологічних рішень стосується конкретних технічних аспектів, що забезпечують захист ІТ-систем і мереж. Цей рівень охоплює питання криптографії, захисту від вірусів, виявлення шкідливих програм, а також налаштування систем моніторингу та реагування на інциденти. Політика на цьому рівні має на меті забезпечення конфіденційності, цілісності та доступності даних у реальному часі та збереження ефективності захисту від зовнішніх і внутрішніх загроз.

Ці рівні політики безпеки не є ізольованими і працюють у тісній взаємодії. Стратегічна політика визначає загальні принципи і цілі, що забезпечують основу для більш конкретних заходів на тактичному та операційному рівнях. Нормативно-правова політика гарантує відповідність вимогам законодавства і міжнародним стандартам, а технічні аспекти, описані на тактичному рівні для ІТ-рішень, гарантують надійний захист інфраструктури і даних. Така багаторівнева система політики безпеки дає змогу організації створити ефективну, збалансовану стратегію захисту інформаційних ресурсів на всіх етапах їхнього життєвого циклу.

Рішення, які приймаються в рамках політики безпеки можуть бути віднесені до **верхнього, середнього або нижнього рівня**.

▲ **Верхній рівень** політики безпеки включає рішення, що приймаються вищим керівництвом і носять загальний характер. На цьому рівні керівництво встановлює порядок впровадження програми безпеки, визначає цілі програми, розподіляє відповідальність, визначає стратегічне та тактичне значення безпеки для організації, а також вказує на основні напрями її реалізації. Цей рівень визначає основні принципи безпеки, які будуть використані для досягнення встановлених цілей, а також включає критерії оцінки ефективності програм безпеки.

Крім того, верхній рівень політики безпеки має на меті визначити організаційну структуру управління безпекою, призначити відповідальних

осіб або комітети за впровадження і моніторинг безпекових заходів. Він також включає розподіл ресурсів для реалізації політики, забезпечення навчання персоналу і формулювання вимог до зовнішніх постачальників та партнерів організації щодо виконання стандартів безпеки.

Також важливо, що на верхньому рівні приймаються рішення щодо відповідності політики безпеки нормативним вимогам, як національним, так і міжнародним стандартам. Керівництво організації повинно забезпечити відповідність програми безпеки вимогам таких стандартів, як ISO/IEC 27001, GDPR, а також враховувати галузеві специфікації і рекомендації.

Верхній рівень політики безпеки є основою для всіх наступних етапів розробки та впровадження заходів безпеки в організації, оскільки саме з нього починається реалізація всіх стратегічних рішень і детальних політик на тактичному та операційному рівнях.

На цьому рівні також:

- виявляють критично важливі активи;
- встановлюються правила розмежування доступу до інформаційних ресурсів;
- визначають найбільш ймовірні загрози;
- оцінюють можливі втрати;
- приймають концептуальні рішення щодо методів забезпечення захисту (наприклад – створити службу кібербезпеки в організації).

▲ **Середній рівень** політики безпеки є ключовим елементом у забезпеченні ефективного захисту інформаційних ресурсів організації, здійснюючи перехід від стратегічних рішень до конкретних операційних процедур. Він містить чітко визначені правила та методи, які повинні бути виконані для досягнення цілей безпеки на практичному рівні. Одним із основних завдань середнього рівня є встановлення правил доступу до інформаційних ресурсів організації. Це включає в себе впровадження політики контролю доступу на основі ролей (RBAC), яка дозволяє визначити, які співробітники мають право на доступ до різних рівнів даних, і забезпечує їх захист від несанкціонованого доступу. Ключовим елементом цієї політики є також чітке визначення прав доступу в залежності від ролі, що виконується співробітником, і необхідності в роботі з конкретною інформацією.

Захист даних є важливим аспектом середнього рівня політики безпеки, і його реалізація часто передбачає використання сучасних технологій шифрування для забезпечення конфіденційності, цілісності та доступності інформації. Це дозволяє не лише захистити дані під час

зберігання, а й при передачі через мережу, що важливо в умовах, коли організації активно працюють з хмарними технологіями або здійснюють передачу даних між різними географічними локаціями.

Моніторинг і аудит операцій з інформацією є іншою ключовою частиною середнього рівня політики безпеки. Створення системи для запису і аналізу всіх дій, що відбуваються з даними, дозволяє оперативно виявляти і реагувати на аномальні або підозрілі події, що можуть свідчити про спроби порушення безпеки. Регулярні перевірки та аудит журналів доступу дають змогу вчасно виявити інциденти безпеки, а також забезпечують прозорість дій персоналу.

Належне управління інцидентами є критично важливим для своєчасного реагування на інциденти безпеки. Встановлення чітких процедур для реагування на інциденти та відновлення після них допомагає організації швидко мінімізувати наслідки від порушень безпеки. Усі працівники повинні бути навчені діяти за встановленими процедурами у разі виявлення інцидентів, що дозволяє організації швидко відновити нормальну діяльність.

Політика безпеки на середньому рівні також передбачає забезпечення безпеки процесу обробки інформації в межах організації, включаючи чітке визначення термінів зберігання та утилізації даних. Всі чутливі або конфіденційні дані повинні зберігатися відповідно до внутрішніх стандартів безпеки та законодавчих вимог. Після завершення терміну зберігання або по досягненню мети обробки, дані повинні бути безпечно знищені або анонімізовані.

Крім того, важливою частиною середнього рівня є навчання та підвищення обізнаності персоналу. Це включає в себе регулярні тренінги з питань інформаційної безпеки, а також навчання персоналу методам захисту конфіденційної інформації, реагування на інциденти та використання технологій безпеки, таких як шифрування та мультифакторна аутентифікація. Це допомагає забезпечити надійний захист від людських помилок і несанкціонованих дій, що можуть призвести до порушення безпеки.

У свою чергу, використання сучасних технічних засобів захисту, таких як антивірусні програми, брандмауери, системи виявлення вторгнень, а також захист від атак через інтернет, забезпечують додатковий рівень безпеки. Це дозволяє не лише захищати організацію від традиційних кіберзагроз, але й адаптувати захист до нових викликів, зокрема атак через мобільні пристрої або хмарні платформи.

Таким чином, середній рівень політики безпеки є основою, що забезпечує ефективну реалізацію стратегічних цілей безпеки, створюючи

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

конкретні заходи і процедури для захисту інформації та забезпечення її безпеки в межах організації. Він охоплює розподіл прав доступу, моніторинг, реагування на інциденти, навчання персоналу і впровадження технічних рішень для захисту даних, що дозволяє організації забезпечити належний рівень безпеки в умовах сучасних загроз.

До *середнього рівня* політики безпеки відносять рішення і відповідні документи, що стосуються:

- організації режиму охорони;
- організації роботи з співробітниками;
- організації роботи з документами;
- організації роботи з технічними засобами.

Приклад. Нехай в базі даних збирається інформація про здоров'я приватних осіб, яка в більшості країн вважається конфіденційною. База даних потрібна, тому що ця інформація дозволяє ефективно проводити діагностику. Якщо доступ до цієї бази з міркувань захисту інформації сильно обмежений, то в такій основі не буде користі для лікарів, які ставлять діагнози, і не буде користі від самої бази. Якщо доступ відкрити, то можливий витік конфіденційної інформації, за яку з суду може бути пред'явлений великий позов. Яким має бути оптимальне рішення? Результатом рішення є вибір правил розподілу і зберігання інформації, а також поводження з інформацією, що і складає середній рівень політики безпеки.

▲ Політика безпеки на *нижньому рівні* – це сукупність правил, обмежень, рекомендацій, інструкцій, які регламентують порядок дій на рівні використання ІКС в організації. Персонал повинен бути ознайомлений з положеннями ПБ, в тому числі з відповідальністю, яка визначена за її порушення. Це дозволить всім розуміти не тільки те, що від них очікується, а й які будуть наслідки недотримання. Будучи прийнятою, ПБ стає «законом», обов'язковим для виконання всіма співробітниками. Якщо відбувається інцидент, пов'язаний з порушенням безпеки, або система дає збій в роботі, політика безпеки встановлює порядок дій, спрямованих на усунення наслідків цього інциденту.

Політика безпеки на нижньому рівні спрямована на забезпечення захисту інформаційних систем та ресурсів через практичні заходи та процедури, які виконуються безпосередньо співробітниками організації.

Це включає в себе налаштування систем безпеки, контроль доступу, захист мереж та програмного забезпечення, а також моніторинг та управління безпекою в реальному часі. Одним із ключових аспектів є контроль доступу до конфіденційної інформації, де важливо, щоб тільки авторизовані користувачі мали можливість доступу до чутливих даних. Для цього використовуються різноманітні методи аутентифікації, зокрема паролі, біометрія та смарт-карти.

У рамках цього рівня також впроваджуються засоби захисту від кіберзагроз, такі як фаєрволи, антивірусні програми, системи виявлення вторгнень та інші інструменти, що гарантують захист мережі від шкідливих атак. Моніторинг є ще одним важливим елементом, адже завдяки постійному спостереженню за діяльністю в системах можна вчасно виявити та відреагувати на потенційні інциденти безпеки, включаючи зломи, спроби витоку даних або аномальні дії користувачів.

Захист персоналу та навчання є важливим елементом нижнього рівня політики безпеки. Співробітники повинні бути ознайомлені з основними принципами роботи з конфіденційною інформацією та правильно поводитись у випадку виявлення загроз чи інцидентів. Для цього організовуються регулярні тренінги, інструктажі та внутрішні курси з інформаційної безпеки. Підвищення обізнаності серед співробітників дозволяє знизити ризики, пов'язані з людським фактором, що є однією з основних причин інформаційних інцидентів.

Також важливим аспектом є політика обробки даних, яка регламентує всі етапи роботи з інформацією: від її збору та зберігання до обробки, передачі та знищення. Для забезпечення конфіденційності даних використовуються сучасні методи шифрування, а також впроваджуються процедури для безпечного знищення даних після їх використання, що запобігає несанкціонованому доступу до інформації в майбутньому.

Захист фізичних носіїв інформації є ще одним важливим елементом на нижньому рівні. Організації повинні забезпечити безпечне зберігання комп'ютерної техніки, серверів і знімних носіїв, а також організувати належний контроль за доступом до цих пристроїв. Програми для захисту фізичних носіїв інформації включають в себе не лише фізичні заходи, як-от обмеження доступу до серверних приміщень, але й технічні, такі як використання зашифрованих дисків для збереження важливих даних.

Політика безпеки на нижньому рівні забезпечує ефективне виконання стратегічних цілей безпеки шляхом впровадження конкретних, чітко визначених процедур і інструментів для захисту організаційних ресурсів та зниження ризиків. Вона є необхідною складовою частиною загальної стратегії безпеки, оскільки саме на цьому рівні здійснюються

практичні заходи для захисту інформаційних активів організації від зовнішніх і внутрішніх загроз.

3.2. СКЛАД І СТРУКТУРА ПОЛІТИКИ БЕЗПЕКИ

Політики безпеки є основою для управління ризиками та забезпечення належного захисту інформаційних ресурсів в організаціях. Вони визначають правила, процедури та стратегії, які застосовуються для захисту інформаційних активів від несанкціонованого доступу, пошкодження або втрати. Політики безпеки повинні бути розроблені таким чином, щоб охоплювати всі аспекти безпеки, включаючи фізичну, технічну та адміністративну складові, і повинні відповідати вимогам законодавства, а також специфіці діяльності організації. Склад і структура політики безпеки залежить від характеру діяльності підприємства, обсягу та виду інформації, що підлягає захисту, а також вимог законодавства й стандартів у сфері інформаційної безпеки.

При розробці політики безпеки виконують наступні кроки:

- ❖ визначають об'єкти, які треба захистити і їх функції;
- ❖ оцінюють інтерес порушника до цих об'єктів і варіанти нападу;
- ❖ визначають області, в яких наявні засоби протидії не забезпечують достатнього захисту;
- ❖ встановлюють порядок дій для усунення наслідків інцидентів.

При розробці політики безпеки важливо враховувати кілька ключових аспектів, які забезпечать її ефективність та відповідність вимогам організації. Політика безпеки повинна бути чіткою, зрозумілою та застосовуватися на всіх рівнях організації. Основні кроки, які слід виконати при її розробці:

❖ Оцінка ризиків

Першим кроком є проведення аналізу ризиків, який дозволяє визначити, які загрози існують для інформаційних ресурсів і активів організації. Важливо оцінити ймовірність виникнення цих загроз і їх потенційний вплив. Це дозволить правильно визначити пріоритети і зосередити зусилля на найбільш критичних аспектах безпеки. Після проведення аналізу ризиків необхідно розробити стратегію управління ризиками, що включатиме конкретні заходи для зниження, перенесення або прийняття цих ризиків. Наступним етапом є впровадження цих заходів в організаційні процеси, що дозволить зменшити ймовірність виникнення загроз або мінімізувати їхні наслідки. Важливо також здійснювати постійний

моніторинг і оновлення оцінок ризиків, оскільки загрози та умови змінюються з часом. Це забезпечить ефективний захист інформаційних ресурсів і підвищить стійкість організації до потенційних кіберзагроз.

❖ *Визначення цілей і задач політики безпеки*

Політика безпеки повинна мати чітко визначені цілі, такі як захист конфіденційної інформації, забезпечення цілісності даних, доступність інформаційних систем і запобігання несанкціонованому доступу. Визначення цих цілей є основою для подальших дій щодо захисту інформаційних ресурсів. Крім того, важливо визначити конкретні задачі, які допоможуть досягти поставлених цілей, такі як впровадження систем контролю доступу, моніторинг і аудит діяльності користувачів, а також регулярне оновлення програмного забезпечення. Політика безпеки повинна враховувати всі рівні організації, визначаючи відповідальність за безпеку на кожному з них, від технічного до адміністративного. Окрім того, вона повинна бути гнучкою і враховувати зміни в зовнішньому середовищі, такі як нові загрози або зміни в законодавстві. Розробка чітких цілей і задач політики безпеки сприятиме не лише ефективному захисту інформації, а й забезпечить підтримку організаційної стратегії безпеки в цілому.

❖ *Розподіл відповідальності*

Важливо чітко визначити, хто в організації відповідальний за безпеку. Це включає не тільки ІТ-спеціалістів, а й керівників підрозділів, відповідальних за дотримання правил безпеки. Визначення відповідальних осіб дозволяє створити чітку структуру управління безпекою. Розподіл відповідальності також допомагає забезпечити оперативне реагування на інциденти безпеки, оскільки кожен має чітко визначену роль у випадку загрози або порушення політики. Крім того, це сприяє ефективному моніторингу виконання заходів безпеки та забезпечує їх належну реалізацію. Важливо, щоб відповідальність була розподілена на різні рівні організації для забезпечення комплексного підходу до захисту інформаційних ресурсів. Це включає як технічні заходи, так і політики управління доступом та навчання персоналу.

❖ *Розробка заходів та процедур*

Після визначення цілей і відповідальності потрібно розробити конкретні процедури та заходи, які будуть застосовуватися для досягнення встановлених цілей безпеки. Це може включати заходи щодо контролю доступу, використання шифрування, моніторингу і аудиту систем, а також інші методи захисту даних. Зазначені заходи повинні бути чітко документовані та інтегровані в робочі процеси організації, щоб забезпечити їх ефективне виконання. Важливо також визначити механізми

для регулярного оновлення цих заходів, враховуючи зміни в технологічному середовищі та нові загрози. Крім того, розроблені процедури повинні бути зрозумілі для всіх працівників організації, що сприяє підвищенню загальної безпеки та усвідомленості щодо важливості захисту інформації. Не менш важливо також регулярно перевіряти ефективність застосовуваних заходів через проведення тестувань і аудитів.

❖ *Навчання та підвищення кваліфікації персоналу*

Оскільки співробітники є однією з найбільших вразливих ланок у системі безпеки, важливо регулярно проводити тренінги з безпеки для всіх працівників. Це допоможе знизити ризик помилок через людський фактор та підвищити загальний рівень обізнаності про загрози. Регулярні тренінги з інформаційної безпеки дозволяють персоналу освоювати нові методи захисту та вчасно реагувати на потенційні загрози. Підвищення кваліфікації співробітників сприяє формуванню культури безпеки, що знижує ймовірність інцидентів, пов'язаних з людським фактором.

❖ *Контроль і моніторинг виконання політики*

Після впровадження політики безпеки необхідно здійснювати постійний контроль за її виконанням. Це включає проведення аудитів, моніторинг виконання заходів безпеки, а також аналіз ефективності політики та коригування її в разі потреби. Регулярний моніторинг допомагає виявити можливі порушення або недоліки в реалізації політики безпеки. Крім того, важливо залучати зворотний зв'язок від співробітників і користувачів для оцінки ефективності заходів безпеки. У разі виявлення нових загроз або змін у вимогах безпеки політика повинна бути адаптована та оновлена для забезпечення належного захисту. Процес контролю і моніторингу має бути безперервним для підтримки актуальності політики безпеки в умовах змінного технологічного середовища.

❖ *План реагування на інциденти безпеки*

Політика безпеки повинна включати в себе план на випадок інцидентів, що стосуються безпеки, таких як витоки даних, кібератаки чи інші загрози. Це дозволить організації швидко реагувати на інциденти та мінімізувати їхній вплив. План реагування на інциденти має включати чітко визначені кроки для виявлення, оцінки і локалізації загрози, а також заходи для відновлення нормальної роботи систем. Важливо забезпечити належну підготовку персоналу, проводячи тренування та симуляції інцидентів. Крім того, план повинен включати процедури для звітності та комунікації з усіма зацікавленими сторонами, включаючи клієнтів та регулюючі органи. Регулярне оновлення плану дозволить організації ефективно адаптуватися до нових загроз і мінімізувати потенційні збитки.

❖ *Оновлення та адаптація політики*

Оскільки технології та загрози змінюються, політика безпеки повинна бути живим документом, який регулярно переглядається та оновлюється, щоб відповідати новим вимогам і викликам. Оновлення політики безпеки повинно враховувати зміни в законодавстві, нові технологічні досягнення та виникаючі загрози. Крім того, регулярний перегляд дозволяє адаптувати політику до змін в організаційній структурі та бізнес-процесах. Під час оновлення політики також потрібно враховувати результати проведених аудитів та інцидентів безпеки, щоб удосконалити існуючі заходи. Це забезпечить постійну готовність організації до ефективного захисту своїх інформаційних ресурсів.

Таким чином, розробка політики безпеки — це складний і багатогранний процес, який потребує ретельного планування, врахування специфіки організації та її бізнес-процесів. Важливим є те, що політика безпеки повинна бути інтегрована в загальну стратегію управління організацією і постійно адаптуватися до нових умов і загроз.

Для кожної ІКС політика безпеки має бути індивідуальною, оскільки вона повинна враховувати специфіку реалізованої технології обробки інформації, особливості самої системи, фізичне середовище та інші важливі фактори. Якщо в рамках ІКС використовуються різні технології обробки даних, то політика безпеки також буде складатися з кількох частин, причому кожна з них буде відповідати конкретній технології. Це означає, що політика безпеки для кожної з цих технологій може істотно відрізнятися, оскільки кожна з них має свої особливості в питаннях захисту даних, управління доступом і виявлення загроз. Зокрема, в ІКС, де застосовуються різні системи для обробки даних, необхідно точно визначити, як кожна з них буде захищена від конкретних загроз, і адаптувати політику безпеки відповідно до технологічних вимог і специфікацій. Це дозволяє мінімізувати ризики та забезпечити комплексний підхід до захисту інформаційних ресурсів системи.

Компоненти політики безпеки

При розробці політики безпеки організація повинна враховувати кілька ключових компонентів, які забезпечать комплексний підхід до захисту своїх інформаційних ресурсів. Основними компонентами політики безпеки є: загальні положення, розподіл відповідальності, управління доступом, захист конфіденційної інформації, фізична безпека, технічний захист, управління інцидентами безпеки, навчання і підвищення кваліфікації персоналу, контроль та аудит безпеки та оновлення політики.

Загальні положення визначають основні принципи і цілі політики безпеки, пояснюючи її значення для організації. Вони включають місію

організації щодо захисту інформаційних активів та забезпечення довіри до її інформаційних систем. Розподіл відповідальності є важливою частиною, де чітко визначаються ролі та обов'язки співробітників і керівництва щодо захисту інформаційних ресурсів, а також встановлюється відповідальність за виконання політики безпеки на всіх рівнях.

Управління доступом регулює, хто має доступ до яких ресурсів організації, і визначає методи контролю доступу до інформаційних систем і даних. Це включає впровадження технологій для ідентифікації користувачів, а також засоби для контролю і обмеження доступу до конфіденційної інформації. Захист конфіденційної інформації передбачає використання шифрування, обмеження доступу та інших заходів для забезпечення конфіденційності даних на всіх етапах їх обробки.

Фізична безпека охоплює заходи для захисту фізичних активів організації, включаючи приміщення, серверні кімнати та технічні засоби від несанкціонованого доступу, крадіжки чи пошкодження. Технічний захист містить у собі використання сучасних технологій, таких як антивірусні програми, фаєрволи, системи виявлення вторгнень, шифрування даних, що дозволяють захистити інформаційні системи від зловмисних атак і небажаного доступу.

Управління інцидентами безпеки включає визначення процедур для реагування на порушення безпеки, такі як кібератаки чи витоки даних. Політика повинна містити інструкції щодо того, як діяти в разі інцидентів, хто несе відповідальність за їх розслідування та виправлення, а також які заходи будуть вжиті для запобігання подібним подіям у майбутньому.

Навчання і підвищення кваліфікації персоналу є необхідною частиною політики безпеки, оскільки співробітники можуть стати вразливими до загроз через недостатню обізнаність або помилки. Регулярні тренінги та підвищення рівня обізнаності допомагають персоналу ефективно використовувати інструменти безпеки та дотримуватись встановлених правил. Контроль та аудит безпеки включають моніторинг за виконанням політики безпеки, проведення регулярних перевірок і тестування на уразливість систем, а також оцінку ефективності вжитих заходів для забезпечення належного рівня безпеки.

Оновлення політики безпеки є важливою частиною, оскільки загрози та технології швидко змінюються. Політика безпеки повинна бути динамічною та адаптованою до нових умов, щоб ефективно захищати інформаційні активи організації. Це включає регулярний перегляд і коригування політики з урахуванням нових технологій, змін в законодавстві та виникнення нових загроз.

Таким чином, політика безпеки організації має бути всебічною, узгодженою і ефективною, забезпечуючи належний захист усіх інформаційних ресурсів на всіх рівнях діяльності підприємства.

Зазвичай політика безпеки організації включає такі компоненти:

- ❖ базова політика безпеки;
- ❖ спеціалізовані політики безпеки;
- ❖ процедури безпеки.

Базова політика безпеки є основним документом, що визначає підходи та правила, за якими організація обробляє інформацію. Вона встановлює чіткі принципи того, хто має право на доступ до інформаційних ресурсів, які дії дозволені, а які заборонені, а також визначає необхідні засоби для управління та захисту цих ресурсів. Базова політика безпеки створює основу для впровадження інших, більш детальних документів і процедур, таких як специфікації доступу, правила роботи з конфіденційною інформацією, протоколи безпеки тощо.

У базовій політиці безпеки визначаються основні типи доступу, включаючи доступ до фізичних та електронних ресурсів організації. Вона вказує, хто має право на доступ до різних категорій інформації та за яких умов. Доступ до чутливої та конфіденційної інформації може бути обмежений лише певними категоріями користувачів, що мають відповідні повноваження або обов'язки.

Політика також детально описує дозволені та заборонені дії з інформацією. Наприклад, дозволяється використовувати інформацію лише для виконання конкретних робочих завдань, а її передача третім сторонам або несанкціоноване розповсюдження є забороненими діями. Важливо також зазначити, що всі дії з інформацією повинні відповідати вимогам законодавства і внутрішнім регламентам організації.

Окрім цього, базова політика безпеки вказує на необхідні інструменти і методи управління безпекою. Це можуть бути заходи, як технічні, так і організаційні, наприклад, системи контролю доступу, методи шифрування, моніторинг та аудит дій з інформацією, а також навчання персоналу. Використання таких інструментів дозволяє знизити ризики втрати або несанкціонованого доступу до даних.

Загалом, базова політика безпеки є наріжним каменем для побудови ефективної системи захисту інформаційних активів організації, оскільки визначає основи всіх подальших заходів з безпеки.

Спеціалізовані політики безпеки є важливим елементом загальної системи інформаційної безпеки організації, оскільки вони спрямовані на детальне регулювання конкретних аспектів захисту інформаційних ресурсів. Вони орієнтовані на специфічні ситуації, технології та ризики, що виникають у процесі функціонування організації, і дозволяють знижувати вірогідність порушень безпеки у цих сферах. Спеціалізовані політики дають змогу організаціям швидко реагувати на нові виклики, технічні зміни або зовнішні загрози.

Однією з ключових політик є політика управління доступом. Вона визначає правила створення, зміни та скасування облікових записів користувачів, а також принципи аутентифікації і авторизації. Політика управління доступом визначає, хто має право на доступ до різних інформаційних ресурсів, і встановлює правила для контролю цього доступу, що є критичним для забезпечення інформаційної безпеки в організації.

Ще однією важливою складовою є політика конфіденційності, що регулює захист чутливої інформації, наприклад, медичних даних або фінансової інформації. Вона визначає, які типи даних організація вважає конфіденційними та як із ними повинні працювати співробітники. Політика конфіденційності передбачає запровадження заходів для шифрування даних, обмеження доступу і встановлення процедур для захисту персональних та комерційно чутливих даних.

Політика захисту від шкідливого програмного забезпечення (антивірусна політика) також є важливим компонентом спеціалізованої політики безпеки. Вона визначає заходи для виявлення та запобігання проникненню шкідливого програмного забезпечення в інформаційні системи організації. Це включає встановлення антивірусного програмного забезпечення, регулярні сканування на наявність вірусів і забезпечення навчання персоналу щодо безпечного використання технологій.

Політика резервного копіювання та відновлення даних встановлює вимоги до зберігання і архівування важливих даних, а також до створення та збереження резервних копій. Вона гарантує, що в разі пошкодження або втрати даних організація зможе швидко відновити свою роботу без значних втрат.

Політика фізичної безпеки зосереджена на забезпеченні фізичного доступу до організаційних приміщень і технічного обладнання. Вона включає заходи контролю за доступом до серверних кімнат, встановлення відеоспостереження, сигналізації і фізичних бар'єрів для захисту важливих інфраструктурних елементів.

Політика моніторингу і аудиту визначає процедури для відстеження і реєстрації дій користувачів в інформаційних системах організації. Вона передбачає використання систем моніторингу, аудиту доступу та аналізу активності, що дозволяє виявляти порушення безпеки та реагувати на них на ранніх етапах.

Політика обробки інцидентів безпеки є важливою частиною спеціалізованої політики, оскільки вона встановлює процедури для оперативного реагування на інциденти безпеки. Вона визначає, як організація повинна виявляти, класифікувати і розслідувати інциденти, а також яким чином вживати заходи для їх усунення.

Політика безпеки для мобільних пристроїв є особливо актуальною в умовах сучасних технологій. Вона регулює використання мобільних пристроїв для доступу до корпоративних ресурсів, встановлюючи вимоги до шифрування, паролів безпеки та процедур для дистанційного стирання даних у разі втрати пристрою.

Політика управління уразливостями визначає процеси для виявлення, оцінки та усунення уразливостей у інформаційних системах організації. Вона включає регулярні оновлення програмного забезпечення, виправлення уразливостей та застосування патчів для забезпечення належного рівня безпеки систем.

Завдяки таким спеціалізованим політикам організація може забезпечити належний рівень захисту інформаційних ресурсів, адаптуючи стратегію безпеки до змінюваних умов та специфічних потреб. Спеціалізовані політики безпеки дозволяють ефективно справлятися з конкретними ризиками і загрозами, забезпечуючи безпеку в різних сферах діяльності організації.

Поділяються на дві групи:

- *політики, що пов'язані з користувачами;*
- *політики, що пов'язані з технічними засобами.*

До спеціалізованих політик, які пов'язані з користувачами, відносяться:

❖ Політика допустимого використання встановлює норми безпечного використання комп'ютерного обладнання і сервісів у компанії і вказує користувачам, які дії дозволяються, а які заборонені, наприклад, повинні бути пункти про заборону самотійно встановлювати і запускати ПЗ, про регламентацію використання власного обладнання співробітників (ноутбуків, планшетів, смартфонів, USB-накопичувачів) і т. п.

Політика допустимого використання (Acceptable Use Policy, AUP) є важливим елементом інформаційної безпеки в організації. Вона визначає правила та

обмеження щодо використання інформаційних ресурсів, зокрема комп'ютерних мереж, програмного забезпечення, обладнання та інтернет-ресурсів співробітниками організації. Метою цієї політики є забезпечення належного функціонування інформаційних систем, захист від зловживань, запобігання несанкціонованому доступу та зниження ризиків безпеки. Політика допустимого використання є основою для контролю поведінки користувачів і гарантує, що використання інформаційних ресурсів в організації буде здійснюватися відповідно до встановлених норм та процедур, що сприяє захисту інформаційних активів і забезпеченню безпеки корпоративних систем.

Приклад.

Не залишайте будь-який портативний пристрій без нагляду в будь-якому громадському місці, де він може бути загублений або вкрадений. Жорсткі диски ноутбуків повинні бути захищені та зашифровані. Компанія застосовує автоматичний процес шифрування ноутбуків компанії за допомогою BitLocker.

Співробітник повинен знати, що адміністратори можуть відслідковувати всі дії, пов'язані з комп'ютерами, включаючи відвідування вебсайтів.

❖ **Політика доступу** є основним елементом системи інформаційної безпеки, що визначає правила і процеси доступу користувачів та систем до інформаційних ресурсів організації. Вона спрямована на забезпечення того, щоб доступ до чутливих або критичних даних мали лише ті особи або системи, які мають на це відповідні права, що дозволяє мінімізувати ризики несанкціонованого доступу, витоку інформації та зловживань. Метою політики доступу є встановлення норм безпечного з'єднання будь-якого хоста з мережею компанії. Ці норми покликані мінімізувати збиток компанії через можливе неавторизованого використання ресурсів компанії.

Основними принципами політики доступу є принцип найменших привілеїв, що передбачає надання користувачам лише тих прав доступу, які необхідні для виконання їхніх обов'язків, а також ідентифікація та аутентифікація, що гарантують, що тільки авторизовані особи можуть отримувати доступ до системи. Політика доступу включає також визначення ролей та груп користувачів, що дозволяє ефективно управляти правами доступу для великої кількості користувачів і забезпечує мінімізацію помилок у наданні доступу. Крім того, політика доступу визначає моделі контролю доступу, такі як DAC (Discretionary Access

Control), MAC (Mandatory Access Control) та RBAC (Role-Based Access Control), що дозволяють адаптувати систему доступу до специфічних потреб організації. Важливими компонентами є також моніторинг і аудит доступу, що дозволяють відслідковувати всі дії користувачів і виявляти підозрілі активності.

Політика доступу також повинна враховувати специфіку мобільних пристроїв та фізичний доступ до критичних інфраструктурних об'єктів, що забезпечують додатковий рівень захисту. Окрім того, політика доступу передбачає заходи для обмеження доступу у разі звільнення співробітників або їхньої відпустки, що є важливою частиною для запобігання витоку інформації або несанкціонованим діям. Все це робить політику доступу критично важливим інструментом у забезпеченні безпеки інформаційних ресурсів і даних організації.

Приклад.

Не отримуйте доступ до внутрішніх ресурсів компанії із загальнодоступних комп'ютерів (інтернет-кафе).

Політика передбачає, що співробітники повинні уникати доступу до корпоративних систем, баз даних або інших конфіденційних ресурсів через публічні комп'ютери, які можуть бути заражені шкідливим програмним забезпеченням або використовувати слабкі методи захисту. Публічні комп'ютери часто не забезпечують належного рівня безпеки, тому важливо, щоб доступ до таких ресурсів здійснювався тільки з персональних, захищених пристроїв, що мають актуальні антивірусні програми, засоби шифрування та інші елементи захисту. Це дозволяє знизити ризик несанкціонованого доступу або витоку чутливої інформації через уразливості на загальнодоступних комп'ютерах.

❖ **Політика використання Internet** є критично важливим компонентом системи інформаційної безпеки організації, оскільки вона встановлює правила і норми, що визначають допустимі та недопустимі способи доступу до Інтернету для співробітників. Основна мета цієї політики – зберегти баланс між забезпеченням безпеки організації та можливістю ефективного використання Інтернету для виконання професійних обов'язків. Політика використання Інтернету в організації встановлює чіткі обмеження щодо доступу до Інтернет-ресурсів,

визначаючи, які сайти можуть бути використані в робочий час і які є забороненими. Важливим аспектом є визначення доступу до ресурсів, що не пов'язані з робочими процесами, таких як соціальні мережі, ігрові сайти або інші ресурси, що можуть негативно впливати на продуктивність або створювати безпекові ризики.

Крім того, політика повинна регулювати питання безпеки при використанні Інтернету, передбачаючи заходи щодо захисту від шкідливих програм, фішингових атак і кіберзагроз. Вона встановлює вимоги до використання антивірусного програмного забезпечення, фаєрволів і інших систем безпеки для забезпечення захисту інформаційних систем організації від потенційних кіберзагроз. Політика також повинна враховувати аспекти контролю доступу до Інтернету, включаючи моніторинг активності співробітників і ведення журналів доступу до мережі, що дозволяє своєчасно виявляти аномальні дії і порушення.

Важливим є включення правил для мобільних пристроїв, які підключаються до корпоративної мережі. Політика повинна передбачати налаштування безпечного підключення, наприклад, через VPN, а також інші заходи для захисту даних при використанні мобільних пристроїв для роботи в Інтернеті. Одним із ключових моментів є визначення відповідальності співробітників за порушення встановлених правил. Це можуть бути санкції, такі як попередження, дисциплінарні заходи або навіть звільнення у разі серйозних порушень.

Нарешті, для забезпечення ефективної реалізації політики використання Інтернету важливо проводити навчання співробітників. Освітні програми сприяють підвищенню обізнаності персоналу щодо безпеки в Інтернеті, ризиків, що виникають через несанкціоноване використання Інтернет-ресурсів, і відповідальності за збереження конфіденційності та безпеки інформації. Тому політика використання Інтернету не лише регулює доступ до ресурсів, а й є важливим інструментом для створення безпечного і продуктивного робочого середовища.

Приклад.

При роботі з внутрішнім сайтом компанії, не відкривайте жодного іншого сайту за допомогою того самого вебпереглядача.

Політика спрямована на зменшення ризиків кібератак, таких як кросс-сайтове скриптування (XSS) чи маніпуляція сесіями користувача. Використання окремих вебпереглядачів або сеансів для доступу до внутрішніх ресурсів компанії дозволяє

уникнути випадкового доступу до шкідливих чи підозрілих вебсайтів, що можуть скомпрометувати робочі сесії або викрасти облікові дані користувача. Це знижує ймовірність потрапляння в пастки, які можуть бути використані для фішинг-атак або інших типів кіберзагроз, тим самим покращуючи рівень захисту внутрішньої інформації.

❖ **Політика використання електронної пошти** в організації визначає правила та обмеження щодо використання корпоративної електронної пошти співробітниками. Вона передбачає, що електронна пошта є офіційним інструментом для обміну діловою інформацією, тому її використання має бути спрямоване лише на професійні цілі. Політика включає вимоги щодо безпеки, такі як заборона на відкриття підозрілих вкладень і посилань, використання надійних паролів та двофакторної аутентифікації для захисту акаунтів. Крім того, встановлюються правила щодо конфіденційності інформації, заборона на використання корпоративної пошти для особистих цілей та передбачають санкції за порушення. Важливим є також моніторинг поштової активності для запобігання витоку даних і фішингових атак.

Приклад.

Перед відправкою e-mail задайте собі такі питання:

- *чи повинен я шифрувати повідомлення? Так, якщо повідомлення (або додаток) містить конфіденційні дані. Зверніться до команди підтримки компанії, і вони навчать вас налаштовувати шифрування;*
- *чи підходить цифровий підпис? Так, якщо важливо, щоб одержувач перевінив, що ви насправді є відправником;*
- *чи відповідає мова та зміст? Звичайний електронний лист не є конфіденційним, ані приватним. Наглядачі, адміністратори локальної мережі та кожен, хто може отримати переслану копію, зможуть бачити ваше повідомлення, тому ви можете переглянути мову, яку ви використовуєте. У повідомленні не повинно бути сексуальних, расистських та інших образливих слів.*

Ставтесь з насторогою до e-mail, якщо:

- *тема листа дивна або незвична;*
- *ви не знаєте відправника;*

- *це не стосується роботи;*
- *якщо є посилання, що вказує на сайт;*
- *ви не очікували прикріплення.*

Завжди шифруйте будь-які електронні листи, які ви надсилаєте з конфіденційними даними!

❖ **Політика використання паролів** в організації визначає вимоги до створення, зберігання та обміну паролями для доступу до корпоративних систем та інформації. Вона передбачає використання складних паролів, що містять комбінацію великих і малих літер, цифр та спеціальних символів, щоб ускладнити їх здогадування. Паролі повинні мати мінімальну довжину та регулярно змінюватися, наприклад, кожні 60-90 днів. Для додаткової безпеки рекомендується використовувати двофакторну аутентифікацію. Політика також забороняє зберігати паролі в незахищених місцях, таких як текстові файли або на папері. Співробітники повинні бути навчені правилам безпечного управління паролями, а також не використовувати однакові паролі для кількох систем. У разі порушення політики можуть бути застосовані дисциплінарні заходи.

Приклад.

Політика використання паролів

Для обмеження доступу до інформаційних систем чи даних, які є комерційною таємницею, рекомендовано використовувати парольну систему захисту. Реальна політика компанії визначає правила використання паролів і обов'язкова для використання всіма співробітниками компанії.

Співробітнику забороняється:

- *Повідомляти свій пароль будь-кому;*
- *Зберігати паролі, записані на папері, в легкодоступному місці;*
- *Зберігати незашифровані паролі, записані в файлах у відкритому вигляді;*
- *Використовувати один і той же пароль для доступу до різних інформаційних систем.*

Співробітник зобов'язаний:

- *Під час першого входу в інформаційну систему замінити пароль, що встановив адміністратор, на особистий пароль.*
- Передача імені співробітника і пароля іншим категорично*

забороняється, при запиті системи про зміну пароля потрібно замінити його на новий.

- У випадку підозри на те, що пароль став кому-небудь відомий, змінити пароль та сповістити про факт компрометації співробітнику сервісної служби за допомогою електронної пошти на адресу: support@customertimes.com.

- Змінювати пароль кожні 90 днів.

Створювати пароль, що відповідає таким вимогам:

- Мінімальна довжина пароля повинна складатися з 8 символів;

- Пароль повинен мати символи в різних регістрах, а також цифри та спеціальні символи

(!@&\$%^*()-+={}[]?/,<.>).

Співробітнику рекомендується вибирати пароль за допомогою такої процедури:

- Вибрати фразу, яку легко запам'ятати. Наприклад, «Любїть Україну, як сонце, любїть, як вітер, і трави, і води».

- Вибрати перші літери з кожного слова: «луяслявітїв».

- Набрати отриману послїдовність, переключившись на англїйську розкладку клавіатури: «kezckzdsnsd».

- Вибрати номер символа, який буде записуватися в верхньому регістрі і після якого буде спеціальний символ. Наприклад, це буде третїй символ, а в ролї спеціального символа вибрано «\$». Маємо: «keZ\$ckzdsnsd».

Під час відсутності на робочому місці більше як 10 хвилин, необхідно встановити блокування на екран.

Компанія залишає за собою право:

- Здїйснювати періодичну перевірку – наявність пароля для доступу до інформаційних систем;

- Вживати заходи дисциплїнарного стягнення до співробітників, які порушили правила реальної політики компанії.

До спеціалізованих політик, що пов'язані з технічними засобами, відносяться:

- ❖ політика конфїгурації міжмережевих екранів

Політика конфігурації міжмережевих екранів є важливою частиною загальної стратегії забезпечення безпеки мережі. Вона визначає правила та налаштування, які визначають, як саме міжмережеві екрани (фаєрволи) повинні обробляти трафік між внутрішньою мережею організації та зовнішнім світом. Основною метою такої політики є контроль доступу до ресурсів, фільтрація небажаного або шкідливого трафіку, а також запобігання несанкціонованому доступу. Політика конфігурації міжмережевих екранів повинна включати такі аспекти, як визначення правил для дозволених і заблокованих з'єднань, встановлення політик для різних типів трафіку (наприклад, веб-трафік, електронна пошта, VPN), а також налаштування журналів подій для моніторингу активності. Крім того, важливо забезпечити мінімальні права доступу і принцип "найменших привілеїв", що означає надання доступу лише тим службам і користувачам, яким це необхідно для виконання їхніх обов'язків. Політика також повинна включати процедури для регулярного перегляду та оновлення правил, щоб відобразити зміни в інфраструктурі організації чи нові загрози.

❖ політика щодо шифрування і управління криптоключами

Політика щодо шифрування і управління криптоключами є критично важливим елементом стратегії інформаційної безпеки організації, що визначає правила використання шифрування для захисту конфіденційної інформації та забезпечення цілісності даних. Ця політика охоплює всі аспекти, пов'язані з застосуванням криптографічних методів для захисту даних, включаючи вибір алгоритмів шифрування, використання криптоключів, а також забезпечення їх надійного зберігання і передачі. Основною метою цієї політики є гарантування того, що всі чутливі дані, як у процесі зберігання, так і під час передачі, будуть захищені від несанкціонованого доступу. Політика повинна визначати стандарти шифрування для різних типів даних (наприклад, для баз даних, електронної пошти, резервних копій тощо), а також обов'язкові методи управління криптоключами. Важливим аспектом є забезпечення належного контролю за життєвим циклом криптоключів, включаючи їх генерацію, зберігання, використання та оновлення. Також необхідно визначити чіткі процедури для випадків втрати чи компрометації криптоключів, включаючи швидке їх відкликання та заміну. Політика повинна також забезпечувати вимоги до управління доступом до криптоключів, гарантувати їхнє шифрування під час зберігання та передачі, а також встановлювати мінімальні вимоги до складності криптографічних алгоритмів для забезпечення високого рівня захисту даних.

❖ політика використання віртуальних приватних мереж VPN

Політика використання віртуальних приватних мереж (VPN) є важливим елементом політики безпеки організації, що визначає правила та стандарти щодо використання VPN для забезпечення захищеного доступу до внутрішніх ресурсів компанії. Віртуальна приватна мережа дозволяє користувачам здійснювати безпечне підключення до корпоративних систем через Інтернет, забезпечуючи конфіденційність, цілісність даних і автентифікацію користувачів. Політика використання VPN повинна включати вимоги щодо вибору типу VPN, який буде використовуватись, наприклад, IPSec, SSL або MPLS, з огляду на потреби організації та рівень захисту. Вона повинна регламентувати вимоги до шифрування трафіку для забезпечення конфіденційності переданих даних і визначати мінімальні вимоги до автентифікації користувачів, включаючи використання багатофакторної автентифікації (MFA). Політика також повинна визначати правила доступу до корпоративних мереж через VPN, зокрема, хто має право використовувати VPN, в яких випадках підключення дозволено, та які ресурси доступні через VPN-з'єднання. Важливим аспектом є моніторинг і аудит використання VPN для виявлення потенційних загроз і несанкціонованих спроб доступу до системи. Крім того, необхідно встановити вимоги щодо налаштування та підтримки інфраструктури VPN, зокрема, регулярне оновлення програмного забезпечення, перевірку на уразливості і аудит безпеки VPN-сервісів. У разі компрометації VPN-з'єднання, політика повинна передбачати чітку процедуру для швидкого реагування, відновлення доступу і зменшення потенційного впливу інциденту.

❖ політика по обладнанню бездротової мережі та ін.

Політика по обладнанню бездротової мережі є ключовим елементом в стратегії забезпечення інформаційної безпеки організації, яка визначає вимоги та правила використання бездротових мереж для забезпечення надійного захисту даних, доступу та інфраструктури. Метою такої політики є забезпечення конфіденційності, цілісності і доступності інформації, що передається через бездротові мережі, а також мінімізація ризиків несанкціонованого доступу і потенційних атак на мережу. Політика повинна визначати стандарти для вибору обладнання для бездротових мереж, включаючи вимоги до підтримки сучасних протоколів шифрування, таких як WPA3, для захисту переданих даних від перехоплення. Окрім того, політика повинна регламентувати налаштування точок доступу (Access Points) і маршрутизаторів, щоб обмежити доступ до мережі лише для авторизованих користувачів.

Важливо також вимагати використання сильних методів аутентифікації, таких як 802.1X, для забезпечення безпеки підключень до мережі. Також у політиці повинні бути вказані вимоги до фізичного розташування обладнання бездротової мережі, щоб обмежити потенційний доступ до сигналу з вулиці або інших непередбачених місць, що може призвести до витоків даних або несанкціонованого доступу. Політика повинна включати вимоги до регулярного моніторингу бездротової мережі для виявлення аномальних дій або спроб несанкціонованого доступу, а також встановлювати процедури для швидкого реагування у разі виявлення загроз. Окрім того, важливо включити регламенти для оновлення і патчування програмного забезпечення для бездротового обладнання з метою усунення уразливостей і підвищення рівня захисту. Політика повинна також передбачати впровадження сегментації бездротової мережі для відокремлення критичних бізнес-ресурсів від зон із меншою безпекою, щоб мінімізувати потенційний вплив на важливі інформаційні ресурси.

Три теми кожної політики є загальноприйнятими, таким чином, чітке визначення мети, області застосування та відповідальності дозволяє зробити політику безпеки зрозумілою, ефективною та легкою у впровадженні:

➔ мета, яка описує, чому створена та чи інша політика. Наприклад, це може бути забезпечення конфіденційності, цілісності та доступності інформації, мінімізація ризиків, пов'язаних із витоком або втратою даних, а також встановлення стандартів і правил для захисту інформаційних активів підприємства.

➔ область застосування політики чітко визначає, кого і що вона стосується. Це можуть бути всі працівники підприємства, незалежно від їхніх посад, підрядники, партнери, інформаційні системи, процеси чи активи, які обробляють дані. Наприклад, політика може поширюватися на всі інформаційні системи, сервери, мережі, мобільні пристрої та роботу з конфіденційними даними як у фізичному, так і у цифровому форматах.;

➔ відповідальність визначає, хто саме відповідає за дотримання положень політики та її впровадження. Зазвичай це керівники відділів, які забезпечують виконання політики у своїх підрозділах, а також спеціалізовані відділи, такі як ІТ-відділ чи відділ інформаційної безпеки, які займаються технічною реалізацією та моніторингом. Усі працівники підприємства також зобов'язані виконувати вимоги політики, а у разі порушень можуть бути застосовані дисциплінарні заходи.

Загалом, термін **«політика безпеки»** може бути застосований не тільки до окремих компонентів, таких як організація чи інформаційно-

комунікаційна система (ІКС), але й до різних технічних елементів, таких як операційна система, програмне забезпечення чи послуга, що реалізує певні функції для забезпечення захисту від загроз. У сучасному контексті політика безпеки організації включає в себе цілісні підходи, які враховують не тільки захист інформації, але й інші аспекти, такі як захист фізичної безпеки, захист від кіберзагроз, а також відповідність нормативним вимогам та стандартам безпеки.

Політика безпеки інформації в ІКС є частиною загальної політики безпеки організації і визначає принципи доступу до інформаційних ресурсів, вимоги до збереження даних, механізми аутентифікації та авторизації, правила моніторингу та захисту від загроз. Враховуючи розвиток кіберзагроз і необхідність реагування на нові виклики, сучасні політики безпеки також включають інструменти захисту від атак на основі штучного інтелекту, мобільні загрози та забезпечення безпеки при роботі з великими даними (Big Data).

Після формулювання політики безпеки необхідно розробити програму її реалізації, яка включає в себе детальні плани по впровадженню встановлених правил. Це включає розробку процедур для оцінки ризиків, тестування систем на уразливості, навчання співробітників та аудит безпеки. Програма реалізації політики безпеки також передбачає визначення відповідальних осіб і команд, які контролюватимуть виконання кожного етапу, а також механізми моніторингу, щоб забезпечити своєчасне реагування на порушення або нові загрози. Важливим є також постійне оновлення політики в міру змін в технологічному середовищі та зростання нових типів кіберзагроз.



Розробка політики безпеки дійсно не вимагає глибоких технічних знань, оскільки основний акцент робиться на встановлення загальних принципів, правил і процедур для забезпечення безпеки, які мають бути зрозумілими для всіх співробітників організації, а не тільки для ІТ-професіоналів. Однак, для розробки ефективної політики безпеки важливо розуміти потенційні загрози та слабкі місця в системах організації, що вимагає певного співробітництва з ІТ-відділом для врахування технічних аспектів. Незважаючи на те, що політика безпеки може не завжди подобатися співробітникам через обмеження їхніх свобод і можливостей, її роль у забезпеченні захисту організації від внутрішніх і зовнішніх загроз є критично важливою. Обмеження доступу до конфіденційної інформації, застосування контролю за використанням ресурсів і визначення процедур для реагування на інциденти — це необхідні кроки для збереження інформаційної цілісності, доступності та

конфіденційності даних. Політика безпеки також дозволяє зменшити ймовірність порушень законодавчих вимог, таких як загроза витоку даних або порушення вимог до захисту особистої інформації. Тому її розробка є стратегічно важливою роботою для відділу безпеки, який, поряд з ІТ-відділом, забезпечує захист інформаційних ресурсів організації, підтримує довіру клієнтів і партнерів, а також забезпечує безперервність бізнес-процесів.

3.3. ЗРАЗОК СПЕЦІАЛІЗОВАНОЇ ПОЛІТИКИ БЕЗПЕКИ ДОПУСТИМОГО ВИКОРИСТАННЯ

Метою спеціалізованої політики безпеки допустимого використання (AUP) є визначення правил, що регулюють допустиме використання інформаційних технологій, програмного забезпечення, обладнання та ресурсів організації. Політика покликана забезпечити безпеку корпоративних інформаційних систем, знизити ризики, пов'язані з несанкціонованим доступом до інформаційних ресурсів, та визначити обов'язки співробітників щодо дотримання заходів безпеки. Всі співробітники, підрядники та інші особи, які мають доступ до ресурсів організації, зобов'язані дотримуватися цієї політики.



Приклади:

Приклад №1

ПОЛІТИКА БЕЗПЕКИ ДОПУСТИМОГО ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

1. Мета

Ця політика визначає правила та обмеження для використання інформаційних систем підприємства, щоб забезпечити захист конфіденційної інформації, підтримання продуктивності роботи та запобігання порушенням законодавства чи етичних норм.

2. Область застосування

Ця політика поширюється на всіх співробітників підприємства, підрядників, партнерів та інших осіб, які мають доступ до інформаційних систем, включаючи комп'ютери, сервери, мобільні пристрої, мережі, програмне забезпечення та хмарні сервіси, що належать або контролюються підприємством.

3. Основні положення

1. Дозволене використання

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

- ✓ Інформаційні системи призначені виключно для виконання службових завдань, пов'язаних із діяльністю підприємства.
- ✓ Використання обладнання та програмного забезпечення для особистих потреб допускається лише в межах, що не суперечать цій політиці та не впливають на продуктивність роботи.

2. Заборонене використання

- ✓ Використання інформаційних систем для несанкціонованого доступу до внутрішніх або зовнішніх ресурсів.
- ✓ Передача, завантаження або зберігання матеріалів, що порушують авторські права, законодавство або етичні норми.
- ✓ Використання службових ресурсів для комерційних чи особистих проектів, що не стосуються діяльності підприємства.
- ✓ Інсталяція будь-якого програмного забезпечення або змінення налаштувань систем без попереднього схвалення відділу IT.

3. Електронна пошта та інтернет

- ✓ Службова електронна пошта повинна використовуватися лише для офіційної кореспонденції.
- ✓ Заборонено надсилати або отримувати електронні листи із вкладеннями, що можуть містити віруси або шкідливі програми.
- ✓ Доступ до інтернету має бути обмежений службовими потребами. Відвідування сайтів із неналежним контентом суворо заборонено.

4. Безпека паролів

- ✓ Користувачі зобов'язані створювати надійні паролі, які повинні залишатися конфіденційними.
- ✓ Заборонено передавати паролі іншим особам, включаючи колег або керівників.

4. Відповідальність

- Відділ IT несе відповідальність за моніторинг використання інформаційних систем та виявлення порушень.
- Користувачі зобов'язані дотримуватися політики, негайно повідомляти про підозрілі дії або порушення.

- Керівники відділів відповідають за інформування своїх підлеглих про цю політику та забезпечення її виконання.

5. Наслідки порушення політики

Порушення цієї політики може призвести до дисциплінарних заходів, включаючи письмове попередження, позбавлення доступу до інформаційних систем або звільнення. У разі серйозних порушень можуть бути ініційовані юридичні дії відповідно до чинного законодавства.

6. Внесення змін до політики

Ця політика підлягає регулярному перегляду з урахуванням змін у законодавстві, внутрішніх процесах підприємства або загрозах інформаційній безпеці.

7. Підтвердження ознайомлення

Кожен працівник зобов'язаний ознайомитися з цією політикою та підтвердити своє розуміння шляхом підписання відповідного документа.

Дата набрання чинності: [вказати дату]
Відповідальний за політику: [ім'я, посада]

Приклад 2

Політика безпеки допустимого використання комп'ютерів і комунікаційних ресурсів

1. Мета

Ця політика встановлює правила використання комп'ютерів, мереж, програмного забезпечення та інших комунікаційних ресурсів підприємства для забезпечення їх захисту, підвищення ефективності роботи та запобігання зловживанням.

2. Область застосування

Ця політика поширюється на всіх співробітників, підрядників, стажерів та інші сторони, які мають доступ до комп'ютерів і комунікаційних ресурсів підприємства, включаючи робочі станції, сервери, мережеві пристрої, мобільні пристрої, електронну пошту, інтернет та корпоративні застосунки.

3. Основні положення

1. Допустиме використання

- ✓ Комп'ютери та комунікаційні ресурси використовуються виключно для виконання службових обов'язків.

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

- ✓ Обмежене особисте використання дозволяється лише в неробочий час за умови дотримання цієї політики.

2. Заборонене використання

- ✓ Використання ресурсів для незаконної діяльності, зокрема для порушення авторських прав, поширення шкідливих програм або несанкціонованого доступу до інформаційних систем.
- ✓ Перегляд, зберігання або передача матеріалів з непристойним, образливим або незаконним контентом.
- ✓ Використання службових комп'ютерів для ігор, соціальних мереж або стримінгових сервісів без дозволу керівництва.
- ✓ Інсталяція неавторизованого програмного забезпечення чи використання нелегальних копій програм.

3. Електронна пошта та інтернет

- ✓ Електронна пошта використовується лише для службового листування. Надсилання конфіденційної інформації дозволяється виключно через затверджені канали зв'язку.
- ✓ Забороняється відвідувати сайти, які не відповідають службовим завданням, або використовувати мережу для несанкціонованого завантаження файлів.

4. Мобільні пристрої

- ✓ Використання мобільних пристроїв для доступу до корпоративних систем дозволено лише через захищені канали зв'язку.
- ✓ Усі мобільні пристрої повинні мати актуальні антивірусні програми та використовувати надійні паролі.

5. Безпека даних

- ✓ Співробітники зобов'язані захищати конфіденційні дані від несанкціонованого доступу.
- ✓ Забороняється зберігати службову інформацію на особистих пристроях без дозволу.

4. Відповідальність

- Відділ інформаційної безпеки відповідає за моніторинг використання ресурсів, реагування на інциденти та навчання співробітників.
- Керівники підрозділів контролюють дотримання політики своїми співробітниками.

- Користувачі несуть персональну відповідальність за виконання положень цієї політики.

5. Наслідки порушення політики

Порушення політики може призвести до дисциплінарних заходів, включаючи письмове попередження, обмеження доступу до ресурсів, звільнення або передачу справи до відповідних органів у разі серйозних порушень.

6. Підтвердження ознайомлення

Усі співробітники повинні ознайомитися з цією політикою, підписати відповідний документ і дотримуватись її положень.

Дата набрання чинності: [вказати дату]
Відповідальний за політику: [ім'я, посада]

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 3

1. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213.

2. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

3. Криворучко О. В., Костюк Ю. В., Самойленко Ю. О. Методологія тестування системи захисту інформаційної системи на проникнення // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 15-16 квітня 2021 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: О.К. Закусило. (голова) та ін.–К.:ВПЦ"Київський університет", 2021.–190 с. (с. 137-138).

4. Cybersecurity a generic reference curriculum (2016). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-162 curriculum.pdf

5. Криворучко О. В., Костюк Ю. В., Самойленко Ю. О. Інформаційна безпека економічних систем // Глобалізаційні виклики розвитку національних економік : тези доповідей II Міжнар. наук.-практ. конф. (Київ, 19 жовтня 2021 р.) / відп. ред. А. А. Мазаракі. – Київ : Київ. нац. торг.-екон. ун-т, 2021. – с. 275-278 – Укр. та англ. мовами.

6. National Cyber Security Strategy Good Practice Guide (2016). URL: <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>

-
7. Castro D. (2018). Boosting the Cyberworkforce. URL: <http://www.govtech.com/data/Boosting-the-Cyberworkforce.html>
 8. JP 3–12 Cyberspace Operations, 8 June 2018. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
 9. Криворучко О.В., Костюк Ю.М., Захаров Р.Г. Програми моніторингу мереж // VIII Міжнародна науково-практична конференція «Управління розвитком технологій», 26-27 березня 2021 р., Київ, Україна – с. 34-36
 10. DOD Dictionary of Military and Associated Terms. As of January 2019. URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>
 11. Самойленко Ю.О., Костюк Ю.В. Теорія інформаційної безпеки // Кібергігієна. Кібербезпека. Безпека держави : Матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – с. 16-17.
 12. Костюк Ю., Шестак Я. Транспортний рівень моделі ISO/OSI в комп'ютерних мережах. Міжнародний науково-практичний журнал "Товари і ринки". 2021. № 4. С. 49-58.
 13. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
 14. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 374–391.
 15. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.
 16. Костюк Ю.В., Самойленко Ю.О., Костюк І.В. Критерії оцінювання захищеності інформаційних систем та мереж // Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2021) : матеріали тез доповідей XI Міжнародної науково-практичної конференції (м. Чернігів, 26–27 травня 2021 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів: НУ «Чернігівська політехніка», 2021. – Т. 2. – с. 162.
 17. V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Workshop on Cybersecurity

Providing in Information and Telecommunication Systems, vol. 2746 (2020) 23–32.

18. B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.

19. Yuliia Samoilenko, Yuliia Kostiuk. Cybersecurity of industrial control systems based on dial-up access // Захист інформації і безпека інформаційних систем: матеріали VIII Міжнар. наук.-техн. конф. – Львів: Видавництво Львівської політехніки, 2021. – с. 25-25.

20. Костюк Ю.В., Самойленко Ю.О. Моніторинг інформаційної безпеки в інформаційно-комунікаційних системах та мережах // Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці: Матеріали II Міжнародної науково-практичної конференції (м. Київ, 7 грудня 2021 року). К.: ДУІТ, ХНУРЕ. 2021. с. 670.

21. R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, vol. 3800 (2024) 97–105.

22. Костюк Ю. В., Левицький В. Ю. Система захисту передачі даних за допомогою інтернет-протоколів // Матеріали VIII Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами», 26 листопада 2021. [Електронний ресурс] – К: НУХТ, 2021 – с. 245-246.

23. L. Kriuchkova, V. Sokolov, P. Skladannyi, Determining the Zone of Successful Interaction in RFID Technologies, in IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (2024) 168–171.

24. Костюк Ю.В., Самойленко Ю.О. Кіберризика в системах управління безпекою на морському транспорті // International scientific conference «Maritime security of the Baltic-Black sea region: challenges and threats»: conference proceedings, December 23, 2021. Odessa: Izdevnieciba«Baltija Publishing», p.407.

25. V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

РОЗДІЛ 4

ПРОЦЕДУРИ ВПРОВАДЖЕННЯ ТА РЕАЛІЗАЦІЇ ПОЛІТИКИ БЕЗПЕКИ



4.1. Процедури реалізації політики безпеки

4.2. Оновлення ПЗ та зниження привілеїв

4.1. ПРОЦЕДУРИ РЕАЛІЗАЦІЇ ПОЛІТИКИ БЕЗПЕКИ

Процедури реалізації політики безпеки є важливим етапом у забезпеченні ефективного захисту інформаційних ресурсів та активів організації. Вони визначають кроки, необхідні для впровадження заходів безпеки, які були визначені у політиці безпеки, і гарантують належне виконання цих заходів на практиці. Однією з перших процедур є оцінка ризиків, яка передбачає регулярний аналіз потенційних загроз та уразливостей організації, а також визначення рівня ризику для кожного активу з урахуванням новітніх кіберзагроз, технологічних змін і змін у законодавстві.

Наступним кроком є розподіл відповідальностей, який передбачає чітке визначення ролей і обов'язків кожного співробітника в рамках реалізації політики безпеки. Це включає створення команд з управління безпекою, відповідальних за контроль за дотриманням політики та реагування на інциденти безпеки. Важливим етапом є також розробка та впровадження технічних заходів, таких як системи моніторингу, міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних та системи контролю доступу, що дозволяють забезпечити захист інформаційних систем і даних.

Не менш важливим є навчання персоналу, яке передбачає проведення тренінгів та семінарів, спрямованих на підвищення рівня обізнаності співробітників щодо політики безпеки, правил роботи з інформацією та правильного реагування на потенційні інциденти. Процедури реалізації політики безпеки включають також механізми моніторингу та аудиту, що дозволяють виявляти порушення політики та оцінювати ефективність заходів безпеки. Регулярний аудит безпеки дозволяє коригувати стратегії і вдосконалювати заходи безпеки, що застосовуються в організації.

Ключовим елементом є також розробка процедур для реагування на інциденти безпеки, зокрема для швидкого відновлення після інцидентів, таких як витік інформації або кібернапади. Ці процедури включають плани на випадок надзвичайних ситуацій, що забезпечують швидке реагування і мінімізацію шкоди. Процедури реалізації політики безпеки передбачають також необхідність постійного оновлення політики з урахуванням нових загроз, змін у технологічному середовищі та найкращих практик. Оновлення політики безпеки є частиною постійного процесу вдосконалення захисту організації, що дозволяє забезпечити актуальність і ефективність політики у довгостроковій перспективі.

Політика безпеки тільки описує, що має бути захищене і які основні правила захисту. Процедури безпеки визначають механізми виконання цих правил (покрокові інструкції). Наприклад, політика безпеки паролів формулює правила конструювання паролів, правила про те, як захистити пароль і як часто замінювати паролі. Процедура управління паролями, в свою чергу, описує процеси створення нових паролів, розподілу їх, а також гарантованої зміни паролів на критичних пристроях.

Багато процедур, пов'язаних з безпекою, повинні бути стандартними. Як приклади можна вказати процедури для резервного копіювання даних та позасистемного зберігання захищених копій, а також процедури для виведення користувача з активного стану і архівування його логіна і пароля.

Деякі важливі процедури безпеки, які необхідні майже кожній організації

Деякі важливі процедури безпеки, які необхідні майже кожній організації, включають процедуру створення та управління паролями, яка забезпечує контроль за складністю і зміною паролів для доступу до інформаційних систем, що гарантує, що тільки авторизовані користувачі можуть отримати доступ до конфіденційної інформації. Не менш важливим є впровадження процедури резервного копіювання даних, що

передбачає регулярне створення резервних копій для захисту від втрати даних у разі технічних збоїв чи атак, що дозволяє відновити критичну інформацію після катастрофи.

Процедура доступу до інформаційних систем є ще одним важливим елементом, який обмежує доступ користувачів до інформації на основі їхніх прав, що дозволяє чітко контролювати, хто може переглядати, змінювати або знищувати дані. Моніторинг безпеки є ключовим для своєчасного виявлення аномальних дій або спроб несанкціонованого доступу, за допомогою систем виявлення вторгнень та журналів аудиту, які фіксують всі важливі події та дозволяють оперативно реагувати на загрози. У разі інциденту безпеки, важливо мати розроблену процедуру реагування, яка визначає, як швидко зреагувати на інциденти, мінімізуючи їхні наслідки і відновлюючи систему після атак.

Процедура навчання персоналу забезпечує підвищення рівня обізнаності співробітників щодо безпеки, їхнього навчання використанню засобів захисту та розпізнаванню фішингових атак, що допомагає створити культуру безпеки в організації. Управління пристроями та програмним забезпеченням забезпечує контроль за встановленням і використанням програм, а також мобільних пристроїв, що може допомогти мінімізувати ризики, пов'язані з небажаними програмами або пристроями.

Процедура управління уразливостями передбачає регулярне сканування інформаційних систем для виявлення і усунення потенційних загроз, виявлених у програмному забезпеченні, а процедура контролю фізичного доступу визначає, як забезпечити безпеку приміщень і критичних інфраструктур, використовуючи системи контролю доступу. І нарешті, процедура виконання плану відновлення після катастроф допомагає організації швидко відновлювати свою діяльність після серйозних інцидентів, зберігаючи функціональність і цілісність інформаційних систем. Ці процедури є важливою частиною загальної стратегії безпеки організації та допомагають мінімізувати ризики, пов'язані з інформаційними загрозами.

Процедура управління персоналом

Процедура управління персоналом у контексті безпеки інформації передбачає відбір, навчання та контроль за діяльністю співробітників організації з метою забезпечення належного рівня захисту інформаційних ресурсів. Вона включає процеси рекрутування, перевірки кандидатів, ознайомлення персоналу з політиками безпеки, регулярне навчання щодо загроз кібербезпеки та процедур збереження конфіденційності. Також важливим аспектом є моніторинг виконання посадових обов'язків

співробітниками, перевірка дотримання вимог безпеки і застосування санкцій у разі порушення. Управління персоналом включає **підбір персоналу, прийом на роботу, звільнення і поточний контроль**. Кожне з перерахованих дій має відношення до безпеки.

При підборі працівників слід перевіряти минуле кандидатів, їх рекомендації, в деяких випадках потрібна додаткова перевірка професійних сертифікатів, кредитної історії, записів в базах даних про злочинців, інші більш ретельні перевірки.

У процедурі прийому на роботу має бути передбачено ознайомлення співробітника з правилами політики безпеки. Працівник повинен офіційно підтвердити свою згоду дотримуватися політики безпеки та нести відповідальність за її порушення, підписати угоду про нерозголошення конфіденційних даних.

Процедура звільнення є критичним етапом у забезпеченні безпеки організації, оскільки вона допомагає запобігти можливим інцидентам, пов'язаним із несанкціонованим доступом до конфіденційної інформації. Особливо важливо, щоб ця процедура була чітко визначена і виконувалася згідно з політиками безпеки.

Перш за все, необхідно негайно заблокувати доступ звільненого працівника до всіх облікових записів і систем, змінити паролі, а також заблокувати віддалений доступ до ресурсів організації. Крім того, потрібно провести інвентаризацію всього майна, яке може бути у володінні звільненого працівника, включаючи ноутбуки, телефони, флеш-накопичувачі та інші пристрої, що можуть містити чутливу інформацію.

Особлива увага повинна приділятися звільненим співробітникам, які мали доступ до критичних систем, зокрема системним адміністраторам. Для таких випадків має бути розроблена окрема процедура, яка включає додаткові заходи безпеки, зокрема проведення повного аудиту системи для виявлення будь-яких змін або несанкціонованих дій до моменту звільнення. Цей аудит допоможе виявити можливі загрози і забезпечити цілісність інформаційних систем організації.

Такий підхід дозволяє мінімізувати ризики, пов'язані з виходом працівників з організації, і захистити організацію від потенційних інцидентів, що можуть бути спричинені колишніми співробітниками.

Особливу увагу служба безпеки повинна приділяти процедурі звільнення, оскільки за статистикою велика кількість порушень політики безпеки здійснюється якраз особами, які втратили роботу. Кожен звільнений з негативних обставин являє собою загрозу розкриття конфіденційної інформації, до якої він мав допуск. Процедура звільнення

повинна включати негайно блокування всіх облікових записів, зміну паролів, блокування віддаленого доступу.

Особливо серйозна загроза виходить від звільненого системного адміністратора, в таких випадках повинна бути застосована спеціальна процедура, що включає крім звичайних заходів повний аудит системи.

Поточний контроль у процедурі управління персоналом є важливою частиною для забезпечення безпеки в організації. Він включає моніторинг режиму роботи співробітників, що дозволяє виявляти будь-які аномалії або порушення внутрішніх політик безпеки. Це може стосуватися як фізичного доступу до робочих місць (наприклад, використання карток доступу), так і контролю за робочими процесами через систему управління завданнями або моніторинг дій в інформаційних системах.

Окрім цього, поточний контроль охоплює моніторинг переміщення персоналу в межах організації, що важливо для запобігання несанкціонованому доступу до конфіденційної інформації або обладнання. Це також може включати перевірку відповідності дій співробітників встановленим стандартам безпеки та регулярну оцінку їх поведінки щодо дотримання правил конфіденційності та інформаційної безпеки.

Завдяки поточному контролю забезпечується раннє виявлення потенційних загроз або порушень, що дозволяє оперативно вжити необхідні заходи для їх усунення, підтримуючи безпеку організації на належному рівні.

До процедури управління персоналом також відноситься поточний контроль над режимом роботи і переміщенням персоналу. *Існує два загальних принципи*, які слід мати на увазі при поточному контролі:

- ❖ поділ обов'язків;
- ❖ мінімізація привілеїв.

▲ **Принцип поділу обов'язків** приписує як розподіляти ролі та відповідальність, щоб одна людина не могла порушити критично важливий для організації процес. Наприклад, небажана ситуація, коли великі платежі від імені організації виконує одна людина. Надійніше доручити одному співробітнику оформлення заявок на подібні платежі, а іншому – завіряти ці заявки. Інший приклад – процедурні обмеження дій супер-користувача ІКС. Можна штучно «розщепити» пароль супер-користувача, повідомивши першу його частину одному співробітнику, а другу – іншому. Тоді критично важливі дії по адмініструванню ІКС вони зможуть виконати лише вдвох, що знижує ймовірність помилок і зловживань.

▲ **Принцип мінімізації привілеїв** наказує виділяти користувачам тільки ті права доступу, що необхідні їм для виконання службових обов'язків. Призначення цього принципу очевидно – зменшити шкоду від

випадкових або навмисних некоректних дій. У кожній організації повинна бути розроблена процедура перегляду прав доступу співробітників при їх переміщенні всередині організації. До процедури управління персоналом також відноситься технічний контроль над режимом роботи і переміщенням персоналу.

Процедура реагування на події

Процедура реагування на події безпеки є ключовим елементом у забезпеченні захисту інформаційних систем і включає кроки, необхідні для виявлення, оцінки та усунення інцидентів безпеки. Вона передбачає оперативне виявлення аномальних чи підозрілих дій, фіксацію інциденту, аналіз та визначення рівня загрози. Після цього здійснюється коригувальна дія, яка може включати ізоляцію заражених систем, оновлення чи виправлення уразливостей, а також відновлення даних з резервних копій. Паралельно із реагуванням важливо вести детальне документування інциденту для подальшого аналізу і запобігання схожим ситуаціям у майбутньому. Після інциденту проводиться аналіз причин і вдосконалення політик та процедур безпеки для покращення захисту організації. Процедуру реагування на події іноді називають процедурою реагування на інциденти. Ця процедура має три головні цілі:

- ❖ локалізація інциденту і зменшення шкоди;
- ❖ виявлення порушника;
- ❖ попередження повторних порушень.

Процедури підтримки працездатності інформаційних систем

Процедури підтримки працездатності інформаційних систем включають комплекс заходів для забезпечення стабільної і безперебійної роботи систем, а також своєчасного реагування на технічні проблеми. Це включає регулярне технічне обслуговування і оновлення програмного забезпечення, виявлення і усунення уразливостей, моніторинг стану системи для виявлення потенційних проблем до того, як вони стануть критичними.

Крім того, важливо проводити резервне копіювання даних і перевірку відновлення для забезпечення відновлення інформації після катастроф або збоїв. У разі виникнення інцидентів або збою, процедури підтримки включають оперативне діагностування проблеми, локалізацію та відновлення працездатності системи. Постійний моніторинг і аудит допомагають у виявленні слабких місць у системах, що дозволяє проводити необхідні коригувальні заходи для забезпечення їх стабільності та захищеності.

Ненавмисні помилки системних адміністраторів користувачів і неналежне виконання інструкцій політики безпеки загрожують ушкодженню апаратури, руйнуванню програм і даних.

Можна виділити такі напрями діяльності:

- ❖ підтримка користувачів;
- ❖ підтримка програмного забезпечення;
- ❖ конфігураційне управління;
- ❖ резервне копіювання.

▲ ***Підтримка користувачів*** – навчання, консультування та надання допомоги при вирішенні різного роду проблем.

▲ ***Підтримка програмного забезпечення*** – складається з контролю за відсутністю неавторизованої зміни програм і прав доступу до них, а також своєчасного оновлення, особливо якщо оновлення стосується питань безпеки. Підтримка програмного забезпечення також включає моніторинг і виявлення потенційних уразливостей, що можуть бути використані зловмисниками для доступу до системи. Важливо, щоб усі використовувані програмні продукти мали сертифікацію безпеки та регулярно перевірялися на відповідність політикам організації. Окрім цього, необхідно забезпечити наявність резервних копій програмного забезпечення, щоб у разі інцидентів чи атак можна було швидко відновити систему. Всі дії з підтримки програмного забезпечення повинні фіксуватися для можливого аудиту та контролю.

▲ ***Конфігураційне управління*** дозволяє контролювати і фіксувати зміни в поточній конфігурації ІКС, надаючи можливість у випадку якихось модифікацій в системі повертатися до працюючої версії, наприклад після аварії. Цей процес забезпечує систематичний підхід до управління змінами, що допомагає уникнути непередбачених проблем і забезпечити стабільність інформаційної та комунікаційної системи. Конфігураційне управління також включає перевірку та тестування нових конфігурацій перед їх впровадженням, щоб мінімізувати ризик виникнення уразливостей. Воно передбачає створення і підтримку детальних записів про всі зміни, що дозволяє ефективно відстежувати історію модифікацій та проводити аудит. Збереження надійної і перевіреної конфігурації є основним елементом для забезпечення безпеки та стабільності ІКС. Процедура управління конфігурацією визначає:

- ➔ хто має повноваження виконувати зміни конфігурації апаратного та програмного забезпечення;
- ➔ як тестується і інсталюється нове апаратне та програмне забезпечення;

- ➔ хто повинен бути проінформований, коли вносяться зміни в апаратному та програмному забезпеченні;
- ➔ як документуються зміни в апаратному та програмному забезпеченні.

▲ **Резервне копіювання** необхідно для відновлення програм і даних після інцидентів. Потрібно налагодити періодичність резервного копіювання та розміщення копій в безпечному місці, захищеному від несанкціонованого доступу, пожеж, затоплень, тобто від всього, що може призвести до крадіжки або пошкодження носіїв. Доцільно мати кілька екземплярів резервних копій і частину з них зберігати поза територією організації, захищаючись таким чином від великих аварій і аналогічних інцидентів.

Приклад.

Щоб зрозуміти відмінності між політикою безпеки і процедурами безпеки, розглянемо наступний сценарій. Нехай компанія-виробник автомобілів бажає захистити проекти нових моделей від своїх конкурентів. Компанія вирішує обмежити доступ в ту будівлю, де розробляються моделі нових автомобілів, і пропускати туди тільки співробітників групи проектування.



Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials>

З цією метою пропонується використовувати зчитувач карток із магнітною смугою. Двері повинні автоматично відкриватися, коли співробітник групи проектування «прокатує» через пристрій-зчитувач свою ідентифікаційну картку, і автоматично закриватися на замок, коли співробітник закриває двері за собою.



Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials>

Компанія наймає за контрактом фахівця, який встановлює новий зчитувач карток протягом одного тижня, коли всі службовці компанії знаходяться на різдвяних канікулах. Він переносить необхідні дані про співробітників групи проектування на картки з магнітною смугою і розсилає по електронній пошті інструкції всім співробітникам додому. Інструкції описують, як відкрити двері за допомогою ідентифікаційної картки і зчитувача. Самі картки з магнітною смугою доставляються службовцям на домашню адресу поштою.



Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials>

У цьому прикладі компанія вибирає правильну політику безпеки, обмежуючи доступ до будівлі, де ведеться розробка нових моделей автомобілів.

Механізмом реалізації політики безпеки служить зчитувач карток. Процедури полягають у діях фахівця з кодування карток, розсилці кожному співробітнику повідомлень з інструкцією на його електронну адресу та доставку карток поштою на його домашню адресу. Проте не

можна сказати, що в результаті процес проектування нових моделей автомобілів буде добре захищений. Компанія має просту і розумну політику. Однак запропоноване поєднання механізмів і процедур – досить обмежена за коштами реалізація цієї політики. Даний механізм повністю не запобігає проникненню зломисника в будівлю, оскільки ідентифікує співробітників групи проектування тільки за ознакою володіння картою. Зломисник може увійти за власником картки, якщо той не зачинив за собою двері, або забезпечити собі доступ до будівлі, будь-яким чином отримавши ідентифікаційну картку співробітника, що має право доступу (наприклад, купивши у фахівця, який встановив зчитувач карток, додаткову картку або викравши картку при поштової розсилці).

Компанія могла б удосконалити реалізацію своєї політики, посилюючи механізми безпеки або процедури, або і те й інше разом.

1. Установка додаткового турнікета гарантувала б прохід до будівлі по кожній пред'явленій картці тільки одній людині.



Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials>

2. Використовуючи зчитувач з додатковою клавіатурою, компанія могла б вимагати від співробітників групи проектування для проходу в будівлю не тільки користуватися картою, а й вводити PIN-код. У цьому випадку завдання зломисника ускладнюється: щоб отримати можливість пройти в будівлю, необхідно дістати картку і дізнатися PIN-код користувача.

3. Наступним удосконаленням може бути додавання до зчитувача картки біометричного пристрою, тоді

зловмисникові потрібно відбиток пальця або малюнок сітківки ока працівника, який має право доступу.



Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials>

Але, навіть, якщо компанія не має можливості придбати нові засоби захисту, вона може підвищити безпеку, удосконаливши процедури.

По-перше, користувачів необхідно зобов'язати закривати за собою двері.

По-друге, можна розробити процедури доставки ідентифікаційних карток, що знижують ризик потрапляння картки в чужі руки.

По-третє, для кодування магнітних карток компанія може використовувати свою власну службу безпеки, а також видавати картки службовцям персонально після пред'явлення ними посвідчень особи за списком, поданим керівництвом компанії або сформованого відділом кадрів.

4.2. Оновлення ПЗ та зниження привілеїв

Оновлення програмного забезпечення (ПЗ) та зниження привілеїв є важливими процедурами для забезпечення інформаційної безпеки організації. Оновлення ПЗ є одним із основних способів захисту від нових загроз, таких як уразливості в програмному коді або відомі експлойти. Регулярне оновлення програмного забезпечення допомагає не лише виправляти виявлені уразливості, але й додавати нові функціональні можливості та підвищувати ефективність роботи системи.

Процедура оновлення ПЗ має бути частиною політики безпеки організації, і повинна включати перевірку на наявність оновлень, тестування оновлень на сумісність з існуючими системами та їхнє впровадження без порушення робочих процесів. Оновлення повинні здійснюватися відповідно до встановлених процедур, включаючи моніторинг успішності впровадження, контроль за відновленням систем після оновлення та своєчасне реагування на проблеми, які можуть виникнути після оновлення.

Зниження привілеїв – це принцип мінімальних прав доступу, який є важливою частиною стратегії безпеки. Користувачі і системи повинні мати лише ті права доступу, які необхідні для виконання їхніх функцій. Зниження привілеїв передбачає обмеження доступу до систем, даних та ресурсів для мінімізації можливостей для здійснення шкідливих дій. Це особливо важливо для обмеження доступу до чутливих даних і критичних систем організації.

Заходи щодо зниження привілеїв можуть включати створення політики доступу на основі ролей (RBAC), використання багатофакторної аутентифікації, обмеження прав адміністратора та регулярний перегляд доступу користувачів до різних ресурсів. В результаті, зниження привілеїв допомагає зменшити ймовірність того, що порушення безпеки стане результатом внутрішніх загроз або неправомірного доступу до інформації.

Ці два процеси — оновлення ПЗ та зниження привілеїв — є взаємодоповнюючими заходами, що допомагають організації забезпечити належний рівень безпеки та захисту від різноманітних загроз.

Яскравим прикладом використання організаційних заходів для підвищення безпеки ІКС є своєчасне оновлення ПЗ ІКС і зниження привілеїв користувачів *ІКС*.

Сучасне програмне забезпечення дуже складне і включає багато рядків коду, а тому дуже ймовірна наявність помилок (*багів*) в цьому коді, навіть після ретельної перевірки його роботи. Ці помилки можуть впливати на безпеку систем, де цей код використовується. За дослідженнями *SyLab університета Карнегі* кожні 1000 рядків коду мають 20–30 помилок, з яких 5 % впливають на безпеку, а 1 % відкриває можливості для зламу системи, тобто наслідками помилок у коді – є уразливість (*vulnerability*) системи. Деякі фахівці навіть вважають, що помилка в коді програми (баг) і уразливість це одне і те саме. Для мінімізації цих ризиків важливо здійснювати регулярні оновлення програмного забезпечення, яке включає виправлення виявлених уразливостей і багів. Оновлення повинні бути частиною системи безпеки і здійснюватися оперативно після випуску патчів розробниками. Програмні оновлення не лише усувають помилки, але й часто покращують захист від нових типів атак, що використовують раніше невідомі уразливості.

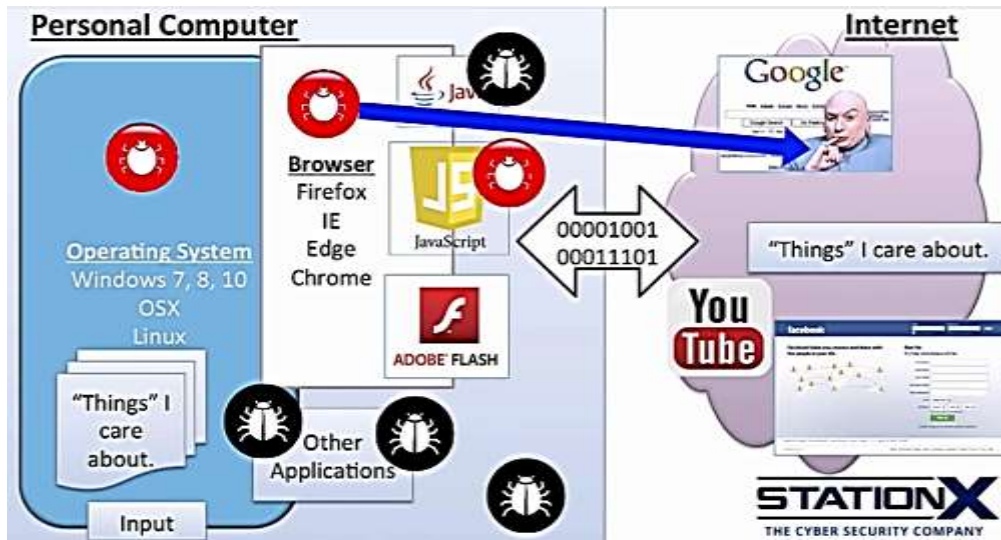


Рис. 4.1. Приклад уразливості в браузері

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Щоб забезпечити ефективне управління уразливостями, організації повинні застосовувати процеси тестування безпеки на етапі розробки ПЗ, а також проводити регулярний аудит та моніторинг існуючих систем. Важливою складовою є й автоматизація процесів виявлення уразливостей, наприклад, за допомогою інструментів сканування безпеки та аналізу коду, що дозволяє швидко виявляти і усувати проблеми на ранніх етапах.

Крім того, зниження привілеїв користувачів і застосування принципу "найменших прав" в доступі до системи також допомагають обмежити потенційний вплив помилок або уразливостей, оскільки навіть якщо злоумисник зможе скористатися багом у коді, обмежений доступ не дозволить йому нанести значної шкоди системі.

В якості окремої загрози, уразливість може перебувати в браузері. Під час відвідування вебсайта через такий браузер, спеціальний код на сайті може встановити шкідливе програмне забезпечення за допомогою цієї уразливості.

Уразливості системи можуть бути ще не виявленими (уразливості нульового дня, 0-day), відомими тільки теоретично, або ж загальновідомими, що активно використовуються злоумисниками. Уразливості нульового дня — це проблеми в безпеці програмного забезпечення або апаратного забезпечення, які ще не були виявлені або виправлені розробниками. Ці уразливості можуть бути використані злоумисниками до того, як розробники стануть обізнаними про їх існування і випустять відповідний патч або оновлення. Оскільки вони є

невідомими для виробника, такі уразливості не можуть бути захищені стандартними засобами безпеки, що робить їх особливо небезпечними. Уразливості нульового дня можуть бути дуже важкими для виявлення, оскільки вони не мають патчів чи оновлень, які б усували проблему. Це створює великий ризик для організацій, оскільки зловмисники можуть експлуатувати ці уразливості, щоб отримати несанкціонований доступ до систем або зламати їх. Іноді такі уразливості можуть бути використані в рамках складних атак, що включають кілька етапів, таких як впровадження шкідливого коду, ескалація привілеїв і збирання конфіденційної інформації. Оскільки на момент виявлення цієї уразливості немає захисту, важливо, щоб організації мали проактивні заходи для виявлення та моніторингу потенційних загроз. Вчасне виявлення таких уразливостей і застосування спеціальних засобів безпеки може мінімізувати шкоду від можливих атак. Для зниження ризиків потрібно також регулярно оновлювати програмне забезпечення і використовувати різноманітні методи захисту від атак, зокрема поведінкові та евристичні аналізи.



Рис. 4.2. Відомі і невідомі уразливості

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Інший тип уразливостей — це уразливості, які відомі теоретично, тобто дослідники або спеціалісти вже виявили слабкі місця в системах, але не всі з них можуть бути експлуатовані на практиці через відсутність відповідних інструментів чи знань. Однак, навіть такі уразливості можуть бути використані зловмисниками, коли вони розробляють нові методи атак або з'являються нові інструменти для їх експлуатації.

Загальновідомі уразливості — це ті, які були виявлені і опубліковані, що дозволяє зловмисникам легко знайти інформацію про них і використовувати ці знання для атак. Це особливо небезпечно, якщо організації або користувачі не оновлюють свої системи своєчасно, оскільки

такі уразливості можуть бути активно експлуатовані через застарілі версії програмного забезпечення, які не містять необхідних патчів безпеки.

Один із ключових способів боротьби з усіма типами уразливостей — це регулярне оновлення систем, моніторинг за новими загрозами і застосування виявлених патчів безпеки, а також використання системи управління уразливостями для оцінки і мінімізації ризиків від відомих і потенційних загроз.

Для загальновідомих уразливостей в програмних продуктах виробники регулярно випускають виправлення, звані патчами (*patch* – *латка*), і якщо пропатчити систему, подібні уразливості нейтралізуються. Патчі є важливими елементами стратегії безпеки, оскільки вони дозволяють закривати відомі уразливості, які можуть бути використані зловмисниками для проникнення в систему або викрадення даних. Застосування патчів має бути регулярним і своєчасним процесом. Затримка з їх впровадженням може призвести до серйозних наслідків для безпеки. Для автоматизації цього процесу багато організацій використовують інструменти для управління патчами, які дозволяють виявляти та швидко застосовувати оновлення без необхідності вручну перевіряти кожну систему. Це дозволяє знижувати ризики, пов'язані з використанням вразливих версій програмного забезпечення, і підвищує рівень загальної безпеки ІТ-інфраструктури.

Патч (латка) – це програмний код, який застосовується для модифікації або виправлення конкретної програми. Іншими словами, латка — це додаткова програма, яку необхідно запустити, коли в уже існуючому програмному забезпеченні виявлено помилку чи уразливість. Патчі дозволяють усувати дефекти, додавати нові функції або закривати уразливості без необхідності повністю переінсталювати програму.

Часто патч можна встановити без видалення основної програми, а також без завершення її роботи. Це особливо важливо для операційних систем та інших критичних програм, де безперервність роботи системи є важливою. Патчі можуть бути випущені розробниками для виявлених уразливостей або для поліпшення безпеки, тому регулярне їх застосування є важливим етапом у підтримці стабільної і безпечної роботи програмного забезпечення.

Патчінг – це вкрай важливий засіб забезпечення безпеки, який полягає в регулярному оновленні програмного забезпечення. Важливо оновлювати всі програмні додатки, фірмове ПЗ, операційні системи та інші компоненти ІТ-інфраструктури. Оновлення є ключовим етапом у нейтралізації виявлених уразливостей у програмному забезпеченні. Багато загрози безпеки виникають саме через використання застарілих версій програм, що містять відомі уразливості. Регулярне оновлення патчів допомагає забезпечити захист від атак, які використовують ці уразливості. Без своєчасного встановлення патчів організації можуть стати вразливими до кібератак, оскільки зловмисники активно використовують відомі уразливості в застарілих версіях програмного забезпечення. Крім того, патчінг допомагає підтримувати стабільну і безпечну роботу систем, запобігаючи збоям або витокам даних. Для ефективного управління патчами важливо мати налагоджений процес моніторингу і тестування оновлень перед їх впровадженням у робоче середовище.



Оновлення, пов'язані з нейтралізацією уразливості, називаються *оновленнями безпеки*.

Оновлення програмного забезпечення – це найважливіша річ, яку можна зробити для того, щоб залишатися захищеними в мережі.

Продукти, які найбільше потребують оновлення:

1. *Програми, які безпосередньо пов'язані з інтернетом:*

- браузері *Opera, Edge, Firefox, Chrome*;
- розширення браузерів і плагіни типу *Java, Flash, Silverlight*;
- поштові клієнти типу *Outlook* або *Thunderbird*, вони також важливі, оскільки безпосередньо взаємодіють з інтернетом.

Все це – найбільший вектор атаки.

2. *Додатки, які використовують, програють, переглядають файли різних форматів, які скачують з інтернету, або отримують з будь-яких неперевіраних джерел:*

- *Windows Media Player*, який програє фільми;
- *Adobe Reader*, який переглядає PDF-файли;
- програма для перегляду зображень формату JPEG;
- *Excel i Word*, які обробляють завантажені файли (макровіруси в *Excel* або *Word*).

3. *Операційна система.*

Це важливо, оскільки операційна система підтримує ключову складову вашого захисту, тому її також необхідно оновлювати.

В оновленні є потенційно негативна сторона. Не всі оновлення безпечні. Це нечасто трапляється, особливо у **Microsoft**, оскільки іноді **патч** виходить з іншим **багом**, що може призвести до проблем працездатності. Тому перед впровадженням оновлень необхідно проводити тестування в контрольованому середовищі, щоб оцінити їхній вплив на систему. Оновлення можуть також конфліктувати з іншими програмами або налаштуваннями, що може призвести до непередбачених наслідків. Крім того, іноді виправлення у патчах можуть не усувати всі уразливості або вводити нові, що вимагає додаткових перевірок і моніторингу після оновлення. Таким чином, процес оновлення має бути частиною більш широкої стратегії управління ризиками і безпекою, щоб уникнути негативних наслідків.



ВАЖЛИВО!!!

- 1. Якщо втрачаєте з поля зору питання установки патчів, то питання, зламують систему чи ні, навіть не виникає, це лише питання часу.*
- 2. Забудьте про налаштування безпеки, якщо не виконується оновлення операційної системи.*

«Вівторок патчів» — це неофіційна назва регулярного оновлення безпеки від Microsoft, яке публікується кожного місяця. Оновлення виходять у другий вівторок місяця, а іноді, в окремих випадках, також можуть бути випущені в четвертий вівторок. Ці оновлення часто включають виправлення уразливостей безпеки, які можуть бути використані зловмисниками для атак, а також покращення стабільності та функціональності програмних продуктів Microsoft. Це важлива подія для адміністраторів та користувачів, оскільки своєчасне встановлення таких оновлень є ключовим елементом підтримки належного рівня безпеки інформаційних систем. Крім того, кожне оновлення містить критичні патчі, які усувають відомі уразливості та знижують ризик кібератак. Для зручності користувачів і адміністраторів Microsoft часто публікує детальну інформацію про зміни в оновленнях, щоб вони могли оцінити їх вплив на інфраструктуру та забезпечити належну сумісність. Зважаючи на важливість таких оновлень, рекомендується автоматизувати процес їх встановлення, щоб уникнути людського фактора і забезпечити максимальний рівень захисту. Ігнорування "Вівторка патчів" може призвести до того, що система залишатиметься вразливою до відомих загроз, що активно використовуються зловмисниками.

Бюлетень з безпеки від Microsoft

Бюлетень з безпеки від Microsoft – це офіційна документація, що публікується компанією Microsoft для інформування користувачів про виявлені уразливості у програмних продуктах і сервісах компанії, а також про оновлення безпеки для усунення цих уразливостей.

Основні характеристики бюлетеня з безпеки від Microsoft:

1. Опис проблеми

Бюлетень містить інформацію про знайдену уразливість, її потенційний вплив на системи користувачів та можливі сценарії експлуатації.

2. Рівень важливості

Microsoft класифікує уразливості за рівнем критичності, наприклад:

- **Критичний (Critical)** - може призвести до серйозних наслідків, таких як несанкціонований доступ або виконання коду.
- **Високий (Important)** - значний ризик для даних або конфіденційності.
- **Помірний (Moderate)** - менш серйозні наслідки, але можуть викликати незручності.
- **Низький (Low)** - мінімальний ризик.

3. Продукти, які зачіпає уразливість

У бюлетені чітко зазначено, які версії операційних систем, програмного забезпечення чи хмарних сервісів Microsoft зазнали впливу.

4. Рекомендації щодо оновлення

Microsoft надає деталі про оновлення безпеки, які потрібно встановити для усунення уразливостей. Оновлення можуть бути доступні через:

- **Windows Update**
- **Microsoft Update Catalog**
- **WSUS (Windows Server Update Services)**

5. Технічні деталі

У бюлетені наводяться технічні аспекти уразливості, включаючи її тип (наприклад, переповнення буфера, SQL-ін'єкція, уразливість віддаленого виконання коду), а також інформація для фахівців з кібербезпеки.

6. Можливі способи захисту до встановлення оновлення

Якщо виправлення ще недоступне, Microsoft може надати тимчасові заходи, які користувачі можуть застосувати для захисту. Наприклад, відключення певних функцій або зміну налаштувань безпеки.

Як отримати бюлетені з безпеки?

- **Офіційний сайт Microsoft**

Бюлетені доступні на сторінці [Microsoft Security Update Guide](#).

- **Розсилка від Microsoft**

Користувачі можуть підписатися на сповіщення про нові бюлетені.

- **Інструменти адміністрування**

Наприклад, через Центр адміністрування Microsoft Defender для корпоративних користувачів.

Приклад інформації з бюлетня

- **Код уразливості** - CVE-2025-XXXXX
- **Продукти** - Windows 11, Microsoft Office 365, Azure.
- **Тип** - уразливість віддаленого виконання коду.
- **Критичність** - критична.
- **Рішення** - встановлення оновлення KBXXXXXX.

Регулярне ознайомлення з бюлетенями з безпеки Microsoft є важливим кроком для підтримання захищеності систем і даних.

Приклад:

Адреса *Бюлетеня з безпеки від Microsoft*:

<https://technet.microsoft.com/en-us/security/bulletin/dn602597.aspx>,

де можна побачити останні оновлення безпеки.

В цьому бюлетені: *KB* – номер оновлення; *CVE* – номер уразливості.

Якщо вибрати конкретний *патч (KB3089656)*, то помітимо, яку проблему він заклав, побачимо *CVE* з певним номером (*CVE-2019-2507*). Якщо натиснути на цей номер, то потрапимо на сайт з типовими уразливостями і помилками конфігурації. На цьому сайті зазначено, що дана уразливість була виявлена групою *Hacking Team*, вони використовували цей *баг* для зламу комп'ютерів.

Якщо зайти на сайт *CVE Details* по даній уразливості, то можна побачити, що вона особливо небезпечна. Оцінка за загальною системою уразливостей *CVSS* – *9.3*. «Дозволяє віддаленим атакуючим виконувати довільний код».



Подібні уразливості з віддаленим запуском довільного коду або переповненням буфера особливо небезпечні. Всі уразливості, які оцінюються як критичні, отримують цю оцінку обґрунтовано, і їх обов'язково потрібно виправляти за допомогою *патчів*.

Деталі уразливостей всіх типів програмного забезпечення та операційних систем можна знайти на сайтах:

www.cve.mitre.org

<https://nvd.nist.gov>

<https://www.cvedetails.com>

Підвищення безпеки системи за допомогою організаційних заходів

Підвищення безпеки системи за допомогою організаційних заходів передбачає створення ефективної структури управління, яка охоплює всі аспекти захисту інформаційних ресурсів. Основним елементом є розробка і впровадження політики безпеки, яка визначає чіткі стандарти для управління доступом до інформаційних систем і встановлює правила роботи з даними, їх зберігання, передачу і захист. Це дозволяє організації мінімізувати ризики і забезпечити належний контроль за безпекою. Важливим аспектом є також впровадження системи контролю доступу, що обмежує доступ до чутливої інформації лише авторизованим особам. Регулярна перевірка прав доступу та моніторинг користувачів допомагають вчасно виявити підозрілі дії. Одним із важливих заходів є навчання співробітників з основ безпеки, що дозволяє підвищити їх обізнаність та зменшити ймовірність людських помилок, які можуть призвести до витоків або пошкодження даних. Окрім того, організація повинна розробити плани реагування на надзвичайні ситуації, що включають інциденти з компрометацією даних. Це дозволяє оперативно реагувати на загрози та мінімізувати їх наслідки. Постійний моніторинг та аудит безпеки також є важливими процедурами, які дозволяють виявити аномальні дії та своєчасно на них реагувати. Регулярне оновлення програмного забезпечення і патчінг є необхідними заходами для усунення відомих уразливостей у системах. Чітке визначення відповідальних осіб за безпеку гарантує виконання політики та контролює відповідність усіх процедур безпеки. Всі ці організаційні заходи формують комплексний підхід до забезпечення безпеки системи, поєднуючи технічні рішення з ефективним управлінням і контролем.

Другим надзвичайно ефективним способом підвищення безпеки системи за допомогою організаційних заходів є зниження дефолтних привілеїв користувачів системи. Це допоможе стримати шкідливий код або атакуючого, оскільки вони користуються рівнем привілеїв заложененого користувача. **Обмеження привілеїв** – це стандартний підхід в *Linux* і *Unix-подібних операційних системах*, де обліковий запис адміністратора або *root-аккаунт* – *superuser* використовуються рідко. Проте в *Windows* це не так. Адміністраторські привілеї для користувача стоять за замовчуванням при інсталяції ОС. Адміністратори можуть міняти параметри безпеки, установлювати програмне забезпечення й устаткування, а також мають доступ до всіх файлів на комп'ютері.

Хоча обліковий запис адміністратора дозволяє повністю контролювати комп'ютер, використання стандартного облікового запису

користувача може сприяти забезпеченню більш високого рівня безпеки комп'ютера. Тому що інші особи, діставши доступ до комп'ютера, на якому користувач увійшов до системи зі стандартним обліковим записом, не зможуть зіпсувати параметри безпеки комп'ютера. Тому для підвищення рівня безпеки в *Windows* потрібно для постійної роботи використовувати тип облікового запису – звичайного користувача, а обліковий запис адміністратора використовувати епізодично, тільки в разі потреби.

Забезпечення максимальної безпеки комп'ютера

Для забезпечення максимальної безпеки комп'ютера рекомендується увімкнути контроль облікових записів користувачів (UAC). Контроль облікових записів допомагає запобігти несанкціонованим змінам у системі, які можуть бути здійснені шкідливими програмами або неправомірними діями. При спробі внести зміни, що вимагають прав адміністратора, UAC виводить діалогове вікно з відповідним повідомленням. Якщо користувач працює під обліковим записом без прав адміністратора, система запитує пароль адміністратора для підтвердження змін. Це дозволяє заблокувати виконання дій, які не були схвалені користувачем, і захищає систему від потенційних загроз.

Для ефективного використання UAC важливо перевіряти джерело запиту перед введенням пароля адміністратора. Завжди переконуйтесь, що запит є законним і стосується програм або дій, яким ви довіряєте. Не вводьте пароль сліпо — зверніть увагу на назву програми чи дії, що викликала запит. У разі сумнівів скасуйте дію та перевірте систему на наявність шкідливого програмного забезпечення. Для щоденних завдань рекомендується працювати під обліковим записом з обмеженими правами, щоб мінімізувати ризик несанкціонованих змін.

Увімкнути або налаштувати UAC можна, відкривши налаштування контролю облікових записів. Для цього потрібно натиснути Win + S, ввести "uac" і вибрати пункт "Змінити параметри контролю облікових записів користувачів". У діалоговому вікні слід вибрати рівень сповіщень. Рекомендований рівень — другий згори: "Сповіщати мене тільки тоді, коли програми намагаються внести зміни в мій комп'ютер". Після вибору параметрів необхідно натиснути "ОК" і, якщо це потрібно, ввести пароль адміністратора.

Додатково для підвищення безпеки комп'ютера слід використовувати антивірусне програмне забезпечення, регулярно оновлювати бази даних вірусів, підтримувати актуальність операційної системи та програм, створювати складні паролі для облікових записів і періодично їх змінювати. Якщо це можливо, варто налаштувати

двофакторну аутентифікацію. Регулярна перевірка комп'ютера на наявність загроз за допомогою інструментів для сканування безпеки також є важливим кроком. Дотримання цих рекомендацій дозволить забезпечити високий рівень захищеності комп'ютера.



Відповідно до щорічного звіту про уразливість продуктів Microsoft від Avesto, видалення адміністративних привілеїв у користувача в Windows дійсно призводить до зупинки 86% всіх загроз, пов'язаних з операційною системою. Цей показник підкреслює важливість правильної організації прав доступу в межах операційної системи. Замість використання адміністративних облікових записів для повсякденної роботи, набагато безпечніше використовувати звичайні облікові записи користувачів. Оскільки багато зловмисних атак спрямовані на отримання адміністративних прав для контролю над системою, обмеження таких прав дозволяє значно знизити ймовірність успішних атак.

Щоб забезпечити більшу безпеку в Windows-системах, рекомендується:

1. Використовувати принцип найменших привілеїв (Least Privilege Principle), тобто надавати користувачам тільки ті права, які необхідні для виконання їхніх обов'язків.
2. Активно застосовувати технології обмеженого доступу, такі як User Account Control (UAC), для підвищення контролю над адміністративними правами.
3. Регулярно оновлювати операційну систему та програми для захисту від нових уразливостей.
4. Використовувати багаторівневу аутентифікацію (наприклад, двофакторну), щоб зменшити ризик несанкціонованого доступу.

Така стратегія дозволяє значно знизити потенційні загрози та покращити загальний рівень безпеки в організації чи на окремому комп'ютері.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 4

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.

2. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

3. Костюк Ю.В., Самойленко Ю.О., Костюк І.В. Особливості захисту конфіденційної інформації в професійному інформаційному середовищі // Інформація та документ у сучасному науковому дискурсі: матеріали VII

Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.). Івано-Франківськ: ІФНТУНГ, 2022. с. 59-63.

4. Даник Ю. Г., Воробієнко П. П., Чернега В. М. (2019) Основи кібербезпеки та кібероборони: підручник. 2-ге вид., перероб. і доп. Одеса: ОНАЗ ім. О. С. Попова. 320 с.

5. S. Shevchenko, et al., Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 333–342.

6. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.

7. V. Buhas, et al., AI-Driven Sentiment Analysis in Social Media Content, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 (2024) 12–21.

8. Костюк Ю.В., Самойленко Ю.О., Костюк І.В. Захист інформації в корпоративній інформаційній системі на основі інтелектуальних технологій // Інноваційні технології ХХІ століття: зб. наук. пр. / гол. ред. Л. Г. Білий. Хмельницький : Вид-во МАУП, 2022. Вип. 7. С. 85-93.

9. P. Anakhov, et al., Hybrid Study of the Geophysical Situation in the Depressed Zone of Hydroelectric Power Plants Reservoir, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 269-274.

10. Костюк Ю.В., Самойленко Ю.О., Костюк І., Ковальова Л.І. Використання коригуючих кодів для інформаційного захисту комп'ютерних мереж // Тези доповідей дев'ятої міжнародної науково-практичної конференції «Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. // Відповідальна за випуск завідувач кафедри ІТ С.В. Цюцюра, – К.: КНУБА, 2022. – С. 69-70.

11. D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II-2, vol. 3188 (2021) 135–148.

12. V. Buhas, et al., Cybersecurity Role in AI-Powered Digital Marketing, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 (2024) 1–11.

13. Костюк Ю.В. Контроль інцидентів інформаційної безпеки в корпоративній телекомунікаційній мережі // Управління та адміністрування в умовах протидії гібридним загрозам національній

безпеці: Матеріали III Міжнародної науково-практичної конференції (м. Київ, 22 листопада 2022 року). К.: ДУІТ, ХНУРЕ. 2022.- с. 518-520.

14. G. Otto, et al., Parametric Model of a Laser with External Distributed Feedback in the System of Remote Measurement of Nanovibrations, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3421 (2023) 284–292.

15. Криворучко О.В., Костюк Ю.В. Інтелектуальне управління мережевою безпекою в інформаційно-телекомунікаційних системах // Міжнародна наукова конференція «Інтелектуальні Транспортні Системи: Екологія, Безпека, Якість, Комфорт». – К.: НТУ, 2022, Вип. 1 – с 86-87.

16. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.

17. Костюк Ю.В., Самойленко Ю.О. Трансформація загроз економічній безпеці держави // Всеукраїнська науково-практична конференція за міжнародною участю «Сучасні тенденції та суперечності розвитку світової економіки та бізнесу»: збірник матеріалів конференції, м. Київ, 25 січня 2022 р. / ред. кол.: І. А.Семенець-Орлова (гол. ред.), І. І. Каліна (заст. гол. ред), Ю. В. Мазур (упоряд. і відп. ред.) та ін. Київ: Міжрегіональна Академія управління персоналом, 2022. С. 239-241.

18. S. Kulibaba, et al., Linked System of Data Organization and Management, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 117–126.

19. K. Tkachenko, et al., Ontological Approach in Modern Educational Processes, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 88–97. Костюк Ю.В., Самойленко Ю.О. Проблеми захисту корпоративних інформаційно-телекомунікаційних мереж // Сучасні тенденції розвитку фінансових та інноваційно-інвестиційних процесів в Україні. Матеріали V Міжнародної науково-практичної конференції 25 лютого 2022 року : збірник наукових праць [Електронний ресурс]. – Вінниця: ВНТУ, 2022. – с. 781-783.

20. Y. Dreis, et al., Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection, in: Cyber Security and Data Protection, vol. 3800 (2024) 1–11.

РОЗДІЛ 5 УПРАВЛІННЯ РИЗИКАМИ



- 5.1. Підходи до аналізу ризиків безпеки ІКС**
- 5.2. Реалізація змішаного підходу до аналізу ризиків**
- 5.3. Оцінювання ризиків**
- 5.4. Типові витрати на забезпечення безпеки ІКС**

5.1. Підходи до аналізу ризиків безпеки ІКС

Перед початком будь-якої діяльності, пов'язаної з аналізом ризиків, підприємство має розробити чітку стратегію, що визначає основні принципи, методи та технології її реалізації. Ця стратегія повинна бути інтегрована в методику забезпечення інформаційної безпеки підприємства та враховувати специфіку його діяльності. Засоби й критерії вибору методів аналізу ризиків мають узгоджуватись із вимогами підприємства, забезпечуючи адаптацію підходів до реального середовища. Стратегія повинна гарантувати, що зусилля з інформаційного захисту спрямовані саме туди, де вони необхідні найбільше.

Аналіз усіх інформаційних систем без урахування пріоритетів є неефективним. Оптимальний підхід передбачає спочатку високорівневий аналіз ризиків, здійснюваний керівниками підприємства, для визначення критичних точок, а вже потім – детальне дослідження зосереджене на системах, які мають підвищений рівень ризику. Потреби в захисті залежать від розміру підприємства, його галузевої специфіки, регуляторного середовища та внутрішньої політики безпеки.

У деяких випадках підприємство може прийняти рішення про тимчасове зупинення впровадження засобів захисту. Такі рішення повинні прийматися

лише після детального аналізу потенційних ризиків, їх серйозності та ймовірності виникнення небажаних інцидентів. Ігнорування цих аспектів може призвести до порушення законодавства, репутаційних втрат або суттєвих фінансових збитків.

Методика аналізу ризиків може ґрунтуватися на чотирьох основних підходах. Перший підхід передбачає застосування єдиного стандартного підходу до всіх систем. Він мінімізує витрати на детальний аналіз, забезпечуючи базовий рівень захисту. Проте цей підхід може бути недостатньо ефективним, якщо рівень загроз значно відрізняється між системами.

Другий підхід базується на неформальному аналізі ризиків, що спирається на досвід і знання фахівців. Цей підхід є швидким і недорогим, але має низку недоліків, таких як суб'єктивність оцінок, відсутність формалізованого підходу та можливість пропустити критичні ризики.

Третій підхід передбачає докладний аналіз усіх систем, що дозволяє ідентифікувати активи, оцінити загрози та уразливості, а також розробити відповідні засоби захисту. Хоча цей підхід є найбільш ґрунтовним, він вимагає значних ресурсів і часу.

Четвертий підхід комбінує елементи перших трьох і починається з високорівневого аналізу ризиків для виявлення найбільш критичних систем. Далі для таких систем проводиться детальний аналіз, а для інших застосовується базовий захист. Цей підхід є збалансованим, забезпечуючи оптимальне співвідношення між витратами часу, ресурсами та ефективністю захисту.

Вибір конкретного підходу залежить від особливостей підприємства, його ресурсів і стратегічних пріоритетів. У будь-якому випадку, для забезпечення ефективної інформаційної безпеки, важливо, щоб адміністрація розуміла потенційні наслідки своїх рішень. Пасивність або відкладання впровадження заходів захисту можуть призвести до суттєвих загроз, які вплинуть не лише на діяльність підприємства, але й на його репутацію. Тому аналіз ризиків повинен бути частиною комплексної стратегії управління інформаційною безпекою.

Ризики безпеки інформаційно-комунікаційних систем (ІКС) є ключовим аспектом управління інформаційною безпекою в організаціях, адже з кожним роком технології стають все більш складними, а кількість загроз — значно зростає. Цей підхід часто застосовується в ситуаціях, коли ймовірність реалізації ризику є низькою або потенційні збитки від нього є незначними в порівнянні з витратами на запобігання. Прийняття ризику вимагає чіткої оцінки та розуміння можливих наслідків для організації, а також постійного моніторингу цього ризику на випадок зміни умов. Це дозволяє заощадити ресурси, які можна спрямувати на інші, більш критичні напрямки безпеки. Однак важливо

розуміти, що прийняття ризику не означає повну бездіяльність, а лише обґрунтоване зважування витрат і вигод від захисту.

Основні типи ризиків, які можуть вплинути на безпеку ІКС:

✓ **По-перше,** важливим ризиком є несанкціонований доступ до інформації, який порушує конфіденційність даних. Це може статися через використання слабких паролів або їх крадіжку, а також через злом облікових записів користувачів за допомогою фішинг-атак або методів соціальної інженерії. Такі випадки можуть призвести до витоку чутливої інформації та серйозних фінансових і репутаційних втрат для організації. Тому вкрай важливо використовувати облікові записи з мінімальними правами доступу, які обмежують можливість доступу до конфіденційних даних.

✓ **По-друге,** ще одним серйозним ризиком є витік даних. Це може статися через неправильно налаштовані права доступу до файлів чи баз даних або через використання ненадійних зовнішніх каналів передачі даних. Витік даних також може бути результатом крадіжки або втрати фізичних носіїв інформації, що містять чутливу інформацію. Важливо впроваджувати суворі політики контролю доступу та шифрування даних для захисту від таких загроз.

Ризики мережевих атак є ще однією важливою категорією. Атаки типу "Denial of Service" (DoS) або "Distributed Denial of Service" (DDoS), а також поширення шкідливих програм, таких як віруси, трояни або руткіти, можуть серйозно порушити роботу інформаційних систем. Такі атаки можуть призвести до блокування доступу до ресурсів або пошкодження даних, що вимагає швидкого реагування та впровадження ефективних засобів захисту, таких як брандмауери і системи виявлення вторгнень (IDS).

Не менш важливими є ризики, пов'язані з внутрішніми загрозами. Вони виникають через помилки або навмисні дії співробітників організації, які мають доступ до чутливої інформації. Такі загрози можуть включати неправомірний доступ до даних або їх зміну, що може бути спричинено як недбалістю, так і навмисними порушеннями з боку працівників. Для запобігання таким загрозам необхідно регулярно проводити навчання співробітників, впроваджувати багаторівневі механізми контролю доступу та аудиту, а також забезпечувати надійний моніторинг діяльності користувачів.

Фізична безпека також є важливою складовою ризиків безпеки ІКС. Неавторизований доступ до серверних приміщень або втрата фізичних носіїв даних може призвести до серйозних наслідків, тому важливо вживати заходів для обмеження доступу до фізичних ресурсів та зберігання носіїв з чутливою інформацією в безпечних умовах.

Ще одним ризиком є недоліки в управлінні інцидентами та відновленням після катастроф. Невизначеність у тому, як реагувати на інциденти або відновити систему після атаки чи технічного збою, може призвести до тривалих перерв у роботі організації. Тому необхідно мати чіткі плани реагування на інциденти та відновлення, а також регулярно перевіряти їх ефективність через тренування та тестування.

Загрози, пов'язані з оновленням програмного забезпечення та патчами, також є важливими. Оскільки програмне забезпечення постійно розвивається, в ньому можуть з'являтися нові уразливості, які можуть бути використані зловмисниками. Тому важливо регулярно оновлювати програмні продукти, встановлювати патчі та перевіряти їх на наявність уразливостей.

І, нарешті, ризики, пов'язані з використанням хмарних технологій, також набувають актуальності. Використання хмарних сервісів може викликати питання щодо безпеки та конфіденційності даних, що зберігаються в хмарі. Оскільки дані часто знаходяться під контролем сторонніх постачальників послуг, важливо забезпечити належний рівень захисту та виконання вимог безпеки для запобігання витоку або втрати інформації.

Таким чином, для забезпечення належного рівня безпеки ІКС необхідно застосовувати комплексний підхід, включаючи впровадження належних механізмів захисту, навчання співробітників, моніторинг систем і регулярне оновлення програмного забезпечення для мінімізації ризиків і захисту від потенційних загроз.

Абсолютна безпека ІКС не може бути забезпечена ніякими засобами: завжди є вірогідність появи нових помилок і проведення нових атак з боку зловмисників. При достатній кількості часу зловмисники можуть подолати будь-який захист. Тому всі прийняті заходи захисту ІКС можуть тільки знизити ймовірність негативних впливів або збиток від них, але не виключити їх повністю.



Виходячи з цього, метою забезпечення безпеки ІКС є мінімізація збитків.

Суб'єктами нанесення шкоди урешті-решт завжди є люди. Навіть, якщо постраждають матеріальні об'єкти або інформаційні ресурси, збиток (непрямий) у результаті буде заподіяно людям, які пов'язані з цими об'єктами або зацікавленим в їх збереженні і цілісності.

Аналіз ризиків

Аналіз ризиків є важливим етапом у забезпеченні безпеки інформаційно-комунікаційних систем (ІКС), який полягає в ідентифікації, оцінці й управлінні можливими загрозами. Його мета — виявити

потенційні небезпеки, оцінити ймовірність їх виникнення та наслідки для системи і, в кінцевому рахунку, впровадити заходи для мінімізації або нейтралізації цих загроз. Перший етап аналізу полягає в ідентифікації ризиків, які можуть вплинути на інформаційні системи. До таких загроз відносяться як уразливості в програмному забезпеченні, так і людські помилки чи навмисні дії співробітників, а також фізичні загрози, наприклад, стихійні лиха або пожежі.

Після виявлення ризиків наступним кроком є оцінка ймовірності їх виникнення та потенційного впливу на функціонування організації. Для цього використовуються як якісні методи, так і кількісні, зокрема статистичний аналіз або моделювання. Оцінка ризиків допомагає зрозуміти, які загрози мають найбільшу ймовірність та який вплив можуть мати на організацію. Одна з популярних методик для класифікації ризиків — це використання матриці ризиків, де оцінюються ймовірність і рівень впливу кожного ризику. На основі цієї оцінки ризики можна ранжувати за ступенем критичності.

Наступним етапом є управління ризиками, яке включає розробку стратегії для їх зниження або нейтралізації. Залежно від природи ризиків, для кожного з них можуть бути застосовані різні стратегії: уникнення, зниження, передача чи прийняття ризику. Уникнення ризику передбачає вжиття заходів для повного усунення загрози, наприклад, шляхом відмови від використання вразливого програмного забезпечення. Зниження ризику полягає в мінімізації ймовірності або наслідків загрози, що може бути досягнуто, наприклад, через оновлення програмного забезпечення або впровадження додаткових засобів захисту. Якщо загроза є невідворотною або недостатньо значною, може бути обрано рішення про її прийняття або перекладання відповідальності на зовнішніх постачальників за допомогою страхування чи аутсорсингу.

Важливим етапом є моніторинг ризиків та перегляд стратегії управління ними. Це дозволяє організації адаптуватися до змін у технологічному середовищі, нових загрозах або змін у структурі самої організації. Регулярний моніторинг забезпечує своєчасне виявлення нових загроз і необхідність коригування існуючих планів безпеки. Моніторинг ризиків і перегляд стратегій управління ними є важливим елементом постійного вдосконалення системи управління безпекою. З появою нових технологій, таких як штучний інтелект, блокчейн, або розширення використання хмарних рішень, організації повинні адаптувати свої стратегії для ефективної боротьби з новими типами кіберзагроз. Регулярний перегляд та оновлення політик безпеки також включає врахування змін у законодавстві та нормативних вимогах, що мають

прямий вплив на процеси захисту даних. Цей підхід забезпечує не лише зниження потенційних ризиків, але й підвищує загальну стійкість організації до кіберзагроз.

До інструментів і методів, що використовуються для оцінки і управління ризиками, належать методи аналізу загроз і уразливостей (TVA), аналіз критичності бізнес-процесів (BIA), метод FMEA (Failure Modes and Effects Analysis), а також методика FAIR (Factor Analysis of Information Risk), яка дозволяє оцінювати фінансові наслідки ризиків. Застосування таких методик дозволяє комплексно підходити до оцінки ризиків, забезпечуючи більш точне та обґрунтоване прийняття рішень. Окрім традиційних методів, все більш актуальними стають підходи, що включають використання великих даних (Big Data) та штучного інтелекту для автоматизації процесу оцінки та прогнозування ризиків. Наприклад, аналіз даних у реальному часі з використанням алгоритмів машинного навчання дозволяє виявляти нові, непередбачувані загрози та швидко реагувати на зміни в кіберсередовищі. Інтеграція цих технологій у процеси управління ризиками значно підвищує ефективність виявлення і зменшення впливу потенційних загроз. У результаті організації можуть швидше адаптуватися до нових умов та забезпечити стійкість своїх інформаційних систем.

Таким чином, аналіз ризиків є основою для створення ефективної стратегії безпеки ІКС. Він дозволяє своєчасно виявляти загрози, оцінювати їх можливий вплив та розробляти заходи для їх нейтралізації. Безперервний моніторинг і постійна адаптація до нових умов забезпечують надійний захист організації від інформаційних та кіберзагроз.

Оцінку можливих збитків надає аналіз ризиків. Останній полягає в тому, щоб виявити існуючі загрози і уразливості, оцінити їх небезпеку, тобто оцінити можливі втрати і потенційні збитки, які компанія може понести у разі реалізації будь-якої з цих загроз і забезпечити економічний баланс між шкодою від впливу загроз і вартістю контрзаходів. Аналіз ризиків також включає прогнозування сценаріїв розвитку подій, що допомагає визначити ймовірність виникнення загроз та їх потенційний вплив на діяльність організації. Для цього використовуються моделі оцінки впливу, які враховують різноманітні фактори, такі як фінансові втрати, репутаційні збитки та юридичні наслідки. Сучасні інструменти для оцінки ризиків дозволяють враховувати фактори, які раніше не мали належної уваги, зокрема, кіберзагрози, атаки з використанням штучного інтелекту та вплив кліматичних змін. Таким чином, результатом оцінки є не лише виявлення загроз, але й ефективне розподілення ресурсів для зменшення ризиків і підвищення стійкості організації до можливих кризових ситуацій.

Кроки процесу аналізу ризиків

Крок 1. Визначити цінність активів.

Визначення цінності активів є важливим етапом у процесі управління ризиками, оскільки це дозволяє організації оцінити, скільки коштують її інформаційні, фінансові та матеріальні ресурси. Цінність активів визначається з урахуванням їх значущості для функціонування організації, можливих втрат при їх пошкодженні або втраті, а також їх впливу на бізнес-процеси. Цінність активу можна оцінити за кількома підходами: фінансовий підхід, який передбачає оцінку вартості активу на основі його ринкової вартості або вартості заміщення, включаючи матеріальні активи, такі як комп'ютерне обладнання, сервери, будівлі або інші засоби; операційний підхід, що оцінює важливість активу для підтримки критичних бізнес-процесів, таких як сервери, бази даних або програмне забезпечення, втрата яких може суттєво вплинути на роботу організації; репутаційний підхід, що враховує значення активів з точки зору репутації організації, наприклад, інформаційні ресурси або інтелектуальна власність, які можуть використовуватися для підтримки іміджу компанії; а також інтерпретацію юридичних і нормативних вимог, яка оцінює активи, що підлягають регулюванню за законами або нормативними актами, такими як медичні дані або фінансова інформація, що потребують особливого захисту згідно з вимогами стандартів безпеки та конфіденційності. Після визначення цінності активів організація може виявити найбільш критичні елементи, які потребують найбільшого захисту, і на основі цього приймати рішення щодо пріоритетів у заходах безпеки. Це дозволяє створити стратегію захисту, яка зосереджується на найбільш важливих для організації ресурсах. Також, визначення цінності активів допомагає більш точно спрогнозувати фінансові витрати, необхідні для відновлення після інцидентів або атак. Використання різних підходів до оцінки активів забезпечує всебічне розуміння їх важливості та дозволяє ефективніше управляти ресурсами та ризиками. Урахування таких аспектів допомагає організації вчасно реагувати на зміни та адаптувати заходи безпеки до нових вимог і реалій.

Крок 2. Виконати аналіз загроз.

Для аналізу загроз потрібно зібрати інформацію про ймовірності кожної загрози. На цьому кроці повинні бути виявлені всі значущі загрози, тобто загрози з великою частотою (ймовірністю) реалізації і ті, що призводять до суттєвих втрат (наприклад, ймовірність пожежі вкрай мала, а принесений збиток – величезний, тому в організаціях завжди виділяються кошти на протипожежні заходи). При цьому необхідно

ранжування загроз, щоб вирішити, якими з них можна знехтувати, а на які звернути основну увагу. Для цього використовуються методи класифікації загроз за критеріями ймовірності та масштабу наслідків, що дозволяє побудувати пріоритети в управлінні ризиками. Одним із таких інструментів є метод матриці ризиків, де кожен тип загрози оцінюється за двома основними характеристиками: ймовірність її реалізації та величина потенційних збитків. Використання сучасних аналітичних інструментів, таких як алгоритми машинного навчання, дозволяє виявляти приховані загрози та робити прогнози щодо їх можливого впливу на організацію. Це дозволяє більш ефективно розподіляти ресурси на запобігання критичним загрозам, оптимізуючи витрати на безпеку.

Крок 3. Оцінити потенційні втрати (грошова оцінка збитку) від кожної з розглянутих загроз.

Оцінка потенційних втрат дозволяє зрозуміти, який вплив може мати кожна загроза на фінансовий стан організації. Враховуючи різні аспекти, такі як вартість відновлення даних, втрати від простоїв, штрафи за порушення нормативних актів або відшкодування за збитки клієнтам, можна підрахувати загальний розмір збитку. Оцінка також включає врахування непрямих витрат, таких як зниження довіри клієнтів і репутаційні ризики, що можуть мати довгострокові наслідки. Всі ці фактори допомагають визначити пріоритетність заходів для захисту від загроз і направити ресурси на найбільш критичні напрямки безпеки. Для цього використовуються методи фінансового моделювання, які дозволяють передбачити не лише безпосередні витрати, але й потенційні втрати на відновлення репутації та клієнтської бази. Крім того, сучасні підходи враховують вплив на довгострокову стійкість організації, наприклад, зменшення ринкової вартості або падіння конкурентоспроможності. Врахування юридичних аспектів, таких як можливі судові витрати або штрафи від регулюючих органів, також є невід'ємною частиною процесу оцінки ризиків. Точність такої оцінки дозволяє організації приймати більш обґрунтовані рішення щодо інвестування в системи безпеки та формування стратегії зниження ризиків.

Крок 4. Розрахувати загальний ризик.

Загальний ризик — це ймовірність настання певної небезпеки, яка може призвести до збитків або негативних наслідків для підприємства чи організації, без врахування вже прийнятих заходів для його зменшення або усунення. Це комплексний показник, що враховує всі потенційні загрози та уразливості, які можуть виникнути в організації, а також можливі наслідки

їх реалізації. Загальний ризик враховує як зовнішні фактори (наприклад, природні катастрофи чи зміни в законодавстві), так і внутрішні (наприклад, технічні неполадки або людські помилки). Оцінка загального ризику дозволяє організації визначити, чи потрібні додаткові заходи для зниження рівня небезпеки та покращення захисту.

Для розрахунку загального ризику необхідно використовувати формулу, що поєднує ймовірність виникнення загрози і її потенційний вплив на організацію. Загальний ризик можна обчислити за допомогою формули: ризик дорівнює ймовірності події, помноженій на вплив. Ймовірність (P) — це ймовірність того, що загроза насправді виникне, виражена у вигляді числа від 0 до 1 (де 0 — неможлива подія, 1 — подія, яка точно відбудеться). Вплив (I) — це фінансові чи інші втрати, які організація зазнає в разі реалізації загрози. Для кожної окремої загрози розраховується ризик, а потім ці ризики сумуються для отримання загального ризику для організації. Наприклад, якщо ймовірність загрози складає 0.3 (30%), а потенційний вплив дорівнює 100 000 грн, то ризик буде дорівнювати 30 000 грн. Цей розрахунок дозволяє оцінити вплив кожної загрози на організацію та визначити пріоритети для вжиття заходів безпеки.

Вважається, що ризик є функцією вірогідності реалізації певної загрози і величини можливого збитку:

$$R = Y \cdot p,$$

де Y — грошова оцінка збитку від загрози; p — ймовірність здійснення цієї загрози.

Наприклад, якщо збиток від загрози становить 100 тис., а ймовірність здійснення загрози дорівнює 0,05, то ризик становить 5 тис. ($R = 100\,000 \times 0,05 = 5\,000$).

Недоліком такого кількісного підходу є складності, пов'язані з такими причинами:

- ➔ відсутністю достовірної статистики вірогідності загроз у мінливому світі ІТ;
- ➔ труднощами оцінки збитку по нематеріальних активів (репутація, конфіденційність відомостей, ідеї, бізнес-плани, здоров'я персоналу);
- ➔ труднощами оцінки всіх непрямих втрат від реалізації загроз;

- ➔ знеціненням результатів тривалої кількісної оцінки ризиків через постійну модифікації і реконфігурацію ІКС.

Тому в основному для аналізу ризиків у цей час використовується якісний підхід, який передбачає просте ранжування загроз і пов'язаних з ними ризиків за ступенем їх небезпеки. Цей підхід допомагає організаціям швидко оцінити потенційні загрози без необхідності використовувати складні кількісні моделі, що може бути доречним в умовах обмежених ресурсів або коли точні дані для розрахунків недоступні. Якісні методи часто застосовуються для визначення пріоритетності дій, допомагаючи зосередитись на найбільш критичних загрозах, які можуть серйозно вплинути на безпеку та діяльність організації.

Водночас якісний підхід забезпечує можливість гнучкого реагування на зміну умов або появу нових загроз. Він не потребує значних витрат часу на збори детальних даних, що особливо важливо для підприємств із динамічним середовищем функціонування. Однак, його недоліком є суб'єктивність оцінок, яка може призвести до недооцінки або переоцінки певних ризиків. Тому для підвищення точності та ефективності аналізу часто рекомендується поєднувати якісний підхід із кількісними методами, використовуючи їх переваги у різних аспектах управління ризиками. Комбінація якісного та кількісного підходів дозволяє досягти більш об'єктивної оцінки та знизити ризик помилок через суб'єктивні оцінки. Завдяки цьому організація отримує можливість не тільки швидко реагувати на зміни, але й точніше прогнозувати потенційні наслідки різних загроз, що сприяє більш збалансованому управлінню ризиками.

Величина збитків з описом (у балах)

<i>Величина збитків, бали</i>	<i>О п и с</i>
0	<i>Загроза не завдає збитків або вони мінімальні</i>
1	<i>Збитки є, але фінансові операції та позиція підприємства не постраждали</i>
2	<i>Фінансові операції не проводяться протягом деякого часу</i>
3	<i>Підприємство зазнає збитків, але позиція його та клієнтура змінюється не значно. Збитки значні від підприємства, втрачається значна частина клієнтів</i>
4	<i>Збитки дуже значні. Підприємство на період до 1 року втрачає позиції на ринку. Для відновлення роботи потрібні значні фінансові кредити</i>
5	<i>Підприємство перестає існувати</i>

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

ПРИКЛАД ОЦІНКИ РИЗИКІВ			
Ймовірність атаки (умовні бали)		Опис (частота появи)	
0		Цей тип атаки відсутній	
1		Приблизно 1 раз на 5 років	
2		Приблизно 1 раз на рік	
3		Приблизно 1 раз на місяць	
4		Приблизно 1 раз на тиждень	
5		Щоденно	
Опис	Збитки	Імовірність	Ризик (Збитки * Імовірність)
Зараження вірусами	3	5	$3 \times 5 = 15$
Відмови обладнання та ПЗ	3	2	6
Викрадення ключової інформації «Клієнт-банк»	4	5	20
Наслідки стихійних лих	4	1	4
Помилки персоналу	2	4	8
Хакерські атаки	4	2	8
РАЗОМ			61

Рис. 5.1. Приклад оцінки ризиків

Джерело: [3-7]

ПРИКЛАД розрахунку загального ризику за рік
1. Викрадення ключової інформації - $20/61 \approx 33\%$ 2. Зараження системи вірусами - $15/61 \approx 25\%$ 3. Помилки персоналу - $8/61 \approx 13\%$ 4. Хакерська атака - $8/61 \approx 13\%$ 5. Відмови обладнання та ПЗ - $6/61 \approx 10\%$ 6. Наслідки стихійних лих - $4/61 \approx 7\%$

Рис. 5.2. Приклад розрахунку загального ризику за рік

Джерело: [3-7]

Крок 5. Вибрати контрзаходи для протидії кожній загрозі (створити службу кібербезпеки, контролювати фізичний і логічний доступи до ІКС, встановити додаткове ПЗ і т. п.), виконати аналіз витрат обраних контрзаходів. Після вибору контрзаходів для протидії загрозам, необхідно оцінити їх ефективність і відповідність до ризиків, які вони повинні зменшити. Важливо провести порівняльний аналіз витрат на впровадження контрзаходів з потенційними збитками від реалізації загроз, щоб забезпечити економічно обґрунтоване рішення. Це може включати оцінку

вартості нових систем безпеки, навчання персоналу, підтримки та оновлення програмного забезпечення, а також можливих витрат на інциденти безпеки, яких вдасться уникнути. Після проведення цього аналізу організація зможе визначити найбільш ефективні та доцільні заходи для захисту своїх інформаційних систем.

Для вибору контрзаходів протидії загрозам в інформаційно-комунікаційних системах (ІКС) важливо здійснити комплексний підхід, який поєднує технічні, організаційні та правові засоби. Першим кроком є оцінка кожної загрози, визначення її потенційного впливу на активи організації, а також ймовірності її реалізації. Далі необхідно вибрати найбільш відповідні контрзаходи, керуючись принципом розумної достатності, тобто забезпечення максимального рівня безпеки при мінімальних витратах. Наприклад, для загрози несанкціонованого доступу до ІКС можна створити службу кібербезпеки, що відповідає за моніторинг і реагування на інциденти. Окрім цього, слід впровадити систему багатофакторної аутентифікації для доступу до системи, а також забезпечити контроль фізичного і логічного доступу до ІКС, включаючи встановлення контрольних точок доступу і обмеження прав доступу на основі ролей. З метою запобігання витоку конфіденційної інформації доцільно впровадити систему шифрування даних як на рівні передачі, так і зберігання, а також регулярно оновлювати програмне забезпечення для усунення відомих уразливостей. Важливою складовою є захист від кібератак, для чого необхідно встановити мережеві фільтри і міжмережеві екрани для блокування несанкціонованих з'єднань, а також використовувати антивірусне програмне забезпечення та системи виявлення вторгнень (IDS). Для боротьби з внутрішніми загрозами з боку недобросовісних працівників важливо впровадити систему моніторингу доступу до чутливої інформації та регулярно проводити аудит прав доступу. Витрати на захисні заходи повинні бути обґрунтованими й економічно доцільними, тобто мінімізувати ймовірність великих фінансових втрат при помірних витратах на впровадження заходів безпеки.

При цьому захисні заходи вибираються на основі принципу розумної достатності, виходячи з мінімізації загальних витрат (економічної доцільності, порівнянності можливого збитку і витрат на захист).

Часто компанії купують нові продукти безпеки, проте не розуміють, що в них будуть додаткові витрати на підтримку роботи цього засобу, або навіть буде потрібен додатковий персонал для використання цих продуктів. З урахуванням сучасних тенденцій у сфері кібербезпеки, описаний приклад є актуальним для організацій, які прагнуть покращити захист своїх інформаційних систем. Для того щоб організація отримала

реальну користь від системи реагування на втручання (IPS), важливо враховувати не лише початкову вартість самої системи, але й всі витрати, пов'язані з її впровадженням, обслуговуванням і підтримкою.

Наприклад, компанія А вирішує захистити свої ключові ресурси за допомогою IPS вартістю \$5000. Однак, окрім початкової ціни, необхідно врахувати додаткові витрати, пов'язані з тестуванням системи для перевірки її безпеки та ефективності. Процес тестування може включати в себе перевірку продуктивності та здатності системи виявляти різні типи атак. Також потрібно налаштувати сенсори та програмне забезпечення для моніторингу мережевої активності, конфігурувати комунікаційне обладнання для направлення всіх трафіків через IPS, а також обмежити доступ до консолі управління системою.

До цього додаються додаткові витрати на навчання персоналу для ефективного використання нової системи, що також може коштувати \$2,500. Важливо враховувати можливе зниження продуктивності користувачів, що може виникнути через впровадження IPS, на що можуть піти додаткові \$2,600. Крім того, не обійдуться витрати час і гроші на налаштування комунікаційного обладнання, встановлення самих сенсорів, усунення помилок і встановлення необхідних патчів, що коштує ще \$4,000.

Таким чином, загальна реальна вартість цього заходу складе \$18,000, що значно більше початкової вартості системи. Якщо при цьому розрахована ймовірна величина збитків від можливих інцидентів у системі становить лише \$9,000, то застосування IPS стає неефективним з економічної точки зору. У такому випадку організація ризикує перевищити бюджет на забезпечення безпеки без реальної необхідності.

Цей приклад підкреслює важливість точного аналізу витрат і вигод при прийнятті рішень про впровадження засобів безпеки. Організації повинні враховувати всі можливі витрати, а також правильно оцінювати потенційні збитки від уразливостей для того, щоб обрати найбільш ефективні й економічно обґрунтовані заходи безпеки.

Крок 6. Оцінити залишковий ризик.

Оцінка залишкового ризику є важливою частиною процесу управління ризиками, яка дозволяє визначити рівень ризику, що залишається після вжиття заходів для його зниження чи нейтралізації. Залишковий ризик — це частина загального ризику, яку неможливо повністю усунути через обмеження ресурсів, технічні чи економічні фактори. Для його оцінки необхідно визначити залишкові загрози та уразливості. Після впровадження заходів безпеки потрібно з'ясувати, які загрози ще можуть впливати на активи, а також чи залишаються уразливості в системах. Далі

необхідно оцінити ймовірність того, що ці загрози реалізуються після застосування всіх можливих заходів для їх нейтралізації. Оцінка впливу залишкових ризиків полягає в тому, щоб визначити можливі збитки або шкоду, яку може зазнати організація, якщо залишковий ризик реалізується. Це може включати фінансові збитки, репутаційні втрати чи порушення законодавчих вимог. Також важливо визначити рівень прийнятного залишкового ризику. Кожна організація повинна визначити, який рівень залишкового ризику є прийнятним для неї, з огляду на власні стратегії, ресурси та рівень готовності до управління цими ризиками. Останнім кроком є розрахунок залишкового ризику, що можна здійснити за допомогою формули, яка враховує ймовірність та вплив залишкових загроз. Залишковий ризик дозволяє організації приймати інформовані рішення щодо подальших заходів для зниження або моніторингу цього ризику, а також визначати, чи потрібно інвестувати додаткові ресурси для його мінімізації.

Коли будуть розраховані загальний та залишковий ризики, необхідно прийняти рішення про подальші дії. Існує чотири варіанта дій, які можна запровадити щодо ризику: перенести, уникнути, зменшити або прийняти ризик. Перенесення ризику передбачає передачу частини або всього ризику іншій стороні, наприклад, через страхування або укладення контракту з постачальниками послуг. Уникнення ризику може означати зміну бізнес-процесів або операцій для усунення можливості виникнення загрози. Зменшення ризику включає впровадження додаткових заходів безпеки або технологічних рішень для зниження ймовірності або впливу загрози. Прийняття ризику означає, що організація визнає певний рівень ризику як прийнятний і готова нести його можливі наслідки.

▲ **Перенесення, або переадресація ризику** виконується шляхом укладення страхової угоди з страховою компанією. Цей підхід дозволяє зменшити фінансовий вплив негативних наслідків ризику на підприємство, передавши частину відповідальності на страховика. Страхування може охоплювати різні види ризиків, від кіберзагроз до фізичних збитків від стихійних лих або аварій. Вибір конкретних умов страхування залежить від оцінки ймовірності ризику та потенційних збитків, а також від рівня необхідного покриття. Важливо правильно оцінити вартість страхових премій у контексті загальної стратегії управління ризиками, щоб переконатися в доцільності цього підходу.

▲ **Уникнення ризику** виконується шляхом припинення діяльності, що викликає ризик. Це може включати відмову від певних проектів, технологій або бізнес-процесів, які можуть створювати небажані ризики для організації. Уникнення ризику часто застосовується в ситуаціях, коли

ймовірність негативних наслідків занадто висока і не можна забезпечити ефективні контрзаходи. Цей підхід дозволяє повністю усунути можливість виникнення ризику, проте він може призвести до втрати можливостей для розвитку або конкурентних переваг. Однак, для досягнення стійкої безпеки і збереження ресурсів, уникнення ризиків може бути важливим кроком у стратегії управління ризиками підприємства.

▲ **Прийняття ризику** – змиритися з ризиком і не витратити гроші на захист від нього (це доцільно, якщо вартість захисних заходів перевищує величину можливого збитку). Цей підхід часто застосовується в ситуаціях, коли ймовірність реалізації ризику є низькою або потенційні збитки від нього є незначними в порівнянні з витратами на запобігання. Прийняття ризику вимагає чіткої оцінки та розуміння можливих наслідків для організації, а також постійного моніторингу цього ризику на випадок зміни умов. Це дозволяє заощадити ресурси, які можна спрямувати на інші, більш критичні напрямки безпеки. Однак важливо розуміти, що прийняття ризику не означає повну бездіяльність, а лише обґрунтоване зважування витрат і вигод від захисту.

Перерахування кроків показує, що управління ризиками – процес циклічний. По суті, останній крок – це оператор кінця циклу, який переводить до **кроку 1**. Ризики потрібно контролювати постійно, періодично проводячи їх переоцінку. Циклічний характер процесу управління ризиками дозволяє організаціям адаптуватися до змін у зовнішньому середовищі та технологіях, а також ефективно реагувати на нові загрози. Періодична переоцінка ризиків допомагає виявити нові вразливості, які могли з'явитися після оновлень чи змін у системах, а також коригувати існуючі контрзаходи в разі їх недостатньої ефективності. В результаті, постійне вдосконалення процесу управління ризиками допомагає забезпечити більш високий рівень захисту та зменшення потенційних збитків. Цей підхід дозволяє організації бути готовою до будь-яких змін і забезпечити стійкість своїх інформаційних систем.

5.2. РЕАЛІЗАЦІЯ ЗМІШАНОГО ПІДХОДУ ДО АНАЛІЗУ РИЗИКІВ

Реалізація змішаного підходу до аналізу ризиків передбачає комбінування різних методів і інструментів для досягнення найбільш точної і обґрунтованої оцінки ризиків в умовах складності та невизначеності. Такий підхід дає змогу врахувати різноманітність факторів, що впливають на ризики, і знижує ймовірність отримання перекошених або неповних результатів, якщо використовувати лише один метод. Змішаний підхід дозволяє комбінувати як якісні, так і кількісні

методи аналізу, що дає змогу отримати більш глибоке розуміння ризиків. Наприклад, можна поєднувати експертні оцінки з математичними моделями, що дозволяє не тільки оцінити ймовірність і наслідки ризиків, але й забезпечити більш точні прогнози для майбутніх сценаріїв. Така гнучкість підходу дозволяє організаціям адаптувати аналіз під специфічні потреби та умови, зберігаючи при цьому високий рівень надійності результатів. Крім того, змішаний підхід сприяє кращій інтеграції різних стратегій управління ризиками, що дозволяє створити більш комплексний і ефективний план дій.

Аналіз ризиків високого рівня

Аналіз ризиків високого рівня є початковим етапом оцінювання ризиків для інформаційних систем, який дозволяє визначити оптимальний підхід для подальших дій: основний чи детальний аналіз ризиків. У цьому контексті аналіз ризиків високого рівня враховує практичну цінність інформаційної системи, оброблювану нею інформацію, а також ризики, що впливають на діяльність підприємства. Для вибору відповідного підходу використовують такі критерії: ділові цілі, які досягаються завдяки використанню системи; рівень залежності підприємства від її функціонування; вплив на конфіденційність, цілісність, доступність та надійність інформації; а також рівень інвестицій у розробку, підтримку чи заміну системи. Цей етап також включає оцінку ймовірності реалізації загроз та їх потенційного впливу на операційну ефективність і репутацію підприємства. В результаті аналізу ризиків високого рівня визначаються найбільш критичні аспекти безпеки, що потребують подальшого дослідження через більш детальні методи оцінки. Після цього розробляється план для вибору конкретних заходів щодо зменшення або уникнення виявлених ризиків, враховуючи ресурси та можливості підприємства. Оскільки цей процес є частиною загальної стратегії управління безпекою, він має бути тісно інтегрований з іншими бізнес-процесами і регулярно оновлюватися в залежності від змін в зовнішньому та внутрішньому середовищі.

Якщо система має критичне значення для ділової активності підприємства, заміна її є фінансово затратною або ризики активів системи оцінюються як високі, необхідно проводити детальний аналіз ризиків. Такий аналіз дозволяє глибоко оцінити потенційні загрози та уразливості, визначити можливі наслідки небажаних подій, а також розробити заходи для зниження ризиків до прийняттого рівня. Основне правило вимагає проведення детального аналізу ризиків для тих систем, уразливість яких може завдати значної шкоди підприємству, його процесам чи активам.

Основний підхід до аналізу ризиків

Основний підхід до аналізу ризиків передбачає встановлення мінімально необхідного рівня захисту для систем інформаційних технологій. Цей підхід дозволяє зменшити витрати на оцінювання ризиків, адже ґрунтується на використанні каталогів стандартних засобів захисту. Основний підхід ефективний для систем із низьким рівнем ризиків, де докладне оцінювання загроз та уразливостей не є обов'язковим. Каталоги засобів захисту, які можуть бути створені на основі міжнародних стандартів, рекомендацій галузі чи досвіду інших підприємств, дозволяють забезпечити узгоджений рівень захисту для всієї організації.

Процес реалізації змішаного підходу починається з ідентифікації активів підприємства, що включає інформаційні, людські та фізичні ресурси, та оцінки загроз, які можуть вплинути на ці активи. Для цієї мети використовуються як традиційні якісні методи, зокрема опитування експертів і співробітників, так і кількісні методи, такі як статистичний аналіз даних або моделювання, що допомагає зрозуміти можливі наслідки певних загроз і уразливостей.

Наступним етапом є оцінка уразливостей, тобто визначення слабких місць у системах та процесах організації, через які можуть бути реалізовані загрози. Тут поєднуються як експертні оцінки, так і автоматизовані сканери уразливостей для визначення технічних недоліків. Це дозволяє отримати більш точні результати та зменшити ймовірність пропуску критичних слабких місць.

Далі проводиться оцінка ймовірності виникнення загрози та її потенційного впливу на бізнес-процеси. Для цього використовуються кількісні методи, засновані на аналізі історичних даних і статистики, а також якісні підходи, що базуються на досвіді і знаннях експертів. Для визначення ймовірності загрози використовуються різноманітні техніки, такі як моделювання сценаріїв і методи, що базуються на даних з реального світу. Це дозволяє більш точно оцінити рівень загроз і правильно розставити пріоритети для їхнього управління.

Оцінка ризиків включає комбінування даних про ймовірність загрози та її впливу на організацію. Результат цього аналізу дає змогу створити детальну картину ризиків і визначити рівень кожного з них. Тут також застосовуються методи, що дозволяють комбінувати якісні й кількісні оцінки для отримання повнішого результату, наприклад, через використання матриць ризиків, які дозволяють чітко візуалізувати рівень кожного ризику.

Завершальним етапом є розробка заходів для зниження або усунення ризиків. Змішаний підхід передбачає використання як технічних, так і організаційних засобів захисту, що можуть включати програмні рішення

для виявлення загроз, системи шифрування, а також організаційні заходи, як-от навчання персоналу, зміна політики або перегляд внутрішніх процесів. Вибір методів залежить від специфіки загрози та активу, що підлягає захисту.

Здійснивши оцінку та розробку заходів захисту, важливо проводити регулярний моніторинг ефективності цих заходів, використовуючи як автоматизовані інструменти, так і ручні перевірки та аудити. Це дає змогу своєчасно виявляти нові загрози чи уразливості, коригувати стратегію захисту та адаптувати її до змін у зовнішньому середовищі.

Змішаний підхід до аналізу ризиків базується на ітераційному процесі, що дозволяє постійно оновлювати та вдосконалювати стратегії управління ризиками. Це означає, що оцінка ризиків і заходи захисту повинні постійно переглядатися й коригуватися відповідно до нових умов, таких як зміни в технологіях, ринкових умовах чи законодавчих вимогах. Завдяки цьому змішаний підхід дає змогу організаціям більш ефективно реагувати на нові виклики та зміни в середовищі загроз, забезпечуючи високий рівень захисту своїх активів і діяльності.

Детальний аналіз ризиків

Детальний аналіз ризиків забезпечує повне оцінювання всіх аспектів безпеки інформаційної системи, включаючи ідентифікацію активів, оцінку їхньої значущості, аналіз загроз, уразливостей і визначення ризиків. Для його проведення використовуються сучасні методи, такі як автоматизовані системи оцінки ризиків, які спрощують збір та обробку даних, а також дозволяють створювати моделі ризиків для подальшого моніторингу та аналізу. Зміни в конфігурації системи чи зовнішніх умовах можуть вимагати перегляду аналізу ризиків. Отримані результати, включаючи ідентифіковані ризики та запропоновані засоби захисту, зберігаються у вигляді бази даних, що дозволяє швидко адаптуватися до нових умов. Перенесення ризику передбачає передачу частини або всього ризику іншій стороні, наприклад, через страхування або укладення контракту з постачальниками послуг. Уникнення ризику може означати зміну бізнес-процесів або операцій для усунення можливості виникнення загрози. Зменшення ризику включає впровадження додаткових заходів безпеки або технологічних рішень для зниження ймовірності або впливу загрози. Прийняття ризику означає, що організація визнає певний рівень ризику як прийнятний і готова нести його можливі наслідки.

У сучасних умовах актуальним є використання інноваційних технологій, таких як штучний інтелект і машинне навчання, для автоматизації процесу аналізу ризиків. Ці технології дозволяють ефективніше виявляти потенційні загрози, прогнозувати сценарії їхнього

розвитку та розробляти адаптивні стратегії захисту. Завдяки цьому підприємства отримують змогу більш оперативно реагувати на змінні умови безпеки, підтримуючи високий рівень захисту своїх інформаційних активів.

Керування ризиком з використанням детального аналізу ризику є важливим етапом у створенні стратегії захисту активів організації від можливих загроз. Детальний аналіз ризику дозволяє не лише ідентифікувати і оцінити потенційні ризики, а й зрозуміти їх вплив на бізнес-процеси, фінанси, репутацію та інші важливі аспекти діяльності організації. Для цього застосовуються кілька основних етапів:

1. **Ідентифікація ризиків** — на першому етапі важливо виявити всі можливі загрози, які можуть вплинути на організацію. Це може бути технічні проблеми, людські помилки, природні катастрофи чи кіберзагрози. Для цього застосовуються різноманітні методи, такі як аналіз історичних даних, опитування експертів, а також використання автоматизованих систем для виявлення потенційних загроз. Ретельна ідентифікація дозволяє створити детальний список всіх можливих ризиків, що є основою для подальшого аналізу і визначення пріоритетів у заходах безпеки.

2. **Оцінка ймовірності та наслідків** — кожен ризик оцінюється за двома критеріями: ймовірність його виникнення і потенційні наслідки для організації. Для цього використовуються різні методи, такі як аналіз ймовірностей, методи FMEA, аналіз впливу на бізнес-процеси (BIA) тощо.

3. **Ранжування ризиків** — на основі отриманих даних ризику ранжуються за рівнем їх критичності для організації. Це дозволяє визначити пріоритети для впровадження контрзаходів і ресурсного забезпечення. Ранжування ризиків допомагає зосередити зусилля на найбільш небезпечних загрозах, що мають найбільший потенціал до збитків. Таким чином, організація може ефективніше розподіляти ресурси та забезпечити максимальний захист від найважливіших ризиків.

4. **Вибір і впровадження контрзаходів** — після оцінки і ранжування ризиків розробляються заходи, спрямовані на зниження ймовірності виникнення або мінімізацію наслідків кожного ризику. Це можуть бути як технологічні, так і організаційні заходи, включаючи оновлення програмного забезпечення, навчання персоналу, зміна політик безпеки тощо.

5. **Моніторинг і перегляд** — ефективність обраних контрзаходів повинна регулярно перевірятися, щоб забезпечити адаптацію до нових загроз та змін у середовищі функціонування організації. Це включає в себе регулярне оновлення політик безпеки, перевірку вразливостей та оцінку

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

поточних ризиків. Моніторинг і перегляд дозволяють своєчасно коригувати стратегії управління ризиками та підтримувати високий рівень захисту інформаційних систем. Цей процес є безперервним і циклічним, що дозволяє зберігати високий рівень безпеки і оперативно реагувати на нові ризики або зміни в існуючих.

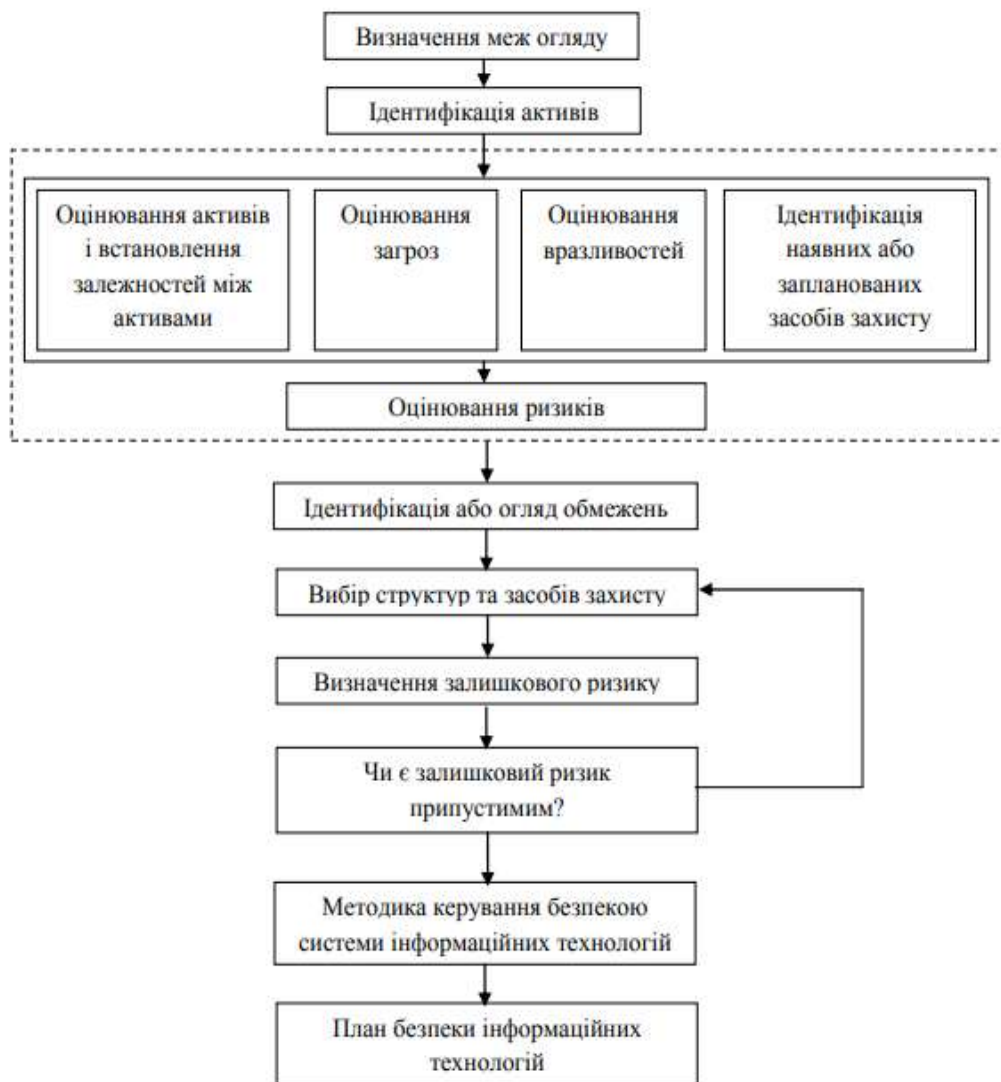


Рис. 5.3. Керування ризиком з використанням детального аналізу ризику
Джерело: [3-7]

Визначення меж огляду є ключовим етапом аналізу ризиків інформаційних систем, що забезпечує чітке окреслення сфери оцінювання. Перед початком ідентифікації активів і їхнього оцінювання необхідно визначити межі огляду, щоб уникнути зайвої роботи та спрямувати ресурси на найважливіші аспекти аналізу. Це дозволяє підвищити

ефективність оцінки ризиків і забезпечує структурований підхід до аналізу. Межі огляду визначають, які саме елементи потрібно враховувати під час аналізу. До таких елементів належать активи інформаційних технологій (апаратне забезпечення, програмне забезпечення, дані та інформація, що є критично важливими для функціонування системи), люди (внутрішні співробітники, підрядники або зовнішній персонал, що мають доступ до системи або впливають на її функціонування), оточення (фізичні об'єкти, такі як будівлі, приміщення, серверні кімнати, а також обладнання, що використовується для забезпечення інформаційної безпеки), а також діяльність (усі процеси, функції або операції, що виконуються в межах інформаційної системи чи з її допомогою).

Кінцевий опис меж огляду має бути максимально точним, щоб уникнути врахування нерелевантних аспектів під час аналізу ризиків. Наприклад, у процесі ідентифікації активів необхідно врахувати залежності між ними, оцінити їхню важливість та визначити їхній вплив на загальну безпеку системи. Окрім визначення меж огляду, важливо також провести огляд обмежень, що можуть вплинути на процес аналізу, таких як обмеження ресурсів, доступу або часу. Після цього слід здійснити вибір структур і засобів захисту, проаналізувати існуючі чи заплановані заходи безпеки для зниження ризиків, а також оцінити залишкові ризики, визначивши, чи є вони прийнятними для підприємства.

Ці етапи формують основу для створення ефективної методики керування безпекою інформаційних систем, що передбачає розробку плану безпеки. План охоплює оцінювання активів, загроз, уразливостей і засобів захисту, створюючи умови для комплексного управління ризиками та підвищуючи рівень інформаційної безпеки підприємства.

5.3. ОЦІНЮВАННЯ РИЗИКІВ

Оцінювання ризиків є одним із основних етапів процесу управління інформаційною безпекою, який передбачає визначення потенційних загроз, уразливостей і оцінку їхнього впливу на інформаційну систему підприємства. Ризик у цьому контексті розглядається як функція цінності активів, ймовірності виникнення загроз, здатності уразливостей бути використаними цими загрозами та ефективності заходів захисту. Метою оцінювання є визначити та оцінити ці фактори, щоб розробити відповідні заходи для зниження ризиків.

Перше, що необхідно зробити в процесі оцінювання ризиків — це визначити активи інформаційної системи, їхню цінність та значення для підприємства. Активи можуть бути різноманітними: від апаратного і

програмного забезпечення до інформації, людських ресурсів або інфраструктури. Цінність активу визначається його важливістю для безперервної роботи підприємства, витратами на його відновлення або заміну, а також потенційними репутаційними втратами у разі компрометації активу.

Наступним етапом є оцінка загроз, які можуть виникнути для активів. Загрози поділяються на внутрішні (наприклад, помилки співробітників) і зовнішні (наприклад, хакерські атаки або природні катастрофи). Імовірність їх виникнення залежить від кількох факторів: привабливості активів для зловмисників, технічних можливостей загроз, а також історії подібних інцидентів в іншій частині індустрії чи регіону. Імовірність реалізації загрози визначається також врахуванням часу, протягом якого активи залишаються критичними для функціонування підприємства.

Ключовим елементом у оцінці ризиків є аналіз уразливостей, тобто слабких місць системи, які можуть бути використані для реалізації загроз. Уразливості можуть бути технічними, наприклад, некоректні налаштування програмного забезпечення або незахищені канали зв'язку, а також організаційними, такими як відсутність належних політик безпеки або недостатня кваліфікація співробітників. Оцінка уразливостей допомагає з'ясувати, які саме елементи системи потребують покращень або додаткового захисту.

Одним із важливих етапів є також оцінка заходів захисту, які вже впроваджені або плануються для зниження ризиків. Це можуть бути технічні засоби, такі як антивірусне програмне забезпечення або файрволи, організаційні заходи, як політики безпеки і тренінги для співробітників, а також фізичні засоби захисту, такі як системи контролю доступу чи відеоспостереження. Оцінка ефективності цих заходів дозволяє зрозуміти, наскільки вони здатні зменшити ризики для активів та знизити ймовірність реалізації загроз.

Загалом, оцінювання ризиків передбачає інтеграцію всіх вищезгаданих аспектів. Ризик обчислюється як добуток трьох основних компонентів: цінності активу, ймовірності загрози і уразливості. Потім це значення коригується в залежності від ефективності заходів захисту. У підсумку результат оцінки дозволяє визначити рівень ризику для кожного активу та систему в цілому, що дозволяє приймати рішення щодо управління цими ризиками.

У процесі оцінювання ризиків можуть застосовуватись різні підходи. Кількісний підхід включає використання фінансових оцінок для визначення втрат, які можуть виникнути у разі реалізації загрози, наприклад, фінансові збитки або витрати на відновлення. Якісний підхід

передбачає описовий аналіз рівня ризику за допомогою категорій, таких як "високий", "середній" або "низький". У деяких випадках застосовується комбінований підхід, який поєднує обидва методи для більш об'єктивного оцінювання ризиків.

Метою всього цього процесу є вибір найбільш ефективних і економічно обґрунтованих заходів захисту для зменшення виявлених ризиків. Оцінка ризиків також передбачає постійне оновлення і коригування стратегії управління безпекою, щоб вона відповідала новим викликам, загрозам і технологіям. Тому оцінювання ризиків не є одноразовим процесом, а вимагає регулярного перегляду та адаптації до змінних умов.

5.4. ТИПОВІ ВИТРАТИ НА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІКС

Типові витрати на забезпечення безпеки інформаційно-комунікаційних систем (ІКС) можуть бути різноманітними та охоплювати широкий спектр напрямків, залежно від специфіки організації, типу ІКС та рівня загроз. Витрати поділяються на кілька основних категорій, зокрема витрати на обладнання та програмне забезпечення для безпеки. Це включає в себе придбання спеціалізованих апаратних засобів для захисту, таких як брандмауери, системи виявлення та запобігання вторгнень, антивірусні програми, а також засоби для криптографії та фізичної безпеки, зокрема системи доступу та відеоспостереження. Крім того, необхідно враховувати ліцензії на програмне забезпечення для безпеки, такі як антивірусні програми, брандмауери, системи управління уразливостями та моніторингу безпеки.

Наступною категорією витрат є персонал та навчання. Це включає витрати на зарплату фахівців з безпеки, таких як адміністратори безпеки, аналітики кібербезпеки, інженери з підтримки та моніторингу безпеки, а також витрати на підвищення кваліфікації співробітників через навчання та сертифікаційні курси. Важливою частиною є витрати на оцінку та управління ризиками, що передбачають залучення сторонніх фахівців для проведення оцінки ризиків, тестування на проникнення, аудиту безпеки та перевірки на відповідність стандартам безпеки. Це також включає використання інструментів для моделювання та аналізу ризиків.

Регулярне оновлення програмного забезпечення є важливим напрямком витрат, адже виявлені уразливості можуть бути нейтралізовані через патчі, що випускаються виробниками програмного забезпечення. Витрати на це включають оновлення всіх програмних додатків, операційних систем та фірмового ПЗ. Відновлення після катастроф та аварій також вимагає витрат на

резервне копіювання даних та підтримку резервних систем, що забезпечують безперервність бізнесу в разі виникнення проблем із основними системами.

Не менш важливими є витрати на фізичну безпеку та захист інформації, зокрема на встановлення систем контролю доступу, охорони та відеоспостереження. Ці витрати також можуть включати створення безпечних серверних кімнат, які відповідають вимогам до зберігання критичної інформації. Витрати на страхування та юридичні послуги складаються з вартості полісів страхування кіберризиків та консалтингу в галузі кібербезпеки.

Окремою категорією є витрати на моніторинг та реагування на інциденти безпеки, що передбачає створення та підтримку Центру операцій безпеки (SOC) для постійного моніторингу, виявлення та реагування на інциденти в реальному часі. Ці витрати також включають обробку інцидентів, включаючи збирання доказів та відновлення систем. Витрати на аудит безпеки та регулярне тестування на проникнення також є важливою частиною забезпечення безпеки системи.

Таким чином, витрати на забезпечення безпеки ІКС є комплексними і включають різні напрямки, що потребують як капітальних, так і операційних витрат. Визначення оптимального рівня інвестицій у безпеку має бути обґрунтоване на основі оцінки потенційних загроз та можливих збитків, які можуть виникнути в разі порушення безпеки.

Загалом, витрати, пов'язані з безпекою ІКС, поділяються на кілька категорій:

1. Витрати на формування та підтримку ланки управління системою захисту інформації (організаційні витрати);
2. Витрати на контроль (визначення і підтвердження досягнутого рівня захищеності ресурсів ІКС);
3. Внутрішні витрати на ліквідацію наслідків порушень політики безпеки ІКС (витрати, понесені в результаті того, що необхідний рівень захищеності НЕ був досягнутий);
4. Зовнішні витрати на ліквідацію наслідків порушення політики безпеки ІКС;
5. Витрати на технічне обслуговування системи безпеки ІКС і заходи щодо запобігання порушенням політики безпеки ІКС (попереджувальні заходи).

Витрати на формування та підтримку ланки управління системою захисту інформації

Витрати на формування та підтримку ланки управління системою захисту інформації включають закупівлю та впровадження технологій безпеки, навчання персоналу, розробку процедур реагування на інциденти, а також постійну підтримку та оновлення систем безпеки для забезпечення ефективного захисту інформаційних активів. Витрати на формування і підтримання ланки управління системою захисту інформації (організаційні витрати) поділяються на:

- ➔ *витрати на формування політики безпеки ІТ;*
- ➔ *витрати на придбання та введення в експлуатацію програмно-технічних засобів – серверів, комп'ютерів кінцевих користувачів (настільних і мобільних), периферійних пристроїв і мережевих компонентів;*
- ➔ *витрати на придбання та налаштування засобів захисту інформації;*
- ➔ *витрати на утримання персоналу, вартість робіт і аутсорсинг.*

Витрати на контроль

Витрати на контроль в системі захисту інформації включають витрати на моніторинг та аудиторські перевірки, регулярне оновлення та тестування засобів безпеки, а також витрати на аналіз інцидентів безпеки та перевірку відповідності політикам безпеки. Це також охоплює витрати на автоматизовані інструменти для контролю доступу, виявлення уразливостей та моніторинг мережевого трафіку. Витрати на контроль (визначення і підтвердження досягнутого рівня захищеності ресурсів ІКС) поділяються на:

- ➔ *контроль за дотриманням політики безпеки ІКС:*
 - ✱ витрати на контроль реалізації функцій, що забезпечують управління безпекою ІКС;
 - ✱ витрати на організацію взаємодії між підТЕМАами для вирішення конкретних завдань по забезпеченню безпеки ІКС;
 - ✱ витрати на проведення аудиту безпеки по кожній частині ІКС;
 - ✱ матеріально-технічне забезпечення системи контролю доступу до об'єктам і ресурсам.
- ➔ *планові перевірки та випробування:*
 - ✱ витрати на перевірки і випробування засобів захисту інформації;
 - ✱ витрати на перевірку навичок експлуатації засобів захисту персоналом;

- ✱ витрати на забезпечення роботи осіб, відповідальних за реалізацію конкретних процедур безпеки по підТЕМАах;
- ✱ оплата робіт по контролю правильності введення даних у прикладних системах;
- ✱ оплата інспекторів із контролю вимог, що пред'являються до засобів захисту при розробці систем (контроль на стадії проектування і специфікації вимог).
- ➔ **позапланові перевірки та випробування:**
 - ✱ оплата роботи випробувального персоналу спеціалізованих організацій;
 - ✱ забезпечення випробувального персоналу матеріально-технічними засобами.
- ➔ **витрати на зовнішній аудит:**
 - ✱ витрати на контрольно-перевірочні заходи, пов'язані з ліцензійно-дозвільної діяльністю в сфері безпеки ІКС.

Внутрішні витрати на ліквідацію наслідків порушень політики безпеки ІКС

Внутрішні витрати на ліквідацію наслідків порушень політики безпеки ІКС включають витрати на відновлення інформаційних систем після інцидентів безпеки, таких як кібератаки або витоки даних. Це охоплює витрати на ремонт і відновлення систем, включаючи сервери, бази даних і мережеве обладнання. Важливим аспектом є також витрати на аналіз інциденту, зокрема розслідування причин порушення, аудит і аналіз журналів системи. Якщо була виявлена уразливість, необхідно оновити програмне забезпечення або встановити патчі, що теж передбачає певні витрати. Крім того, виникають витрати на комунікацію та звітність, які включають повідомлення зацікавлених сторін, таких як користувачі, регулятори або партнери, а також юридичні консультації і можливі штрафи. Витрати на навчання персоналу також є важливим компонентом, оскільки підвищення обізнаності і навчання співробітників допомагає уникати подібних інцидентів у майбутньому. Усі ці витрати можуть значно перевищувати витрати на попередження порушень безпеки, що підкреслює важливість превентивних заходів і необхідність оцінки та оптимізації заходів безпеки задовго до виникнення інцидентів. Внутрішні витрати на ліквідацію наслідків порушень політики безпеки ІКС (витрати, понесені в результаті того, що необхідний рівень захищеності не досягнутий) поділяються на:

- ➔ **перегляд політики безпеки ІКС (проводиться періодично):**

- ✱ витрати на ідентифікацію загроз безпеки ІКС;
 - ✱ витрати на пошук уразливостей системи безпеки ІКС;
 - ✱ оплата фахівців, які виконують роботи по визначенню можливих збитків і переоцінки ступеня ризику.
- ➔ **витрати на ліквідацію наслідків порушення режиму безпеки:**
- ✱ відновлення системи безпеки ІКС до відповідності вимогам політики безпеки;
 - ✱ установка патчів або придбання останніх версій програмних засобів захисту інформації;
 - ✱ придбання технічних засобів замість, що прийшли в непридатність;
 - ✱ проведення додаткових випробувань і перевірок технологічних інформаційних систем;
 - ✱ витрати на утилізацію скомпрометованих ресурсів.
- ➔ **відновлення інформаційних ресурсів:**
- ✱ витрати на відновлення баз даних і інших інформаційних масивів;
 - ✱ витрати на проведення заходів із контролю достовірності даних, піддалися атаці на цілісність.
- ➔ **витрати на виявлення причин порушення політики безпеки:**
- ✱ витрати на проведення розслідувань порушень політики безпеки ІКС (збір даних про способи вчинення, механізм і способи приховування неправомірного діяння, пошук слідів, знарядь, предметів посягання, виявлення мотивів неправомірних дій і т. п.);
 - ✱ витрати на оновлення планів безперервності діяльності служби безпеки.
- ➔ **витрати на переробки:**
- ✱ витрати на впровадження додаткових засобів захисту, які потребують істотної перебудови системи безпеки ІТ;
 - ✱ витрати на повторні перевірки і випробування системи безпеки ІТ.

Зовнішні витрати на ліквідацію наслідків порушення політики безпеки ІКС

Зовнішні витрати на ліквідацію наслідків порушення політики безпеки ІКС включають витрати, які організація несе у взаємодії з третіми сторонами для відновлення безпеки і ліквідації наслідків інциденту. Це може бути витрати на залучення сторонніх експертів, таких як компанії з

кібербезпеки, аудиторські фірми та консультанти, які займаються аналізом інциденту, виявленням уразливостей та наданням рекомендацій щодо їх усунення. Крім того, може бути необхідність у послугах юридичних фірм, які займаються вирішенням правових питань, включаючи можливі позови від постраждалих осіб, штрафи або судові витрати.

Інші зовнішні витрати включають витрати на відшкодування збитків постраждалим сторонам, зокрема клієнтам або партнерам, у разі витоку конфіденційної інформації чи порушення прав користувачів. Також можуть виникати витрати на комунікацію з державними органами, регуляторами, а також витрати на репутаційні заходи, включаючи виплати компенсацій, публічні вибачення або проведення інформаційних кампаній для відновлення довіри до організації.

Зовнішні витрати можуть значно перевищувати витрати на внутрішнє реагування і відновлення, тому організаціям важливо враховувати всі потенційні зовнішні наслідки при плануванні політики безпеки та заходів для запобігання інцидентам.

Зовнішні витрати на ліквідацію наслідків порушення політики безпеки ІКС поділяються на:

- ➔ **зовнішні витрати на ліквідацію наслідків порушення політики безпеки ІТ:**
 - ✱ зобов'язання перед державою і партнерами;
 - ✱ витрати на юридичні суперечки і виплати компенсацій;
 - ✱ втрати в результаті розриву ділових відносин з партнерами.
- ➔ **витрати новаторства:**
 - ✱ витрати на проведення додаткових досліджень і розробки нової ринкової стратегії;
 - ✱ відмова від організаційних, науково-технічних або комерційних рішень, що стали неефективними в результаті витоку відомостей, і витрати на розробку нових засобів ведення конкурентної боротьби;
 - ✱ втрати від зниження пріоритету в наукових дослідженнях і неможливості патентування та продажу ліцензій на науково-технічні досягнення.
- ➔ **інші витрати:**
 - ✱ заробітна плата секретарів і службовців, організаційні та інші витрати, які безпосередньо пов'язані з попереджувальними заходами;
 - ✱ інші види можливого збитку, в тому числі пов'язані з неможливістю виконання функціональних завдань.

Витрати на технічне обслуговування системи безпеки ІКС

Витрати на технічне обслуговування системи безпеки ІКС включають регулярні витрати, пов'язані з підтримкою і оновленням технічних засобів захисту інформації. Це можуть бути витрати на оновлення програмного забезпечення, встановлення патчів, забезпечення антивірусних баз і сигнатур, а також регулярне тестування систем безпеки, зокрема проведення аудитів, перевірки на уразливості та penetration testing.

До витрат на технічне обслуговування також відносяться витрати на підтримку обладнання (системи виявлення вторгнень, фаєрволи, мережеві монітори), оновлення ліцензій на програмне забезпечення безпеки, а також витрати на заміну або оновлення старих компонентів, що можуть втратити ефективність у процесі експлуатації.

Окрім цього, важливо враховувати витрати на регулярне навчання персоналу для підтримки належного рівня обізнаності з актуальними загрозами і технологіями безпеки, а також витрати на обслуговування резервних копій даних, що забезпечують цілісність і доступність інформації в разі інцидентів.

Загалом витрати на технічне обслуговування є постійними і необхідними для забезпечення ефективної роботи системи безпеки та своєчасного реагування на нові загрози.

Витрати на технічне обслуговування системи безпеки ІКС і заходи щодо запобігання порушенням політики безпеки ІКС (попереджувальні заходи) поділяються на:

➔ **витрати на управління системою безпеки ІКС:**

- ✱ витрати на планування системи безпеки ІКС;
- ✱ витрати на вивчення можливостей інфраструктури щодо забезпечення безпеки ІКС;
- ✱ витрати на технічну підтримку персоналу при впровадженні засобів захисту інформації та процедур, а також планів з безпеки ІКС;
- ✱ перевірка співробітників на лояльність, виявлення загроз безпеки ІКС;
- ✱ організація системи допуску виконавців і співробітників до захисту.

➔ **регламентне обслуговування засобів захисту інформації:**

- ✱ витрати, пов'язані з обслуговуванням і налаштуванням програмно-технічних засобів захисту інформації, ОС і мережевого обладнання;

- ✱ витрати, пов'язані з організацією мережевої взаємодії і безпечного використання ІКС;
- ✱ витрати на підтримку системи резервного копіювання та ведення архіву даних;
- ✱ проведення інженерно-технічних робіт по встановленню сигналізації, обладнання сховищ конфіденційних документів, захисту телефонних ліній зв'язку і т. п.

➔ **аудит системи безпеки ІКС:**

- ✱ витрати на контроль змін стану інформаційного середовища;
- ✱ витрати на систему контролю за діями виконавців.

➔ **забезпечення відповідності використовуваних ІКС заданим вимогам:**

- ✱ витрати на забезпечення відповідності використовуваних ІТ вимогам по безпеки, сумісності і надійності, в тому числі аналіз можливих негативних аспектів ІКС, які впливають на цілісність і доступність;
- ✱ витрати на доставку (обмін) конфіденційної інформації;
- ✱ задоволення суб'єктивних вимог користувачів (стиль, зручність інтерфейсу та ін.).

➔ **забезпечення вимог стандартів:**

- ✱ витрати на забезпечення відповідності прийнятим стандартам і вимогам.

➔ **навчання персоналу:**

- ✱ підвищення кваліфікації працівників, відповідальних за використання наявних засобів захисту, виявлення і запобігання загрозам безпеки ІКС;
- ✱ розвиток нормативної бази та технічної оснащеності.



У сучасних умовах ефективна система захисту інформаційно-комунікаційних систем дійсно потребує значних фінансових витрат, а також великих обчислювальних ресурсів. Підвищення рівня безпеки може зажадати встановлення додаткових засобів захисту, які використовують значну частину доступних ресурсів комп'ютерної системи, що може призвести до зниження продуктивності. Крім того, надмірні заходи безпеки можуть викликати дискомфорт і роздратування серед користувачів, що, в свою чергу, знижує ефективність роботи персоналу. Тому критично важливо здійснити правильний баланс, обираючи оптимальний рівень захисту, який дозволяє мінімізувати ризики і при цьому є економічно обґрунтованим.

Основною метою захисту ІКС є мінімізація ризиків для учасників процесу, що дозволяє забезпечити безпеку інформаційних активів і знизити ймовірність

негативних наслідків для організації. Захист ІКС має бути безперервним процесом, який включає в себе не лише виявлення та оцінку активів, що потребують захисту, але й визначення їх вартості та потенційних збитків у разі їх компрометації. Аналіз ризиків є ключовим етапом у процесі розробки плану безпеки, який передбачає вибір ефективних технологій та засобів для реалізації заходів захисту.

На практиці, досягнення ефективного рівня захисту полягає у зведенні всіх значущих загроз до прийнятного рівня залишкового ризику. Це означає, що потрібно зберігати можливість для захисту найважливіших інформаційних ресурсів без перевищення наданих фінансових можливостей та наявних технічних ресурсів. Тому розробка і реалізація політики безпеки повинна базуватися на принципах раціонального розподілу ресурсів, де пріоритет надається найбільш критичним елементам інфраструктури, що потребують захисту, а також враховуються конкретні загрози, що можуть мати серйозні наслідки для діяльності організації.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 5

1. Лахно В. А., Васіліу Є. В., Гладких В. М., Домрачев В. М., Сивкова Н. М. (2020) Методи та засоби захисту інформації: навч. посіб. Київ: Компрінт О. В. 444 с.
2. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
3. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
4. Браїловський М.М. Аналіз кіберзахищеності інформаційних систем: монографія/ Браїловський М.М., Зибін С.В., Кобозева А.А., Хорошко В.О., Хохлачова Ю.Є. К.: ФОП Ямчинський О.В., 2021. – 360 с.
5. Костюк Ю.В., Ковальова Л.І., Повна Н.І. Захист інформації у сегменті інформаційної системи на основі інтелектуальних технологій // Збірник тез VI Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2023. – с. 77-79.
6. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 390–400.
7. P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, J. Theor. Appl. Inf.

Technol. 100(22) (2022) 6635–6644. Костюк Ю.В., Степашкіна К.В. Моделювання інтелектуальних систем управління захистом інформації в інформаційно-телекомунікаційних системах // Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2023) : матеріали тез доповідей XIII Міжнародної науково-практичної конференції (м. Чернігів, 25–26 травня 2023 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2023. – Т. 2. – с. 252–253.

8. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 338–347.

9. Y. Dreis, et al., Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 277–289.

10. Костюк Ю.В. Математичне моделювання захищених інформаційних систем // Інноваційний потенціал сучасної науки: зб. наук. праць IV Всеукраїнської наук.-практ. інтернет-конф., (18 травня 2023 року. Кам'янець-Подільський). - Кам'янець-Подільський Заклад вищої освіти «Подільський державний університет», 2023. с. 171–174.

11. A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 1–13.

12. Крючкова, Л., & Ємельяненко, М. (2024). Захист web-ресурсу intranet від зовнішніх і внутрішніх загроз. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 318–327.

13. A. Zahynei, et al., Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 432–439.

14. Костюк Ю.В. Математичне моделювання комп'ютерних мереж, керованих протоколами випадкового множинного доступу // Актуальні питання науки, освіти та технологій в умовах сучасних викликів: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 9 травня 2023 р.): у 2 ч. Кременчук: ЦФЕНД, 2023. Ч. 1. С. 57–58.

15. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 68–83.

16. Костюк Ю.В. Виявлення загроз порушення інформаційної безпеки в мережах з динамічною топологією з використанням інтелектуальних методів //

Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023).

17. M. Astafieva, et al., Formation of High School Students' Resistance to Destructive Information Influences, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 87-96.

18. H. Shevchenko, et al., Information Security Risk Analysis SWOT, Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021) 309-317.

19. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроектні рішення щодо побудови системи авторизації на основі концепції ZERO TRUST. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242.

20. O. Bahatskyi, V. Bahatskyi, V. Sokolov, Smart Home Subsystem for Calculating the Quality of Public Utilities, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 168–173.

21. Костюк Ю. В Впровадження інтелектуальних систем у процес оцінки ризиків інформаційної безпеки в безпроводових мережах // Сьомі Геретівські читання: наукові статті, тези доповідей та інші матеріали Всеукраїнської науково-практичної конференції (м. Тернопіль, Україна, 22 вересня 2023 року). Науковий, методичний, інформаційний збірник Тернопільського обласного комунального інституту післядипломної педагогічної освіти / Редколегія: О. М. Петровський, В. С. Мисик, І. М. Вітенко, О. І. Когут, Ю. Ч. Шайнюк, Т. В. Магера, Ф. І. Полянський, Н. Б. Стрийвус, Г. І. Герасимчук. Тернопіль: ТОКІППО, 2023. С. 162-168.

22. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке організаційний захист і з чого він складається?
2. Назвіть основні адміністративні заходи забезпечення безпеки ІКС.
3. Що таке політика безпеки і з яких рівнів вона складається?
4. Назвіть структуру політики безпеки.
5. Дайте характеристику спеціалізованим політикам безпеки.
6. Назвіть особливості процедури управління персоналом з точки зору безпеки ІКС.

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

-
7. У чому полягає і для чого впроваджується принцип мінімізації привілеїв?
 8. Які основні етапи включає процедура реалізації політики безпеки для оновлення програмного забезпечення в організації?
 9. Як регулярне оновлення програмного забезпечення допомагає в мінімізації уразливостей інформаційних систем?
 10. Які ризики можуть виникнути при відсутності регулярного оновлення ПЗ у компанії?
 11. Як процес зниження привілеїв користувачів сприяє посиленню захисту ІКС?
 12. Які стратегії використовуються для забезпечення мінімальних прав доступу у політиці безпеки організації?
 13. Як ефективно контролювати оновлення ПЗ для забезпечення безпеки інформаційних систем?
 14. Як зниження привілеїв користувачів допомагає зменшити ймовірність внутрішніх загроз безпеки?
 15. Які методи і інструменти використовуються для автоматизації процесу оновлення ПЗ в ІКС?
 16. Як провести аудит та моніторинг після оновлення ПЗ, щоб підтвердити його ефективність щодо захисту від загроз?
 17. Які додаткові заходи безпеки слід вжити після зниження привілеїв користувачів для забезпечення максимального захисту системи?
 18. Що таке патчінг і для чого він проводиться?
 19. Яке ПЗ найбільш потребує своєчасного оновлення?
 20. Що таке «вівторок патчів» і в чому полягає його зміст?
 21. Назвіть джерела інформації по виявленим вразливостям і методики їх усунення.
 22. Що таке аналіз ризиків безпеки ІКС?
 23. Приклади використання методів аналізу ризиків.
 24. Назвіть основні кроки аналізу ризиків.
 25. В чому полягає змішаний підхід?
 26. Які основні переваги змішаного підходу?
 27. У чому різниця між кількісним і якісним підходами до аналізу ризиків безпеки?
 28. Як розраховується загальний ризик? Наведіть приклад.
 29. Назвіть типові витрати на забезпечення безпеки ІКС.

ТЕМА 3. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІКС

РОЗДІЛ 6 МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ



- 6.1. Загальна характеристика інженерно-технічних засобів безпеки**
- 6.2. Методи фізичного захисту інформації**
- 6.3. Характеристика технічних каналів витоку інформації**
- 6.4. Захист інформації від витоку електричними та електромагнітними каналами**
- 6.5. Методи захисту від витоку інформації за рахунок акустичних та оптичних каналів**
- 6.6. Технічні канали витоку інформації на основі закладних пристроїв**
- 6.7. Заходи захисту інформації від витоку каналами на основі закладних пристроїв**

"Безпека – це не тільки про захист від атаки, а й про те, як захищати інформацію від витоку через будь-які канали."

Брюс Шнайер

Інженерно-технічний захист ІКС — це сукупність заходів, спрямованих на забезпечення безпеки даних, що обробляються, зберігаються і передаються в ІКС. Він включає використання різноманітних технологій та методів для захисту від технічних і фізичних

загроз, таких як несанкціонований доступ, витік інформації, кібернапади і пошкодження обладнання.

Технічні канали витоку інформації — це різні способи, через які конфіденційна інформація може бути передана або витікати з інформаційної системи без дозволу. Вони можуть включати канали зв'язку (мережеві канали), фізичні канали, електромагнітні канали, канали виведення інформації та канали через програмне забезпечення. Загроза виникає, коли дані передаються через незахищені або недостатньо захищені мережі, такі як локальні мережі або глобальні Інтернет-з'єднання. Крім того, витoki можуть бути спричинені фізичним доступом до пристроїв, таких як комп'ютери, сервери або носії даних. Іншими каналами можуть бути електромагнітні випромінювання, які можуть бути перехоплені спеціальними пристроями для злomu, а також пристрої, які виводять інформацію через акустику, екрани або принтери. Витoki можуть статися також через уразливості в програмному забезпеченні, яке не контролює належним чином доступ до даних або не шифрує передану інформацію.

Для захисту від витоків інформації застосовуються різні заходи інженерно-технічного захисту, такі як шифрування даних, фізична безпека (захист від несанкціонованого фізичного доступу), контроль доступу (впровадження суворих правил доступу до інформації і багатофакторної аутентифікації), моніторинг і аудит систем, а також навчання користувачів щодо безпеки і правильного поводження з чутливою інформацією. Такий комплексний підхід дозволяє ефективно запобігати витокam інформації через різні технічні канали.

6.1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАСОБІВ БЕЗПЕКИ

Некомпетентність і неакуратність співробітників при виконанні своїх обов'язків є однією із значущих загроз безпеки ІКС, що може впливати на збитки організації. Процедурні механізми адміністративно-організаційного захисту, що спрямовані на діяльність співробітників, у даному випадку — малоефективні. Нейтралізація таких загроз можлива виключенням людини, схильної по своїй природі до помилок, і автоматизацією процесів з використанням інженерно-технічних засобів захисту ІКС.

Комп'ютери автоматизували багато областей людської діяльності, тому цілком природним є бажання покласти на них і забезпечення власної безпеки. Навіть фізичний захист все частіше доручають не охоронцям, а

інтегрованим комп'ютерним системам, що дозволяє одночасно відстежувати переміщення співробітників і по організації, і по кіберпростору.

Інженерно-технічні засоби безпеки (ІТЗБ) є важливим елементом у системах захисту інформації, призначеними для запобігання несанкціонованому доступу до інформаційних ресурсів, збереження їх цілісності та конфіденційності, а також захисту від фізичних та кібернетичних загроз. Ці засоби включають як апаратні, так і програмні рішення, що використовуються для охорони комп'ютерних систем, мереж, сервісів, а також інформаційних ресурсів.

Загальна характеристика інженерно-технічних засобів безпеки

Фізичний захист

Інженерно-технічні засоби фізичної безпеки призначені для забезпечення безпеки від несанкціонованого доступу до об'єктів, де зберігаються інформаційні ресурси. Це включає системи контролю доступу, відеоспостереження, охоронні сигналізації, а також фізичні бар'єри, такі як замки, двері, перегородки. Вони сприяють мінімізації ризиків, пов'язаних із фізичним проникненням у приміщення, де зберігаються сервери або інші інформаційні системи. Фізичний захист також включає регулярні перевірки та технічне обслуговування засобів безпеки, щоб забезпечити їх справність та ефективність у будь-який час. Важливим аспектом є також контроль за доступом до критичних зон через використання систем ідентифікації, що дозволяє обмежити доступ лише уповноваженому персоналу.

Контроль доступу

Важливою складовою ІТЗБ є механізми контролю доступу, що гарантують доступ до інформації лише уповноваженим користувачам. Це можуть бути системи аутентифікації та авторизації (біометричні системи, карти доступу, паролі), а також засоби моніторингу і запису подій, пов'язаних з доступом до систем. Контроль доступу включає також використання різних рівнів доступу, де користувачі отримують доступ лише до тих даних і ресурсів, які необхідні для виконання їхніх обов'язків. Це може бути реалізовано через політики, засновані на ролях (RBAC), де кожному користувачеві призначається певна роль із відповідними правами доступу. Крім того, регулярне оновлення і перевірка прав доступу допомагає зменшити ризики несанкціонованого доступу через зміну ролей або неактивних облікових записів.

Шифрування та криптографія

Для захисту інформації від витоку або несанкціонованого доступу використовуються шифрування даних як на етапі їх зберігання, так і під час передачі. Системи шифрування забезпечують захист чутливої інформації від

перехоплення чи зміни, навіть якщо дані потрапляють до рук зловмисників. Шифрування може бути симетричним, коли один і той самий ключ використовується для шифрування та розшифрування даних, або асиметричним, де використовуються пари ключів (публічний та приватний) для забезпечення безпечної передачі інформації. Криптографічні алгоритми, такі як AES (Advanced Encryption Standard) або RSA (Rivest–Shamir–Adleman), є стандартами для забезпечення конфіденційності та цілісності даних. Крім того, шифрування допомагає в реалізації функцій автентифікації та непідробності даних, забезпечуючи додаткові рівні захисту від несанкціонованих змін або витоків інформації. Регулярне оновлення та управління криптографічними ключами є важливою частиною загальної стратегії безпеки інформаційних систем.

Антивірусні та антималварні програми

Одним з основних аспектів захисту інформаційних систем є програмне забезпечення, яке запобігає потраплянню шкідливих програм (вірусів, троянів, червів тощо) до системи. Антивірусні програми здійснюють моніторинг системи на наявність загроз і виконують їх нейтралізацію до того, як шкідливі програми можуть завдати шкоди. Антивірусні та антималварні програми використовують різні методи для виявлення та блокування шкідливих програм. Одним із таких методів є підпис бази даних, яка містить відомі зразки шкідливих програм, що дозволяє швидко ідентифікувати загрози. Інші методи включають евристичний аналіз, який виявляє нові або змінені віруси шляхом аналізу їхньої поведінки в системі, а також технології машинного навчання, що дозволяють програмам адаптуватися до нових загроз. Для підвищення рівня захисту важливо, щоб ці програми регулярно оновлювали свої бази даних і алгоритми, забезпечуючи захист від нових типів вірусів і шкідливого програмного забезпечення.

Мережеві засоби безпеки

Інженерно-технічні засоби безпеки мережі включають різноманітні фаєрволи, засоби виявлення і запобігання вторгненням (IDS/IPS), а також системи VPN (віртуальні приватні мережі) для захищеного обміну даними через інтернет. Вони дозволяють здійснювати контроль за мережевим трафіком, блокувати несанкціоновані спроби доступу та забезпечувати захист від атак на мережеву інфраструктуру. Фаєрволи виконують роль бар'єра між внутрішньою мережею та зовнішнім світом, фільтруючи трафік за визначеними правилами та дозволяючи або блокуючи певні типи з'єднань. Засоби виявлення і запобігання вторгненням (IDS/IPS) допомагають виявляти аномалії у мережевому трафіку та попереджати про можливі атаки або порушення безпеки. Системи VPN створюють захищені канали для передачі даних між віддаленими точками,

забезпечуючи конфіденційність і цілісність інформації під час її пересилання через незахищені мережі, такі як Інтернет. Використання цих засобів дозволяє значно підвищити рівень безпеки мережевої інфраструктури та мінімізувати ризики кіберзагроз.

Моніторинг і аудит

Важливою частиною ІТЗБ є системи моніторингу та аудиту, які дозволяють відстежувати події в інформаційних системах і мережах. Це включає в себе реєстрацію доступів, змін, спроб несанкціонованого проникнення, а також ведення журналів для подальшого аналізу і виявлення можливих порушень безпеки. Системи моніторингу забезпечують оперативне виявлення аномалій та інцидентів безпеки, дозволяючи швидко реагувати на потенційні загрози. Аудит, у свою чергу, дозволяє проводити ретельний аналіз подій, що сталися, і оцінювати відповідність існуючих заходів безпеки встановленим стандартам. Регулярний аудит допомагає ідентифікувати слабкі місця у системах та розробити рекомендації для їх усунення. Поєднання моніторингу та аудиту є основою для забезпечення прозорості, підвищення надійності інформаційних систем і зниження ризиків порушень безпеки.

Резервне копіювання і відновлення

Для забезпечення стійкості інформаційних систем до різних видів загроз важливим елементом є системи резервного копіювання і відновлення даних. Вони дозволяють зберігати копії важливих даних у безпечному місці і відновлювати їх у разі втрати або пошкодження оригіналів. Системи резервного копіювання забезпечують регулярне створення копій даних, які можуть зберігатися як у локальному середовищі, так і в хмарних сховищах. Це знижує ризик втрати критичної інформації через технічні збої, кібератаки чи людські помилки. Відновлення даних із резервних копій дозволяє мінімізувати час простою системи та зменшити фінансові й операційні втрати. Ефективна стратегія резервного копіювання включає регулярне тестування процесів відновлення, щоб забезпечити їхню працездатність у разі надзвичайної ситуації.

Загалом, інженерно-технічні засоби безпеки є багатокомпонентною і складною системою, яка включає в себе як апаратні засоби (сервери, мережеві пристрої, системи контролю доступу), так і програмні рішення (антивірусні програми, системи шифрування, фаєрволи, системи моніторингу), що працюють у комплексі для забезпечення високого рівня безпеки та захисту інформації.

Загалом, за своїм функціональним призначенням засоби інженерно-технічного захисту інформації діляться на фізичні та технічні.

Фізичні засоби захисту

Фізичні засоби захисту є важливою частиною системи безпеки, що забезпечують захист інформаційних систем і ресурсів від несанкціонованого доступу, фізичних пошкоджень або крадіжки. Вони створюють фізичні бар'єри, що унеможливають чи обмежують доступ до чутливих даних, серверів, комп'ютерних мереж і іншої важливої інфраструктури. Ці засоби поділяються на кілька основних груп:

✱ **Контроль доступу:**

- ✓ **Замки та ключі** — використовуються для фізичного блокування доступу до дверей, серверних приміщень та інших важливих зон. Існують різні типи замків, такі як механічні, електронні та біометричні.
- ✓ **Системи контролю доступу** — ці системи обмежують доступ до приміщень або пристроїв, використовуючи різні методи аутентифікації, такі як картки доступу, PIN-коди, біометричні дані (відбитки пальців, сітківка ока).

✱ **Фізичне укріплення приміщень:**

- ✓ **Броньовані двері та вікна** — використовуються для захисту серверних кімнат, лабораторій та інших важливих зон, що забезпечують надійний захист від несанкціонованого фізичного доступу.
- ✓ **Перегородки та бар'єри** — застосовуються для розмежування зон та створення додаткових бар'єрів для доступу до критичних ресурсів.

✱ **Системи відеоспостереження** - відеокамери та системи моніторингу допомагають стежити за ситуацією в реальному часі, фіксувати події, що відбуваються в охоронюваних зонах, а також забезпечують доказову базу для реагування на порушення безпеки.

✱ **Охоронні сигналізації:**

- ✓ **Датчики руху та відкриття дверей/вікон** — реагують на несанкціоновані спроби проникнення, включаючи відкриття дверей або вікон, і сповіщають охоронців або відповідальних осіб про можливу загрозу.
- ✓ **Тривожні кнопки та сирени** — встановлюються для швидкого реагування на порушення безпеки в приміщенні або на території.

✱ **Охоронні засоби:**

- ✓ **Охоронці та патрулі** — людські ресурси, що здійснюють моніторинг доступу, перевірки та оперативно реагують на спроби несанкціонованого доступу до критичних зон або пристроїв.
- ✱ **Захист від фізичних пошкоджень:**
 - ✓ **Біометричні системи доступу** — використовують унікальні біологічні характеристики людини (відбитки пальців, розпізнавання обличчя, сітківка ока) для надання або відмови в доступі до певних зон або систем.
 - ✓ **Захист від пожежі** — системи сповіщення про пожежу, вогнегасники та обробка матеріалів протипожежними речовинами для захисту критичних компонентів і збереження цілісності даних у разі загоряння.
- ✱ **Фізичний захист носіїв інформації:**
 - ✓ **Зберігання носіїв даних у захищених сейфах або депозитаріях** — важливі носії інформації (жорсткі диски, флеш-накопичувачі, магнітні стрічки) повинні зберігатися в захищених місцях, щоб запобігти їх крадіжці або пошкодженню.
- ✱ **Захист від електромагнітних загроз:**
 - ✓ **Екранування приміщень та обладнання** — спеціальні екрани або захисні плівки використовуються для запобігання несанкціонованому перехопленню електромагнітних сигналів або викидів від обладнання, що може призвести до витoku чутливої інформації (захист від атаки через канали електромагнітного випромінювання).

Таким чином, фізичні засоби захисту охоплюють широкий спектр заходів, спрямованих на забезпечення безпеки фізичного доступу до інформаційних систем і захист від різних загроз, що можуть виникнути в результаті несанкціонованого вторгнення або фізичного пошкодження. Використання цих засобів у поєднанні з іншими технічними і організаційними заходами дозволяє створити ефективну систему безпеки, яка мінімізує ризики для інформаційних ресурсів підприємства.

Технічні засоби захисту

Технічні засоби захисту — це сукупність апаратних і програмних рішень, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, захист від несанкціонованого доступу, кіберзагроз, атак і уразливостей. Вони складають важливу частину системи інформаційної безпеки підприємства, організації чи іншої установи, а

також застосовуються для захисту даних, мереж, пристроїв і інформаційних систем від різноманітних загроз.

Основні технічні засоби захисту можна розділити на кілька категорій:

✿ **Засоби контролю доступу:**

- ✓ **Системи аутентифікації та авторизації** - програмне забезпечення для контролю доступу до інформаційних систем. Це може включати використання паролів, карток доступу, біометричних даних (відбитки пальців, розпізнавання обличчя) або багатофакторну аутентифікацію для підтвердження особи користувача.
- ✓ **Механізми обмеження прав доступу** визначають, які користувачі мають доступ до конкретних ресурсів, файлів, програм або сервісів в межах інформаційної системи. Це може бути реалізовано через групові політики доступу, ACL (списки контролю доступу) або рольову модель доступу.

✿ **Засоби захисту мережі:**

- ✓ **Міжмережеві екрани (фаєрволи)** - пристрої або програмні рішення, які перевіряють трафік, що надходить і виходить із мережі, і блокують небажаний або шкідливий трафік, забезпечуючи контроль над вхідними та вихідними з'єднаннями.
- ✓ **Системи виявлення та запобігання вторгненням (IDS/IPS)** - системи, які постійно моніторять мережевий трафік і шукають ознаки спроб вторгнення, зловмисних атак або підозрілих дій. IPS також може здійснювати блокування таких атак.
- ✓ **VPN (Virtual Private Network)** - захищений канал зв'язку, який використовується для безпечного підключення до корпоративної мережі через публічні мережі (наприклад, Інтернет). VPN забезпечує конфіденційність і захист даних при передачі.

✿ **Засоби шифрування:**

- ✓ **Шифрування даних** - використання криптографії для захисту інформації під час її зберігання або передачі. Це дозволяє забезпечити конфіденційність даних, гарантуючи, що тільки авторизовані особи можуть їх прочитати.
- ✓ **Шифрування каналів зв'язку** - використання протоколів безпеки, таких як SSL/TLS, для захищеного обміну даними між клієнтами та серверами через Інтернет.

- ✱ *Антивірусне програмне забезпечення та засоби боротьби з шкідливим ПЗ:*
 - ✓ **Антивірусні програми** - програмне забезпечення, що здатне виявляти, нейтралізувати та видаляти віруси, трояни, шпигунські програми та інші види шкідливого програмного забезпечення, які можуть завдати шкоди системам або вкрати інформацію.
 - ✓ **Системи виявлення шкідливого ПЗ (Malware Detection Systems)** - інструменти, які сканують файли, трафік і активність у системі на наявність шкідливих програм і проводять їх блокування.
- ✱ *Засоби резервного копіювання і відновлення:*
 - ✓ **Резервне копіювання даних** - створення копій важливих даних з метою їх збереження на випадок збоїв системи, атак або втрати даних через технічні несправності. Це включає програмне забезпечення для планового створення резервних копій та відновлення даних.
 - ✓ **Системи відновлення після катастроф** - процедури та інструменти, які дозволяють швидко відновити функціонування організації в разі серйозного збою, атаки або природної катастрофи.
- ✱ *Системи моніторингу та аудиту:*
 - ✓ **Моніторинг подій безпеки** - програмні інструменти для постійного спостереження за станом інформаційної системи, виявлення аномальних або підозрілих дій, які можуть вказувати на порушення безпеки.
 - ✓ **Аудит доступу та подій** - програмне забезпечення для запису та аналізу дій користувачів і адміністраторів, що дозволяє виявляти та реагувати на порушення безпеки, зловживання правами або інші загрози.
- ✱ *Засоби фізичного захисту:*
 - ✓ **Фізична безпека серверів і інформаційних систем** - використання спеціальних захищених приміщень для зберігання серверів і обчислювальних потужностей, що включають броньовані двері, камери відеоспостереження, контролю доступу і охоронні системи.
- ✱ *Засоби управління патчами і оновленнями:*
 - ✓ **Управління уразливостями** - використання програмного забезпечення для автоматичного застосування патчів і оновлень для операційних систем, програмного забезпечення і

мережевих пристроїв для виправлення уразливостей, які можуть бути використані зловмисниками для атак.

Таким чином, технічні засоби захисту становлять основу комплексної системи безпеки, де різні інструменти й технології працюють в єдиному механізмі для забезпечення захисту від різноманітних загроз, що виникають в інформаційних системах і мережах. Вони допомагають ефективно захищати дані, підтримувати цілісність і доступність ресурсів, а також запобігати несанкціонованому доступу та атакам.

Сучасні технічні засоби захисту повинні відповідати новим вимогам безпеки, оскільки технології постійно розвиваються, а загрози стають все складнішими. Враховуючи ці зміни, важливо не лише застосовувати традиційні методи захисту, але й використовувати новітні рішення, спрямовані на боротьбу з сучасними кіберзагрозами, а також враховувати вплив електромагнітних випромінювань і нові способи їх перехоплення. Робота сучасної електронної техніки супроводжується генерацією електромагнітних випромінювань, які можуть бути використані для відновлення оброблюваної інформації. Наприклад, за допомогою електромагнітного аналізу можна отримати чутливі дані, що передаються через провідні лінії або навколишнє середовище. Для цього можуть використовуватись спеціальні радіоелектронні засоби, навіть доступні для широкого загалу, для прийому та декодування електромагнітних випромінювань.

Заходи захисту включають екранування технічних засобів і кабельних ліній для зниження рівня випромінювань та запобігання перехопленню інформації, спеціалізовані пристрої для захисту від електромагнітних атак, такі як фарадєєві клітини для захисту приміщень, а також мікропроцесори та чіпи з поліпшеним захистом від електромагнітних витоків. Що стосується засобів захисту мереж і даних, вони включають міжмереві екрани (фаєрволи) для фільтрації та блокування небажаного трафіку на рівні мережі, а також системи виявлення та запобігання вторгненням (IDS/IPS), які дозволяють аналізувати трафік і фіксувати підозрілі дії, блокуючи атаки в реальному часі. Іншими важливими засобами є VPN для безпечного з'єднання між користувачами та корпоративними мережами. Для захисту даних використовуються методи шифрування, які залишаються основним інструментом забезпечення конфіденційності. Сучасні алгоритми шифрування, такі як AES, застосовуються для захисту інформації від несанкціонованого доступу як під час зберігання, так і при передачі даних. Крім того, важливими є антивірусні та антишкідливі програми для виявлення та боротьби з новими типами шкідливих програм,

а також аналіз поведінки програм для виявлення нових загроз, які ще не зафіксовані в базах даних антивірусів.

Механізми захисту від атак через фізичні канали включають використання спеціальних систем глушення або захисту від акустичних та оптичних витоків, а також захищені приміщення з екрануванням, що блокують витoki інформації через електромагнітні канали.

Одним з інноваційних напрямків є інтеграція технологій блокчейн для забезпечення цілісності даних і запобігання їх підробці чи несанкціонованому доступу, що забезпечує прозорість і контроль за всіма операціями, пов'язаними з даними, без необхідності залучення централізованих органів. Сучасні технічні засоби захисту постійно адаптуються до нових реалій кіберзагроз, і їх використання дозволяє ефективно протистояти як традиційним, так і новим видам атак, що виникають в результаті розвитку електронних і цифрових технологій.

Об'єкт технічного захисту інформації

Під об'єктом технічного захисту інформації зазвичай розуміють будівлі, приміщення, окремий основний технічний засіб або їх групу, об'єднану загальним призначенням, які підлягають захисту від проведення технічної розвідки.

Об'єкт може бути як однією зі складових, так і поєднувати у собі всі зазначені складові. Це залежить від таких факторів:

- Які види інформації необхідно захистити.
- У яких приміщеннях об'єкта циркулює ця інформація.

Якщо необхідно захистити велику кількість приміщень, то об'єктом захисту може бути вся будівля. У разі захисту кількох видів інформації, які циркулюють у приміщеннях, слід застосовувати комплексний підхід до захисту інформації.

Особливості розташування об'єктів захисту

Об'єкт захисту може знаходитися всередині іншого об'єкта, який в цілому не є об'єктом технічного захисту інформації. Наприклад, у будівлі з широким доступом можуть бути створені приміщення з обмеженим доступом для роботи з певними видами інформації.

Технічні засоби захисту інформації

До основних технічних засобів захисту інформації належать пристрої для обробки, зберігання та передавання закритої інформації. Також існують допоміжні технічні засоби для обробки відкритої інформації, які, однак, можуть утворювати технічні канали витoku закритої інформації.

Організація технічного захисту інформації

При організації технічного захисту інформації на об'єкті необхідно:

1. Визначити види інформації, що підлягають захисту.
2. Оцінити, які приміщення у будівлі (або сама будівля) потребують захисту.
3. З'ясувати ступінь «таємності» інформації з обмеженим доступом.
4. Виявити можливі загрози для інформації, які можуть бути реалізовані потенційним зловмисником.

Загрози для інформації

Загроза для інформації з технічного погляду – це:

- Витік інформації з обмеженим доступом.
- Блокування або порушення цілісності інформації.

Такі загрози можуть виникати під час використання технічних засобів, недосконалих із погляду захисту інформації, або через інші канали витоку інформації. Отже, для забезпечення надійного захисту необхідно враховувати потенційні загрози та вживати відповідних заходів для їх нейтралізації.

6.2. МЕТОДИ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Фізичний захист є критично важливою складовою загальної системи безпеки, оскільки він дозволяє забезпечити безпеку не лише фізичних приміщень, а й зберігати цілісність і доступність інформаційних систем. Фізичні методи захисту використовують автоматизовані механічні, електричні, електронні та інші пристрої, системи, що захищають споруди і приміщення від різноманітних загроз, таких як вогонь, вода, пил, корозійні гази, електромагнітне випромінювання, а також вандалізм і несанкціонований доступ. Сучасні технології для фізичного захисту можуть включати системи контролю доступу, відеоспостереження, інтелектуальні системи безпеки, а також активні та пасивні бар'єри.

Один з основних аспектів фізичного захисту — це підтримка оптимальних умов для роботи інформаційних систем, зокрема, контролювання температури (10–26 °C) та вологості (35–50%) в приміщеннях. Це важливо для запобігання перегріву електронних пристроїв і запобігання їх пошкодженню через надмірну вологість або сухість.

Захист від вогню здійснюється шляхом використання вогнестійких матеріалів для будівель, встановлення вогнегасних систем, автоматичних спринклерних систем та застосування матеріалів з низькою горючістю. Системи автоматичного виявлення і гасіння пожеж, оснащені сучасними

датчиками диму і температури, дозволяють оперативно виявити початок пожежі і нейтралізувати її до того, як вона стане неконтрольованою.

Захист від води включає використання спеціальних засобів для попередження затоплення, таких як системи водовідведення, аварійні резервуари для збору води, а також герметичні системи для зберігання критичних електронних і інформаційних компонентів. Системи, які стежать за рівнем води в підвальних приміщеннях та інших критичних зонах, допомагають швидко виявляти проблеми до того, як вони стануть серйозною загрозою.

Захист від пилу і корозійних газів реалізується через використання фільтруючих систем, що забезпечують чистоту повітря і запобігають забрудненню обладнання. Для цього використовуються високоякісні системи вентиляції та кондиціонування, які не тільки регулюють температурний режим, але й очищають повітря від пилу, диму, токсичних газів та інших шкідливих речовин.

Електромагнітне випромінювання може створювати серйозні ризики для інформаційних систем, тому важливо використовувати системи екранування, такі як фарадееві клітини, що блокують електромагнітні поля. Це дозволяє захистити комп'ютерні та телекомунікаційні мережі від несанкціонованого доступу через електромагнітні витоки.

Захист від несанкціонованого доступу до приміщень та обладнання включає фізичні бар'єри, такі як замки, контроль доступу через електронні системи (наприклад, біометричні сканери або карткові системи), а також відеоспостереження для моніторингу ситуації в реальному часі. Додатково можуть застосовуватися системи тривожної сигналізації, які автоматично повідомляють про спробу несанкціонованого доступу.

Всі ці засоби повинні бути інтегровані в єдину систему безпеки, де кожен бар'єр і засіб захисту визначається на основі цінності захищуваної інформації і ймовірного ризику. Важливою складовою є також регулярний моніторинг і обслуговування фізичних засобів захисту, що дозволяє вчасно виявляти та усувати потенційні загрози безпеці.

Напрями фізичного захисту

Існують кілька ключових напрямів фізичного захисту, які спрямовані на забезпечення безпеки інформаційних систем та їхньої інфраструктури. Кожен з цих напрямів включає в себе різноманітні заходи та технічні рішення, що дозволяють захистити від різноманітних загроз.

- ➔ захист від несанкціонованого доступу захист підтримуючої інфраструктури;
- ➔ захист від природних і техногенних катастроф;

- ➔ екранування від електромагнітних випромінювань;
- ➔ захист від вандалізму та фізичних пошкоджень;
- ➔ захист від зовнішніх атак через фізичні канали;
- ➔ захист інформації в перехідних зонах.

Заходи фізичного управління доступом

Заходи фізичного управління доступом є основою для забезпечення безпеки на підприємствах і в організаціях, особливо коли мова йде про захист чутливої інформації та обладнання. Одним із основних елементів фізичного контролю є електронні замки, що використовують картки доступу, PIN-коди або біометричні дані, такі як відбитки пальців, розпізнавання обличчя чи сітківки ока. Це дозволяє обмежити доступ до окремих приміщень лише для уповноважених осіб. Водночас, біометричні системи забезпечують додатковий рівень захисту завдяки унікальним фізіологічним характеристикам людини, що ускладнює можливість підробки доступу.

Для підвищення безпеки застосовуються також карткові системи доступу, де співробітники використовують спеціальні картки або електронні пристрої для входу в приміщення. Важливу роль у захисті мають кодові замки, які вимагають введення PIN-коду для доступу. Ці методи можуть використовуватися окремо або в поєднанні з іншими методами, створюючи мультимодальний контроль доступу, що забезпечує більш високий рівень безпеки.

Одним із важливих компонентів фізичного управління доступом є системи відеоспостереження. Вони дозволяють здійснювати моніторинг об'єктів у реальному часі та фіксувати всі події, що відбуваються на території підприємства. Системи інтелектуального відеоспостереження можуть автоматично виявляти підозрілі дії або спроби несанкціонованого доступу. Крім того, для виявлення спроб порушення безпеки вчасно встановлюються тривожні кнопки, які сповіщають охорону чи відповідні служби про несанкціоновані дії. Сучасні системи відеоспостереження часто інтегруються з іншими засобами фізичної безпеки, такими як системи контролю доступу чи сигналізації. Це дозволяє створити комплексну інфраструктуру, яка забезпечує максимальний рівень захисту. Записи відеоспостереження можуть бути використані як доказ у разі розслідування інцидентів безпеки. Регулярне обслуговування і оновлення обладнання відеоспостереження гарантує його надійну роботу та високу якість фіксації подій.

З метою обмеження доступу до найбільш чутливих територій використовуються фізичні бар'єри і огорожі. Вони можуть включати міцні

двері, що забезпечують захист від вандалізму, або огорожі на території, що обмежують доступ до важливих об'єктів. Для забезпечення належного контролю над переміщенням людей всередині будівлі застосовуються турнікети та бар'єрні системи, які дозволяють обмежити доступ до специфічних зон лише для осіб, що мають відповідні дозволи.

Під час встановлення фізичного контролю доступу важливим є також моніторинг і аудит всіх спроб входу в охоронювані приміщення. Системи контролю записують усі спроби доступу та зберігають дані для подальшого аналізу. Періодичний аудит доступу дозволяє перевіряти, чи відповідають записи про доступ дійсності, та виявляти можливі порушення політики безпеки. Такі системи можуть інтегруватися з іншими засобами безпеки, наприклад, з відеоспостереженням, для підвищення ефективності контролю. Звіти про доступ допомагають виявляти підозрілі дії, аналізувати поведінку співробітників і відстежувати несанкціоновані спроби проникнення. Це сприяє створенню прозорості системи безпеки, де всі події документуються і можуть бути перевірені. Крім того, регулярне оновлення систем і перевірка їхньої працездатності є критично важливими для забезпечення безперервного захисту.

Завдяки комплексному використанню цих заходів можна ефективно контролювати доступ до критичних приміщень і забезпечити належний рівень захисту від несанкціонованого проникнення, зменшити ризик фізичних пошкоджень обладнання і технічних ресурсів, а також мінімізувати загрози витоку або втрати важливої інформації. Важливим елементом цього процесу є не лише технічні засоби, а й чітка організація внутрішніх політик безпеки, навчання персоналу і регулярне оновлення систем захисту відповідно до нових загроз. Тільки такий підхід може гарантувати стабільний захист інформаційних активів і ефективне функціонування організації в умовах постійно змінюваного кіберзагрози.



Рис. 6.1. Приклади заходів фізичного управління доступом

Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity>

Заходи фізичного управління доступом є:

- ✱ надвисокочастотні, ультразвукові й інфрачервоні системи, призначені для виявлення об'єктів, що рухаються в межах розташування ІКС та її ресурсів з умов визначення їхніх розмірів, швидкості й напрямку переміщення;
- ✱ лазерні й оптичні системи, що реагують на перетинання порушниками світлових променів;
- ✱ периметрові телевізійні системи, призначені для спостереження за охоронюваними об'єктами, в межах яких знаходиться ІКС та її ресурси;
- ✱ пропускні системи на базі технологій *smart-card, touch-memory*, це охорона, двері із замками, перегородки, телекамери, датчики руху і багато іншого.



Все це дозволяє ефективно контролювати і обмежувати вхід та вихід співробітників і відвідувачів на території організації, а також в окремі зони, де зберігається чутлива інформація. Особливо важливо контролювати доступ до приміщень, де розташовані сервери, комунікаційна апаратура, обладнання для зберігання даних та інші критичні елементи інформаційної інфраструктури. Сервери, наприклад, не повинні знаходитися відкрито або в кімнатах без належного захисту. Такі приміщення повинні бути закритими на замок, а також перебувати під цілодобовим наглядом охорони або систем відеоспостереження.

Особливу увагу слід приділяти мобільним та портативним комп'ютерам, які є привабливими об'єктами для крадіжки. Ці пристрої часто залишаються без нагляду, як у робочих приміщеннях, так і в автомобілях чи інших відкритих місцях. Вкрасти мобільний комп'ютер, на якому можуть зберігатися важливі дані, досить легко. З цієї причини організаціям, які дбають про безпеку своїх інформаційно-комунікаційних систем (ІКС), необхідно вживати заходів для захисту мобільних пристроїв та носіїв інформації від крадіжки. Це можуть бути як фізичні засоби захисту (надійні замки, сейфи для зберігання пристроїв), так і програмні рішення, такі як системи шифрування даних і віддалене стирання даних при втраті пристрою.

Що стосується витоку даних, то сучасні загрози включають не тільки традиційні методи, як-от зчитування документів зі сміття або копіювання

інформації з незащитених пристроїв, а й складніші методи перехоплення даних. Наприклад, сучасні методи деаудіту мережних пакетів дозволяють зловмисникам отримувати доступ до інформації, що передається через зашифровані канали зв'язку. Крім того, існують супутникові канали зв'язку, які можуть бути використані для перехоплення переданих даних, особливо якщо організація використовує ці канали для передачі критично важливої інформації.

Також можуть бути використані технічні канали витоку інформації, які важко виявити та блокувати. Наприклад, електромагнітні випромінювання комп'ютерної техніки можуть бути використані для відновлення оброблюваної інформації, що дає змогу здійснювати електронний шпигунство. Для цього можуть використовуватись не лише складні та дорогі технічні засоби, але й прості доступні прилади, що зловмисник може легко придбати. Тому важливо враховувати усі потенційні канали витоку і використовувати різні методи захисту, такі як екранування приміщень, захист від електромагнітних витоків, а також застосування фільтрації мережевого трафіку та шифрування даних на всіх етапах їх передачі.

З метою запобігання витокам важливо також здійснювати регулярний моніторинг і аудит безпеки, впроваджувати сучасні засоби захисту інформації, що дозволяють своєчасно виявляти потенційні загрози, а також оперативно реагувати на інциденти безпеки.

6.3. ХАРАКТЕРИСТИКА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Інформаційно-комунікаційні системи, зокрема комп'ютери, мережеві пристрої та інші електронні засоби, при своєму функціонуванні створюють різноманітні випромінювання, що можуть стати каналами витоку інформації. Ці випромінювання можуть бути як електромагнітними, так і акустичними, а іноді й оптичними, і вони виникають внаслідок обробки, зберігання або передачі даних. Подібні побічні ефекти можуть поширюватися в навколишньому просторі на досить значні відстані, іноді до сотень метрів, що дозволяє зловмисникам виявляти їх і використовувати для отримання чутливої інформації без прямого доступу до самих систем.

Електромагнітне випромінювання є однією з основних загроз у цьому контексті. Кожен електронний пристрій генерує електромагнітні хвилі, які можуть не тільки впливати на інші пристрої, але й бути зловмисно використаними для збору даних. Для цього зловмисники можуть використовувати спеціалізовані засоби, які дозволяють приймати ці

сигнали і відновлювати з них важливу інформацію, наприклад, дані, що передаються через незахищені канали або зберігаються на пристроях.

Акустичні випромінювання також є серйозною загрозою. Такі пристрої, як клавіатури, комп'ютерні миші, принтери або навіть дисплеї, можуть створювати звукові коливання, що в подальшому можуть бути перехоплені і проаналізовані для відновлення вхідних або вихідних даних. Всі ці акустичні та електромагнітні ефекти створюють потенційні канали витоку інформації, особливо коли йдеться про особливо чутливі дані, такі як паролі, фінансова інформація або інші важливі документи.

Захист від таких витоків включає застосування різноманітних методів екранування і захисту, таких як використання спеціальних матеріалів, які блокують електромагнітні хвилі, шумоізоляція для уникнення акустичних витоків, а також забезпечення надійної фізичної безпеки самих інформаційних систем. Застосування шифрування даних та регулярний моніторинг інформаційних потоків є додатковими заходами для запобігання витокам через технічні канали.

Технічний канал витоку інформації – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки. Також враховуються і завади, що діють на вході засобу технічної розвідки.



Рис. 6.1. Технічний канал витоку інформації

Джерело: побудовано автором

Залежно від природи походження розрізняють такі типи каналів витоку інформації з обмеженим доступом:

- ❖ *радіоканали, або електромагнітні канали* – є наслідком електромагнітних хвиль навколо електронних та електричних пристроїв і зумовлені протіканням змінного струму в провідниках;
- ❖ *віброакустичні* – зумовлені поширенням звукових хвиль (аудіоінформація) у матеріальному середовищі (зокрема, у повітрі, рідині, елементах конструкцій і облаштування приміщень);

- ❖ *електричні* – виникають під час роботи електронних засобів обробки інформації внаслідок протікання струму в різних провідниках;
- ❖ *візуально-оптичні* – зумовлені випромінюванням або відбиттям від деяких об'єктів потоку фотонів (світла);
- ❖ *канали несанкціонованого доступу* – є наслідком неправомірного втручання у роботу комп'ютерної техніки;
- ❖ *матеріально-речові* – зумовлені можливістю крадіжки деяких матеріальних носіїв або об'єктів, які містять інформацію з обмеженим доступом.

Крім того, слід зазначити, що залежно від умов виникнення інформативного сигналу технічні канали витоку інформації можна поділити на природні та спеціально створені:

- природні канали витоку інформації утворюються за рахунок побічних електромагнітних випромінювань, що виникають при обробці інформації засобами обчислювальної техніки і зв'язку (ЗОТЗ) (електромагнітні канали витоку інформації), а також внаслідок наведень інформативних сигналів у лініях електроживлення та заземлення ЗОТЗ, сполучних лініях допоміжних технічних засобів і сторонніх провідниках (електричні канали витоку інформації); спеціально створювані канали витоку інформації створюються через впровадження в ЗОТЗ електронних пристроїв прихованого перехоплення інформації (закладних пристроїв) та шляхом реалізації методу високочастотного опромінення ЗОТЗ.

Слід звернути увагу на особливості перших двох технічних каналів витоку інформації, оскільки вони є найбільш поширеними на практиці та складними для блокування. Розглянемо їх більш детально.

Виникнення радіоканалів витоку зумовлене випромінюванням різноманітними радіо- та електроприладами електромагнітних хвиль у діапазонах від наддовгих із довжиною хвилі 10 тис. м (частоти менше 30 Гц) до субміліметрових із довжиною хвилі 1–0,1 мм (частоти від 300 до 3000 ГГц). Залежно від властивостей, зокрема особливостей розповсюдження у просторі, під час розгляду електромагнітних випромінювань розрізняють кілька діапазонів хвиль: наддовгі, довгі, середні, короткі та ультракороткі.

Випромінювання з відносно великою довжиною хвилі (орієнтовно не менше 15–20 м) за рахунок відбиття від верхніх шарів атмосфери здатні розповсюджуватися на значні відстані, що перевищують сотні кілометрів. На відміну від них, випромінювання з довжиною хвилі, що не перевищує 10 м, зазвичай розповсюджуються в межах прямої видимості на кілька десятків кілометрів. На розповсюдження хвиль суттєво впливає наявність

на їхньому шляху природних та штучних перешкод, суцільних конструкцій з бетону та металу. Можливість на певній відстані скористатися інформацією, яку вони переносять, також залежить від потужності випромінювання та рівня природних і штучних завад, які завжди присутні в ефірі. Зокрема, відповідні завади у містах утворюються обладнанням електротранспорту, електрозварювальними апаратами, роботою теле- та радіостанцій тощо.

Утворення побічних (не пов'язаних із безпосереднім функціонуванням обладнання) електромагнітних випромінювань у засобах електронної та електричної техніки зумовлюється низкою фізичних процесів у цих засобах. Наприклад, для отримання зображення на екрані монітору до нього подаються досить високі змінні напруги, що утворюють відповідні електромагнітні коливання. Унаслідок цього може виникати радіоканал витоку інформації з обмеженим доступом. Радіоканали витоку інформації мають ще одну назву – канали побічних електромагнітних випромінювань та наведень (ПЕМВН).

Слух людини є другим за інформативністю джерелом отримання відомостей про навколишній світ. Під час проведення нарад, конференцій тощо можуть обговорюватися дані, що становлять таємницю. При цьому коливання молекул повітря, яке послідовно та синхронно зі звуком передається у просторі, призводить до виникнення віброакустичного каналу витоку інформації.

Якщо на шляху звуку немає перешкод, він рівномірно розповсюджується у всіх напрямках. У разі виникнення у певному напрямку перешкоди у вигляді стін, вікон, стель, дверей, радіаторів опалення або інших конструкцій, ці конструкції під тиском звукових хвиль також починають коливатися та передавати зазначені інформативні сигнали далі.

Звичайна людина може почути звук у звуковому діапазоні частот (від 16 до 20 000 Гц). Діапазон звуків мови охоплює полосу частот від 100 до 6 000 Гц. У віброакустичному каналі перенесення інформації про роботу певних видів обладнання може відбуватися у ширших межах – ультразвуковому (вище 20 000 Гц) та інфразвуковому (нижче 16 Гц) діапазонах. У більш щільних і кристалічних середовищах (метал, камінь тощо) звук розповсюджується значно краще й на більшу відстань, ніж у нещільних та аморфних.

Технічні канали витоку інформації є одним із ключових аспектів у сфері інформаційної безпеки. Вони являють собою будь-які засоби чи механізми, за допомогою яких інформація може бути несанкціоновано передана, витікати або бути зчитана сторонніми особами. Витоки

інформації через технічні канали можуть статися як через фізичні, так і через електронні або електромагнітні канали. Основні типи технічних каналів витоку інформації:

✱ **Електромагнітні випромінювання (EMI):**

✓ Кожна електронна техніка, зокрема комп'ютери, сервери та інші пристрої, генерує електромагнітне випромінювання, яке можна використовувати для витоку інформації. Зловмисники можуть здійснювати електромагнітне шпигунство, збираючи сигнали, що передаються з пристроїв. Це дозволяє відновити дані, що обробляються, навіть без прямого доступу до системи.

✓ Методи захисту включають використання спеціальних екранувальних матеріалів, що знижують рівень випромінювання, а також засоби для контролю за рівнем електромагнітних випромінювань.

✱ **Акустичний витік (акустичний шпигунство):**

✓ Акустичний витік інформації відбувається через звукові хвилі, які генеруються технічними пристроями, зокрема через клавіатуру комп'ютера, мишу, екрани тощо. Також можливе використання звукових витоків через вентиляційні системи або відбитки голосу користувачів під час розмов.

✓ Захист від акустичних витоків включає в себе шумопоглинальні матеріали та моніторинг звукових каналів в критичних приміщеннях.

✱ **Мережеві канали витоку:**

✓ Перехоплення даних, що передаються через комп'ютерні мережі (наприклад, через Інтернет або локальні мережі), є одним з найпоширеніших методів витоку інформації. Включає перехоплення незашифрованих пакетів даних, спостереження за мережевим трафіком (наприклад, через man-in-the-middle атаки), а також недобросовісне використання відкритих Wi-Fi мереж.

✓ Для захисту використовуються технології шифрування, VPN-з'єднання, фаїрволи, а також моніторинг і фільтрація мережевого трафіку.

✱ **Оптичний витік:**

✓ Технічні засоби можуть видавати інформацію через оптичні канали, такі як пристрої відображення або передачі зображення, екран монітора. Можливий витік даних через відбитки на екрані або через відкриті веб-камери.

✓ Захист від таких витоків включає екранування моніторів або використання спеціальних антиглейз-сіток на екранах, що дозволяють зменшити відображення даних для сторонніх осіб.

✱ **Витік через порти вводу/виводу (I/O порти):**

✓ Витік може здійснюватися через несанкціоноване підключення зовнішніх пристроїв до комп'ютера або інформаційної системи, таких як USB-накопичувачі, зовнішні жорсткі диски, мережеві кабелі і т. д.

✓ Проти цього використовуються системи контролю доступу до портів, шифрування даних на пристроях і політики щодо використання зовнішніх пристроїв.

✱ **Фізичний витік через документи та носії інформації:**

✓ Поширеним методом витоку інформації є крадіжка або несанкціоноване копіювання документів або носіїв інформації. Документи можуть бути викинуті в смітник без належної утилізації або залишені без нагляду.

✓ Для запобігання цьому використовуються системи утилізації документів, безпечне зберігання носіїв інформації в спеціальних сховищах і жорсткі політики щодо доступу та зберігання чутливої інформації.

✱ **Супутникові канали витоку:**

✓ Витік інформації може відбуватися через супутникові канали зв'язку, які використовуються для передачі даних на великі відстані. Це стосується як зашифрованих, так і нешифрованих даних.

✓ Для захисту використовуються системи криптографічного захисту і обмеження доступу до супутникових каналів.

Захист від витоків інформації через технічні канали вимагає комплексного підходу, включаючи як фізичний захист, так і застосування сучасних технологій безпеки, таких як шифрування, моніторинг, аудит, екранування та системи контролю доступу.

Витік інформації – неконтрольоване поширення інформації від носія інформації через фізичне середовище до технічного засобу, який здійснює перехоплення інформації.

Перехоплення інформації – неправомірне отримання інформації з використанням технічного засобу, який здійснює виявлення, прийом і обробку інформативних сигналів.

Безконтрольний витік інформації, що зберігається та обробляється в ІКС, може відбуватися через різноманітні технічні канали. Це являє собою серйозну загрозу для конфіденційності та цілісності даних, оскільки витіки можуть бути здійснені без явного фізичного доступу до системи або її компонентів. Технічні канали витіку включають:

1. Електромагнітні випромінювання

Будь-яка електронна система, що обробляє або передає інформацію, генерує електромагнітні хвилі. Вони можуть використовуватися зловмисниками для відновлення даних без необхідності безпосереднього підключення до системи. Спеціалізовані пристрої дозволяють виявляти та аналізувати ці випромінювання на відстані, що створює потенційний канал для витіку інформації.

2. Акустичні випромінювання

Всі пристрої, що мають механічні або електронні компоненти, можуть створювати звукові коливання (акустичні сигнали), які можуть бути зафіксовані мікрофонами або іншими спеціалізованими пристроями. Наприклад, навіть звуки натискання клавіатури можуть бути використані для відновлення введених даних, що становить загрозу витіку.

3. Інфрачервоні та оптичні канали

Оптичні випромінювання, які генеруються моніторами, принтерами чи іншими пристроями, можуть також бути використані для перехоплення інформації, особливо якщо система не забезпечена достатнім рівнем захисту.

4. Мережеві канали

Під час передачі даних через мережу існує ризик перехоплення інформації. Ненадійні або незашифровані канали зв'язку є відкритими для атак, таких як прослуховування або аналіз мережевих пакетів, що дозволяє зловмисникам отримати доступ до конфіденційних даних.

5. Електричні наводки

На електричні лінії, що з'єднують комп'ютерні системи та інші пристрої, можуть бути накладені електричні імпульси, що дозволяють витікати інформацію під час її обробки або передачі.

Технічні канали витіку є складною проблемою, оскільки часто вони не є очевидними і можуть не мати фізичних проявів, що ускладнює їх виявлення. Тому для ефективного захисту ІКС необхідно вжити низку заходів, таких як використання екранів для електромагнітних випромінювань, акустичну ізоляцію, застосування шифрування даних при їх передачі, а також контроль доступу до технічних засобів і моніторинг активності у мережі.

Технічний канал витоку інформації, так само як і канал передачі інформації, складається з:

➔ **джерела сигналу**

Це пристрій або система, що генерує інформаційний сигнал, який може стати основою для витоку. У випадку інформаційних систем, джерелом можуть бути комп'ютери, мережеві пристрої, сервери, принтери та інші електронні компоненти, що обробляють або передають дані. Цей сигнал може бути як електричним, так і акустичним або навіть оптичним, залежно від типу витоку.

➔ **фізичного середовища його поширення**

Це простір або середовище, через яке сигнал передається до приймальної апаратури. Це може бути повітря, що передає електромагнітні хвилі, або матеріали, що служать середовищем для акустичних або оптичних випромінювань. Природа середовища визначає, на які відстані сигнал може бути поширений і яку потужність він має для виявлення. Наприклад, електромагнітні хвилі можуть передаватися на сотні метрів, а акустичні сигнали — лише на кілька десятків метрів, залежно від умов.

➔ **приймальної апаратури зломисника**

Це пристрій або система, яка призначена для виявлення, прийому та декодування сигналу, що витікає. Це можуть бути спеціалізовані радіоелектронні засоби для прийому електромагнітних випромінювань, мікрофони для запису акустичних сигналів, або інші технічні пристрої, які дозволяють відновити передану інформацію. Приймальна апаратура може використовуватися для аналізу мережевих пакетів, перехоплення інформації з електричних ліній або навіть для прослуховування звуків у приміщенні.

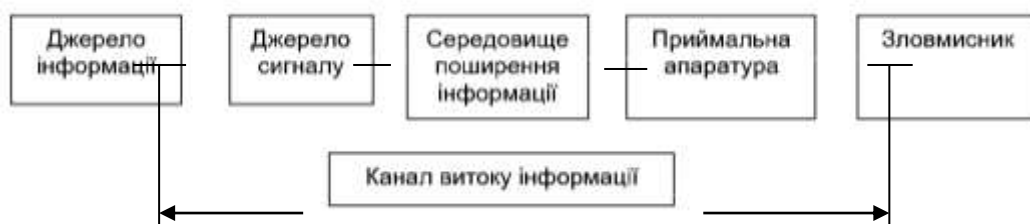


Рис. 6.2. Схема технічного каналу витоку інформації

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Загалом, ці компоненти створюють технічний канал витоку інформації, де кожен етап може бути використаний зломисником для здійснення несанкціонованого доступу до конфіденційних даних. Тому важливо вживати заходів для контролю і обмеження доступу до кожного з цих

компонентів, щоб забезпечити захист від витоків інформації через технічні канали.

Джерела сигналу

Джерелами сигналу є технічні засоби, які здійснюють обробку інформації, а також:

- об'єкти, що віддзеркалюють електромагнітні або акустичні хвилі;
- об'єкти, що випромінюють власні електромагнітні хвилі в різних діапазонах;
- джерела акустичних сигналів;
- передавачі функціональних каналів зв'язку;
- спеціальні приховані технічні пристрої, так звані «жучки» різної природи;
- побічні електромагнітні випромінювання і наведення (ПЕВН).

Середовище поширення сигналу

Середовище поширення сигналу — це фізичне або електромагнітне середовище, через яке сигнал передається від джерела до приймальної апаратури. Це критичний компонент технічного каналу витoku інформації, оскільки від його властивостей залежить ефективність і дальність передачі сигналу, що може бути використаний зловмисниками для несанкціонованого доступу до інформації. Середовище поширення сигналу може бути різним і включати такі основні типи:

1. Повітря

Це найпоширеніше середовище для поширення електромагнітних хвиль, акустичних сигналів і радіосигналів. Електромагнітні випромінювання можуть поширюватися через повітря на великі відстані, що дозволяє зловмисникам отримувати дані через бездротові мережі, навіть без фізичного доступу до пристроїв. Середовище повітря дозволяє також передавати акустичні сигнали, що може використовуватися для прослуховування і відновлення інформації.

2. Кабельні системи (провідні середовища)

Сигнали можуть передаватися через дроти та кабелі, такі як електричні лінії, телефонні та мережеві кабелі. Вони можуть бути схильні до перехоплення електричних наводок або впливу зовнішніх сил, що дозволяє зловмисникам зчитувати інформацію, що передається через кабелі (наприклад, через витік даних через неекрановані кабелі). Ці канали часто використовуються для передачі даних у комп'ютерних мережах, що створює потенційну загрозу витoku через компрометацію середовища поширення сигналу.

3. Оптичні середовища

Світлові сигнали, що передаються через волоконно-оптичні лінії, також можуть бути об'єктом перехоплення. Хоча оптичні волокна забезпечують високий рівень безпеки завдяки тому, що вони обмежують можливості витоку інформації в порівнянні з електричними або радіохвилями, вони все ж можуть піддаватися фізичному втручанню або бути уразливими для лазерних атак, коли зломисник може зчитати світлові сигнали.

4. Механічні середовища

Механічні випромінювання, такі як вібрації, також можуть бути середовищем для поширення сигналів. Наприклад, звуки, що виникають при роботі технічних пристроїв (наприклад, натискання клавіатури або робота принтерів), можуть поширюватися через тверді поверхні, стіни або інші матеріали. Вібрації можуть бути записані за допомогою спеціальних датчиків або мікрофонів, що дозволяє зломисникам відновити інформацію, яка була оброблена на комп'ютері.

5. Електричні наводки

Певні матеріали і пристрої можуть спричиняти електричні наводки, через які можуть передаватися сигнали з електричних ліній, що з'єднують різні пристрої в мережі. Ці наводки можуть використовуватися для перехоплення даних на відстані, що є ще одним потенційним каналом витоку інформації.

6. Вода та інші природні середовища

У специфічних умовах, таких як підводні комунікації, сигнали можуть також поширюватися через воду. Це вимагає спеціалізованих технологій для зчитування сигналів у таких середовищах, але також може бути використано зломисниками для перехоплення інформації в таких середовищах, як морські або підземні мережі.

Середовище поширення сигналу визначає не лише фізичні властивості каналу витоку інформації, але й певні методи захисту, які повинні бути впроваджені для запобігання витоку. Наприклад, екранізація кабелів, використання спеціальних засобів для захисту від радіовипромінювань, ізоляція акустичних сигналів і шифрування даних дозволяють зменшити ризик витоку через технічні канали.

Розподіл технічних каналів витоку інформації

- ➔ акустичні;
- ➔ оптичні;
- ➔ радіоелектронні.

Акустичні канали

Витік інформації через акустичні хвилі, що можуть бути перехоплені за допомогою спеціальних мікрофонів або інших слухових пристроїв. Наприклад, шуми або звуки, які виникають при натисканні клавіатури, роботі комп'ютерних систем або обладнання, можуть бути використані для витоку інформації.

Акустичний канал – це канал передачі інформації, що здійснюється через акустичні хвилі, які можуть бути перехоплені за допомогою спеціалізованих пристроїв для слуху або запису. Витік інформації через акустичні канали може бути здійснений в кілька способів, і це є важливим аспектом захисту інформації в різних організаціях.

Приклади технологій на основі акустичних каналів витоку інформації:

✿ Електронні пристрої, що створюють шуми

Практично всі електронні пристрої, такі як комп'ютери, сервери, мережеві пристрої, генератори сигналів і т. п., створюють певні акустичні сигнали під час роботи. Наприклад, шум вентилятора, звуки від натискання клавіш на клавіатурі, а також різні інші механічні звуки можуть використовуватися для отримання інформації. Спеціалізовані мікрофони можуть використовуватися для запису цих звуків, що дозволяє відновити частину переданої або оброблюваної інформації, включаючи введені дані, паролі чи навіть важливі повідомлення, що зберігаються або передаються через комп'ютерні мережі. Щоб уникнути такого роду витоків інформації, важливо застосовувати захисні заходи, зокрема обмеження акустичної доступності до чутливих пристроїв, використання спеціальних шумопоглинаючих матеріалів і програмного забезпечення для шифрування введених даних.

✿ Витік інформації через звуки від натискання клавіатури

Спостереження за звуками, що виникають при натисканні клавіатури, може дозволити зловмиснику зробити висновки про те, які клавіші натискалися, а отже, отримати частину введеної інформації. Наприклад, можна використовувати високочутливі мікрофони для запису звуків натискання клавіш, що дозволяє відновити текст, який був введений. Такі атаки часто базуються на аналізі частотних характеристик та тривалості звуків, які видають різні клавіші. Подібні методи можуть використовуватися для перехоплення паролів або інших конфіденційних даних, введених на клавіатурі. Для захисту від такого типу витоку

інформації рекомендується використовувати програмні засоби, які генерують білий шум, або спеціальні клавіатури з низьким рівнем звукового сигналу. Крім того, можна застосовувати фізичні екрани для звукової ізоляції робочих місць, що ускладнює запис і аналіз акустичних сигналів.

✳ Акустичні випромінювання з дисплеїв

Сучасні дисплеї, особливо старі екрани CRT, можуть випромінювати акустичні хвилі, що є результатом їхньої роботи. Спеціалізовані пристрої можуть захоплювати ці звуки і намагатися відновити інформацію, яка відображається на екрані. Це явище, яке відоме як акустичне виявлення зображень, використовує технології для аналізу звуків, що виникають при роботі екрана, і дозволяє зловмисникам відновити частину або всю інформацію, що відображається на дисплеї, без фізичного доступу до пристрою. Для зменшення таких ризиків рекомендується використовувати екрани з меншим рівнем акустичних випромінювань, а також застосовувати методи захисту, такі як екранування і використання захисних фільтрів для екранів, які блокують акустичні хвилі.

✳ Еманація електричних і магнітних полів

Акустичні хвилі також можуть виникати внаслідок електричних і магнітних полів, які створюються електронними пристроями. Відомо, що комп'ютери, телевізори, монітори і навіть мобільні телефони можуть випромінювати певні акустичні сигнали, які можна фіксувати. Типовими прикладами таких загроз є атаки типу TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmission), коли використовується спеціальне обладнання для зчитування електромагнітного випромінювання, що виходить із комп'ютерів, моніторів або мережевих пристроїв, щоб відновити введену або передану інформацію. Виявлення та перехоплення таких сигналів може призвести до витоку конфіденційних даних, таких як паролі, кредитні картки, тексти чи навіть зображення.

✳ Акустичні канали з допомогою ультразвукових сигналів

Акустичні канали за допомогою ультразвукових сигналів — це одна з найновіших загроз у сфері кібербезпеки, яка використовує високочастотні звукові сигнали для передачі даних без фізичного з'єднання. Ультразвукові сигнали, які не чутні людським вухом, можуть бути використані для дистанційного перехоплення, передачі або відновлення інформації, що обробляється на пристроях, таких як комп'ютери, мобільні телефони, або інші мережеві пристрої. Як це працює? Високочастотні ультразвукові хвилі (зазвичай вище 20 кГц) можуть бути використані для передачі даних на короткі відстані, що дозволяє створити акустичний канал зв'язку між

пристроями. Це може бути зроблено за допомогою спеціалізованих мікрофонів або сенсорів, які здатні захоплювати ці сигнали. Ультразвукові канали можуть бути використані зловмисниками для таких цілей: передача даних між пристроями — зловмисники можуть відправляти конфіденційну інформацію, наприклад, паролі або важливі дані з однієї системи на іншу без використання звичайних мережевих каналів; шифрування даних — за допомогою ультразвукових сигналів можна передавати зашифровані дані, що забезпечує більшу непомітність для засобів моніторингу; атаки на бездротові системи — зловмисники можуть використовувати ультразвукові канали для знищення або викрадення даних з пристроїв, що перебувають у фізичній близькості, без необхідності підключатися до мережі. Механізм атаки включає пошук уразливості, коли ультразвукові канали можуть бути налаштовані через спеціальне програмне забезпечення, яке перетворює дані на ультразвукові сигнали, що можуть передаватися через акустичні канали, та використання пристроїв для зловмисників, зокрема спеціалізованих мікрофонів або приймачів, здатних фіксувати ці ультразвукові сигнали і відновлювати передану інформацію. Для захисту від ультразвукових атак застосовуються різні методи, зокрема екранування акустичних каналів, використання матеріалів, які блокують або поглинають ультразвукові хвилі, шумопоглинальні технології, встановлення генераторів шуму, що перешкоджають передачі ультразвукових сигналів, моніторинг акустичних каналів, регулярне аудиторське спостереження та перевірка на наявність нестандартних акустичних сигналів, а також шифрування даних, що знижує ризик витоку важливої інформації при їх передачі через будь-які канали, в тому числі акустичні. Акустичні канали з ультразвуковими сигналами є важливою новою загрозою, яка потребує особливої уваги при розробці заходів безпеки для захисту конфіденційної інформації, що передається через мережі та інші системи.

Акустичні канали можна класифікувати на **повітряні, вібраційні, електроакустичні і оптико-акустичні**.

В акустичному каналі витоку інформації джерелом сигналу можуть бути людські розмови, звуковідтворююча апаратура або інші звукові коливання, що виникають під час обробки даних чи взаємодії з технічними пристроями. Середовище поширення для цих звукових хвиль може бути різноманітним, включаючи повітря, рідини або тверді тіла, в яких звукові хвилі викликають механічні коливання, що в свою чергу передають акустичну інформацію.

Як приймачі акустичних сигналів для цього каналу витоку інформації використовуються різноманітні пристрої, включаючи спрямовані та ненаправлені мікрофони, радіомікрофони, диктофони, стетоскопи та інші технічні засоби

знімання звукової інформації. Спрямовані мікрофони, завдяки своїй високій чутливості та здатності фокусувати звук на конкретній точці, дозволяють прослуховувати розмови або звуки на відстані до 300-500 метрів в умовах відкритого простору. У міських умовах ця відстань може зменшуватися до 50-70 метрів через наявність шуму та перешкод.

Ці пристрої дозволяють зловмисникам збирати важливу інформацію без фізичного контакту з об'єктом, що робить акустичний канал одним із найбільш небезпечних каналів витоку для конфіденційної інформації. Оскільки ці пристрої можуть бути приховані або віддалені від об'єкта, важливо застосовувати спеціальні методи для зниження ймовірності витоку звукової інформації, такі як використання звукопоглинаючих матеріалів і шумових маскування, що мінімізують можливість перехоплення сигналу.

В основному використовуються три види спрямованих мікрофонів:

➤ **параболічні (рефлекторні)**

Ці мікрофони мають форму параболи, що дозволяє концентрувати звукові хвилі в одну точку, забезпечуючи високий рівень чутливості. Параболічні мікрофони здатні ефективно прослуховувати звуки на великих відстанях, часто використовуються для запису звуків, що виникають на значних відстанях від джерела. Вони ідеально підходять для використання в охоронних системах або в природничих дослідженнях, де необхідно фіксувати звуки, недоступні звичайним мікрофонам. Завдяки своїй спрямованості, параболічні мікрофони зводять до мінімуму фонові шуми, забезпечуючи чистий і точний звук.

➤ **трубчасті («мікрофон-труба»)**

Вони відомі своєю високою чутливістю та здатністю фіксувати навіть найменші звукові коливання. Ці мікрофони широко використовуються в системах прослуховування завдяки точності та широкому діапазону частот. Вони працюють на основі змінювання електричного поля між двома пластинами, одна з яких є тонким діафрагмою, що реагує на звукові хвилі. Трубчасті мікрофони забезпечують високу спрямованість, що дозволяє мінімізувати вплив сторонніх шумів і записувати звук виключно з визначеного напрямку. Завдяки компактному дизайну та простоті у використанні, вони ідеально підходять для спеціалізованих задач, таких як акустичний моніторинг чи приховане прослуховування.

➤ **плоскі (мікрофонні ґрати)**

Ці мікрофони використовують ґантельну форму, щоб зібрати звук з певного напрямку. Ґантельний мікрофон має дві антени, що дають можливість зібрати звук із двох різних точок, фокусуючи сигнал на конкретному напрямку. Це дозволяє зменшити шум з інших напрямків та

підвищити чіткість сигналу, що перехоплюється. Плоскі мікрофони (мікрофонні ґрати) зазвичай застосовуються для запису звуку в умовах, де важливо уникати сторонніх шумів і фокусуватися на джерелі звуку. Вони ефективно працюють у великих приміщеннях або на відкритих майданчиках, забезпечуючи високу якість запису навіть у складних акустичних умовах. Завдяки своїй конструкції ці мікрофони також можуть бути використані для сканування звукових сигналів у певному діапазоні частот.



Рис. 6.3. Технічні канали витоку акустичної інформації
Джерело: [1-7]

Щоб перехопити інформацію через акустичні канали за допомогою спрямованого мікрофону, необхідно забезпечити точне націлювання на джерело звукових коливань. Це є важливим аспектом, оскільки такі мікрофони мають високу чутливість і здатні вловлювати звукові сигнали на значних відстанях, однак для цього вони повинні бути спрямовані на конкретне джерело звуку. Сучасні спрямовані мікрофони можуть вловлювати звуки на відстані до кількох сотень метрів, що робить їх ефективним інструментом для перехоплення акустичних сигналів, таких як звуки натискання клавіатури, розмови чи інші шуми, що виникають

внаслідок роботи комп'ютерних або електронних пристроїв. Для ефективного перехоплення важливо мати доступ до простору, в якому знаходиться джерело звуку, і використовувати відповідне обладнання для фіксації звукових хвиль.

Зловмисники можуть також використовувати спеціалізоване обладнання для обробки отриманих акустичних сигналів, що дозволяє відновити інформацію, яку передають або обробляють пристрої. Це може бути корисним для відновлення введених даних, таких як текст, паролі або інші конфіденційні дані, що звучать під час роботи з пристроєм. Для запобігання перехоплення інформації через акустичні канали важливо застосовувати заходи, що включають використання шумопоглинаючих матеріалів, регулярний контроль за акустичним середовищем, а також застосування засобів для перешкоджання акустичному моніторингу, наприклад, генератори білого шуму.

Таким чином, для перехоплення інформації через акустичні канали справді потрібна не лише висока точність націлювання, а й наявність спеціалізованого обладнання та технологій для збору і аналізу звукових коливань. Використання чутливих мікрофонів, спеціалізованих сенсорів та програмного забезпечення для обробки акустичних сигналів дозволяє зловмисникам захоплювати звуки, які видають пристрої під час обробки інформації. Це може включати шифровані дані, введені паролі, текст, що набирається на клавіатурі, або навіть інформацію, що відображається на екрані пристроїв.

Такий тип атаки є важким для виявлення через його акустичну природу, і традиційні засоби захисту, орієнтовані на мережеві або програмні загрози, не завжди можуть запобігти такому перехопленню. Це робить акустичні канали серйозною загрозою для інформаційної безпеки, що вимагає розробки спеціалізованих стратегій захисту, зокрема використання шумопоглинальних матеріалів, генераторів білого шуму та постійного моніторингу акустичних характеристик середовища.



Рис. 6.4. Спрямовані мікрофони

Джерело: [1-7]

Радіомікрофони або мікрофонні радіозакладки — це мініатюрні радіопередавачі, що вбудовані в мікрофони і здатні передавати звук на відстань. Завдяки своїм компактним розмірам, ці пристрої можуть бути легко приховані в різних об'єктах, таких як елементи декору, технічні пристрої, звичайні розетки електроживлення або навіть в елементах одягу, авторучках, запальничках та інших предметах. Це дає змогу зловмисникам безшумно та непомітно здійснювати прослуховування без потреби в очевидних або великих пристроях. Мікрофонні радіозакладки працюють на різних частотах і можуть передавати звук на значні відстані, що робить їх небезпечними інструментами для порушення конфіденційності, зокрема в умовах, де є потреба в захисті інформації. Важливим аспектом є те, що ці пристрої можуть бути активовані без необхідності фізичного контакту з об'єктами, що дозволяє їх використовувати для тривалого спостереження за інформацією без ризику виявлення.

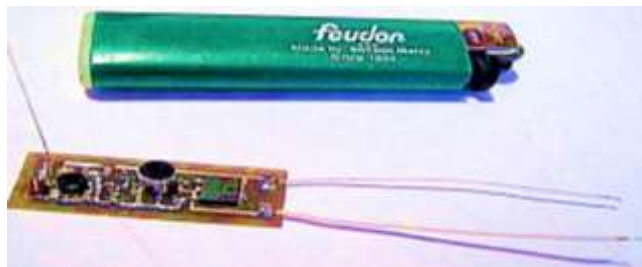


Рис. 6.5. Мікрофонні радіозакладки

Джерело: [1-8]

Повітряні акустичні канали — це канали витоку інформації, що використовують звукові хвилі, які поширюються через повітря. Вони можуть бути використані для перехоплення акустичних сигналів, що генеруються в процесі обробки інформації в комп'ютерних та інших електронних пристроях. Звук, що створюється в результаті роботи механізмів, натискання клавіатури, голосових розмов або інші звуки, що виникають під час обробки даних, може бути зафіксований через повітря. Зловмисники можуть використовувати спрямовані мікрофони, які здатні уловлювати навіть слабкі звукові коливання, що передаються через повітря. Ці мікрофони мають високу чутливість і можуть фіксувати звуки на значних відстанях, що робить їх ефективним інструментом для перехоплення інформації.

Завдяки розвитку технологій акустичного моніторингу, навіть звуки, які неможливо почути людським вухом, можуть бути зафіксовані та оброблені для відновлення переданої інформації. Одним із прикладів є

використання "білих шумів", що дозволяють створювати фоновий шум, здатний маскувати важливі звукові сигнали.

Важливою характеристикою повітряних акустичних каналів є те, що вони не потребують фізичного контакту з об'єктами, що робить їх більш небезпечними з точки зору витoku інформації, адже зловмисник може здійснювати перехоплення на відстані, що ускладнює виявлення загрози. Тому для забезпечення безпеки важливо застосовувати спеціалізовані методи захисту, такі як шумопоглинаючі матеріали, акустичні екрани та інші заходи для мінімізації акустичних витоків.

У вібраційних каналах витoku інформації акустичні сигнали поширюються через тверді тіла, зокрема через конструкції будівель, споруд (стіни, стелі, підлоги), а також труби водопостачання, опалювання, каналізації та інші елементи інфраструктури. Ці матеріали передають механічні коливання, які виникають під час обробки або передачі інформації, що робить їх потенційними каналами витoku звукової інформації.

Для перехоплення таких акустичних коливань використовуються контактні мікрофони, зокрема стетоскопи. Ці пристрої здатні вловлювати вібрації, що виникають на поверхнях, до яких вони прикріплені, і перетворювати їх на електричні сигнали. Стетоскопи дозволяють прослуховувати звукові коливання, які передаються через конструкції будівель, що дає змогу зловмисникам отримати інформацію, навіть якщо вона не чути на відкритому просторі.

Контактні мікрофони особливо ефективні для виявлення тих звуків, які поширюються через матеріали, що поглинають звукові хвилі або які не є видимими для звичайних мікрофонів. Вони можуть бути встановлені на стінах або інших поверхнях, де відбуваються вібрації, і використовуватися для зняття інформації з високою точністю, навіть при відсутності прямого доступу до джерела сигналу. Це робить вібраційні канали важливими для контролю та захисту в умовах, де інші способи спостереження неефективні.

Також електронні стетоскопи використовуються, якщо немає можливості встановити радіомікрофон безпосередньо в приміщенні. Стетоскопи посилюють акустичний сигнал, що поширюється крізь стіни, підлогу, стелю в 20–30 тис. разів, і так само здатні вловлювати шерехи і цокання годинника:

- у залізобетонних будівлях через 1–2 поверхи;
- використовуючи інженерні комунікації через 2–3 поверхи;

- по вентиляційних каналах до 20–30 м.



Рис. 6.6. Середовище поширення акустичних сигналів
Джерело: [1-8]

Електроакустичні канали витоку інформації виникають внаслідок перетворення акустичних сигналів на електричні в пристроях, що мають мікрофонний ефект. Це означає, що певні електронні компоненти, такі як мікрофони, динаміки або інші елементи оргтехніки, здатні змінювати свої електричні параметри (ємність, індуктивність, опір) під впливом акустичних хвиль, наприклад, звукових коливань, які створюються людською розмовою чи іншими звуковими джерелами. Коли акустичні хвилі взаємодіють з такими електронними елементами, зміна їх параметрів призводить до модуляції електричних струмів, що протікають через ці елементи. Модуляція, у свою чергу, переносить акустичну інформацію в електричній формі, яка може бути випромінена в простір, де вона може бути перехоплена пристроями радіорозвідки. Це створює потенційний канал витоку інформації, який використовує фізичні властивості елементів оргтехніки. Інший спосіб перехоплення інформації через електроакустичні канали — це високочастотне наві'язування (ВЧ-наві'язування). Цей метод полягає в опроміненні приміщення потужним високочастотним сигналом, що збуджує елементи оргтехніки, які мають мікрофонний ефект. У результаті, в відбитій хвилі можна отримати модульований сигнал, що містить акустичну інформацію, яка була перетворена на електричну форму. Така техніка активно застосовувалась під час «холодної війни», зокрема при прослуховуванні посольства США в Москві, де радіорозвідка використовувала цей метод для збору конфіденційної інформації.

Цей тип витоку інформації є небезпечним, оскільки він не потребує фізичного доступу до інформаційної системи чи комп'ютерів і може здійснюватися на значних відстанях без прямого контакту з об'єктом спостереження. Для боротьби з таким видом витоку необхідні спеціальні засоби захисту, зокрема, екранування електронних пристроїв, застосування

спеціальних шумопоглинаючих матеріалів та контролю за фізичним середовищем.

У 1945 році посол США в СРСР Аверел Гарріман отримав від піонерів Москви вирізаний з дерева герб Сполучених Штатів Америки, який був встановлений на стіні кабінету посла. Цей подарунок прикрашав стіну протягом кількох років, під час перебування чотирьох різних послів, і лише на початку 50-х років фахівці з виявлення прихованих електронних засобів у посольстві звернули увагу на підозрілу деталь у гербі.

Як згадує С. Пітер Карлоу, начальник служби спеціального обладнання ЦРУ: «Ми знайшли його, але не знали принципу дії». Виявилося, що в середині дерев'яного герба був прихований підслуховуючий пристрій. Він виглядав як маленький пристрій, схожий на пуголовка з маленьким хвостиком. Цей пристрій працював за допомогою довгохвильового сигналу, який використовувався в СРСР, і змушував датчики всередині герба резонувати.

Коли звучала людська мова, голос впливав на резонансні коливання пристрою, що дозволяло здійснювати перехоплення розмов на значній відстані через організований радіоканал. Цей випадок став відомим прикладом раннього застосування технологій для здійснення електронного шпигунства і підкреслив важливість забезпечення безпеки інформації в умовах глобальної напруги і технологічних викликів того часу.

Ця історія також демонструє розвиток технологій шпигунства в середині 20-го століття, коли сховані мікрофони та радіопередавачі ставали дедалі більш ефективними засобами перехоплення конфіденційної інформації. Сучасні технології електронного моніторингу стали ще складнішими і невидимими для звичайних засобів виявлення, що робить забезпечення інформаційної безпеки вкрай важливим завданням у сучасному світі.

Опто-акустичний канал витоку інформації

утворюється утворюється за допомогою лазера, і тому його часто називають лазерним каналом. У цьому випадку лазерний промінь використовується для детекції акустичних коливань, що виникають в результаті звукових хвиль, які відображаються або проходять через різні

об'єкти. Принцип дії цього каналу ґрунтується на зміні інтенсивності лазерного променя або його параметрів під впливом коливань звукових хвиль.



*Рис. 6.7. Оптико-акустичний канал (лазерний канал)
Джерело: [1-7]*

Лазерний промінь спрямовується на об'єкт, що є джерелом акустичних коливань (наприклад, стіни приміщення або вікно), і акустичні хвилі змінюють параметри відбитого променя. Спеціальні фотодіоди або інші сенсори можуть фіксувати ці зміни в інтенсивності променя або його фазі, таким чином, отримуючи інформацію, що міститься в звукових коливаннях. За допомогою цього методу можна перехоплювати розмови або іншу інформацію з дистанції без прямого контакту з об'єктом.

Лазерні системи для перехоплення акустичних коливань мають низку переваг, зокрема можливість дистанційного спостереження, високу точність і можливість працювати через стіни та інші перешкоди. Однак вони також мають обмеження, такі як необхідність точного спрямування лазера на джерело звуку і чутливість до умов навколишнього середовища.

Відомо, що під дією звукової хвилі тонкі поверхні, наприклад, скло або дзеркало, починають вібрувати. При опроміненні лазерним променем таких вібруючих поверхонь відбите лазерне випромінювання модулюється по амплітуді або фазі і надходить на вхід приймача оптичного випромінювання. У приймачі отриманий сигнал демодулюється і посилюється, так що можна отримати акустичний сигнал. У такій схемі використовується невидимий інфрачервоний лазерний промінь, за допомогою якого проводиться підслуховування розмов, причому лазер і приймач оптичного випромінювання можуть бути встановлені в одному або різних місцях (радіус дії до 500 м).

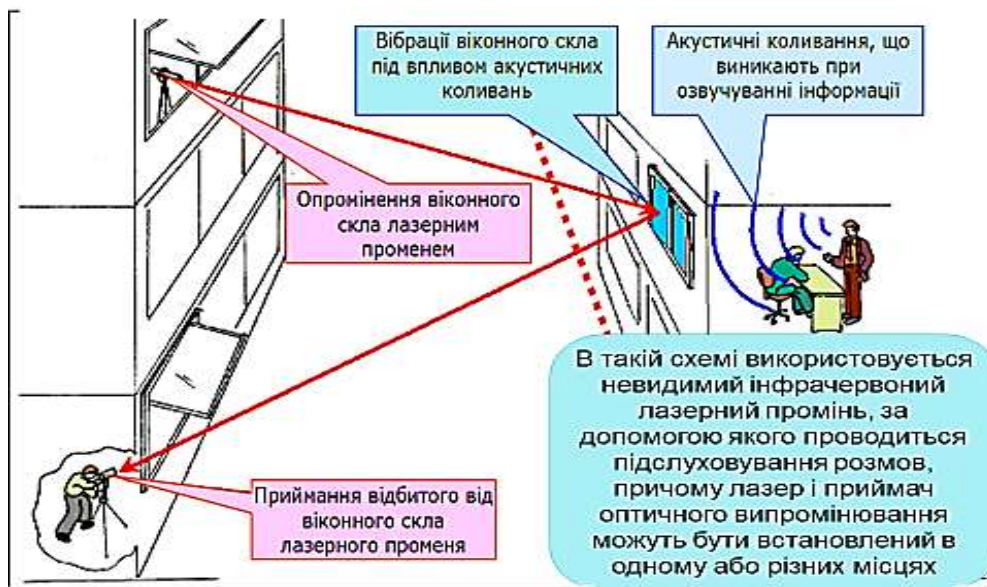


Рис. 6.8. Оптико-акустичний канал (в схемі використовується невидимий інфрачервоний лазерний промінь, за допомогою якого проводиться підслуховування розмов)

Джерело: [1-7]

Слід зауважити, що акустичні канали можуть бути джерелом витоку не лише мовної інформації, а й інформації з механічних замків, з принтера чи клавіатури комп'ютера тощо.

Захист від акустичних каналів витоку інформації:

- **Шумозаглушення**

Використання спеціальних звукопоглинальних матеріалів у приміщеннях, де обробляється конфіденційна інформація, може значно знизити ризик витоку через акустичні канали.

- **Шумоперешкодження**

Встановлення систем "білого шуму", які створюють постійний звук у фоні, може заважати спостереженню за акустичними сигналами.

- **Захист обладнання**

Установлення пристроїв для обмеження акустичних випромінювань або використання пристроїв з мінімальними акустичними виходами може бути корисним для зменшення ризику витоку.

- **Контроль за доступом до приміщень**

Обмеження доступу до приміщень, де зберігаються важливі комп'ютерні системи або де обробляються чутливі дані, також може знижувати ймовірність витоку через акустичні канали.

Таким чином, акустичні канали є важливим аспектом захисту інформації, і відповідні заходи повинні бути впроваджені для запобігання витоку інформації через цей канал.

Оптичний канал витоку інформації

Оптичний канал витоку інформації базується на використанні оптичних технологій для перехоплення або спостереження за інформацією, що передається або зберігається в інформаційно-комунікаційних системах (ІКС). Такий канал може використовувати різноманітні методи для витоку даних, і один із найбільш поширених способів — це використання лазерних технологій, оптичних волокон або навіть випромінювання, яке виникає в результаті роботи технічних пристроїв.

Основні види оптичних каналів витоку інформації:

✳ Лазерний канал витоку

Лазери можуть використовуватися для фіксації змін інтенсивності світлового потоку, який виникає через звукові або механічні коливання в середовищі, що оточує інформаційне обладнання. Наприклад, лазер може відправляти світловий промінь на вікно, де виникають звукові коливання від розмов у приміщенні. Ці коливання змінюють параметри відбитого лазерного проміння, і ці зміни можуть бути зафіксовані приймачами для відновлення звуку або навіть текстової інформації.

✳ Оптичне волокно

У випадку неправомірного використання оптичних кабелів або мереж може бути здійснений витік інформації, що передається через них. Зловмисники можуть маніпулювати з'єднаннями в оптичних кабелях або використовувати спеціальні пристрої для перехоплення сигналу, що проходить через оптичне волокно. Це дозволяє отримати доступ до даних без необхідності підключатися до комп'ютерної мережі.

✳ Оптичні сенсори

Деякі системи використовують спеціальні сенсори, які можуть вловлювати несанкціоновані зміни у фізичних параметрах, таких як температура, вологість або електричні поля. При зміні цих параметрів можуть з'являтися мікроскопічні зміни в оптичних властивостях середовища (наприклад, відбиття світла), що може свідчити про наявність витоку інформації.

Оптичні канали витоку інформації можуть бути важко виявлені через складність моніторингу і можливість використання технологій дистанційного спостереження. Це робить їх потенційно небезпечними для захисту чутливої інформації, оскільки навіть незначні зміни в навколишньому середовищі можуть призвести до витоку даних.

Витік інформації через оптичні сигнали, які можуть бути перехоплені за допомогою лазерних систем або іншого оптичного обладнання. Це можуть бути сигнали, що передаються через оптичні кабелі, або випромінювання від екранів комп'ютерів, які можуть бути зафіксовані за допомогою спеціалізованих пристроїв.

Оптичний канал – це канал, у якому інформація передається або витікає через оптичні сигнали, що можуть бути зловмисниками використані для перехоплення або спостереження за переданими даними. Цей тип каналу зазвичай використовує світлові хвилі для передачі інформації або збору даних, що вимагає специфічних технічних засобів для його контролю і захисту.

Для спостереження можуть використовуватися різні технічні засоби:

- **для спостереження вдень** – оптичні прилади (монокуляри, підзорні труби, біноклі, телескопи і т. д.), телевізійні системи;
- **для спостереження вночі** – прилади нічного бачення, телевізійні системи, тепловізори;
- **для спостереження з великої відстані** – засоби з довгофокусними оптичними системами, а при спостереженні зблизька – встановлені телевізійні камери, що розміщують скритно.



Рис. 6.10. Оптичні канали витоку інформації (технічні засоби для спостережень)

Джерело: [1-7]

Відеозображення з телевізійних камер може передаватися на монітори як по кабелю, так і по радіоканалу.

Загалом, оптичні канали витоку інформації є одними з найбільш складних для виявлення, оскільки вони використовують світлові хвилі, які важко засікти за допомогою традиційних методів моніторингу або перехоплення. Захист від таких каналів витоку включає використання

зашифрованих або оптично захищених ліній передачі, фізичних бар'єрів та активних систем моніторингу.

Електромагнітний канал витоку інформації

Електромагнітний канал витоку інформації — це канал, через який інформація може бути перехоплена або витікати в результаті електромагнітних випромінювань, що виникають під час роботи електронних пристроїв, комп'ютерних систем, а також інформаційно-комунікаційних мереж.

Електромагнітні випромінювання з'являються як побічний ефект роботи електронних пристроїв (наприклад, комп'ютерів, серверів, мережних пристроїв, мобільних телефонів, радіоапаратури тощо). Це випромінювання може містити корисну інформацію, якщо правильним чином перехопити і декодувати відповідні сигнали. У таких каналах витоку інформації важливо враховувати як невидимі, так і явні електромагнітні впливи.

Основні типи електромагнітних каналів витоку інформації:

✱ Електромагнітні випромінювання

Кожен електронний пристрій, коли він працює, створює електромагнітне випромінювання. Це можуть бути як низькочастотні, так і високочастотні сигнали. Такі випромінювання можуть містити частини інформації, що передається або обробляється в пристрої. Випромінювання можуть бути зафіксовані зломисниками за допомогою спеціалізованих радіоприймачів або антен.

✱ Електромагнітні хвилі від кабелів та проводів

Інформація може також витікати через електричні проводи або кабелі, що передають сигнал. Наприклад, комп'ютерні мережі (Ethernet), телефонні лінії, кабелі живлення можуть випромінювати низькочастотні електромагнітні хвилі, які можна перехопити або відновити для отримання доступу до інформації, що передається. Для захисту від таких витоків використовуються спеціальні захисні кабелі з екрануванням, що знижують рівень випромінювання і мінімізують ризик перехоплення даних. Також важливо застосовувати методи шифрування для передачі чутливої інформації через електричні мережі, щоб навіть у разі витоку даних, інформація залишалася захищеною.

✱ Електромагнітні поля поблизу інформаційних систем

Під час роботи інформаційних систем, наприклад, серверів, можуть виникати радіо- або електричні поля, що є джерелами витоку інформації.

Це може статися навіть на відстані, достатній для того, щоб використовувати спеціалізовані засоби для збору або аналізу інформації. Для мінімізації ризику витоку через електромагнітні поля використовуються методи екранування та ізоляції обладнання. Це може включати встановлення спеціальних захисних матеріалів, що поглинають або відбивають електромагнітні хвилі, а також обмеження зони доступу до таких систем.

Методи захисту від електромагнітного витоку інформації включають:

- ***Екранування*** — використання спеціальних матеріалів (металевих екранів, фольги, спеціальних кабелів), які поглинають або відбивають електромагнітне випромінювання, запобігаючи його витоку.
- ***Шифрування даних*** — у разі передачі інформації через мережу або кабелі застосовуються методи шифрування для запобігання витоку.
- ***Фільтрація і захист від електромагнітного впливу*** — застосування фільтрів для зменшення випромінювання або випромінювання, що виходить за межі захищеного простору.
- ***Моніторинг і аудит електромагнітного випромінювання*** — регулярні перевірки на наявність підозрілих випромінювань або порушень стандартів безпеки, що дозволяють вчасно виявити канали витоку.

В ***електромагнітних каналах*** витоку інформації носієм інформації є електромагнітні випромінювання (ЕМВ), що виникають при обробці інформації технічними засобами. Це небажане ЕМВ і його ще називають побічне ЕМВ (ПЕМВ). Причиною виникнення ПЕМВ є електромагнітне поле, що пов'язане з проходженням електричного струму в апаратних компонентах ІКС. ПЕМВ може поширюватися як через повітряний простір, так і через провідники, наприклад, електроживлення чи заземлення. Зловмисники можуть використовувати спеціалізовані пристрої для перехоплення цих випромінювань і подальшого відновлення оброблюваної інформації. Основною небезпекою є можливість відновлення текстових даних, графічної інформації або навіть звукових сигналів. Для мінімізації ризику витоку через електромагнітні канали застосовуються методи екранування апаратних засобів, використання фільтрів і спеціальних заземлювальних пристроїв. Також ефективним є зниження рівня випромінювання шляхом використання технічних засобів, сертифікованих за стандартами захисту від ПЕМВ. Важливим аспектом є регулярний моніторинг рівня електромагнітного випромінювання для виявлення можливих слабких місць системи.

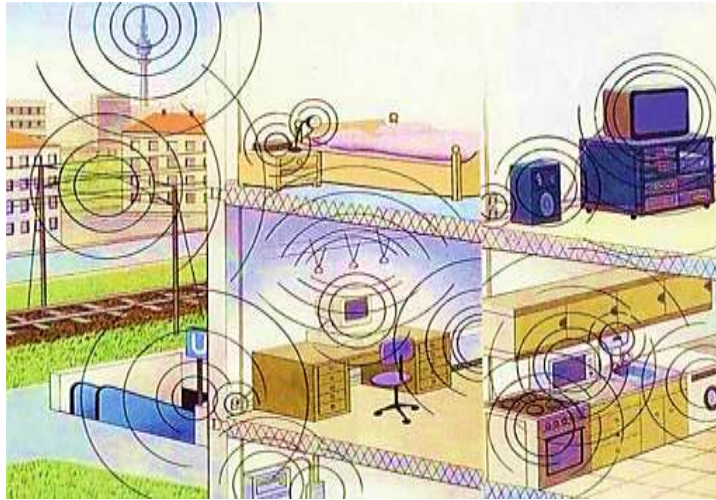


*Рис. 6.10. Електромагнітний канал витоку інформації
(носієм інформації – електромагнітні випромінювання)*

Джерело: [1-7]

Захист від електромагнітних каналів витоку є важливою частиною комплексної інформаційної безпеки, оскільки такі канали часто не є очевидними і можуть бути використані для витоку чутливої інформації без фізичного доступу до пристроїв. Захист від таких витоків включає застосування спеціальних матеріалів для екранізації, які блокують або зменшують рівень електромагнітних випромінювань. Важливими заходами є також регулярне проведення аудиту на виявлення потенційних уразливостей, що дозволяють зловмисникам отримувати доступ до електромагнітних каналів. Для ефективного захисту використовуються спеціалізовані пристрої, що дозволяють визначати рівень випромінювання і вчасно виявляти аномалії. Крім того, для критичних об'єктів можуть бути введені суворі стандарти з фізичного та електронного екранування всіх чутливих електронних пристроїв.

Радіоелектронні канали

Радіоелектронні канали витоку інформації — це тип технічних каналів, через які інформація може витікати через електромагнітне випромінювання в радіочастотному діапазоні. Такий витік може відбуватися через радіосигнали, які створюються електронними пристроями під час їхньої роботи, зокрема через радіо-, телевізійні передавачі, комп'ютерні та мобільні пристрої, а також через бездротові мережі.

Витік інформації через електромагнітні хвилі. Цей тип каналу охоплює випромінювання від електронних пристроїв, таких як комп'ютери, мобільні телефони, мережеве обладнання тощо. Спеціалізовані радіоелектронні засоби можуть захоплювати сигнали на різних частотах і відновлювати передану інформацію.

Основні види радіоелектронних каналів витоку інформації:

✳ Випромінювання від електронних пристроїв

Під час роботи будь-якого електронного пристрою (наприклад, комп'ютера, смартфона, телевізора) виникає електромагнітне випромінювання. Це випромінювання може бути використано зловмисниками для перехоплення інформації, що обробляється або передається пристроєм. Випромінювання може мати різну інтенсивність і частотний діапазон, включаючи радіочастотні, що може бути зафіксовано радіоприймачем.

✳ Випромінювання від бездротових мереж

Усі сучасні бездротові технології, такі як Wi-Fi, Bluetooth, NFC, а також мобільні мережі (3G, 4G, 5G), створюють електромагнітні хвилі, які можуть бути використані для витоку інформації. Наприклад, зловмисник може прослуховувати Wi-Fi трафік або перехоплювати мобільний сигнал, щоб отримати доступ до переданих даних. Особливо небезпечними є незашифровані канали зв'язку або недосконалі методи шифрування.

✳ Радіоактивні мікрофони та радіозакладки

Радіоелектронні канали витоку можуть включати використання мікрофонних радіозакладок або прихованих радіопередавачів, які монтуються в різні об'єкти або приміщення. Вони можуть передавати акустичну інформацію або відновлювати її через радіохвилі на відстані.

✳ Інтерференція і перехоплення сигналів

Зловмисники можуть використовувати інтерференцію для перехоплення електромагнітних сигналів, що передаються через відкриті канали зв'язку. Вони можуть встановлювати спеціальні приймачі для збору радіоелектронної інформації або здійснювати перехоплення даних у реальному часі через радіоелектронні пристрої.

✳ Випромінювання від енергетичних систем

Важливими джерелами радіоелектронного витоку можуть бути енергетичні системи, що містять електричні кола високої напруги. Вони можуть створювати непрямі радіохвилі, які використовуються для зловмисного перехоплення даних.

Електромагнітний канал витоку інформації поділяється на кілька основних категорій залежно від виду випромінювання та фізичних процесів, через які цей канал діє:

▲ **Радіоелектронні канали** – це канали, що використовують радіохвилі для передачі інформації. Вони можуть включати як випромінювання, що безпосередньо виходить від електронних пристроїв, так і наведення на близько розташовані кабелі та проводи, по яких розповсюджується електромагнітна енергія. Зловмисники можуть використовувати спеціалізовані пристрої для перехоплення радіохвиль, які генеруються або відбиті від обладнання ІКС.

▲ **Канали електромагнітного випромінювання** – передача інформації відбувається через електромагнітні хвилі, що поширюються в повітрі. Це включає не тільки радіохвилі, але й інші види електромагнітних хвиль (наприклад, мікрохвильові, інфрачервоні). Випромінювання може бути викликане роботою комп'ютерних систем, серверів, комунікаційних пристроїв, які можуть відправляти невидимі сигнали, що потім можуть бути перехоплені спеціальними пристроями. канал заземлення (наведення на лінії заземлення).

▲ **Канали наведення** – виникають, коли електромагнітне випромінювання від пристроїв ІКС індукуює струм у довколишніх металевих об'єктах (кабелях, трубах, проводах). Це створює додаткові канали для передачі інформації, і така передача може відбуватися на значні відстані. Ці канали можуть бути використані для перехоплення сигналів з втратою конфіденційності даних, що передаються через мережі.

Методи захисту від радіоелектронних каналів витоку:

❖ Екранування

Захист від радіоелектронного витоку часто включає використання екрануючих матеріалів (металевих обшивок, спеціальних захисних фільтрів), що знижують рівень випромінювання від пристроїв або кабелів.

❖ Шифрування бездротових каналів

Важливим кроком у захисті від радіоелектронного витоку є використання шифрування на всіх етапах передачі інформації. Це робить перехоплення даних через бездротові канали зв'язку безглуздом для зловмисника.

❖ Інтенсивний моніторинг радіоелектронного середовища

Системи моніторингу та аудиту радіоелектронних хвиль можуть допомогти виявити потенційні джерела витоку або впливу радіоелектронних каналів. Це можуть бути спеціалізовані пристрої, що фіксують підозрілі сигнали або визначають джерела випромінювання.

❖ Використання фізичних бар'єрів

Окрім екранування, можна використовувати спеціальні конструкції приміщень, такі як захищені кімнати з низьким рівнем електромагнітного випромінювання, щоб звести до мінімуму можливість витоку інформації через радіоелектронні канали.

❖ Безпека апаратного забезпечення

Апаратура, яка обробляє чутливу інформацію, повинна бути захищена від несанкціонованого доступу та впливу. Використання спеціальних захисних шторок, фільтрів або плівок для блокування електромагнітного випромінювання може допомогти запобігти витоку.

Таким чином, радіоелектронні канали витоку є важливим напрямком у сфері інформаційної безпеки, і для їхнього контролю потрібно застосовувати комплексні заходи для захисту чутливої інформації.



Електромагнітне поле, що виникає під час роботи електронних пристроїв в інформаційно-телекомунікаційних системах (ІКС), поширюється в навколишньому просторі і може бути прийняте за допомогою спеціальних пристроїв для подальшого виявлення та аналізу. Це поле може бути використане для перехоплення інформації через випромінювання, яке створюють компоненти ІКС. У разі цього випромінювання, зломисники можуть використовувати пристрої для збору даних, що дозволяють віддалено доступити важливу інформацію.

Крім того, електромагнітне поле, яке виникає в процесі функціонування технічних засобів, може індукціювати струм в близько розташованих дротових лініях, що також створює потенційні канали для витоку інформації. Це наведення струму може впливати на кабелі і проводи, що знаходяться поряд з джерелом випромінювання — наприклад, на лінії живлення, заземлення, телефонні та інші комунікаційні лінії, а також на металеві труби опалення чи водопостачання, чи навіть на дроти системи пожежної сигналізації. Таким чином, з'являються додаткові шляхи для витоку інформації, які можуть бути використані для її перехоплення.

Особливу небезпеку становлять канали витоку, які виходять за межі організації чи підприємства. Це дає можливість зломисникам дистанційно отримувати доступ до чутливої інформації без фізичного проникнення в приміщення. Для перехоплення електромагнітних випромінювань та наведень на кабельні лінії існують спеціальні пристрої, що використовуються у технічних засобах розвідки побічних електромагнітних випромінювань і наведень (ТЗР ПЕМВН). Ці пристрої дозволяють виявити та зафіксувати електромагнітне випромінювання на певних частотах, що використовуються технічними засобами, і таким

чином зібрати інформацію з наведених кабельних систем, що працюють в межах певної ділянки.

Для запобігання таким витокам важливо впроваджувати заходи по екрануванню електронних пристроїв, використанню заземлення і фільтрації сигналів у комунікаційних системах, а також застосовувати спеціалізовані технічні засоби для виявлення і блокування побічних електромагнітних випромінювань.

6.4. ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЕЛЕКТРИЧНИМИ ТА ЕЛЕКТРОМАГНІТНИМИ КАНАЛАМИ

Захист інформації від витоку через побічні електромагнітні випромінювання та наводки (ПЕМВН) — це комплекс організаційних, технічних та технологічних заходів, спрямованих на зниження ризику розголошення інформації, що має обмежений доступ, шляхом мінімізації небезпечних випромінювань та наводок. Метою таких заходів є виключення або суттєве зменшення імовірності перехоплення інформації з контрольованої зони.

Основні методи захисту від ПЕМВН

Методи захисту поділяються на **пасивні** та **активні**:

1. **Пасивні методи** спрямовані на зниження потужності випромінювань, зменшення інформативності сигналів або повну ізоляцію від перехоплення.
2. **Активні методи** передбачають створення електромагнітних завад, які ускладнюють приймання і виділення корисної інформації. Це можуть бути генератори шумів або активні системи перешкод, які блокують можливість аналізу перехоплених сигналів. Активні методи включають генерацію широкосмугових шумів, які перекривають спектр перехоплених сигналів. Сучасні системи активного захисту використовують інтелектуальні пристрої для адаптивного налаштування завад, залежно від типу перехоплюваного сигналу, що дозволяє значно підвищити ефективність захисту.

Пасивні методи захисту від ПЕМВН

Пасивні методи забезпечують зменшення рівня небезпечного (інформативного) сигналу або зниження його інформативності. Активні методи спрямовані на створення електромагнітних завад, які ускладнюють приймання й виділення корисної інформації з перехоплених сигналів порушником.

Пасивні методи захисту від ПЕМВН поділяються на три основні групи:

1. Екранування засобів обробки інформації (наприклад, комп'ютерів) або створення екранованих приміщень для розміщення серверів інформаційної системи.
2. Зменшення потужності випромінювань і наведень.
3. Зниження інформативності сигналів.

1. Екранування

Екранування є одним із найефективніших методів захисту від електромагнітних випромінювань. Це передбачає розміщення елементів автоматизованої системи, що створюють електричні, магнітні та електромагнітні поля, у просторово-замкнених конструкціях. Способи екранування залежать від типу створюваних електромагнітних полів. Основними видами екранування є:

- ❖ Електростатичне екранування (електричне поле) полягає у замиканні силових ліній електростатичного поля через електропровідний шар екрана з відведенням наведених електричних зарядів на землю. Цей метод ефективний для постійного струму та коливань низької частоти, проте ефективність знижується зі зростанням частоти сигналів.
- ❖ Магнітостатичне екранування (магнітне поле) засноване на замиканні силових ліній магнітного поля в матеріалі екрана, який має низький магнітний опір. Воно ефективне для постійного струму та низькочастотних коливань.
- ❖ Електромагнітне екранування (електромагнітне поле) використовується для ослаблення високочастотного електромагнітного поля шляхом створення вихрових струмів у матеріалі екрана, які генерують поле протилежного напрямку.

Екранування дозволяє не лише захистити обладнання автоматизованих систем від випромінювання небезпечних сигналів, але й зменшити ризик впливу зовнішніх електромагнітних та акустичних полів. Якщо відстань між елементами системи становить до 10% від чверті довжини хвилі сигналу, зв'язок між ними визначається переважно електричними та магнітними полями, що дозволяє розглядати їх окремо.

Заземлення та металізація корпусів апаратури забезпечують ослаблення паразитних зв'язків і наведень між окремими колами електричних схем, а також ефективне відведення наведених сигналів на землю.

2. Зменшення потужності випромінювань і наведень

Методи зменшення потужності випромінювань та наведень поділяються на:

- ❖ Реалізовані під час створення системи технічного захисту інформації, зокрема:
 - ✓ Використання оптоволоконних з'єднань і оптичних інтерфейсів.
 - ✓ Застосування спеціальних електронних та електричних фільтрів.
 - ✓ Впровадження гальванічних розв'язок у колах електроживлення.
- ❖ Реалізовані під час проектування засобів інформатизації, включаючи зміни електричних схем або конструкції пристроїв.

Зменшення потужності побічних випромінювань шляхом удосконалення електричних схем включає:

- ✱ Використання електронних і електричних компонентів з низьким рівнем випромінювання.
- ✱ Уникнення регулярності повторень в інформаційних сигналах.
- ✱ Зміну форми сигналів (зокрема, крутизни фронтів) для запобігання паразитній генерації.

Загалом, ефективне застосування цих методів дозволяє значно знизити ймовірність витоку інформації через побічні електромагнітні випромінювання та наведення.

Одним із найбільш ефективних підходів до подолання побічних електромагнітних випромінювань та наведень (ПЕМВН) є застосування сучасних оптичних каналів зв'язку. Волоконно-оптичні кабелі стали стандартом для передачі інформації на великі відстані завдяки їхній здатності забезпечувати високу швидкість передачі даних, стійкість до електромагнітних перешкод та мінімальний ризик витоку інформації за умови правильної інсталяції.

Для локальної передачі даних, наприклад, у межах одного приміщення чи об'єкта, широко використовуються бездротові системи передачі даних, що працюють у видимому та інфрачервоному діапазонах. Ці системи є ефективними для зменшення ризиків витоку інформації, оскільки інфрачервоне випромінювання менш вразливе до перехоплення в порівнянні з радіохвилями.

Проте, основним способом захисту від ПЕМВН залишається використання сучасних електромагнітних фільтрів. Ці пристрої, створені на основі високоефективних матеріалів і компонентів, встановлюються у критичних вузлах інформаційних систем для мінімізації випромінювання небажаних сигналів. Фільтри розраховуються таким чином, щоб

забезпечувати безпечний рівень сигналу та не спотворювати корисну інформацію.

Зниження інформативності сигналів

Пасивні методи захисту від ПЕМВН (пульсуючих електромагнітних випромінювань високої частоти), орієнтовані на зниження інформативності сигналів, включають різноманітні підходи, спрямовані на ослаблення або блокування випромінювання без використання активних технологій або джерел енергії. Метою таких методів є зниження можливості зчитування або перехоплення інформації через електромагнітні хвилі. Ось основні методи:

❖ Екранирування (екранування):

Використання матеріалів, які ефективно поглинають або відбивають електромагнітні хвилі. Це можуть бути металічні екрани або спеціальні композитні матеріали, що встановлюються навколо чутливого обладнання або кабелів. Вони блокують випромінювання і знижують інформативність сигналу, що проходить через них.

❖ Поглинання електромагнітної енергії:

Застосування матеріалів, які поглинають електромагнітні хвилі, зменшуючи їх енергію та інформативність. Це можуть бути спеціальні фарби, покриття або матеріали, які розсіюють або поглинають енергію в конкретних частотних діапазонах, що дозволяє знизити рівень випромінювання, яке може бути зафіксовано зовнішніми пристроями.

❖ Фільтрація сигналів:

Використання фільтрів для ослаблення або блокування певних частот, які можуть бути використані для перехоплення або витоку інформації. Фільтри можуть бути встановлені на електричних і оптичних лініях зв'язку, щоб знизити інтенсивність сигналів, які можуть містити конфіденційну інформацію.

❖ Шумові бар'єри:

Створення "шумового" середовища, яке ускладнює розпізнавання корисних сигналів серед перешкод. Це можуть бути спеціальні джерела шуму або матеріали, що створюють інтерференцію з електромагнітними хвилями, тим самим ускладнюючи можливість їх аналізу чи дешифрування.

❖ Розсіювання сигналу:

Використання методів для розсіювання або дифузії сигналів, що виходять з обладнання. Це може включати спеціальне розташування обладнання, прокладання кабелів або застосування матеріалів, які змінюють напрямок та інтенсивність випромінювання, що знижує ймовірність його перехоплення або використання для витоку інформації.

❖ Використання матеріалів з низькою провідністю:

Встановлення обладнання та кабелів в спеціальні канали або корпуси з матеріалів, які мають низьку електричну провідність для конкретних частот. Це дозволяє знижувати можливість передачі ПЕМВН через матеріали та зменшувати їх інформативність.

❖ Ізоляція електронних компонентів:

Ізоляція чутливих компонентів або пристроїв від можливих електромагнітних випромінювань шляхом розміщення їх в спеціально захищених корпусах або приміщеннях, що перешкоджають виходу електромагнітних хвиль.

Активні методи захисту від ПЕМВН

Активні методи захисту від ПЕМВН (пульсуючих електромагнітних випромінювань високої частоти) орієнтовані на виявлення та нейтралізацію небажаних електромагнітних впливів у реальному часі. Вони передбачають застосування технологій, які активно взаємодіють з джерелами ПЕМВН або з їхнім впливом, щоб забезпечити захист електронних пристроїв та систем. Основні напрямки таких методів включають:

1. Екранирування (екранування пристроїв та кабелів)

Встановлення спеціальних екранів для блокування електромагнітних хвиль. Це можуть бути металічні чи композитні матеріали, які поглинають або відбивають електромагнітне випромінювання, знижуючи його вплив на електронні системи.

2. Фільтрація сигналів

Використання фільтрів для блокування чи ослаблення шкідливих електромагнітних сигналів у різних діапазонах частот. Це може бути реалізовано через апаратні фільтри, які відсіюють частоти, які можуть бути потенційно небезпечними.

3. Активні антени

Впровадження спеціальних активних антен, які можуть спрямовувати або гасити електромагнітні випромінювання. Такі антени здатні фільтрувати або навіть перенаправляти електромагнітні хвилі, знижуючи їх негативний вплив на систему.

4. Системи захисту зворотного зв'язку

Використання систем, які активно виявляють зміни в електромагнітному середовищі та коригують роботу обладнання для мінімізації впливу ПЕМВН. Такі системи можуть автоматично налаштовувати параметри роботи пристроїв для компенсації виникаючих випромінювань.

5. Шумоподібні генератори

Використання генераторів, які створюють "шум" в тих частотах, які можуть бути джерелами перешкод. Це може допомогти "маскувати" електромагнітні сигнали, що генеруються іншими джерелами, тим самим знижуючи ймовірність витоку інформації через ПЕМВН.

6. Активні системи моніторингу

Системи, які постійно спостерігають за рівнями електромагнітних випромінювань в зоні, де розташовані критичні системи. У разі виявлення підвищеного рівня випромінювання автоматично активуються заходи захисту, що дозволяють нейтралізувати потенційно небезпечні джерела.

Ці методи активно протидіють зовнішнім електромагнітним загрозам, даючи змогу знижувати ймовірність впливу ПЕМВН на обладнання та захищати важливу інформацію.

6.5. МЕТОДИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК АКУСТИЧНИХ ТА ОПТИЧНИХ КАНАЛІВ

Для проведення робіт із захисту акустичної інформації використовуються спеціалізовані прилади для загальних акустичних вимірювань, а також апаратура, побудована на тих самих принципах, що й прилади для зняття акустичної інформації. Це дозволяє ефективно виявляти канали витоку та застосовувати відповідні заходи для їх блокування чи ізоляції. Важливим етапом є органолептична перевірка всіх приміщень, які можуть бути пов'язані з об'єктом захисту створеними навмисно звуководними каналами. Для цього використовуються повні будівельні плани будівлі, де розміщено об'єкт захисту, і перевіряється наявність чи відсутність засобів для несанкціонованого зняття інформації через виявлені канали витоку.

Особливу увагу слід звертати на можливість несанкціонованого зняття акустичної інформації через металеві трубопроводи, зокрема трубопроводи опалення, вентиляції та водопостачання. Металеві конструкції таких труб можуть створювати акустичні канали, через які інформація може бути передана до зовнішніх пристроїв. Це може стосуватися не тільки трубопроводів, але й інших металевих конструкцій будівлі, таких як каркаси чи інші елементи інфраструктури. Для захисту від таких витоків застосовуються методи додаткової ізоляції труб, використання акустичних екранів та спеціальних шумоізоляційних матеріалів.

Після обстеження на основі отриманих результатів вимірювань та розрахунків складається паспорт об'єкта і проектується система захисту, що включає вибір необхідної апаратури для захисту. Це можуть бути спеціалізовані засоби для блокування акустичних сигналів або пристрої для створення перешкод у звукових каналах. Визначаються місця розміщення акустичних генераторів або іншого типу захисного обладнання, яке ускладнює або повністю блокує можливість витоку акустичної інформації. Також визначається типи апаратури та їх кількість, що оптимально покривають об'єкт захисту і забезпечують належний рівень безпеки. Ці заходи спрямовані на мінімізацію ризику витоку акустичної інформації через різноманітні канали, що можуть існувати в будівлях, і створення умов для максимальної безпеки та конфіденційності передачі даних.

Визначають такі класи методів протидії підслуховуванню інформації з обмеженим доступом:

- 1) методи захисту мовної інформації при передачі її каналами зв'язку;*
- 2) методи захисту від прослуховування акустичних сигналів у при міщеннях.*

Методи захисту мовної інформації при передачі її каналами зв'язку

Для захисту від прослуховування мовної інформації під час її передачі каналами зв'язку використовуються різні методи, зокрема зашумлення кабелів, аналогове скремблювання та шифрування. Останній метод буде розглянуто окремо в контексті криптографічного захисту інформації.

❖ Аналогове скремблювання

Скремблювання є процесом зміни характеристик мовного сигналу таким чином, щоб він займав ту ж саму смугу частот, але став нерозбірливим для сторонніх осіб. Це ускладнює ідентифікацію учасників розмови. Основні методи аналогового скремблювання включають:

- ✓ Частотна інверсія (обернення) спектра сигналу: змінюється порядок частот в спектрі сигналу, що робить його незрозумілим для стороннього слухача.
- ✓ Частотна інверсія спектра зі зсувом несучої частоти: додатково змінюється несуча частота сигналу, що ускладнює ідентифікацію сигналу.
- ✓ Поділ смуги частот мовного сигналу на піддіапазони з подальшою перестановкою й інверсією: мовний сигнал розбивається на

піддіапазони, які потім перерозподіляються і інвертуються для того, щоб ускладнити відновлення оригінального сигналу.

Ці методи не забезпечують абсолютного захисту, але вони значно знижують можливість прослуховування.

❖ Дискретизація та шифрування

Дискретизація мовної інформації з подальшим її шифруванням забезпечує найвищий рівень захисту від прослуховування. У процесі дискретизації мовний сигнал перетворюється на цифрову форму, що дозволяє застосовувати сучасні криптографічні алгоритми для його захисту. Шифрування дозволяє повністю приховати зміст переговорів і забезпечити їх конфіденційність. Це може бути досягнуто за допомогою таких криптографічних методів, як симетричне шифрування (AES, DES) або асиметричне шифрування (RSA, ECC), що дозволяє значно підвищити безпеку інформації.

❖ Акустичні канали витоку

Акустичні канали витоку є одним із основних шляхів несанкціонованого прослуховування. Вони можуть бути:

- ✓ Конструктивними, пов'язаними з особливостями приміщення (наприклад, порожнечі в стінах або каналізаційні труби, що можуть передавати звуки).
- ✓ Навмисними, створеними для спеціального збору інформації, наприклад, через замасковані отвори у стінах або звуководні канали. Це є особливо актуальним для старих будівель та споруд з блоків бетонних панелей, де такі канали можуть утворюватися на стиках блоків.

Захист від витоку через акустичні канали передбачає використання спеціальних технологій, таких як акустичні екрани, шумоізоляція, активне шумопоглинання або зниження чутливості акустичних систем. Крім того, для захисту можуть застосовуватися динамічні системи шумоподібних сигналів, які маскують звуки та перешкоджають збору інформації через акустичні канали. Загалом, ефективний захист від прослуховування мовної інформації потребує комплексного підходу, включаючи як фізичні методи (екрани, шумоізоляція), так і технічні методи (скремблювання, шифрування).

Методи захисту від прослуховування акустичних сигналів у при міщеннях

Захист акустичної інформації у виділених приміщеннях є важливим напрямом протидії підслуховуванню, що передбачає застосування різних

методів для запобігання несанкціонованому доступу до конфіденційної інформації. До основних методів захисту від прослуховування акустичних сигналів відносяться звукоізоляція та звукопоглинання акустичного сигналу, зашумлення приміщень для маскування сигналів, захист від несанкціонованого запису мовної інформації на диктофон та виявлення й вилучення закладних пристроїв для підслуховування.

Основними заходами для захисту конфіденційних переговорів є організаційні та технічні заходи. **Організаційні заходи** включають архітектурно-планувальні заходи, які застосовуються на етапі проектування або реконструкції приміщень з метою виключення неконтрольованого поширення звукових полів, а також режимні заходи для суворого контролю за перебуванням співробітників і відвідувачів в охоронних зонах. **Технічні заходи** передбачають використання спеціальних засобів і систем для протидії підслуховуванню й запису інформації. Сюди належать системи виявлення електромагнітних полів, що забезпечують рух записуючих носіїв, програмно-апаратні комплекси для виявлення диктофонів з флеш-пам'яттю, пристрої придушення диктофонів, а також системи протидії мобільним телефонам, які можуть використовуватись як підслуховуючі пристрої.

Для виявлення звукозаписувальних приладів у відвідувачів організацій можуть використовуватися звичайні детектори металу, хоча для більш ефективного контролю можуть бути застосовані індикаторні прилади для виявлення диктофонів, що працюють на основі вібрації при наближенні до працюючого диктофона на відстань 0,5–1 м. Для придушення несанкціонованого запису інформації використовуються спеціальні прилади з випромінюванням акустичних або електромагнітних завад. Однак важливо зазначити, що електромагнітні пристрої зазвичай випромінюють сильне електромагнітне поле, тому їх використання має бути обмежене за часом, не перевищуючи 1-2 години на добу.

Організаційно-технічні заходи захисту акустичної інформації передбачають використання як пасивних, так і активних заходів. Пасивні заходи включають забезпечення звукоізоляції та звукопоглинання в приміщеннях, що допомагає зменшити рівень акустичного сигналу до такого рівня, при якому неможливо здійснити його перехоплення. Активні заходи, зокрема застосування генераторів випадкових або псевдовипадкових коливань, створюють маскуючі сигнали, що порушують акустичний канал витоку інформації. Генератори розміщуються на стінах, підлозі, стелях і навіть на склі вікон. Цей захист особливо ефективний, коли вікна приміщення виходять на незахищену територію, і охоронна

зона не перевищує 200 м. Такі методи також захищають від лазерного підслуховування через вікна.

Комбіновані заходи, які ґрунтуються на принципі того, що завада не повинна заважати легітимним користувачам, включають використання зворотного зв'язку для регулювання спектра шуму в залежності від рівня акустичного сигналу. Інший підхід — це створення закритого каналу зв'язку, що ізолює переговори від навколишнього акустичного середовища або застосування спеціальної завади для маскування сигналу за межами ізольованого кола. Третій напрямок полягає в використанні змішаної завади, що складається з тихої музики, шуму та голосових сигналів кількох учасників, зсунутих у часі та інвертованих за спектром, що робить неможливим зняття розбірливих сигналів навіть після обробки.

Таким чином, для ефективного захисту акустичної інформації від витоку через акустичні канали необхідно використовувати поєднання організаційних, технічних та інженерних заходів, що включають як пасивні методи ізоляції, так і активні способи створення маскуючих сигналів для порушення акустичних каналів витоку.

Захист інформації від витоку візуально-оптичним каналом

З метою захисту інформації від витоку через візуально-оптичний канал важливо врахувати низку ефективних заходів:

❖ *Просторова організація*

Розміщення об'єктів так, щоб виключити можливість відбиття світла в бік потенційного розташування зломисника. Це досягається через правильне планування простору та використання огорожень для блокування напрямків, де можуть виникнути відображення.

❖ *Зменшення відбиваючих властивостей*

Важливо знижувати відбиваючі властивості поверхонь об'єктів захисту. Це допомагає мінімізувати можливість відображення світла, що може бути використано для виявлення інформації.

❖ *Енергетичні обмеження*

Пониження рівня освітленості на об'єктах, що підлягають захисту, може значно знизити ймовірність відображення світла. Це також включає обмеження інтенсивності освітлення.

❖ *Засоби ослаблення відбитого світла*

Використання спеціальних екранів, ширм, штор або віконниць, а також застосування темного скла для зменшення відбиття та проникнення світла допомагає захистити інформацію.

❖ *Маскування та імітація*

Застосування методів маскування об'єктів і створення імітаційних перешкод може значно ускладнити виявлення інформації зловмисником, збільшуючи ефективність захисту.

❖ *Активний і пасивний захист*

Використання як пасивних, так і активних засобів для блокування неконтрольованого поширення відбитого світла та інших випромінювань є важливим елементом для забезпечення належного рівня безпеки.

❖ *Зміна фону та контрасту*

Маскування за допомогою варіацій у відбивних властивостях та контрасті фону також є важливою складовою захисту. Це дозволяє ефективно приховати критичні об'єкти від можливих спроб їх візуального виявлення.

Такий підхід забезпечує комплексний захист від витоку інформації через візуально-оптичні канали, що критично важливо для безпеки в умовах сучасних технологій та постійно зростаючих загроз.

6.6. ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ НА ОСНОВІ ЗАКЛАДНИХ ПРИБОРІВ

Одним з шляхів витоку інформації з об'єкта інформаційної діяльності (ОІД) є використання засобів несанкціонованого перехоплення. Суть цього каналу полягає в тому, що ці засоби, перебуваючи в межах контрольованої зони (КЗ) ОІД, приймають (перехоплюють) сигнал, що циркулює в системі, і передають його без відома власників інформації чи операторів системи.

Засоби несанкціонованого перехоплення, як правило, приховано розміщують на об'єкті і маскують під звичайні предмети або інші елементи інтер'єру, що ускладнює їх виявлення. Це може бути як класичне обладнання для прослуховування, так і високотехнологічні пристрої, такі як мікрофони або пристрої для перехоплення електронних сигналів, що використовують різні методи камуфляжу, наприклад, у вигляді зарядних пристроїв, меблів або навіть технічного обладнання.

Умовно цей канал витоку можна зобразити у вигляді схеми, де показано, як сигнал від джерела інформації перехоплюється такими засобами та передається до зловмисника. Використання таких каналів витоку є однією з основних загроз для інформаційної безпеки, оскільки дозволяє здійснювати таємне стеження за інформаційними потоками без можливості виявлення у реальному часі.

Актуальні методи боротьби з подібними загрозами включають комплексні заходи з фізичного захисту, технічного моніторингу та використання спеціальних засобів для виявлення й нейтралізації несанкціонованих пристроїв, а також організаційні заходи щодо підвищення обізнаності персоналу та контролю за доступом до важливих об'єктів.



Рис. 6.11. Канали витоку інформації на основі закладних пристроїв
Джерело: побудовано автором

Розміщення засобів несанкціонованого перехоплення на об'єкті інформаційної діяльності (ОІД) або в межах контрольованої зони (КЗ) може відбуватися через кілька можливих шляхів, серед яких основними є:

1. Несанкціоноване проникнення сторонніх осіб на ОІД або в межі КЗ

Може статися внаслідок недосконалого фізичного захисту, порушення пропускового режиму, або внаслідок недостатнього контролю за зовнішнім доступом. Наприклад, при неповному огляді приміщень або обладнання, що використовуються на об'єкті, сторонні особи можуть розмістити шкідливі пристрої для перехоплення сигналу.

2. Порушення правил режиму доступу штатних осіб на ОІД

Інший шлях включає порушення внутрішніх регламентів доступу до об'єктів, коли штатні співробітники можуть без належного контролю або дозволу розмістити обладнання для несанкціонованого перехоплення. Це може статися через несанкціоновану роботу з технічними засобами або через неувважність до відповідних процедур безпеки.

3. Закладка засобів перехоплення під час обладнання приміщень для ОІД або комплексу технічних засобів захисту інформації (ТЗІ)

Цей шлях передбачає приховану установку несанкціонованих пристроїв під час початкової інсталяції або реконструкції об'єкта. Такі засоби можуть бути замасковані під елементи системи ТЗІ, що згодом використовується для безпечного зберігання та обробки інформації, або для захисту мережевих інфраструктур.

Зважаючи на різноманітність таких загроз, ефективні заходи захисту повинні включати не лише технічні засоби для виявлення та нейтралізації перехоплених сигналів, але й організаційні заходи, що сприяють забезпеченню цілісності і безпеки на всіх етапах експлуатації та обслуговування ОІД. Сюди входять контроль за доступом, регулярні перевірки, наявність систем моніторингу і обробки інцидентів безпеки, а також тренування персоналу для виявлення потенційних загроз.

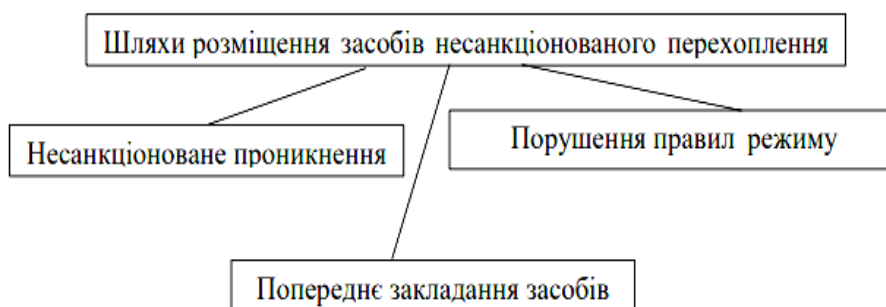


Рис. 6.12. Шляхи розміщення засобів несанкціонованого перехоплення
Джерело: побудовано автором

Закладні пристрої: класифікація та особливості

Засоби несанкціонованого перехоплення, відомі як закладні пристрої, широко застосовуються зловмисниками для перехоплення інформації з об'єктів інформаційної діяльності (ОІД). Саме так їх позначають у сучасній літературі та підручниках.

Закладні пристрої класифікуються за:

1. Видом та способом прийому інформації.
2. Способом передачі перехопленої інформації до приймача технічних засобів розвідки (ТЗР) противника.

Класифікація за видом та способом прийому інформації

❖ Аудіо-закладні пристрої

Призначені для отримання мовної акустичної інформації, що циркулює в приміщенні. Використовуються для перехоплення розмов, сигналів голосового характеру.

❖ *Телевізійні закладні пристрої*

Призначені для отримання аудіо- та відеоінформації. Застосовуються для стеження, отримання візуального контенту з приміщень.

❖ *Закладні пристрої для телефонних ліній зв'язку*

Підключаються до телефонних ліній, пристроїв обробки або передачі інформації. Забезпечують перехоплення сигналів, переданих через телекомунікаційні системи.



Рис. 6.13. Класифікація закладних пристроїв

Джерело: побудовано автором

Сучасні закладні пристрої становлять серйозну загрозу інформаційній безпеці через їхню технічну досконалість та широкі функціональні можливості. Однією з основних характеристик таких пристроїв є підтримка бездротових технологій, як-от Wi-Fi та Bluetooth, що значно розширює зону їхньої дії та забезпечує можливість передачі перехопленої інформації на значні відстані. Крім того, вони часто оснащуються вбудованими елементами штучного інтелекту, які здатні автоматизувати процеси перехоплення, аналізу та передачі даних, роблячи їх більш ефективними та менш помітними. Важливим аспектом є також мініатюризація цих пристроїв, яка дозволяє зловмисникам приховувати їх

у звичайних предметах, роблячи їх практично непомітними навіть для спеціалізованих засобів виявлення.

Для мінімізації ризиків витоку інформації через закладні пристрої необхідно впроваджувати комплексні заходи безпеки. Регулярні технічні перевірки приміщень із використанням спеціалізованого обладнання дозволяють виявляти й нейтралізувати такі пристрої. Важливим є також створення систем активного виявлення сторонніх пристроїв, які здатні виявляти їх у режимі реального часу. Суворий контроль доступу до об'єктів, включно з перевіркою персоналу та зовнішніх підрядників, допомагає запобігти несанкціонованому встановленню закладних пристроїв. Додатково рекомендується використовувати засоби глушіння або шифрування інформації, що передається через лінії зв'язку, аби ускладнити перехоплення даних.



Рис. 6.14. Класифікація пристроїв несанкціонованого зняття інформації
Джерело: побудовано автором

Впровадження цих заходів значно зменшує ймовірність витоку інформації через закладні пристрої, забезпечуючи захист критично важливої інформації та підвищуючи рівень інформаційної безпеки на підприємствах.

Закладні пристрої класифікують за способом передачі перехопленої інформації до противника на кілька категорій:

1. *Радіо-закладні пристрої* – передають перехоплену інформацію через радіоефір, використовуючи різні частотні діапазони. Вони дозволяють зловмиснику отримувати дані на значній відстані від об'єкта без фізичного доступу до пристрою.

2. *Пристрої з передачею інформації через мережі зв'язку та живлення* – використовують існуючі комунікаційні лінії (мережі управління, живлення, локальні мережі) для передачі даних. Такий спосіб є складним для виявлення, оскільки дані передаються по вже функціонуючим каналам.

3. *Радіо-закладні пристрої з перевипромінюванням (пасивні)* – ці пристрої не мають власного джерела живлення і активуються зовнішнім сигналом, після чого перевипромінюють інформацію. Вони особливо небезпечні через низьку ймовірність їхнього виявлення під час стандартних перевірок.

4. *Закладні пристрої, що використовують телефонні канали* – такі пристрої передають перехоплену інформацію через стандартний телефонний канал. До цієї категорії відносяться, зокрема, пристрої типу "довге вухо" або "зі штучно піднятою трубкою", які використовують телефонну мережу для передачі даних у режимі реального часу.

Сучасні технології значно підвищують ефективність цих пристроїв, забезпечуючи вищу швидкість передачі, захищеність каналів зв'язку та інтеграцію з автоматизованими системами управління перехопленням даних. Це вимагає від підприємств впровадження сучасних методів виявлення, моніторингу та нейтралізації таких загроз.

Загальні характеристики та особливості деяких типів закладних пристроїв

Оформлення та спосіб монтажу:

Закладні пристрої можуть бути виконані з використанням двох основних підходів до монтажу:

- Прихований монтаж — передбачає попереднє розміщення закладного пристрою у приміщенні або об'єкті до його експлуатації.
- Після проникнення — закладні пристрої виконуються у вигляді технічних модулів або компонентів, замаскованих під побутові предмети, технічні елементи, одяг тощо.

Потужність випромінювання:

- Мала потужність: до 10 мВт, використовується для локальних завдань.
- Середня потужність: від 10 до 100 мВт, забезпечує середню дальність передачі.
- Велика потужність: більше 100 мВт, застосовується для віддалених об'єктів.
- Регульована потужність: адаптується до умов використання для оптимізації роботи пристрою.

Використовуваний вид модуляції:

- Амплітудна модуляція (АМ) — проста та широко поширена.
- Частотна модуляція (ЧМ) — забезпечує вищу стійкість до завад.
- Широкосмугова модуляція (WFM) та вузькосмугова (ICPM) — використовуються залежно від характеристик каналу.
- Сучасні методи: OFDM (мультиплексування із ортогональним частотним поділом), шумоподібні сигнали для підвищення непомітності передачі.

Стабілізація частоти:

- Нестабілізовані пристрої легко виявляються через недосконалість.
- Стабілізація схемотехнічна забезпечує помірну точність.
- Кварцова стабілізація гарантує підвищену точність частоти.

Дальність перехоплення та способи підключення:

- До 10 м: акустична хвиля через мікрофон.
- До 1 м: вібраційна хвиля через стіни (цегляні або бетонні).
- Контактне підключення: до ліній зв'язку або систем передачі даних.

Типи модуляції та стандарти:

- Модуляція з інверсією спектра.
- Частотна мозаїка.
- Дельта-модуляція.
- Рандомізація та криптографічне шифрування сигналів.

Типи закладних пристроїв

❖ Радіозакладні пристрої

Ці пристрої використовують радіоэфір для передачі інформації:

- Радіомікрофони — активні пристрої для перехоплення мовних сигналів.
- Пасивні перевипромінювачі — активуються під впливом радіохвиль і не потребують постійного живлення.

❖ Закладні пристрої типу «довге вухо» або «зі штучно піднятою трубкою»

Використовуються в телефонних лініях і забезпечують дистанційний контроль приміщення. Їх особливостями є:

- Велика дальність дії (до 10 км або без обмежень у цифрових мережах).
- Використання сигналів відбою для уникнення випадкових підключень.

❖ Мережеві закладні пристрої

Використовують мережу електроживлення як для передачі даних, так і для живлення. Камуфлюються під побутові прилади (наприклад, електролампа або чайник).

❖ Радіозакладні пристрої з перевипромінюванням

Ці пристрої взаємодіють із акустичними або електромагнітними резонаторами. Переваги: не потребують живлення, можуть працювати необмежений час і є складними для виявлення.

Сучасні методи виявлення закладних пристроїв

Одним із ключових аспектів забезпечення інформаційної безпеки є виявлення закладних пристроїв, які можуть використовуватися для несанкціонованого перехоплення даних. Для цього застосовуються як технічні засоби виявлення, так і комплексні методи захисту.

Технічні засоби виявлення ґрунтуються на використанні сучасних технологій аналізу та сканування. Одним із основних методів є аналіз спектру випромінювання, що дозволяє виявляти сигнали, які передаються прихованими пристроями. Цей метод забезпечує високу точність і ефективність, особливо при роботі в умовах із високим рівнем радіоелектронних перешкод. Додатково використовуються скануючі пристрої, які здатні визначати частоту та тип модуляції сигналів, що дозволяє ідентифікувати джерела прихованих передач.

Для підвищення ефективності виявлення закладних пристроїв використовуються програмно-апаратні комплекси, які об'єднують у собі функції моніторингу та локалізації загроз у реальному часі. Такі системи інтегруються у загальну інфраструктуру інформаційної безпеки, забезпечуючи автоматичний аналіз сигналів і швидке реагування на підозрілі активності.

Методи захисту відіграють важливу роль у запобіганні використанню закладних пристроїв. Одним із найефективніших підходів є шифрування переданих даних, що унеможливує їх використання навіть у разі перехоплення. Для блокування роботи закладних пристроїв широко застосовуються пристрої глушіння радіочастот (RF Jammer), які створюють перешкоди на заданих частотах. Крім того, електромагнітне екранування приміщень забезпечує захист від проникнення радіосигналів

зовні та запобігає витоку інформації через електромагнітне випромінювання.

Таким чином, сучасні методи виявлення та захисту від закладних пристроїв базуються на використанні високотехнологічних рішень, які забезпечують надійну ідентифікацію загроз та ефективний захист конфіденційної інформації. Ці підходи є важливим елементом комплексної системи інформаційної безпеки.

6.7. ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ НА ОСНОВІ ЗАКЛАДНИХ ПРИСТРОЇВ

Закладні пристрої є технічними засобами, що створюють рукотворні канали витоку інформації для несанкціонованого перехоплення даних. Їх установка часто супроводжується застосуванням маскувальних технологій, що значно ускладнює виявлення таких пристроїв. Це становить серйозну загрозу для безпеки інформаційних об'єктів. Для ефективного захисту інформації використовуються комплексні заходи, які спрямовані на попередження встановлення закладних пристроїв, їхнє виявлення та протидію їхній роботі.



Рис. 6.15. Методи виявлення пристроїв несанкціонованого зняття інформації

Джерело: побудовано автором

Заходи із захисту інформації поділяються на організаційні та технічні, причому кожен тип має свої глобальні та локальні рівні реалізації.

Організаційні заходи спрямовані на створення умов, що унеможлиблюють встановлення закладних пристроїв. До глобальних заходів належить організація режиму роботи виділених приміщень, контроль доступу співробітників та відвідувачів, перевірка приміщень і техніки, включно з новим обладнанням, на наявність прихованих пристроїв. Аналіз методів і технологій встановлення закладних пристроїв дозволяє врахувати можливі загрози та адаптуватися до новітніх технічних рішень зловмисників.

Локальні організаційні заходи охоплюють аналітичну роботу з визначення можливих місць встановлення закладних пристроїв, моніторинг радіочастотного спектру та аналіз способів роботи таких пристроїв. Це включає організацію спеціалізованої служби безпеки, яка займається контролем за радіовипромінюваннями, мережами зв'язку та управлінням.

Технічні заходи спрямовані на створення і використання спеціалізованих засобів виявлення та протидії закладним пристроям. Глобальні технічні заходи передбачають встановлення систем охоронної сигналізації, відеоспостереження, контролю доступу, а також використання технічних засобів, які сигналізують про підключення сторонніх пристроїв до ліній зв'язку чи мереж живлення. Інноваційні рішення, такі як апаратура нелінійної радіолокації, рентгенівські установки, тепловізори та металодетектори, підвищують ефективність перевірки приміщень та обладнання.

Локальні технічні заходи включають моніторинг сигналів у лініях зв'язку, живлення, управління та охоронних системах, а також контроль інфрачервоних і радіовипромінювань у районі ОІД. Для цього використовуються спеціальні пристрої, такі як сканери радіочастот, нелінійні локатори та апаратура для підповерхневої локації. У разі виявлення закладних пристроїв застосовуються заходи з їх демонтажу, руйнування або відключення.

Сучасні інноваційні підходи включають використання алгоритмів штучного інтелекту для автоматичного аналізу аномалій у радіосигналах і мережах зв'язку, а також інтеграцію захисних систем в «розумні» приміщення з датчиками IoT. Крім того, дрони з пристроями виявлення можуть перевіряти важкодоступні місця, а квантова криптографія забезпечує захист переданих даних на принципово новому рівні.

Комплексний підхід до виявлення закладних пристроїв базується на поєднанні фізичних та електронних методів. Фізичні методи передбачають ретельний огляд приміщень, меблів та обладнання, тоді як електронні

методи включають сканування радіочастотного спектру, тепловізійну перевірку та використання рентгенівського обладнання.

Таким чином, ефективний захист інформації від витоку через закладні пристрої потребує як організаційних, так і технічних заходів, які інтегруються в загальну систему безпеки підприємства. Сучасні технології та інноваційні підходи дозволяють значно підвищити рівень безпеки та мінімізувати ризики, пов'язані з використанням закладних пристроїв.

Захист інформації від витоків через канали на основі закладних пристроїв є важливою частиною інформаційної безпеки. Закладні пристрої, такі як апаратні ключі, шифрувальні модулятори чи елементи біометричної аутентифікації, можуть застосовуватись для захисту інформації на різних рівнях: від доступу до фізичних приміщень до захисту даних в інформаційних системах.

Основні заходи захисту інформації за допомогою таких пристроїв:

✿ ***Шифрування даних за допомогою апаратних модулів (HSM - Hardware Security Modules)***

Використання спеціалізованих апаратних пристроїв для генерації і зберігання криптографічних ключів дозволяє запобігти витокам інформації через вразливості програмного забезпечення.

✿ ***Системи біометричної аутентифікації***

Використання відбитків пальців, сканерів райдужної оболонки ока або інших біометричних даних для підтвердження особистості користувача допомагає запобігти несанкціонованому доступу.

✿ ***Механізми контролю доступу до пристроїв***

Встановлення фізичних обмежень на доступ до критичних пристроїв (наприклад, серверів або робочих станцій) через використання роз'ємів, закладних елементів або перехідників для авторизації дозволяє знизити ризики витоку інформації.

✿ ***Інтелектуальні карти та токени***

Використання інтелектуальних карт, токенів або інших форм апаратної автентифікації, які містять закладені криптографічні ключі, дозволяє посилити захист від несанкціонованого доступу до систем.

✿ ***Виявлення та моніторинг фізичних каналів***

Для виявлення потенційних витоків інформації через фізичні канали (наприклад, електромагнітні випромінювання) використовуються спеціалізовані системи моніторингу та детектори.

✿ ***Захист від витоку через мережеві канали***

Використання закладних пристроїв для забезпечення безпеки мережі, таких як апаратні засоби для шифрування трафіку (VPN, IPSec, SSL/TLS).

Всі ці заходи можна комбінувати для забезпечення всебічного захисту інформації на всіх етапах її обробки та передачі, враховуючи можливі канали витоку.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 6

1. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.
2. Лахно В. А., Терещук А. М., Петренко Т. А. (2016) Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак. *Захист інформації*. Т. 18. № 2. С. 99–106.
3. Гришук Р.В. Основи кібернетичної безпеки : Монографія / Ю.Г. Даник, Р.В. Гришук ; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2019. – 636 с.
4. Сунь-Цзи. (2014) Мистецтво війни: переклад Г. Латника. Київ: Арій. 128 с.
5. Рекомендації CERT-UA щодо протидії АРТ (Advanced Persistent Threat). URL: <https://cert.gov.ua/recommendations/18>.
6. Костюк Ю.В., Ковальова Л.І., Повна Н.І. Захист інформації у сегменті інформаційної системи на основі інтелектуальних технологій // Збірник тез VI Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2023. – с. 77-79.
7. Довженко, Н., Мазур, Н., Костюк, Ю., & Рзаєва, С. (2024). Інтеграція іот та штучного інтелекту в інтелектуальні транспортні системи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 430–444.
8. Костюк Ю.В. Використання нейронних механізмів штучного інтелекту для кластеризації вузлів та маршрутизації даних у бездротових сенсорних мережах // Тези доповідей десятої міжнародної науково-практичної конференції «Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. // Відповідальна за випуск завідувач кафедри ІТ С.В. Цюцюра, – К. : КНУБА, 2023. – с. 85-86.
9. S. Abramov, A. Bessalov, V. Sokolov, Properties of Isogeny Graph of Non-Cyclic Edwards Curves, in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3550 (2023) 234–239.
10. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та

безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

11. V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36.

12. Костюк Ю.В. Використання нейронних механізмів штучного інтелекту для кластеризації вузлів та маршрутизації даних у бездротових сенсорних мережах // Тези доповідей десятої міжнародної науково-практичної конференції «Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. // Відповідальна за випуск завідувач кафедри ІТ С.В. Цюцюра, – К. : КНУБА, 2023. – с. 85-86.

13. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 390–400.

14. V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4.

15. Марценюк, М., Козачок, В., Богданов, О., Іосіфов, Є., & Бржезьська, З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 148–155.

16. Shevchenko, S., Zhdanova Y. ., & Spasiteleva, S. (2023). Математичні методи в кібербезпеці: теорія катастроф. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 165–175.

17. Костюк Ю.В., Степашкіна К.В. Моделювання інтелектуальних систем управління захистом інформації в інформаційно-телекомунікаційних системах // Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2023) : матеріали тез доповідей XIII Міжнародної науково-практичної конференції (м. Чернігів, 25–26 травня 2023 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2023. – Т. 2. – с. 252-253.

18. O. Trofymchuk, et al., On the Use of Gray Codes for Solving 0-1 Combinatorial Problems of Optimization and Decision-Making in Environmental and Economic Systems, in: Workshop on Information Technology and Mathematical Modeling for Environmental Safety, vol. 3021 (2021) 1–17.

19. A. Ilyenko, et al., Practical Aspects of Using Fully Homomorphic Encryption Systems to Protect Cloud Computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 226-233.

20. Костюк Ю.В. Математичне моделювання захищених інформаційних систем // Інноваційний потенціал сучасної науки: зб. наук. праць IV Всеукраїнської наук.-практ. інтернет-конф., (18 травня 2023 року. Кам'янець-Подільський). - Кам'янець-Подільський Зклад вищої освіти «Подільський державний університет», 2023. с. 171-174.

21. D. Virovets, et al., Soul Bound Token as Digital Twins in Peer-to-Peer Economic Systems, in: Digital Economy Concepts and Technologies, vol. 3665 (2024) 97–105.

22. Y. Sovyn, et al., Minimization of Bitsliced Representation of 4×4 S-Boxes based on Ternary Logic Instruction, in Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 12–24.

23. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.

24. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

25. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

26. O. Mykhaylova, et al., Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 239–251.

27. V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.

РОЗДІЛ 7

ПРИНЦИПИ ТЕХНІЧНОЇ РОЗВІДКИ



7.1. Поняття та принципи технічної розвідки

7.2. Основні задачі, органи та види технічної розвідки

7.3. Поняття промислового шпигунства

7.4. Принципи захисту від технічної розвідки

"Технічна розвідка — це очі та вуха на передовій, які дозволяють передбачити можливі загрози та отримати ключову інформацію для стратегічних рішень."

*Сунь Цзи, китайський полководець і автор
"Мистецтва війни"*

Технічна розвідка є важливою складовою стратегічного управління, яка зосереджується на зборі, аналізі та використанні технічної інформації з метою отримання переваги в різних сферах. Це процес, який дозволяє виявляти вразливості в інформаційних системах, передбачати потенційні загрози та оптимізувати процес прийняття рішень. Одним із основних аспектів технічної розвідки є збір даних із різноманітних джерел, таких як телекомунікаційні мережі, супутникові зображення, радіочастотні спектри та відкриті джерела інформації, включаючи Інтернет і соціальні мережі. Всі ці дані допомагають формувати повну картину ситуації і на основі них приймати обґрунтовані рішення.

Однією з основних цілей технічної розвідки є виявлення та аналіз вразливостей в інфраструктурі, технологіях чи системах безпеки. Це дозволяє оперативно виявляти потенційні загрози, які можуть призвести до витоку або знищення важливої інформації, а також пропонувати методи для їхнього запобігання. Наприклад, в контексті кібербезпеки технічна розвідка може допомогти виявити уразливості в програмному забезпеченні чи мережах компаній, що дозволяє вчасно вжити заходів щодо їхнього усунення. Користуючись технічними засобами шифрування та контррозвідки, можна забезпечити високий рівень захисту від несанкціонованого доступу до критичної інформації, що особливо важливо в умовах сучасних кіберзагроз.

Технічна розвідка також сприяє розвитку нових технологій та дозволяє державам, корпораціям і організаціям зберігати стратегічну перевагу. Збір та аналіз інформації про нові технологічні досягнення дозволяє здійснювати прогнозування тенденцій і своєчасно адаптуватися до змін у технічному середовищі. Також це дає змогу розпізнавати та протидіяти конкурентам, що використовують новітні інструменти для досягнення своїх цілей. Важливим аспектом є застосування технічної розвідки для забезпечення безпеки на всіх етапах — від збору і зберігання даних до їхнього транспортування і обробки.

Таким чином, технічна розвідка є надзвичайно важливим інструментом для розвитку ефективних стратегій в галузях, пов'язаних з інформаційною безпекою, обороною, а також бізнесом і технологіями. Вона забезпечує своєчасне реагування на нові загрози та можливості, що дозволяє організаціям і державам залишатися на крок попереду у сучасному високотехнологічному середовищі.

7.1. ПОНЯТТЯ ТА ПРИНЦИПИ ТЕХНІЧНОЇ РОЗВІДКИ

Технічна розвідка (ТР) — це процес здобування, аналізу та використання технічних засобів для отримання інформації, що має стратегічне значення, зокрема в галузі національної безпеки. Цей процес включає не лише традиційні методи збору даних, але й інтеграцію новітніх технологій та розширених інструментів збору інформації, що дозволяють отримувати більш точні та актуальні відомості у режимі реального часу. Основна мета технічної розвідки полягає в забезпеченні своєчасною, достовірною та високоякісною інформацією для вищого політичного керівництва держави щодо різних аспектів національної безпеки, зокрема про стан збройних сил, військово-економічний потенціал, критичні

інфраструктури, а також про загрози з боку інших держав або неурядових акторів.

У сучасних умовах технічна розвідка включає в себе не лише традиційні способи збору даних за допомогою радіолокаційних станцій, шпигунських супутників або підслуховування радіочастотних каналів, але й використовує новітні цифрові технології, такі як кіберрозвідка, інтернет-розвідка та аналіз великих даних. Кіберрозвідка стала невід'ємною частиною технічної розвідки, оскільки з розвитком інформаційних технологій виникла потреба в моніторингу кіберзагроз, таких як атаки на інформаційні системи, мережі, електронні платформи та інші елементи критичної інфраструктури. Для цього активно використовуються спеціалізовані системи, що здатні виявляти аномалії, слідкувати за потенційними кіберзагрозами та реагувати на них в реальному часі.

Додатково, використання технологій штучного інтелекту (ШІ) та машинного навчання значно підвищує ефективність технічної розвідки. Ці технології дозволяють швидше обробляти великий обсяг даних, автоматично виявляти патерни та аномалії, що можуть свідчити про загрози, і прогнозувати потенційні атаки або інші негативні події. ШІ також допомагає в автоматизованій обробці супутникових зображень, радіолокаційних даних та моніторингу мережевої активності, що дає змогу приймати більш обґрунтовані рішення на основі актуальних даних.

Не менш важливим аспектом є використання методів та засобів для збору інформації в небезпечних або недоступних для людей місцях. Для цього широко застосовуються безпілотні літальні апарати (дрони) та інші роботизовані системи, що дозволяють отримувати відео- та аудіодані в реальному часі без ризику для людського життя. Наприклад, дрони можуть бути використані для моніторингу військових об'єктів, транспортних систем або для збору інформації про природні катастрофи, терористичні акти чи військові конфлікти в умовах, коли традиційні методи збору інформації є занадто ризикованими або неефективними.

Важливою складовою сучасної технічної розвідки є також інтеграція даних з різних джерел у єдину інформаційну систему, що дозволяє створити комплексний аналіз на основі даних з відкритих джерел, супутникових спостережень, кіберрозвідки, а також з традиційних технічних засобів розвідки. Це дозволяє отримати більш повну картину ситуації та швидко реагувати на зміни, що відбуваються на глобальній або регіональній арені.

Таким чином, сучасна технічна розвідка є важливим інструментом забезпечення національної безпеки та ефективного управління в умовах глобалізації та постійно змінюваних технологічних та геополітичних умов.

Вона є ключовим елементом не лише для державної безпеки, але й для корпоративної безпеки, оскільки дозволяє виявляти загрози з боку конкурентів або зловмисників, а також сприяє оперативному реагуванню на нові виклики в сфері кібербезпеки.

Сучасні об'єкти технічної розвідки включають:

- Збройні сили та військові підрозділи,
- Оборонну промисловість,
- Науково-дослідні центри та лабораторії,
- Полігони для випробувань і навчань,
- Транспортні системи (повітряний, морський, наземний),
- Комунікаційні та зв'язкові мережі,
- Енергетичні системи,
- Системи охорони урядових і стратегічних об'єктів.

Принципи організації технічної розвідки в сучасних умовах включають:

❖ ***Цілеспрямованість*** — вся діяльність з добування інформації зосереджена на конкретних цілях, таких як захист національних інтересів або виявлення потенційних загроз. Це також передбачає використання інформаційних засобів для своєчасного реагування на зміни у військовій ситуації або економічному становищі.

❖ ***Централізація управління*** — технічна розвідка координується в межах вищих політичних структур, що дозволяє зосередити ресурси для максимально ефективного збору та обробки даних з різних відомств. Централізація управління також забезпечує інтеграцію різних видів технічної розвідки, таких як кіберрозвідка, супутникові спостереження та радіолокаційний моніторинг, в єдину координаційну систему. Це дозволяє оперативно реагувати на зміни в ситуації та приймати рішення на основі комплексного аналізу даних з різних джерел. Завдяки централізації, розвідувальні органи можуть ефективно розподіляти ресурси, спрямовуючи їх на найбільш важливі та стратегічні цілі для забезпечення національної безпеки.

❖ ***Розміщення технічних засобів на стратегічних ділянках*** — включає встановлення спеціалізованих засобів для збору інформації на кордонах, в акваторіях і навіть в межах іншої країни. Це можуть бути супутники, радіолокаційні станції, мережі для прослуховування та моніторингу інформації. Ці засоби дозволяють не лише спостерігати за рухом військових сил і важливими об'єктами, але й здійснювати моніторинг комунікацій ворожих структур або потенційних загроз. Встановлення технічних засобів на стратегічних ділянках також включає

використання безпілотних літальних апаратів для збору інформації в важкодоступних або небезпечних зонах. Крім того, технології штучного інтелекту та машинного навчання можуть бути інтегровані в ці системи для аналізу великих обсягів даних і виявлення потенційних загроз в реальному часі.

❖ **Комплексність** — застосування різних типів технічних засобів для збору даних з різних джерел і фізичних полів, що дозволяє підвищити достовірність та точність отриманої інформації. Це включає в себе використання супутникових зображень, радіолокаційних даних, а також сигналів з інших сенсорних систем для аналізу ситуації в різних фізичних просторах, таких як електромагнітні, акустичні та оптичні поля. Крім того, комплексний підхід забезпечує дублювання джерел інформації для виключення можливих помилок або маніпуляцій. В результаті така багаторівнева система дозволяє не лише отримувати більш точні дані, але й створювати цілісну картину, що підвищує ефективність прийняття рішень.

❖ **Оперативність** — здатність швидко реагувати на зміни ситуації і здійснювати збори інформації в найкоротші терміни, що є важливим для оперативних рішень. Оперативність забезпечується завдяки використанню сучасних технологій збору інформації в реальному часі, таких як мобільні розвідувальні системи та автоматизовані платформи для обробки даних. Це дозволяє не тільки виявляти загрози на ранніх етапах, але й швидко реагувати на них, мінімізуючи ризики для національної безпеки. Крім того, оперативність сприяє своєчасному оновленню аналітичних даних, що дозволяє ухвалювати рішення на основі найбільш актуальної та достовірної інформації.

❖ **Безперервність** — технічна розвідка здійснюється постійно, без перерв, навіть в умовах важкої погоди чи вночі, що дозволяє забезпечити неперервний потік інформації. Це досягається завдяки використанню автоматизованих систем та розвідки з орбітальних платформ, які працюють 24/7, незалежно від зовнішніх умов. Безперервність також підтримується завдяки системам самонавчання та адаптації, що дозволяють постійно оновлювати стратегії збору даних в умовах змінюваної обстановки. Такі технології дозволяють забезпечити цілодобову наявність актуальної інформації для вищого керівництва, що є критично важливим для ефективного управління національною безпекою.

❖ **Глобальність** — технічна розвідка проводиться по всій земній кулі, зокрема з використанням супутникових систем, що дозволяє охопити значні території і збирати дані з віддалених регіонів. Це дає можливість здійснювати моніторинг і виявлення загроз на глобальному рівні,

охоплюючи різні континенти та віддалені райони, які можуть бути стратегічно важливими. Використання супутників дозволяє здійснювати спостереження за військовими, економічними та природними змінами в реальному часі, що критично важливо для своєчасного реагування. Глобальність технічної розвідки також забезпечує інтеграцію інформації з різних регіонів, дозволяючи створювати повну картину світових подій і потенційних ризиків.

❖ **Плановість** — всі операції з технічної розвідки виконуються відповідно до заздалегідь розроблених планів і програм, що дозволяє організувати процес максимально ефективно.

❖ **Прихованість** — для збору інформації використовуються пасивні технічні засоби, що не привертають уваги, а також застосовуються різноманітні методи маскування і камуфляжу для розвідувальної апаратури, що дозволяє зберігати розвідувальну діяльність у таємниці. Це включає в себе використання технологій, таких як стелс-техніка для супутників і безпілотних літальних апаратів, а також інтеграцію шифрування та анонімізації для захисту переданих даних. Крім того, застосовуються спеціалізовані методи маскування для розміщення розвідувальних пристроїв в зоні спостереження, щоб уникнути їх виявлення супротивником. Такий підхід дозволяє не лише ефективно здійснювати збір інформації, але й мінімізувати ризик викриття розвідувальної діяльності, що підвищує безпеку операцій.



Рис. 7.1. Принципи технічної розвідки
Джерело: побудовано автором

Сучасні технології, такі як супутникові системи, дрони, радіолокаційні станції та інші високотехнологічні засоби, дозволяють проводити технічну розвідку на новому рівні. Водночас, з розвитком інформаційних технологій, акцент робиться також на кіберрозвідці, яка здатна виявляти загрози та потенційні атаки на критичні інфраструктури, що є важливим аспектом сучасної технічної розвідки.

Загалом технічна розвідка є важливим інструментом для забезпечення національної безпеки, захисту економічних інтересів і своєчасного реагування на глобальні зміни у міжнародній ситуації.

7.2. ОСНОВНІ ЗАДАЧІ, ОРГАНИ ТА ВИДИ ТЕХНІЧНОЇ РОЗВІДКИ

Завдання технічної розвідки (ТР)

Завдання технічної розвідки (ТР) полягають у зборі, обробці та аналізі інформації, що стосується військових, економічних, науково-технічних і політичних аспектів безпеки держави. Основні завдання технічної розвідки включають:

✳ Збір інформації про військово-економічний потенціал противника

Це включає отримання даних про стан, склад і перспективи розвитку військових сил та засобів, а також про економічний потенціал, що підтримує військові зусилля, зокрема оборонну промисловість.

✳ Оцінка бойової готовності військ та сил

Технічна розвідка допомагає визначити стан бойової готовності збройних сил, а також динаміку їх змін, що дозволяє своєчасно реагувати на потенційні загрози та адаптувати стратегію.

✳ Збір даних про розміщення об'єктів оборонної промисловості

Розвідка здійснює моніторинг об'єктів, що займаються виробництвом озброєння, військової техніки та інших критичних матеріалів, а також оцінює їх виробничі потужності.

✳ Моніторинг розробок в області озброєння та військової техніки

Це включає виявлення нових розробок і модернізацій військової техніки, що можуть значно вплинути на баланс сил, а також оцінку їх ефективності.

✳ Аналіз навчань і підготовки військ

Збір інформації про проведення навчань, маневрів і тренувань військових формувань дозволяє оцінити рівень підготовки та координації між підрозділами, а також визначити можливі уразливості.

✳ Збір інформації про ресурси країни

Це включає виявлення і оцінку наявних природних, енергетичних та інших ресурсів, таких як паливо, вода, руди та інші стратегічні матеріали, що мають значення для національної безпеки.

✳ Ідентифікація та аналіз сучасних технологій і інфраструктури

Технічна розвідка займається збором даних про новітні технології та інфраструктуру, яка може бути використана для військових цілей або вплинути на загальний рівень технологічної готовності держави.

✳ Виявлення і аналіз інформаційно-комунікаційних систем противника

Технічна розвідка здійснює аналіз цифрових інфраструктур і комунікаційних каналів, включаючи кібербезпеку, для виявлення уразливостей і оцінки можливих кіберзагроз.

✳ Координація з іншими розвідувальними органами

Технічна розвідка взаємодіє з іншими державними структурами розвідки, щоб забезпечити інтеграцію даних і створити єдину картину ситуації.

Завдання технічної розвідки мають надзвичайно важливе значення для прийняття оперативних і стратегічних рішень, що сприяє забезпеченню національної безпеки та стабільності в умовах глобальних загроз. Різноманітність видів носіїв інформації призвела до появи численних форм технічної розвідки, які класифікуються за різними ознаками. Найбільш широко застосовуються дві основні класифікації: за фізичною природою носіїв інформації та за способами ведення і каналами збору даних. Збройні сили провідних держав світу активно використовують сучасні системи розвідки та цілевказування, що забезпечують оптичну розвідку, реальний час передачі даних про цілі, коригування артилерійського вогню та управління високоточними боєприпасами.



Рис. 7.2. Види технічної розвідки

Джерело: побудовано автором

Органи технічної розвідки

Органи технічної розвідки (ТР) є спеціалізованими підрозділами, що здійснюють збір, обробку та аналіз інформації з різних джерел, використовуючи технічні засоби. Вони діють в межах національних та міжнародних структур, а також можуть бути інтегровані у систему загальної розвідки держави. Основні органи технічної розвідки включають:

▲ *Центральні органи розвідки*

Це основні координаційні органи, які визначають стратегію і пріоритети технічної розвідки на державному рівні. Вони займаються розробкою політики, управлінням ресурсами і координацією між різними підрозділами та спеціалізованими агентствами. Це можуть бути урядові структури, такі як міністерства оборони чи безпеки.

▲ *Військові органи технічної розвідки*

Включають в себе підрозділи та служби, що безпосередньо працюють у складі збройних сил. Вони відповідають за використання технічних засобів для збору розвідданих на території противника, моніторинг бойових ситуацій, аналіз інформації з супутників, радіоелектронної розвідки та інших методів. Ці органи можуть працювати як на фронті, так і на рівні стратегічних командувань.

▲ *Спеціалізовані агентства та служби*

Це органи, які займаються конкретними видами технічної розвідки, наприклад, радіоелектронною, оптичною, хімічною, радіаційною розвідкою, а також інтернет-розвідкою (кіберрозвідкою). Вони відповідають за експертну оцінку і аналіз спеціалізованих даних, які надходять через технічні канали.

▲ *Центри технічної розвідки на території іноземних держав*

Це спеціалізовані підрозділи, які проводять розвідку в іноземних країнах, використовуючи сучасні технічні засоби. Вони можуть бути частинами дипломатичних представництв або діяти незалежно в рамках розвідки.

▲ *Науково-дослідні та технологічні інститути*

Інститути, які займаються розробкою нових методів та технологій для технічної розвідки. Це можуть бути державні науково-дослідні організації або приватні компанії, що надають інноваційні рішення для збору і обробки розвідданих.

▲ *Інтегровані системи технічної розвідки*

Це комплекси, які забезпечують моніторинг і координацію між усіма рівнями технічної розвідки. Вони включають зв'язок між військовими, цивільними і спеціалізованими органами для швидкого збору і аналізу інформації, а також прийняття оперативних рішень.

Ці органи технічної розвідки працюють у тісній взаємодії з іншими органами національної безпеки та розвідки, що дозволяє забезпечити злагоджене і ефективне управління інформацією для підвищення рівня національної безпеки.

Засоби технічної розвідки

Засоби технічної розвідки — це різноманітні пристрої, системи та технології, які використовуються для збору, перехоплення та аналізу інформації, що дозволяє отримати дані про діяльність підприємств, організацій або державних структур без їхнього відома. Вони можуть включати як традиційні методи, так і сучасні засоби кіберрозвідки, орієнтовані на технологічний прогрес.

❖ Системи перехоплення сигналів

Пристрої, які використовуються для перехоплення електронних повідомлень, телефонних розмов або інших видів комунікацій. Сюди входять як традиційні радіоперехоплювачі, так і сучасні системи для перехоплення інтернет-трафіку, наприклад, через програмне забезпечення для моніторингу мереж.

❖ Системи для прослуховування і відеоспостереження

Такі пристрої можуть бути використані для несанкціонованого прослуховування телефонних розмов або для запису аудіо та відео з різних об'єктів. Використовуються як стаціонарні, так і мобільні пристрої, включаючи мікрофони та камери, що можуть бути приховані або інтегровані в звичайні предмети (наприклад, годинники, лампи, зарядні пристрої).

❖ Шпигунське програмне забезпечення (шпигунські програми)

Це програмні засоби, що встановлюються на комп'ютери, смартфони або інші цифрові пристрої для збору та передачі інформації без відома користувача. Вони можуть стежити за діяльністю в мережі, записувати натискання клавіш, перехоплювати паролі або інші конфіденційні дані.

❖ Мобільні пристрої та дрони для стеження

Використовуються для збору інформації з віддалених або важкодоступних місць. Мобільні пристрої, оснащені камерами та сенсорами, можуть використовуватися для відеоспостереження або збору інформації про середовище. Дрони можуть здійснювати аерофотозйомку, фіксувати місця збору даних або навіть доставляти мікрофони та інші сенсори для стеження.

❖ Системи виявлення та аналізу електронних слідів

Ці засоби використовуються для виявлення слідів, залишених у цифровому середовищі. Вони включають програми для аналізу метаданих,

відновлення видалених файлів, а також інструменти для слідкування за активністю в інтернеті (наприклад, IP-адреси, протоколи передачі даних).

❖ Радіоелектронна розвідка (PER)

Засоби для виявлення, прослуховування та аналізу електромагнітних сигналів, що використовуються для збору інформації про діяльність ворожих структур. Такі системи можуть визначати джерела сигналів і стежити за їх діяльністю без фізичного доступу до об'єкта.

❖ Системи для аналізу відкритих джерел (OSINT)

Спеціалізовані програмні засоби, які дозволяють здійснювати моніторинг публічних баз даних, інтернет-форумів, соціальних мереж і інших відкритих джерел інформації. Вони використовуються для збору даних, вивчення інформаційних тенденцій та ідентифікації потенційних загроз.

Застосування цих засобів дозволяє здійснювати ефективне збирання інформації, однак на практиці вони часто використовуються з порушенням етичних або правових норм, що може призвести до серйозних порушень безпеки та конфіденційності. Для захисту від таких засобів використовуються різноманітні технології криптографії, засоби фізичного та інформаційного захисту, а також системи виявлення і протидії кіберзагрозам.

Оптична розвідка

Оптична розвідка — це один із видів технічної розвідки, що використовує оптичні засоби для збору інформації про об'єкти та явища на поверхні землі або в атмосфері. Вона є важливою складовою військової розвідки і допомагає отримувати візуальні дані для оцінки ситуації, а також для управління військовими операціями. Сучасні системи оптичної розвідки здатні працювати в режимах реального часу і інтегруються з іншими технічними засобами, такими як радіолокаційні станції та системи управління вогнем. Вони є частиною більш широкої системи моніторингу і контролю, що забезпечує високу ефективність ведення бойових операцій. Перевагами оптичної розвідки є висока точність виявлення і ідентифікації цілей, швидкість реагування, що дозволяє оперативно змінювати стратегії та тактики на основі отриманої інформації, можливість моніторингу великих територій без необхідності фізичної присутності в зонах розвідки.

Оптична розвідка включає різні методи, такі як:

⇒ Візуально-оптичну

Це спостереження за об'єктами або територіями за допомогою звичайних оптичних засобів, таких як біноклі, телескопи або спеціалізовані прилади

для далекого зору. Цей метод часто застосовується в мирних умовах або для швидкого оцінювання ситуації на місці.

⇒ Фотографічну

Використовуються спеціальні фотокамери для отримання зображень місцевості, об'єктів або військової техніки. Фотографічні матеріали можуть бути отримані як з наземних позицій, так і з повітря (за допомогою літаків, дронів або супутників). Така розвідка дозволяє створювати детальні карти або моделі місцевості, а також фіксувати зміни, що відбуваються на території.

⇒ Інфрачервону

Інфрачервона техніка дозволяє спостерігати за тепловим випромінюванням об'єктів, що є невидимим для людського ока. Вона використовується для виявлення теплових слідів, таких як виділення тепла від техніки, технічного обладнання або навіть особового складу, а також для спостереження в умовах поганої видимості, наприклад, уночі або в умовах туману.

⇒ Телевізійну

Використовуються відеокамери, які передають в реальному часі зображення з об'єктів на відстані. Це дає можливість оперативно оцінити ситуацію, аналізувати поведінку противника, вивчати його позиції та переміщення.

⇒ Лазерну

Лазерні системи використовуються для точного вимірювання відстаней до об'єктів, а також для виявлення і фіксації рухомих цілей. Лазери можуть також застосовуватися для коригування вогню артилерії чи управління високоточними боєприпасами.

Радіоелектронна розвідка

Радіоелектронна розвідка (РЕР) — це вид технічної розвідки, який полягає в зборі, аналізі та використанні радіоелектронних сигналів, що випромінюються різними технічними засобами та пристроями, зокрема радарамі, комунікаційними системами, навігаційними сигналами та іншими електронними пристроями. Метою радіоелектронної розвідки є виявлення, ідентифікація та аналіз джерел радіоелектронних випромінювань, що дозволяє отримати цінну інформацію про активність противника, його технічні засоби, а також про ситуацію на місці. Сучасні системи радіоелектронної розвідки включають в себе не тільки традиційні наземні станції, але й аерофотознімальні системи, безпілотні літальні апарати, а також супутники, що дозволяють вести моніторинг електронної

активності противника з висоти. Радіoeлектронні засоби також інтегруються з іншими видами розвідки, що забезпечує більш точне та всебічне розуміння ситуації на полі бою. Радіoeлектронна розвідка, в залежності від характеру добутої інформації, підрозділяється на кілька основних видів:

- ***Радіорозвідка***

Цей метод включає виявлення, перехоплення та аналіз радіосигналів, які використовуються для комунікації, координування операцій, передачі даних і навігації. Зазвичай це включає дослідження таких сигналів, як радіо- і супутникові зв'язки, сигнали радіолокаційних станцій, сигналів від систем управління вогнем і інше. Радіорозвідка допомагає виявляти місця розташування ворожих радіолокацій, систем управління та зв'язку.

- ***Радіотехнічна розвідка***

Вона здійснюється за допомогою спеціалізованих засобів, що дозволяють визначити місце розташування ворожих технічних систем, таких як радіолокаційні станції, антени, станції радіoeлектронної боротьби (РЕБ). Завданням радіотехнічної розвідки є не тільки виявлення випромінювань, але й визначення характеристик обладнання противника, його частотного діапазону та потужності сигналу.

- ***Радіолокаційна розвідка***

Це підвищеної точності вид радіoeлектронної розвідки, який полягає у виявленні та аналізі радіолокаційних сигналів, що відображаються від об'єктів. Радарні системи, що використовуються в радіолокаційній розвідці, дозволяють точно визначити місце розташування і рух ворожих літаків, суден, ракет та інших об'єктів.

- ***Радіотеплова розвідка***

Включає виявлення та аналіз теплових сигналів, які випромінюються електронними пристроями. Зазвичай це використовують для виявлення джерел тепла, таких як двигуни техніки, системи охолодження технічних пристроїв або навіть теплові сліди від рухомих об'єктів.

- ***Комп'ютерна розвідка***

Зі збільшенням залежності від інформаційних і комунікаційних технологій комп'ютерна розвідка набуває все більшого значення. Вона включає в себе збори інформації з мереж, аналіз трафіку, перехоплення даних та іншого виду електронної активності для виявлення і прогнозування загроз в інформаційних системах.

Завдання радіoeлектронної розвідки:

- ✓ Виявлення та ідентифікація радіoeлектронних джерел.
- ✓ Аналіз структури та функціонування радіoeлектронних систем противника.

- ✓ Створення карт сигналів для побудови детальної ситуаційної обстановки.
- ✓ Спостереження за змінами у використанні електронних систем ворожими силами, що допомагає прогнозувати їхні наступні кроки.
- ✓ Визначення потужностей та ефективності ворожих засобів зв'язку і РЕБ.

Переваги радіоелектронної розвідки:

- ✓ Радіоелектронні засоби дозволяють проводити розвідку на великих відстанях і в складних умовах.
- ✓ Радіоелектронна розвідка дозволяє отримувати інформацію в реальному часі, що є критично важливим для коригування військових дій.
- ✓ Для противника важко виявити самі засоби радіоелектронної розвідки, що забезпечує збереження тактичної переваги.

Хімічна розвідка

Хімічна розвідка здійснюється з метою виявлення отруйних речовин та визначення заражених територій для попередження ураження особового складу хімічною зброєю. Вимоги до хімічної розвідки включають своєчасність, безперервність, достовірність та спадкоємність. Хімічна розвідка використовує спеціалізовані датчики та прилади для взяття проб повітря, води та ґрунту з метою виявлення токсичних хімічних сполук. Вона також включає моніторинг хімічних загроз у районах, де можуть проводитися військові операції або в зонах, де можливе використання хімічної зброї. У разі виявлення загрози хімічного зараження, система розвідки повинна оперативно інформувати командування для вжиття заходів з евакуації, захисту особового складу та застосування протихімічних засобів. Така розвідка є важливою складовою частиною системи забезпечення безпеки військових операцій у хімічно небезпечних зонах.

Радіаційна розвідка

Радіаційна розвідка призначена для виявлення та локалізації радіоактивних заражень місцевості та попередження про загрозу від ядерної зброї. Вимоги до радіаційної розвідки включають безперервність, достовірність, спадкоємність та своєчасність сповіщення. Радіаційна розвідка здійснюється з використанням спеціалізованих приладів для вимірювання рівнів радіоактивного випромінювання та визначення джерел забруднення. Вона проводиться як на наземних, так і на повітряних платформах, що

дозволяє оперативно виявляти заражені зони в різних умовах. У разі виявлення радіоактивного забруднення, радіаційна розвідка дає можливість оцінити рівень загрози та вжити необхідних заходів для захисту військ і цивільного населення. Це важлива складова частина системи захисту в умовах ядерних загроз та забезпечення безпеки під час військових конфліктів.

Магнітометрична розвідка

Магнітометрична розвідка дозволяє виявляти об'єкти з власним магнітним полем, наприклад, підводні човни, шляхом дослідження змін магнітного поля Землі. Це здійснюється за допомогою магнітометрів та аеромагнітометрів для вивчення магнітних аномалій та геологічної будови. Магнітометрична розвідка використовує точні вимірювання магнітних полів для виявлення об'єктів, що мають аномальні магнітні характеристики. Вона є важливим інструментом у пошукових операціях, зокрема для виявлення підводних об'єктів та військових споруд. Цей метод також застосовується в геофізичних дослідженнях для вивчення складу земної кори та пошуку корисних копалин. Результати магнітометричних зйомок можуть бути використані для складання карт магнітних аномалій, що допомагають у плануванні подальших досліджень та операцій.

Акустична розвідка

Акустична розвідка включає повітряно-акустичну, гідроакустичну та сейсмічну розвідку. Звукова розвідка, зокрема артилерійська звукова розвідка (АЗР), дозволяє визначати місце знаходження артилерійської зброї за звуком пострілу, що є важливим для оперативного реагування та коригування вогню. Акустична розвідка може використовувати різні методи для фіксації звукових хвиль, що виникають від вибухів, руху техніки або пострілів, що допомагає визначати точні координати джерел звуку. Гідроакустична розвідка використовується для виявлення підводних об'єктів, таких як підводні човни або торпеди, шляхом аналізу звукових хвиль у водному середовищі. Сейсмічна розвідка застосовується для виявлення землетрусів, вибухів або великогабаритних рухів, що допомагає виявити важливі зміни на полі бою або в стратегічно важливих регіонах. Всі ці методи акустичної розвідки дозволяють підвищити точність оцінки ситуації та сприяти ефективному плануванню бойових операцій.

7.3. Поняття промислового шпигунства

Промислове шпигунство — це протиправна діяльність, спрямована на здобуття конфіденційної або стратегічно важливої інформації щодо технологій, виробничих процесів, бізнес-планів, фінансових даних або інших комерційних секретів підприємства з метою використання цієї інформації для конкурентної переваги або збагачення.

Зазвичай промислове шпигунство включає в себе використання різних методів, таких як прослуховування, незаконне проникнення в інформаційні системи, крадіжка документів, підкуп співробітників або інші тактики для здобуття необхідної інформації. Це може завдати серйозної шкоди підприємствам, зокрема у вигляді фінансових втрат, втрати конкурентоспроможності та репутації. У багатьох країнах промислове шпигунство є кримінальним злочином і карається за законом.

Захист від промислового шпигунства включає в себе використання різноманітних засобів безпеки, таких як шифрування даних, політики доступу, фізична охорона, а також навчання персоналу щодо важливості збереження конфіденційності.

Комерційна розвідка

Комерційна розвідка — це процес збору, аналізу та використання інформації, яка має стратегічне значення для забезпечення конкурентоспроможності підприємства. Основна мета комерційної розвідки — це отримання інформації, яка дозволяє компанії досягти переваги над конкурентами, мінімізувати ризики і максимально ефективно використовувати доступні можливості на ринку. Вона є важливою складовою бізнес-стратегії, яка допомагає не лише у виявленні нових можливостей для розвитку, але й у прогнозуванні змін на ринку та вжитті необхідних заходів для збереження лідерства.

Основні завдання комерційної розвідки включають:

- ✓ Вивчення конкурентів і потенційних партнерів для виявлення їхніх сильних і слабких сторін;
- ✓ Збір та обробка даних про нові технології, інноваційні розробки та тренди у галузі;
- ✓ Аналіз відкритих джерел інформації, таких як публікації, фінансові звіти, новини;
- ✓ Виявлення потенційних ризиків для бізнесу, таких як зміни в законодавстві, зміни в ринкових умовах чи технологічні прориви;
- ✓ Оцінка можливих каналів витоку конфіденційної інформації і захист її від несанкціонованого доступу.

Активний метод комерційної розвідки часто ототожнюється з методами промислового шпигунства, оскільки цей підхід включає використання різноманітних агентурних та технічних методів збору інформації. Однак це не завжди порушує закон, адже основною метою є отримання конкурентної інформації для стратегічного управління. Сучасні компанії активно використовують відкриті джерела інформації, такі як публікації, звіти, соціальні мережі, новини і рекламу для збору даних.

Сукупно-пасивний метод комерційної розвідки передбачає використання вторинних джерел інформації (реклама, публікації, документи) в поєднанні з активними методами (наприклад, агентурними та стеженням за конкурентами).

Агентурний метод одержання інформації

Агентурний метод одержання інформації є одним із найстаріших та найбільш ефективних способів збору важливої інформації в сфері комерційної та промислової розвідки. Цей метод передбачає використання осіб, яких спеціально завербували для виконання розвідувальних завдань — агентів. Агентурна діяльність може бути спрямована на отримання конфіденційної, стратегічної або тактичної інформації, що стосується діяльності конкурентів, ринку, нових технологій або інших аспектів, які можуть вплинути на конкурентоспроможність підприємства.

Агентурний метод включає два основні підходи:

1. **Вербування агентів** — процес залучення осіб, які можуть надати необхідну інформацію, та формування мережі агентів, здатних виконувати розвідувальні завдання. Цей підхід може включати залучення як співробітників інших компаній, так і сторонніх осіб, які мають доступ до важливої інформації.

2. **Впровадження свого агента** — це більш складний та ризикований метод, який полягає у вербуванні людини для роботи в конкурентній організації або в іншому ключовому середовищі з метою здобуття цінних даних. Агент може бути впроваджений в компанію в якості працівника, під виглядом звичайного співробітника, з метою збору необхідної інформації.

Агентурні методи є найбільш ефективними в ситуаціях, коли необхідно отримати конфіденційну або недоступну через відкриті джерела інформацію, таку як внутрішні стратегії, фінансові плани, інноваційні розробки або бізнес-плани конкурентів. Вони також можуть бути використані для отримання даних про вразливі місця в діяльності конкурентів або для виявлення невідповідностей між заявленими та реальними цілями організації. Незважаючи на високу ефективність, агентурний метод часто викликає етичні та правові питання, оскільки він

може перетинати межу законності, зокрема коли йдеться про використання агентів, що працюють у конкурентних компаніях, або здійснення дій, які можуть порушувати права співробітників та організацій.

Методи конкурентної розвідки

Методи конкурентної розвідки можна поділити на два основні типи: законні (білі методи) та сірі методи, які не порушують закони, але можуть бути морально сумнівними. Всі методи спрямовані на збори та аналіз інформації про конкурентів, ринок, технологічні інновації, фінансові дані та інші аспекти бізнес-середовища, які можуть вплинути на стратегію компанії:

1. Законні методи конкурентної розвідки (білі методи)

Ці методи є етично прийнятними і не порушують законів. Вони включають:

- Аналіз публікацій та відкритих джерел - збір і аналіз інформації з офіційних публікацій, звітів, статей у ЗМІ, рецензій на продукцію, маркетингових матеріалів, що публікуються конкурентами або іншими організаціями. Це дозволяє отримати відомості про стратегії компанії, її нові продукти та інновації.
- Вивчення фінансових звітів - перегляд фінансової звітності компаній через публічні реєстри та органи регулювання фінансової діяльності дозволяє оцінити фінансовий стан конкурентів, виявити можливі слабкі місця або показники успішності.
- Аналіз відкритих даних - використання даних, які доступні через інтернет-ресурси, соціальні мережі, відкриті бази даних або платформи, що надають статистику та ринкову інформацію.
- Збір відгуків клієнтів та партнерів - моніторинг відгуків споживачів на продукцію конкурентів через форуми, огляди, соціальні мережі або спеціалізовані сайти для збору думок про якість та попит на товари та послуги.
- Аналіз патентів та наукових публікацій - дослідження патентів, наукових статей та інновацій, поданих конкурентами, дозволяє зрозуміти їхні технологічні досягнення і плани щодо інновацій.

2. Сірі методи конкурентної розвідки

Ці методи не порушують закони прямо, але можуть бути етичними сумнівними через можливі маніпуляції з інформацією або нечесні прийоми.

- Підкуп або заохочення співробітників конкурента - метод, при якому працівники конкурента отримують винагороду за надання конфіденційної інформації. Хоча він не є незаконним, це може суперечити етичним нормам.

- Вивідування через підставних осіб - ведення переговорів або взаємодія з конкурентами під виглядом потенційного партнера чи клієнта з метою отримання конфіденційної інформації.
- "Переманювання" кадрів - залучення ключових співробітників конкурента для того, щоб отримати від них інформацію про внутрішні процеси, технології або стратегії.
- Підставні переговори - проведення переговорів з метою вивідування інформації, яку конкурент не бажає розголошувати, під виглядом потенційної угоди чи співпраці.
- Соціальна інженерія - використання методів маніпуляції, психологічного тиску або обману з метою здобуття конфіденційної інформації, яку конкурент не мав наміру розголошувати.
- Використання взаємодії з правоохоронними органами або контролюючими інстанціями - залучення контактів у правоохоронних органах або державних установах для отримання відомостей про конкурентів, інколи без їхнього ведома.

3. Важливість конкурентної розвідки

Конкурентна розвідка є важливою частиною стратегії бізнесу, оскільки дозволяє:

- Прогнозувати рухи конкурентів та приймати стратегічні рішення.
- Виявляти ринкові можливості та нові тренди.
- Оцінювати ризики, пов'язані з конкурентами, та знаходити шляхи їхнього мінімізації.
- Розуміти слабкі та сильні сторони своїх конкурентів, що дозволяє розробляти більш ефективні стратегії.

Законні методи конкурентної розвідки важливі для підприємств, оскільки вони забезпечують отримання стратегічної інформації для прийняття рішень у рамках правових і етичних норм, тоді як використання сірих методів може призвести до юридичних наслідків та порушення бізнес-етики.

Контррозвідувальна діяльність

Контррозвідувальна діяльність — це спеціальний вид діяльності, спрямований на забезпечення національної безпеки, який здійснюється через застосування комплексних контррозвідувальних, пошукових, адміністративно-правових та режимних заходів. Основна мета такої діяльності — попередження, своєчасне виявлення та запобігання зовнішнім і внутрішнім загрозам національній безпеці України, у тому числі загрозам від іноземних розвідувальних, терористичних та інших

протиправних посягань. Це включає діяльність як спеціальних служб іноземних держав, так і окремих осіб, організацій або груп, які можуть загрожувати державним інтересам України.

Контррозвідувальна діяльність також має важливе значення в контексті кібербезпеки, оскільки сучасні загрози все частіше пов'язані з кібернетичними атаками, спрямованими на інфраструктуру та інформаційні системи держави. Вона передбачає не лише фізичне забезпечення безпеки, а й активну боротьбу з кіберзагрозами, такими як кібершпигунство, хакерські атаки, фішинг та інші види кіберзлочинності. Одним із основних завдань є захист інформаційних ресурсів держави від несанкціонованого доступу, змін або знищення через кіберсистеми, які можуть бути використані як інструмент для здійснення шкідливих дій. У межах контррозвідки кібербезпеки здійснюється моніторинг інформаційних систем, виявлення вразливих місць і профілактика можливих загроз на всіх етапах життєвого циклу інформаційної інфраструктури. Важливим є також виявлення та нейтралізація агентів впливу, які можуть використовувати кіберпростір для проведення інформаційно-психологічних операцій або дезінформаційних кампаній. Контррозвідка в сфері кібербезпеки активно співпрацює з іншими державними органами, міжнародними організаціями та приватними компаніями для забезпечення комплексного захисту від кіберзагроз. Вона також включає підвищення кваліфікації та навчання спеціалістів, що дозволяє оперативно реагувати на нові методи та інструменти кібератак.

Метою контррозвідувальної діяльності є не лише своєчасне виявлення і запобігання загрозам безпеці держави, а й нейтралізація діяльності іноземних спецслужб та інших осіб, що спричиняють небезпеку для національної безпеки. Крім того, важливим є усунення умов, що можуть сприяти виникненню таких загроз.

Основні завдання контррозвідувальної діяльності включають:

- Збір, аналітичну обробку та використання інформації про діяльність, яка може шкодити державній безпеці України, зокрема розвідувальну, терористичну та іншу незаконну діяльність з боку іноземних спецслужб, організацій або окремих осіб.
- Протидія діяльності іноземних спецслужб та терористичних угруповань, спрямованій проти безпеки України.
- Розробка та реалізація заходів щодо запобігання та нейтралізації загроз, що виникають для інтересів держави, прав громадян та суспільства в цілому.

Основні принципи контррозвідувальної діяльності базуються на кількох ключових аспектах, що забезпечують ефективність та законність

усієї діяльності. По-перше, діяльність має здійснюватися виключно в межах законодавства та Конституції України, що забезпечує її легітимність і відповідність національним правовим стандартам. Важливим є також дотримання прав і свобод людини та громадянина: усі заходи контррозвідки повинні бути спрямовані на захист цих прав, не порушуючи їх, що є основою демократичного контролю та дотримання прав людини. Крім того, контррозвідувальна діяльність повинна бути позапартійною, не залежати від політичних переконань чи інтересів, що гарантує нейтральність та об'єктивність виконуваних завдань.

Безперервність діяльності є ще одним важливим принципом, оскільки це дозволяє оперативно реагувати на зміни в ситуації та швидко адаптуватися до нових загроз. Водночас важливим є принцип конспірації: застосування комбінованих гласних та негласних методів і форм діяльності дозволяє ефективно виконувати завдання, не викриваючи при цьому джерела інформації та не наражаючи на небезпеку агентуру. Комплексний підхід до забезпечення безпеки, що включає правові, профілактичні та організаційні заходи, сприяє більш повному і ефективному виконанню контррозвідувальних завдань.

Адекватність заходів є необхідною умовою для ефективного захисту національної безпеки: усі вжиті заходи повинні відповідати реальним і потенційним загрозам. Взаємодія з іншими органами державної влади, органами місцевого самоврядування та іншими структурами, включаючи об'єднання громадян, юридичні та фізичні особи, дозволяє забезпечити скоординовану і комплексну роботу. Підконтрольність та підзвітність контррозвідувальної діяльності є невід'ємною частиною, адже ця діяльність повинна підлягати контролю та звітності перед органами державної влади в межах, передбачених законодавством України.

7.4. ПРИНЦИПИ ЗАХИСТУ ВІД ТЕХНІЧНОЇ РОЗВІДКИ

Принципи захисту від технічної розвідки в кібербезпеці включають ряд стратегічних підходів та інструментів, спрямованих на запобігання несанкціонованому доступу до чутливої інформації та її витоку через технологічні канали. Основним аспектом є моніторинг та аналіз мережевого трафіку, що дозволяє виявляти аномальні або підозрілі дії в реальному часі, такі як несанкціоновані спроби доступу або маніпуляції з даними. Одним із ключових принципів є багатошаровий захист (*defense in depth*), що передбачає використання різноманітних технологічних рішень для захисту на різних рівнях — від фізичної безпеки до програмного

забезпечення та інформаційних систем. Важливим елементом є зашифроване зберігання і передача даних, де застосовуються сучасні криптографічні протоколи для захисту інформації як в стані спокою (на дисках, серверах), так і при її передачі через канали зв'язку.

Захист від кіберрозвідки також включає управління доступом до критично важливої інформації, що передбачає використання політик на основі ролей, щоб обмежити доступ лише до тих користувачів, яким це необхідно для виконання їхніх обов'язків. З метою виявлення потенційних загроз активно застосовуються системи виявлення та запобігання вторгненням (IDS/IPS), що дозволяють виявляти аномалії в мережевій активності та автоматично блокувати спроби атаки. Не менш важливим є управління вразливостями — регулярне оновлення програмного забезпечення та застосування патчів для усунення виявлених вразливостей у системах і мережах, що можуть бути використані кіберзлочинцями для проведення технічної розвідки.

У разі виявлення спроб проникнення або витоку інформації, необхідно мати план реагування на інциденти, що дозволяє оперативно відреагувати на загрози, виявити джерела атаки та мінімізувати її наслідки для компанії. Важливим також є підвищення обізнаності користувачів, які повинні бути навчені розпізнавати фішингові повідомлення, підозрілі вкладення та інші типи атак, що можуть бути використані для збору конфіденційної інформації. І, звісно, постійний аудит та тестування безпеки — проведення регулярних перевірок безпеки інформаційних систем, тестів на проникнення та імітації атак для виявлення слабких місць у системі та оперативного усунення загроз.

Забезпечення кібербезпеки має бути комплексним та постійно вдосконалюваним процесом, оскільки технології та методи атак постійно розвиваються, і організації повинні бути готовими до нових викликів у сфері захисту від технічної розвідки.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 7

1. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.

2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

3. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
4. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(24), 185–195.
5. V. Astapenia, V. Sokolov, P. Skladannyi, Problematic Issues of the Accelerating Lens Deployment, in: IEEE 2nd Ukrainian Microwave Week (2022) 337–341.
6. Костюк Ю. В Впровадження інтелектуальних систем у процес оцінки ризиків інформаційної безпеки в безпроводових мережах // Сьомі Геретівські читання: наукові статті, тези доповідей та інші матеріали Всеукраїнської науково-практичної конференції (м. Тернопіль, Україна, 22 вересня 2023 року). Науковий, методичний, інформаційний збірник Тернопільського обласного комунального інституту післядипломної педагогічної освіти / Редколегія: О. М. Петровський, В. С. Мисик, І. М. Вітенко, О. І. Когут, Ю. Ч. Шайнюк, Т. В. Магера, Ф. І. Полянський, Н. Б. Стрийвус, Г. І. Герасимчук. Тернопіль: ТОКІППО, 2023. С. 162-168.
7. A. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.
8. Жданова, Ю., Шевченко, С., Спасітелева, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.
9. L. Kriuchkova, et al., Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 261-268.
10. Костюк Ю.В., Степашкіна К.В. Моделювання інтелектуальних систем управління захистом інформації в інформаційно-телекомунікаційних системах // Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2023) : матеріали тез доповідей XIII Міжнародної науково-практичної конференції (м. Чернігів, 25–26 травня 2023 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2023. – Т. 2. – с. 252-253.
11. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі

аналізу енергоспоживання та трафіку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 390–400.

12. Костюк Ю.В. Стратегії захисту крайових пристроїв з використанням нейронних мереж Коско // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 26 квітня 2024 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф.-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2024. – с. 17-18.

13. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

14. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148.

15. Костюк Ю.В., Кравченко Д.В. Методи захисту даних на підприємствах соціальної сфери. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1033-1047.

16. V. Zhebka, et al., Stability Method of Connectivity Automated Calculation for Heterogeneous Telecommunication Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188 (2021) 282–287.

17. Костюк Ю.В., Войткевич А.А. Дослідження технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1017-1032.

18. Z. B. Hu, V. Buriachok, V. Sokolov, Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm, Advances in Computer Science for Engineering and Education III, vol. 1247 (2020) 518–533.

19. Костюк Ю.В., Шапран В.О. Технології виявлення аномальних подій та сигнатур в реальному часі. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1069-1084.

РОЗДІЛ 8

ЕКОНОМІЧНА РОЗВІДКА І ПРИНЦИПИ ЗАХИСТУ ВІД НЕЇ



8.1. Технічні засоби економічної розвідки

8.2. Принципи захисту від економічної розвідки

"Економічна розвідка — це не лише про збір інформації, а й про прийняття рішень, які визначають стратегію та розвиток держави чи корпорації. Система захисту від неї повинна бути комплексною, гнучкою і адаптованою до сучасних загроз."

*Роберт Каплан, американський стратег,
автор книг по міжнародним відносинам*

Економічна розвідка є процесом збору, аналізу та використання економічної інформації з метою отримання конкурентних переваг на ринку. Вона включає в себе такі аспекти, як моніторинг діяльності конкурентів, аналіз ринкових тенденцій, отримання даних про технологічні новинки, а також інші елементи, що можуть вплинути на стратегічні рішення компанії чи держави. Принципи економічної розвідки включають легальність та етику, оскільки економічна розвідка повинна здійснюватися в межах закону і з дотриманням етичних норм. Використання незаконних методів, таких як шпигунство, є порушенням міжнародних норм і може привести до серйозних наслідків.

Для збору економічної інформації використовуються відкриті джерела, такі як публікації, аналітичні звіти, фінансові документи,

статистика та інші доступні дані. Крім того, важливою складовою є аналіз та прогнозування зібраної інформації, що дозволяє не лише оцінити поточну ситуацію, але й спрогнозувати можливі зміни в майбутньому. Основними принципами захисту від економічної розвідки є контроль доступу до інформації, що забезпечується обмеженням доступу до конфіденційних і стратегічно важливих даних на основі потреби в знаннях та рівня доступу співробітників. Також використовуються технічні засоби захисту, такі як криптографія, безпечні канали зв'язку та шифрування, для захисту від витоку інформації через технічні канали, наприклад, електронну пошту та мережі. Не менш важливим є забезпечення фізичної безпеки, зокрема контролю за фізичним доступом до важливих приміщень і документів, за допомогою відеоспостереження, контролю доступу та охорони.

Для ефективного захисту також проводиться навчання співробітників з питань збереження комерційної таємниці та основ захисту інформації. Регулярний моніторинг систем інформаційної безпеки і проведення аудитів дозволяє виявити потенційні уразливості і запобігти витокам даних.

Крім того, важливими є юридичні заходи, включаючи укладання договорів конфіденційності з партнерами та співробітниками, а також встановлення юридичної відповідальності за порушення умов захисту інформації. Захист від економічної розвідки вимагає комплексного підходу, який охоплює як технічні засоби, так і організаційні та правові механізми, щоб ефективно протистояти потенційним загрозам та мінімізувати ризики витоку важливої інформації.

8.1. ТЕХНІЧНІ ЗАСОБИ ЕКОНОМІЧНОЇ РОЗВІДКИ

Технічні засоби економічної розвідки включають в себе різноманітні пристрої, які дозволяють здійснювати збір, перехоплення та аналіз економічної інформації з різних джерел, а також надані технологічні можливості для моніторингу діяльності підприємств та конкурентів. Вони можуть включати наступні категорії:

▲ Радіоелектронні засоби

✓ Радіоелектронне спостереження - використання спеціальних радіопередавачів для перехоплення електромагнітних випромінювань, що створюються технічними пристроями, зокрема комп'ютерами, телекомунікаційним обладнанням та іншими апаратами. Це дозволяє отримувати доступ до інформації через радіоканали, навіть на відстані.

✓ Системи перехоплення супутникових сигналів використовуються для моніторингу комунікаційних каналів супутникових мереж, що можуть містити економічно важливу інформацію.

▲ Акустичні засоби

✓ Системи прослуховування включають мікрофони та інші звукові датчики, які можуть бути розташовані у приміщеннях для перехоплення розмов або звукових сигналів. Це можуть бути пристрої, що здатні вловлювати звукові коливання через стіни, вікна або інші конструкції.

✓ Вібраційні мікрофони - це прилади, що дозволяють виявляти акустичні коливання через тверді поверхні, наприклад, стіни, підлогу чи меблі.

▲ Оптичні засоби

✓ Лазерні мікрофони - системи, що використовують лазери для отримання інформації про звукові коливання в приміщенні. Лазерний промінь, відбиваючись від об'єкта (наприклад, скла), може зафіксувати звук, що потім перетворюється в електричний сигнал для подальшого аналізу.

✓ Мікрокамери та системи відеоспостереження використовуються для спостереження за діяльністю співробітників або конкуренції, зокрема через ховані камери, що дозволяють фіксувати візуальну інформацію без відома спостережуваних.

▲ Інтернет-технології та кіберзасоби

✓ Шкідливе програмне забезпечення (віруси, трояни, шпигунські програми) - встановлення цих програм на комп'ютерах конкурента або організації дозволяє отримувати доступ до їхніх даних без їх відома, перехоплювати електронну пошту, переписку, документи тощо.

✓ Фішинг - метод обману, який полягає у створенні підроблених вебсайтів або електронних листів, що імітують офіційні сайти або організації для збору конфіденційної інформації.

▲ Технічні засоби моніторингу інформації в мережах

✓ Інтерсептори та монітори трафіку - спеціальні пристрої або програмне забезпечення для перехоплення інформації, що передається через комп'ютерні мережі. Вони можуть відслідковувати пакети даних, що передаються по мережах, зокрема, в Інтернеті.

✓ Засоби аналізу трафіку використовуються для збору даних про активність користувачів в інформаційних системах або на вебсайтах, щоб зібрати важливу інформацію про бізнес-процеси, стратегії та інші аспекти діяльності організацій.

Технічні засоби економічної розвідки здатні використовувати інноваційні технології для збору, обробки і передачі важливої інформації, що дозволяє конкурентам або іншій стороні отримати цінні відомості без дозволу організації або підприємства. Це робить захист інформаційних ресурсів і комерційних таємниць важливою частиною стратегії безпеки на всіх рівнях.

Економічна розвідка – це широке поняття, що об'єднує в собі промислову та комерційну розвідку. Це діяльність, спрямована на збирання, аналіз і використання інформації про економічну діяльність конкурентів, ринкові умови, нові технології та інші аспекти, що мають стратегічне значення для бізнесу чи держави. Це важливий інструмент у сучасному конкурентному середовищі, який допомагає організаціям приймати більш обґрунтовані рішення та адаптуватися до змін на ринку.

Основні цілі економічної розвідки полягають у зборі інформації, аналізі цієї інформації для визначення можливих загроз і можливостей для організації, прогнозуванні тенденцій і прийнятті рішень. Методи економічної розвідки включають відкриту розвідку, де використовуються загальнодоступні джерела, такі як звіти, публікації в ЗМІ, соціальні мережі, а також технічну розвідку, яка передбачає використання спеціалізованих пристроїв для збору інформації через електронне перехоплення або прослуховування.

Контррозвідка в свою чергу дозволяє виявляти спроби незаконного збору інформації конкурентами. Серед інструментів економічної розвідки виділяються інтернет-ресурси, аналітичні платформи для аналізу фінансових та економічних показників, а також інфраструктура збору даних, що включає агентства та компанії, які спеціалізуються на цих послугах. При цьому економічна розвідка повинна здійснюватися в межах законодавства та етичних стандартів, зокрема, забезпеченням конфіденційності даних та повагою до прав інтелектуальної власності.

Принципи захисту від економічної розвідки включають захист комерційних таємниць, фізичну безпеку приміщень, де зберігається важлива інформація, інформаційну безпеку через шифрування і контроль доступу до мережі, а також контррозвідку і моніторинг для запобігання витоку інформації через канали зв'язку. Економічна розвідка є важливим інструментом для підприємств, які прагнуть підтримувати конкурентоспроможність, але вона повинна здійснюватися етично та в рамках закону, щоб уникнути правових наслідків.

Промислова розвідка – це несанкціоноване отримання науково-технічної та технологічної інформації.

Комерційна розвідка – це несанкціоноване отримання інформації, що представляє собою комерційну таємницю компанії.

Промислова розвідка — це вид економічної розвідки, що займається збором, аналізом і використанням інформації про технології, процеси, продукцію, патенти, новітні досягнення в галузі науково-дослідницької та виробничої діяльності. Метою промислової розвідки є отримання конкурентних переваг, прогнозування змін на ринку та виявлення нових технологічних можливостей для удосконалення виробничих процесів. Це дозволяє компаніям та державам адаптуватися до змін у промислових тенденціях, скорочувати витрати на дослідження та розробки, а також впроваджувати інновації, не порушуючи патентних прав та інших обмежень. Промислова розвідка часто включає не тільки аналіз публічних джерел, але й вивчення діяльності конкурентів, їхніх патентів, результатів наукових досліджень і нових розробок. Важливою складовою є використання відкритих і закритих баз даних, участь у виставках, конференціях, форумах і наукових публікаціях для збору релевантної інформації.

Комерційна розвідка — це більш широке поняття, яке включає в себе збирання та аналіз інформації, яка стосується комерційної діяльності, ринку, конкуренції, споживачів і фінансового стану підприємств. Основною метою комерційної розвідки є виявлення тенденцій на ринку, прогнозування змін у поведінці споживачів, оцінка конкурентних позицій, а також допомога у стратегічному плануванні та прийнятті рішень. Це включає в себе як легальні методи збору інформації (аналіз ринкових звітів, фінансових звітів, опитування споживачів), так і більш агресивні практики (наприклад, проникнення в інформаційні системи конкурентів через кібер-атак або фальшиві компанії).

Оскільки комерційна та промислова розвідка передбачають збір інформації, важливо дотримуватися етичних норм і законів, оскільки використання несанкціонованих методів розвідки, таких як шпигунство чи підкуп, може призвести до серйозних юридичних наслідків.

Розподіл технічних засобів економічної розвідки

Всі технічні засоби економічної розвідки поділяються на групи:

- ➔ спеціальна звукозаписуюча апаратура;
- ➔ апаратура для знімання інформації з вікон;

- ➔ спеціальні системи спостереження і передачі відеозображень;
- ➔ прилади спостереження в денний час і прилади нічного бачення;
- ➔ спеціальні засоби радіоперехоплення і прийому побічного електромагнітного випромінювання і наведення.

Розподіл технічних засобів економічної розвідки за способом застосування

За способом застосування технічні засоби економічної розвідки можна класифікувати наступним чином:

▲ засоби, що встановлюються заходовими методами (тобто вимагають таємного фізичного проникнення на об'єкт):

- *радіозакладки;*
- *закладки з передачею інформації в інфрачервоному діапазоні;*
- *закладки з передачею інформації по мережі 220 В або по телефонній лінії;*
- *диктофони;*
- *провідні мікрофони.*

▲ засоби, що встановлюються незаходовими методами:

- *апаратура, яка використовує мікрофонний ефект;*
- *високочастотне навіязування;*
- *стетоскопи;*
- *лазерні стетоскопи;*
- *апаратура відеоспостереження та фотозйомки;*
- *спрямовані мікрофони.*

Закладні пристрої, що використовують для передачі інформації лінії електроживлення мережі напругою 220 В, відомі як мережеві закладки. Вони часто вбудовуються в електричні розетки, подовжувачі, побутову техніку або безпосередньо в силову лінію. Такі пристрої дозволяють здійснювати передачу інформації через електричну мережу, що є однією з найбільш незапомітних форм витоку інформації. Призначення мережевих закладок полягає в тому, щоб передавати інформацію без необхідності використання окремих кабелів чи бездротових каналів зв'язку, що значно ускладнює виявлення та перехоплення передачі.

Сучасні методи для перехоплення інформації, переданої через мережеві закладки, використовують технології, які здатні експлуатувати електричні та магнітні поля для передачі даних в межах будівель.

Спеціалізовані приймачі можуть підключатися до тієї ж силової мережі, що і джерело інформації, забезпечуючи здатність отримувати сигнал навіть на відстані до 300-500 м. Це можливо завдяки використанню низьковольтних систем живлення, зокрема тих, що належать до одного трансформатора або енергетичної шини.

Такі технології відрізняються від звичайних методів передачі даних тим, що вони використовують існуючу інфраструктуру для бездротового обміну інформацією через електричні кола, що робить їх менш помітними для традиційних систем безпеки, які орієнтовані на захист від радіочастотних або мережевих атак. Відсутність необхідності в окремих кабелях для передачі даних означає, що такі канали складні для виявлення, оскільки немає фізичних слідів, які можна б було відстежити. Це стає серйозною загрозою для інформаційної безпеки, оскільки дозволяє зловмисникам перехоплювати чутливу інформацію без потреби у фізичному доступі до мережі або підключених пристроїв.

Для захисту від подібних атак важливо впроваджувати спеціалізовані методи захисту, включаючи екранування електричних ліній, використання фільтрів та генераторів перешкод для зниження можливості передачі інформації через електричні кола. Крім того, важливими є заходи фізичного захисту, такі як ізоляція ключових комунікаційних ліній та обмеження доступу до критичної енергетичної інфраструктури.

Крім мережі електроживлення, для передачі інформації активно використовуються телефонні лінії зв'язку. Це також є популярним каналом для комунікації, і передача інформації через телефонні лінії може здійснюватися як на високих, так і на низьких частотах. При передачі інформації на високих частотах дальність передачі може досягати кількох кілометрів, що значно перевищує діапазон мережевих закладок. Враховуючи цю можливість, телефонні лінії є зручними для передачі великих обсягів інформації на значні відстані, що робить їх потенційно небезпечними для інформаційної безпеки.

Поряд з основними технічними засобами, безпосередньо пов'язаними з обробкою і передачею інформації, необхідно враховувати і допоміжні технічні засоби і системи, такі як *технічні засоби відкритої телефонного, факсимільного, гучномовного зв'язку, системи охоронної та пожежної сигналізації, електрифікації, радіофікації, часофікації, електропобутові прилади* тощо.

Канали витоку інформації, що виходять за межі контрольованої зони, становлять великий інтерес для кіберзлочинців та зловмисників, оскільки вони можуть використовувати зовнішні засоби, які не перебувають під безпосереднім контролем безпеки організації. Сюди входять сторонні

дроти, кабелі, а також металеві конструкції, що проходять через приміщення з встановленими технічними засобами. Важливою проблемою є те, що ці канали часто не мають жорсткого контролю з боку охорони або систем моніторингу, що дозволяє зловмисникам організувати витік інформації через такі лінії зв'язку або провідні інфраструктури. Крім того, ці канали можуть бути використані для установки шкідливих пристроїв або датчиків, які не можна виявити без спеціального обладнання. Наприклад, зловмисники можуть впроваджувати прослуховувальні пристрої в кабельні канали або металеві конструкції, що дозволяє отримувати конфіденційну інформацію без необхідності фізичного доступу до приміщення. В умовах недостатнього контролю ці канали можуть стати незаміченими і використовуватися протягом тривалого часу, що значно підвищує ризик витоку даних. Така уразливість у системах безпеки може бути критичною для організацій, що мають важливі дані або стратегічні ресурси. Тому важливо ретельно контролювати всі канали зв'язку, що виходять за межі контрольованої зони, і застосовувати додаткові заходи захисту для запобігання несанкціонованому доступу. Це включає як фізичний контроль над кабельними маршрутами, так і технічні рішення для виявлення та блокування потенційних витоків через сторонні канали.

Сторонні дроти та кабелі, що не належать до основної мережі підприємства, можуть служити каналами передачі даних, через які відбувається несанкціонований вихід або передача інформації. Наприклад, електричні або телефонні дроти, що прокладені в межах організації або в безпосередній близькості від важливих технічних пристроїв, можуть бути використані для захоплення електронних сигналів або перехоплення даних через витік радіочастотних хвиль. Крім того, металеві труби систем опалення, водопостачання та інші конструкції з металу можуть виступати в ролі антени, яка передає сигнал або служить провідником для перехоплення інформації, що передається через мережу електроживлення або інші лінії.

Захист від витоку інформації через подібні канали вимагає комплексного підходу, який включає в себе фізичну ізоляцію важливих елементів інфраструктури, екранування дротів і кабелів, а також впровадження політик безпеки, що контролюють використання сторонніх засобів передачі даних у межах організації. Важливою складовою також є моніторинг електричних і телефонних ліній, щоб виявити будь-які аномалії або підозрілі дії в мережі, які можуть свідчити про спроби несанкціонованого доступу або витоку інформації. Узагальнену схему

можливих каналів витоку та несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі:



Рис. 8.1. Узагальнена схема можливих каналів витоку та несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі

Джерело: [3-7]

1 – витік за рахунок структурного звуку в стінах і перекриттях;

2 – зняття інформації зі стрічки принтера;

3 – зняття інформації з використанням відеозакладок;

4 – програмно-апаратні закладки в ЕОМ;

5 – радіозакладки у стінах і меблях;

6 – зняття інформації із системи вентиляції;

7 – лазерне зняття акустичної інформації з вікон;

8 – виробничі й технологічні відходи;

9 – комп'ютерні віруси, логічні бомби і т. п.;

10 – зняття інформації шляхом наведень і «нав'язування»;

11 – дистанційне зняття відеоінформації (оптика);

- 12 – зняття акустичної інформації з використанням диктофонів;*
- 13 – крадіжка носіїв інформації;*
- 14 – високочастотний канал витоку в побутовій техніці;*
- 15 – зняття інформації направленим мікрофоном;*
- 16 – внутрішні канали витоку інформації (через обслуговуючий персонал);*
- 17 – несанкціоноване копіювання;*
- 18 – витік за рахунок побічного випромінювання терміналу;*
- 19 – зняття інформації за рахунок використання «телефонного вуха»;*
- 20 – зняття з клавіатури і принтера за акустичним каналом;*
- 21 – зняття з монітора з електромагнітного каналу;*
- 22 – візуальне зняття з монітора і принтера;*
- 23 – наведення на лінії комунікацій і сторонні провідники;*
- 24 – витік через лінії зв'язку;*
- 25 – витік ланцюгами заземлення;*
- 26 – витік мережею електропроводки;*
- 27 – витік трансляційною мережею та гучномовним зв'язком;*
- 28 – витік охоронно-пожежною сигналізацією;*
- 29 – витік мережею електроживлення;*
- 30 – витік мережею опалювання, газо- і водопостачання.*

Окремо слід виділити поширені засоби шпигунства, що дозволяють перехоплювати інформацію з клавіатури і монітора, це так звані **апаратні кейлоггери і відеологгери**.

Апаратні кейлоггери

Апаратні кейлоггери — це пристрої, які фізично підключаються до комп'ютера або інших пристроїв для запису всіх натискань клавіш на клавіатурі. Вони можуть бути встановлені між клавіатурою та комп'ютером або інтегровані в пристрої, що мають вигляд звичайних периферійних пристроїв, таких як USB-концентратори, клавіатури або миші.

Апаратні кейлоггери здатні захоплювати всі введення, що здійснюються через клавіатуру, і передавати ці дані до злоумисника через різні канали, такі як USB або навіть через бездротові технології. Вони є ефективним інструментом для збору конфіденційної інформації, оскільки вони не потребують програмного забезпечення для роботи і не можуть бути виявлені традиційними антивірусними програмами або іншими засобами виявлення злоумисного ПЗ. Апаратні кейлоггери здатні записувати всі натискання клавіш, включаючи паролі, особисту інформацію, переписку та інші чутливі дані. Вони часто маскуються під звичайні пристрої, що робить їх важко виявити навіть під час

фізичного огляду комп'ютера або робочого місця. Інформація, зібрана такими пристроями, може передаватися через фізичні порти, наприклад, USB, або бездротові канали. Для захисту від таких загроз важливо використовувати надійні методи шифрування даних, регулярно перевіряти фізичну безпеку робочих місць і застосовувати антиспайваре-програмне забезпечення для виявлення аномальної активності на апаратному рівні.

Апаратний кейлоггер – це електронний пристрій, який фіксує у власну пам'ять всі натиски клавіш на клавіатурі і не вимагає установки будь-якого додаткового ПЗ, втручання в ОС, драйвери і т. п.

Запис інформації здійснюється на *flash-пам'ять* об'ємом від 64 Кб до 2 ГГб. Передбачена можливість установки модуля, що дозволяє фіксувати час і дату набраного на клавіатурі тексту з точністю до секунди.

Апаратні кейлоггери є одними з найскладніших для виявлення пристроїв, оскільки вони не взаємодіють безпосередньо з операційною системою комп'ютера і не потребують встановлення спеціального програмного забезпечення. Вони можуть бути підключені до клавіатури або материнської плати і здатні записувати всі натискання клавіш, передаючи зібрані дані на сторонні пристрої або сервери зловмисників. Оскільки ці пристрої не завантажуються через операційну систему, вони не можуть бути виявлені за допомогою традиційних методів захисту, таких як антивірусні чи антишпигунські програми.

Апаратні кейлоггери можуть бути дуже маленькими, що робить їх важкими для фізичного виявлення. Вони можуть бути інтегровані безпосередньо в кабель або працювати за принципом "підключення послідовного порту", що дозволяє їм бути майже невидимими для користувача. Вони також можуть не споживати значної кількості енергії, що дозволяє їм працювати протягом тривалого часу без помітних змін в системі. Такі пристрої можуть передавати зібрані дані через бездротові канали або за допомогою зовнішніх носіїв, що ускладнює їх виявлення під час регулярних перевірок. Їхня здатність працювати в тих умовах, де інші методи збору даних можуть бути помічені, робить апаратні кейлоггери особливо небезпечними для забезпечення інформаційної безпеки.

Захист від апаратних кейлоггерів включає фізичний контроль за робочими станціями та комп'ютерними мережами, регулярний огляд обладнання на наявність підозрілих пристроїв, а також обмеження доступу до комп'ютерів лише для авторизованих осіб. Також важливо регулярно

змінювати паролі та використовувати методи двофакторної аутентифікації для зменшення ризиків при зборі чутливої інформації.



Рис. 8.2. Апаратні кейлоггери

Джерело: URL: <https://www.keelog.com/ru/usb-keylogger/>

Однак у більшості **апаратних кейлоггерів** є недолік – періодично потрібно фізичний доступ до комп'ютера для «перекидання» інформації з пам'яті кейлоггера. Цього недоліку немає у так званих **«радіокейлоггерів» (Wireless Keylogger)**.

Радіокейлоггер складається з двох основних модулів: **передавача** і **приймача**. Всі натискання клавіш клавіатури передаються в реальному часі по радіоканалу. Приймач підключений до іншого комп'ютера, на якому за допомогою спеціального ПЗ відображаються прийняті дані. Максимальний радіус дії складає близько 50 метрів. Радіокейлоггер може бути приховано вбудований у клавіатуру або підключений між комп'ютером і пристроєм введення для збирання даних без відома користувача. Такі пристрої можуть бути використані для збору конфіденційної інформації, такої як паролі та інші чутливі дані, що вводяться на клавіатурі.

Відеологгери

Відеологгер – це апаратна закладка мініатюрних розмірів, встановлена в звичайний відеокабель, що з'єднує системний блок з монітором.

Відеологгери — це спеціалізовані пристрої або програми, які здійснюють запис зображення або відео, що передається через камери спостереження або веб-камери. Вони можуть бути апаратними або програмними, і їх основна мета

— це перехоплення відео- та зображувальної інформації без відома користувача.

Апаратні відеологтери можуть бути інтегровані в пристрої, як-от веб-камери або навіть інші елементи техніки, що використовуються для відеоспостереження, і здатні зберігати або передавати записане зображення до зловмисника. Вони можуть бути підключені безпосередньо до комп'ютерної системи або мережі, передаючи дані через фізичні канали (наприклад, через USB або інші порти), або через бездротові з'єднання, як Wi-Fi або Bluetooth.

Програмні відеологтери зазвичай реалізуються як зловмисне ПЗ, яке активує камери комп'ютера або мобільних пристроїв без відома користувача. Такі програми можуть бути прихованими та працювати у фоновому режимі, автоматично записуючи все, що відбувається перед камерою.

Зловмисники можуть використовувати відеологтери для стеження за особами, збору конфіденційної інформації, або для зловживання приватністю користувачів. Для захисту від таких загроз важливо вживати заходів фізичного захисту пристроїв, регулярно перевіряти наявність несанкціонованих програм, а також використовувати інструменти для блокування доступу до камери, коли вона не використовується.

Цей пристрій підключається до *DVI*, *VGA* або *HDMI* порту комп'ютера і непомітно робить знімки екрану з заданою періодичністю, зберігаючи їх на вбудовану *flash-пам'ять* в форматі *JPEG*. Знімки містять інформацію про дату і час зроблених скріншотів.

З розвідкою за допомогою ПЕМВ часто використовується термін *TEMPEST*. Ця аббревіатура з'явилася в кінці 60-х років як назва секретної програми Міністерства Оборони США з розробки методів запобігання витоку інформації через різного роду демаскуючі і побічні випромінювання електронного обладнання. У цей час термін *TEMPEST* не є аббревіатурою і застосовується як назва технології, що мінімізує ризик витоку секретної інформації шляхом перехоплення і аналізу різними технічними засобами побічних електромагнітних випромінювань. У поняття *TEMPEST* входять також стандарти на обладнання, засоби вимірювання і контролю. Досить часто термін *TEMPEST* використовується і в контексті опису засобів нападу (*TEMPEST-атака*, *TEMPEST-підслуховуючі пристрої*).

TEMPEST-атака (від англ. *Transient Electromagnetic Pulse Emanation Standard*) — це тип атаки, що використовує електромагнітне випромінювання, яке виникає внаслідок роботи електронних пристроїв, зокрема комп'ютерів, телефонів, моніторів та інших апаратних засобів, що обробляють і передають інформацію. Це випромінювання може бути використане для перехоплення конфіденційної інформації без фізичного доступу до пристрою. Під час роботи електронних пристроїв виникає

певне випромінювання (передача даних, обробка сигналів, робота елементів). Це випромінювання може поширюватися через навколишнє середовище і бути виявленим спеціальними пристроями. За допомогою спеціального обладнання, яке здатне детектувати електромагнітні хвилі в певних діапазонах, зломисник може відновити інформацію, що передавалася, або навіть побачити зображення на екрані комп'ютера в реальному часі. Для цього використовуються спеціалізовані технічні засоби, які дозволяють вловлювати слабе електромагнітне випромінювання, що виходить з пристроїв. У деяких випадках це випромінювання може бути настільки сильним, що зломисник може перехоплювати навіть дані, передані на великі відстані.



Рис. 8.3. TEMPEST-атака (можна віддалено проглядати екран вашого комп'ютера і мобільного телефона за допомогою радіохвиль)

Джерело: URL:

<https://www.netacad.com/courses/cybersecurity/cyberops-associate>



Для захисту від TEMPEST-атак використовуються кілька методів. По-перше, це екранування обладнання, що використовується для обробки конфіденційної інформації, спеціальними матеріалами, які блокують електромагнітні хвилі. Також забезпечується фізичний захист, наприклад, створення спеціалізованих захищених приміщень з металевими стінами або кабінетів, що захищені від випромінювання. Встановлення пристроїв для моніторингу рівня електромагнітного випромінювання в робочих зонах

дозволяє вчасно виявляти потенційні витоки. Окрім того, використовуються технічні засоби, які перешкоджають перехопленню даних або спеціальні засоби захисту, що блокують або знижують рівень випромінювання. TEMPEST-атаки є важливою темою в сфері захисту інформаційних систем і використовуються зловмисниками для виведення конфіденційної інформації з надійно захищених комп'ютерних систем, підкреслюючи важливість фізичного захисту технічних засобів і необхідність використовувати більш складні методи захисту в умовах сучасної інформаційної безпеки.

8.2. ПРИНЦИПИ ЗАХИСТУ ВІД ЕКОНОМІЧНОЇ РОЗВІДКИ

Основна мета технічного захисту інформації полягає у реалізації максимальної неможливості отримання порушником інформації по технічних каналах витоку інформації.

Для досягнення цієї мети, по-перше, виявляють існуючі і потенційні технічні канали витоку інформації. Після того, як даний канал виявлено, проводиться оцінка його параметрів з метою визначити, наскільки ймовірна витік інформації з нього, наскільки порушник може дійсно перехопити інформацію і отримати з неї смислову складову.

Після того як такі параметри оцінені, слід здійснити по можливості руйнування або нейтралізацію виявлених каналів витоку інформації. Під руйнуванням мається на увазі порушення трикомпонентної структури у вигляді джерела інформації, середовища передачі інформації та спеціального засобу несанкціонованого знімання інформації.

Принципи захисту від економічної розвідки включають в себе низку заходів, спрямованих на збереження конфіденційності та безпеки стратегічної інформації підприємства, а також на запобігання витокам бізнес-даних і захист конкурентних переваг. Основним принципом є забезпечення конфіденційності інформації, що передбачає чітке визначення категорій інформації, яка є критично важливою для підприємства, таких як фінансові дані, комерційні секрети, технології, а також запровадження обмежень доступу до цієї інформації тільки для тих осіб, які мають необхідність у її знанні. Це реалізується через впровадження надійних механізмів контролю доступу, систем аутентифікації та авторизації.

Іншим важливим аспектом є технічний захист інформації, який включає використання криптографічних засобів для захисту даних під час їх передачі або зберігання в інформаційних системах підприємства. Крім

того, важливо застосовувати засоби, що забезпечують безпеку комп'ютерних мереж, такі як фаєрволи, антивірусні програми та багаторівнева аутентифікація. Важливу роль відіграє також захист від електромагнітних витоків, зокрема за допомогою технологій, що запобігають атакам типу TEMPEST, а також засобів моніторингу електромагнітних випромінювань, які можуть бути перехоплені спеціальними пристроями.

Фізична безпека є ще одним важливим елементом захисту від економічної розвідки. Для цього створюються захищені приміщення, оснащені екранованими стінами, що унеможливають перехоплення електромагнітних сигналів. У таких приміщеннях використовуються замки, системи відеоспостереження і контролю доступу, щоб обмежити можливість проникнення сторонніх осіб до інформаційних систем та важливих документів підприємства.

Контроль за персоналом є також ключовим елементом системи захисту від витоків інформації. Важливо проводити регулярні перевірки співробітників, зокрема тих, хто працює з конфіденційними даними, а також обов'язково вимагати підписання угод про конфіденційність. Крім того, важливими є освітні програми для персоналу, які допомагають підвищити обізнаність працівників щодо можливих загроз і навчити їх методам безпечної роботи з конфіденційною інформацією.

Моніторинг і оперативне реагування на інциденти витоку інформації є важливим елементом. Системи моніторингу мережі дають змогу вчасно виявити підозрілі дії або спроби несанкціонованого доступу, що дозволяє оперативно реагувати і усувати наслідки. Розробка детальних планів реагування на інциденти також є важливим заходом для попередження повторних витоків та зниження їх негативних наслідків.

Нарешті, юридичний захист включає використання правових механізмів для захисту інтелектуальної власності, укладення договорів про конфіденційність з партнерами і постачальниками, а також забезпечення захисту комерційних таємниць через реєстрацію патентів, торгових марок та авторських прав.

Забезпечення захисту від економічної розвідки є комплексним процесом, що вимагає інтеграції технічних, фізичних, організаційних і юридичних заходів, спрямованих на максимальне зменшення ризику витоку важливої інформації і збереження конкурентних переваг підприємства. Це включає в себе розробку та впровадження політик безпеки, контроль доступу до чутливих даних, а також моніторинг та аудит всіх операцій з інформацією. Важливим аспектом є навчання співробітників основам безпеки і регулярне тестування захисних

механізмів на наявність уразливостей. Крім того, застосування сучасних технологій шифрування та антивірусного захисту дозволяє суттєво знизити ймовірність несанкціонованого доступу до критичних даних.

Для нейтралізації або руйнування технічних каналів витоку інформації застосовують один з трьох наступних принципових підходів до здійснення технічного захисту інформації:

- ізолювання джерела інформації від середовища поширення інформації – **екранування**;
- ослаблення сигналу з інформацією в середовищі розповсюдження – **розсіювання**;
- виключення або утруднення для порушника виділення корисної інформації з перехопленого сигналу – **зашумлення**.

Екранування

Екранування є ефективним методом захисту від витоків інформації, спрямованим на блокування небажаного проникнення сигналів з одного середовища в інше. Це включає в себе створення фізичних або електронних бар'єрів, що перешкоджають передачі інформації через канали, які можуть бути використані для її перехоплення.

Простим прикладом екранування є використання спеціально обладнаних приміщень, в яких ведуться важливі переговори. Наприклад, для забезпечення конфіденційності бесід між співробітниками або з клієнтами використовуються кімнати з шумоізоляцією або спеціальні двері, що не дозволяють проникати звуковим коливанням у відкритий простір. У таких приміщеннях навіть присутність сторонніх осіб біля дверей не дає змоги почути, про що йдеться всередині. Такі заходи є частиною стратегії забезпечення конфіденційності у банках, організаціях і бізнес-центрах, де важливі фінансові операції та комунікації потребують максимального захисту.

Екранування також може здійснюватися за допомогою спеціальних матеріалів, що поглинають або відбивають електромагнітні хвилі, запобігаючи їх витоку. Це часто використовується для захисту від перехоплення електронних сигналів у системах зв'язку, комп'ютерних мережах і на підприємствах, де конфіденційні дані можуть бути вразливими до зовнішніх загроз. Таким чином, екранування забезпечує

високий рівень безпеки та конфіденційності для захисту бізнесу і важливої інформації.

Розсіювання

Розсіювання є важливим методом обмеження можливості перехоплення інформації через технічні канали. Цей підхід полягає в ослабленні сигналу за допомогою різних технічних заходів, щоб ускладнити його перехоплення зловмисниками. Основна ідея розсіювання полягає в тому, щоб зменшити інтенсивність сигналу, що поширюється, до такої міри, щоб на межі контрольованої території сигнал виявлявся настільки ослабленим, що його перехоплення стає неможливим або надзвичайно складним.

Один із способів досягти цього — збільшення відстані між джерелом сигналу і приймачем, що сприяє його природному згасненню. Чим більше відстань, тим менше енергії залишається у сигналу, що робить його перехоплення все менш ефективним. Крім того, на шляху поширення сигналу можуть бути створені різноманітні перешкоди або складні середовища, які додатково поглинають або відбивають сигнал, посилюючи ефект ослаблення.

Розсіювання застосовується для зменшення ймовірності несанкціонованого доступу до інформації, зокрема в ситуаціях, коли є необхідність захистити дані, що передаються на великі відстані, наприклад, у бездротових або оптичних системах зв'язку. Цей метод доповнює інші заходи захисту, такі як шифрування або екранування, створюючи додатковий рівень безпеки для запобігання витоку інформації.

Зашумлення

Третій підхід до нейтралізації технічних каналів витоку інформації полягає в так званому зашумленні. *Зашумлення* — це створення додаткового впливу на сигнал, що перешкоджає отримання інформації порушником, тобто це метод захисту інформації, який полягає в створенні додаткових непотрібних сигналів (шумів) в технічних каналах, що перешкоджають або ускладнюють перехоплення корисного сигналу. Ідея цього методу полягає в тому, щоб за допомогою шуму замаскувати передавані дані, роблячи їх недоступними для несанкціонованих осіб або пристроїв, що можуть спробувати перехопити сигнал.

Шум, який додається до інформаційного каналу, може бути різним за характеристиками (наприклад, білим шумом, електричними або акустичними коливаннями), і його основна мета — створити умови, за

яких для перехоплення корисної інформації потрібно буде мати значно більшу кількість ресурсів і часу, що значно знижує ефективність атак. Зашумлення часто застосовується в системах, де передається чутлива або важлива інформація, а будь-яка спроба її перехоплення є небажаною.

Наприклад, у бездротових комунікаційних системах може використовуватися додавання шуму до сигналу для того, щоб зловмисник, який намагається отримати інформацію, не міг точно відокремити корисний сигнал від шуму. Таке зашумлення значно ускладнює процес перехоплення даних, навіть якщо зловмисник використовує сучасні технічні засоби для прослуховування.

Метод зашумлення є ефективним доповненням до інших технік безпеки, таких як шифрування, екранування та розсіювання, створюючи багатоступеневий захист для переданої інформації.

У разі застосування спеціальних пристроїв, створюють **маскуючі перешкоди**, або так званий шум, порушник хоча і в змозі прийняти сигнал за допомогою спеціального пристрою, але не в змозі виділити з нього смислову інформацію, оскільки замість сигналу, з якого така інформація може бути виділена, він чує велику кількість різних сигналів, шум, суміш перешкод, яка виключає виділення з всього прийнятого порушником змістовну частину, а також інформацію, яка є для нього бажаною.

Для блокування каналів витоку інформації з використанням активних засобів використовують **просторове зашумлення** і **просторове електромагнітне зашумлення** з використанням генераторів шуму.

Для блокування каналів витоку інформації з використанням активних засобів застосовуються методи просторового зашумлення і просторового електромагнітного зашумлення. Ці методи спрямовані на ускладнення або повне блокування можливості перехоплення інформації, використовуючи спеціальні генератори шуму.

1. **Просторове зашумлення** включає введення шумових сигналів в оточуючий простір для маскування переданої інформації. Генератори шуму створюють звукові або інші типи перешкод, які заважають виявленню корисного сигналу. Це може бути застосовано, наприклад, у приміщеннях, де проводяться важливі переговори або обробляється конфіденційна інформація. Таким чином, перехоплення акустичних або електричних сигналів стає значно важчим.

2. **Просторове електромагнітне зашумлення** з використанням генераторів шуму застосовується для блокування електромагнітних каналів витоку інформації, таких як радіоелектронні випромінювання. Генератори електромагнітного шуму є ефективними інструментами для

забезпечення безпеки в ситуаціях, де існує ризик перехоплення електромагнітних випромінювань, що можуть бути використані для витоку конфіденційної інформації. Ці пристрої створюють інтенсивний шум в широкому діапазоні частот, що значно ускладнює виявлення та розшифрування справжніх сигналів. Шум може накривати частоти, на яких працюють пристрої, що використовуються для передачі чутливих даних, таких як комп'ютерні системи, телефонні лінії, або інші бездротові комунікаційні канали.

Один з основних принципів роботи генераторів електромагнітного шуму полягає в їх здатності «засліплювати» або зашумлювати вхідні сигнали, які можуть бути виявлені системами моніторингу. Це дозволяє значно зменшити ймовірність того, що зломисники або несанкціоновані користувачі зможуть ефективно перехопити і дешифрувати інформацію, що передається в межах контрольованого середовища. Наприклад, під час передачі важливих даних через радіочастотні канали або мережі Wi-Fi, генератори шуму можуть створювати перешкоди в певних частотних діапазонах, таким чином, запобігаючи перехопленню або фальшивому збору даних.

Крім того, такі генератори можуть використовуватися для створення фальшивих сигналів, які вводять в оману пристрої, що здійснюють моніторинг або спроби перехоплення. Це може бути корисно для створення хибного сліду, який ускладнює для зломисників відстеження справжнього потоку інформації. Така тактика є особливо важливою для захисту високочутливих або секретних даних, коли потрібно не лише захистити інформацію від несанкціонованого доступу, а й зробити складним її виявлення або перехоплення.



Рис. 8.4. Просторове електромагнітне зашумлення комп'ютерного місця
Джерело: [1-7]

Однак важливо зазначити, що використання генераторів електромагнітного шуму повинно бути ретельно сплановане, оскільки їх використання може також призвести до погіршення роботи інших бездротових або електронних пристроїв у зоні дії. Тому при виборі та встановленні таких систем слід враховувати баланс між рівнем захисту та потенційними наслідками для інших комунікаційних каналів і пристроїв, що можуть бути важливими для нормального функціонування інформаційних систем.

Один з основних принципів цих методів полягає в тому, що додавання шуму в середовище поширення сигналу знижує чіткість та точність виявлення корисної інформації. За рахунок створення активних перешкод, таких як шумові генератори, злоумисникам значно ускладнюється задача перехоплення сигналів і отримання цінної інформації. Цей підхід базується на концепції "шумової маскування", коли додатковий сигнал збурює або затушовує реальний інформаційний сигнал, що робить його практично нечитабельним без спеціалізованого обладнання, здатного відфільтровувати шум. В результаті, навіть якщо злоумисник здійснює спробу перехоплення або прослуховування, корисна інформація стає надзвичайно складною для дешифрування чи точного відновлення.

Ці методи захисту надають комплексний підхід до забезпечення інформаційної безпеки, охоплюючи не лише традиційні загрози, але й складніші та більш спеціалізовані форми атак, такі як радіоелектронна розвідка чи перехоплення електромагнітних випромінювань. В умовах, коли конфіденційність даних є критично важливою, наприклад, у військових, урядових або фінансових установах, захист від таких загроз має вирішальне значення.

Радіоелектронна розвідка (PER) включає в себе використання спеціальних засобів для збору інформації з електронних пристроїв, таких як радіочастотне випромінювання, яке може бути використано для аналізу переданої або обробленої інформації. У таких випадках застосування генераторів електромагнітного шуму є ефективним методом для нейтралізації спроб перехоплення. Вони здатні створити перешкоди, які зашумлюють реальні сигнали та роблять їх важкодоступними для радіоелектронних пристроїв, які можуть використовуватись для збору інформації.

Перехоплення електромагнітних випромінювань також становить серйозну загрозу для інформаційної безпеки. Це включає у себе виявлення і аналіз слабких електромагнітних сигналів, які випромінюються комп'ютерними системами, мережевими пристроями або іншими електронними пристроями під час їхньої роботи. Використання

спеціалізованих засобів для захоплення цих сигналів може дозволити зловмисникам отримати чутливу інформацію, що передається або обробляється. Для запобігання таким загрозам генератори шуму і екранування пристроїв можуть стати ключовими елементами стратегії захисту.

Таким чином, інтеграція цих методів у загальну стратегію безпеки значно підвищує захист даних від фізичних загроз, зокрема від несанкціонованого електронного спостереження або перехоплення інформації. Це є важливим кроком до забезпечення безпеки в умовах постійно зростаючої кіберзагрози і розвитку технологій, які дозволяють зловмисникам здійснювати атаки навіть на відстані через електромагнітні канали.



Рис. 8.5. Електромагнітне зашумлення телефонної закладки
Джерело: [1-7]



Рис. 8.6. Створення віброакустичних завад лазерній системі розвідки
Джерело: [1-7]



Рис. 8.7. Зашумлення ліній електроживлення
Джерело: [1-7]



Рис. 8.8. Зашумлення сторонніх провідників і сполучних ліній
Джерело: [1-7]

Для захисту інформації по акустичному каналу застосовують кілька ефективних методів, спрямованих на ускладнення перехоплення та прослуховування звукових сигналів:

❖ Екранування приміщень

Для зниження проникнення звукових хвиль у сусідні приміщення або зовнішнє середовище використовуються спеціальні акустичні екрани. Це можуть бути стіни, двері та вікна з підвищеними звукоізоляційними властивостями. Вибір матеріалів, що мають високу звукоізоляцію, дозволяє ефективно обмежити поширення звукових сигналів.

❖ Шумовий маскування

Важливим методом є створення спеціального шуму в приміщенні, що знижує можливість чіткого сприйняття корисної інформації. Це можуть бути генератори білих шумів або спеціальні шумові пристрої, що маскують розмови або інші звуки. Завдяки цьому сторонні особи, навіть якщо вони знаходяться в безпосередній близькості, не можуть розібрати зміст розмови.

❖ Використання антиакустичних технологій

Застосування активних технологій, таких як антиакустичні системи, дозволяє створювати звукові хвилі, що гасять або нейтралізують зовнішні акустичні сигнали. Вони працюють на принципі "згасання хвиль" — генерація хвиль, які мають протилежну фазу до зовнішнього сигналу, таким чином нейтралізуючи його.

❖ Перехід на закриті зв'язки та шифрування

Використання спеціалізованих засобів для шифрування голосових або звукових повідомлень значно ускладнює їхню перехоплення та розшифровку. Якщо зв'язок є зашифрованим, навіть у разі його перехоплення інформація залишатиметься недоступною без відповідного ключа. Перехід на закриті зв'язки та шифрування дозволяє забезпечити високий рівень конфіденційності переданої інформації, що важливо для захисту корпоративних та державних секретів. Застосування сучасних алгоритмів шифрування, таких як AES або RSA, гарантує, що навіть у разі компрометації каналу зв'язку, перехоплена інформація не буде доступна зловмисникам. Крім того, для додаткового захисту часто використовуються двофакторна аутентифікація та системи безпечних ключів, що забезпечують додаткову перевірку автентичності учасників комунікації.

❖ Контроль доступу до приміщень

Важливо обмежувати доступ до зон, де відбуваються важливі переговори. Для цього використовуються системи контролю доступу, які дозволяють тільки авторизованим особам потрапляти в приміщення, де можуть проводитися конфіденційні переговори.

❖ Використання спеціалізованих телефонних ліній або захищених комунікаційних засобів

Для більш складних і важливих переговорів використовують засоби зв'язку, що забезпечують захищене передавання інформації, включаючи шифровані голосові комунікації через спеціальні канали. Використання спеціалізованих телефонних ліній або захищених комунікаційних засобів є критичним для забезпечення конфіденційності важливих переговорів, особливо у випадках, коли інформація має стратегічну цінність або

стосується національної безпеки. Такі лінії можуть бути побудовані на основі технологій шифрування, що гарантують захист від перехоплення або несанкціонованого доступу до переданих даних. Крім того, ці комунікаційні засоби часто включають системи аутентифікації користувачів для забезпечення ідентифікації учасників переговорів та запобігання можливості їх підміни.

Ці методи можуть комбінуватися для забезпечення комплексного захисту інформації по акустичному каналу, що знижує ймовірність витоку важливих даних.

Якщо необхідно виробляти захист по акустичному каналу, то для цієї мети використовуються:

- ✱ *акустичні генератори шуму;*
- ✱ *пристрої віброакустичного захисту (протидія прослуховування забезпечується внесенням віброакустичних шумових коливань в елементи конструкції будівлі);*
- ✱ *технічні засоби ультразвукового захисту.*

Сунь Цзи, видатний китайський генерал і стратег, у своєму класичному творі «Трактат про військове мистецтво» зазначав, що розвідка є важливою складовою успіху у війні. Він класифікував шпигунів у п'ять категорій, з яких кожна мала своє специфічне завдання:

1. **Інформатори** – це люди, які постачають загальні відомості, корисні для планування стратегії.
2. **Агенти в таборі супротивника** – особи, які перебувають у таборі ворога і збирають інформацію безпосередньо від його ж людей.
3. **Агенти супротивника, використовувані проти своїх** – це особи, які працюють на ворога, але під прикриттям, сприяючи збору інформації або підриву морального стану своїх співвітчизників.
4. **Розвідники і диверсанти** – шпигуни, що спеціалізуються на зборі стратегічної інформації та веденні підривної діяльності.
5. **«Шпигуни життя»** – це найнебезпечніші агенти, які надсилаються до ворога з метою отримати важливі відомості і, найголовніше, повинні повернутися живими, що підвищує їх цінність.

Ці принципи, хоча і походять з військової сфери, мали важливе значення і для розвитку економічної розвідки, інформаційної безпеки та сучасних методів збору та захисту конфіденційних даних у різних сферах діяльності, включаючи корпоративну та державну безпеку. Сьогодні «шпигуни життя» можуть бути адаптовані для сучасних

методів розвідки, де агенти отримують критичну інформацію і використовуються для довготривалого збору даних через соціальні мережі, технології спостереження, або шляхом вербування всередині організацій для відстеження конкурентів або виявлення слабких місць.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 8

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
3. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.
4. Жданова, Ю., Шевченко, С., Спасітелева, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.
5. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.
6. R. Kyrychok, et al., Development of a Method for Checking Vulnerabilities of a Corporate Network using Bernstein Transformations, Eastern-European Journal of Enterprise Technologies, vol. 1, no. 9(115) (2022) 93–101.
7. Костюк Ю.В., Гейдар Гейдаров. Роль токенів та сесійного керування в системах інформаційної безпеки для протидії міжсайтовим атакам. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1216-1231.
8. V. Zhebka, et al., Methodology for Predicting Failures in a Smart Home based on Machine Learning Methods, in: Workshop on Cybersecurity Providing

in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 322–332.

9. Костюк Ю.В., Шапран В.О. Технології виявлення аномальних подій та сигнатур в реальному часі. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1069-1084.

10. O. Romanovskyi, et al., Prototyping Methodology of End-to-End Speech Analytics Software, in: 4th International Workshop on Modern Machine Learning Technologies and Data Science, vol. 3312 (2022) 76–86.

11. Козачок, В., & Драпатий, М. (2024). Аналіз технології Розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 374–391.

12. Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 468–486.

13. Владислав Шапран, Юлія Костюк Виявлення аномальних подій та сигнатур у реальному часі. Інформаційні технології та кібербезпека в умовах воєнного часу [Електронний ресурс] : матеріали студ. наук.-практ. конф. (Київ, 18 квіт. 2024 р.) / відп. ред. К. В. Хорольська. – Київ : Держ. торг.-екон. ун-т, 2024. – с. 237-241 – Укр., англ. мовами.

14. V. Zhebka, et al., Methodology for Choosing a Consensus Algorithm for Blockchain Technology, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 (2024) 106–113.

15. S. Shevchenko, et al., Information Security Risk Management using Cognitive Modeling, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 297–305.

16. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

17. Methods of Modeling Database System Security Rzaieva, S., Rzaiev, D., Kostyuk, Y., Hulak, H., Shcheblanin, O. CEUR Workshop Proceedings This link is disabled., (CPITS 2024), 2024, 3654, pp. 384–390.

18. B. Zhurakovskiy, et al., Modifications of the Correlation Method of Face Detection in Biometric Identification Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 55–63.

19. I. Iosifov, et al., Natural Language Technology to Ensure the Safety of Speech Information, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 216–226.
20. O. Koptika, P. Skladannyi, Use of Service-Oriented Information Technology to Solve Problems of Sustainable Environmental Management. Information Technology and Mathematical Modeling for Environmental Safety 3021 (2021) 66–75.
21. M. Myrontsov, et al., Method for Determining Areas of Stable Solutions of Inverse Problems of Mathematical Physics by the Example of Well Electrometry, in: Workshop on Information Technology and Mathematical Modeling for Environmental Safety, vol. 3021 (2021) 115–126.
22. O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 29–43.
23. V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.

КОНТРОЛЬНІ ПИТАННЯ

1. Дайте характеристику інженерно-технічних засобів безпеки.
2. Що входить до фізичних методів захисту ІКС?
3. Що таке технічний канал витоку і з чого він складається?
4. Що є джерелами сигналу для витоку інформації за межі ІКС?
5. Як класифікуються технічні канали витоку інформації?
6. Що таке радіозакладки і як вони працюють?
7. Назвіть шляхи витоку інформації за рахунок акустоелектричних перетворень
8. Принцип дії «лазерного мікрофону»?
9. Характеристика електромагнітного каналу витоку інформації.
10. Що таке економічна розвідка і які основні групи засобів для її проведення?
11. Назвіть основні канали витоку та несанкціонованого доступу до інформації в типовому офісі.
12. Назвіть принципові підходи для здійснення технічного захисту інформації.

13. Які основні принципи захисту від економічної розвідки можуть бути застосовані в організаціях?
14. Як фізичний захист приміщень може вплинути на захист від економічної розвідки?
15. Що таке екранізація і як вона застосовується для захисту від технічної розвідки?
16. Які методи зашумлення використовуються для ускладнення процесу збору інформації через акустичні канали?
17. Як створення перешкод для передачі сигналів може запобігти технічній розвідці через електронні канали?
18. Як соціальні та інженерні методи захисту інформації використовуються для мінімізації ризиків економічної розвідки?
19. Що таке блокування каналів витоку інформації та як це реалізується в організаціях?
20. Як за допомогою фізичних бар'єрів можна обмежити доступ до чутливої інформації на підприємстві?
21. Як використання засобів моніторингу допомагає виявляти спроби економічної розвідки в реальному часі?
22. Як створення складних середовищ поширення сигналів може бути використано для обмеження можливості збору інформації?
23. Як виявлення та нейтралізація загроз на рівні електронних пристроїв допомагає у захисті від економічної розвідки?
24. Які роль відіграє навчання персоналу в захисті від економічної розвідки та технічних загроз?
25. Яким чином обмеження доступу до фізичних та інформаційних ресурсів може запобігти економічній розвідці?
26. Як важливо застосовувати багаторівневу перевірку при обробці конфіденційних даних у компаніях?
27. Як визначити найслабші місця в системі захисту від економічної розвідки та вжити заходів для їх зміцнення?
28. Які існують основні групи каналів витоку інформації?
29. Поясніть ідею «зашумлення» і приведіть приклади реалізації.
30. Що таке пасивний і активний методи захисту?
31. Коли забезпечується захист інформації від витоку технічними каналами?
32. Шляхи реалізації пасивних методів захисту від ПЕМВН?
33. Що розуміють під поняттям «екранування»?
34. На які види поділяють методи протидії підслуховуванню інформації?
35. Які методи використовують для захисту мовної інформації у приміщеннях?

ТЕМА 4. ПРОГРАМНО-АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІКС

РОЗДІЛ 9 ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ



9.1. Загальна характеристика програмних засобів безпеки ІКС

9.2. Ідентифікація, аутентифікація та авторизація в ІКС

9.3. Види аутентифікації суб'єктів в ІКС

9.4. Парольна аутентифікація

9.5. Аутентифікація на основі PIN-коду

"Ідентифікація та аутентифікація є основою довіри в цифровому світі. Без надійного процесу визначення та перевірки особи, жодна система не може бути впевнена в безпеці своїх ресурсів."

Джон Пірсон, експерт з кібербезпеки та інформаційних технологій

Програмно-апаратне забезпечення безпеки ІКС є критичним елементом для забезпечення цілісності, конфіденційності та доступності інформації, захисту ресурсів системи від загроз, таких як несанкціонований доступ, витоки даних, кібернапади та інші небезпеки. Одним із основних компонентів програмно-апаратного забезпечення є антивірусні програми та засоби захисту від шкідливого програмного забезпечення (ПЗ). Вони відповідають за виявлення, блокування та видалення шкідливих програм, що можуть порушити нормальну роботу системи або завдати шкоди даним.

Сучасні антивірусні рішення здатні до моніторингу і виявлення нових типів шкідливих програм, що забезпечує проактивний захист. Іншим важливим аспектом є механізми аутентифікації та авторизації, які забезпечують перевірку особистості користувачів, що намагаються отримати доступ до ІКС. Вони включають багатофакторну аутентифікацію, паролі, біометричні дані та інші методи перевірки, що дозволяють значно підвищити рівень безпеки та мінімізувати ризик несанкціонованого доступу.

Для захисту конфіденційних даних застосовується шифрування, яке забезпечує нерозбірливість інформації навіть у разі її перехоплення під час передачі через мережу або зберігання. Шифрування даних забезпечує рівень захисту, що важливий для збереження цілісності інформації в усіх аспектах її обробки. Додатково до цього, мережеві екрани та системи виявлення вторгнень (IDS) контролюють трафік, що проходить через мережу, і виявляють потенційно небезпечну активність. Ці системи здатні автоматично реагувати на аномалії та вторгнення, що дозволяє швидко нейтралізувати загрози. Для моніторингу безпеки та оперативного реагування на інциденти використовуються системи управління безпекою інформації (SIEM), які дозволяють централізовано збирати та аналізувати події безпеки з різних джерел. Це дає можливість оперативно виявляти загрози та реагувати на них у реальному часі. Важливою складовою безпеки ІКС є також резервне копіювання та відновлення даних, що забезпечує можливість відновлення інформації в разі її втрати через технічні проблеми або кібератаки. Регулярне створення резервних копій і тестування процедур відновлення є запорукою стійкості системи до непередбачених ситуацій. Водночас фізична безпека апаратних засобів є важливою частиною загального захисту. Використання систем контролю доступу, відеоспостереження та інших методів фізичного захисту допомагає запобігти несанкціонованому фізичному доступу до серверів та іншої техніки, що може призвести до компрометації інформації. Таким чином, програмно-апаратні засоби забезпечують комплексний захист інформаційно-комунікаційних систем, гарантуючи надійність, стійкість і захищеність від зовнішніх і внутрішніх загроз.

9.1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРОГРАМНИХ ЗАСОБІВ БЕЗПЕКИ ІКС

Програмні засоби безпеки ІКС є важливою частиною забезпечення надійного захисту інформаційних ресурсів організації. Вони забезпечують

цілісність, конфіденційність, доступність і автентичність даних, а також надають можливість запобігати, виявляти та реагувати на різні загрози, що можуть виникнути під час роботи системи. Одними з основних програмних засобів є антивірусні та антишкідливі програми, які здатні виявляти, нейтралізувати та блокувати віруси, трояни, шкідливі програми та інші форми шкідливого ПЗ. Вони працюють в реальному часі, забезпечуючи безпеку як у процесі обробки даних, так і в процесі їх зберігання. Крім того, системи виявлення та запобігання вторгнень (IDS/IPS) активно моніторять мережевий трафік, щоб своєчасно виявляти аномалії або спроби несанкціонованого доступу до ІКС, забезпечуючи захист від можливих вторгнень.

Не менш важливими є системи шифрування, які гарантують конфіденційність переданої та збереженої інформації, перетворюючи її на незрозумілий вигляд для сторонніх осіб. Програмні засоби для шифрування можуть бути застосовані як до даних, що передаються по мережі, так і до інформації, яка зберігається на дисках, що мінімізує ризик її втрати чи крадіжки. Для фільтрації трафіку та блокування несанкціонованих з'єднань використовуються фаєрволи, що створюють бар'єр між ІКС та зовнішнім середовищем, контролюючи вхідні та вихідні з'єднання.

Системи аутентифікації та авторизації є ще одним важливим елементом програмного забезпечення безпеки. Вони гарантують, що доступ до критичної інформації та ресурсів отримують лише авторизовані користувачі. Програмне забезпечення для аутентифікації може включати в себе багатофакторну перевірку, біометричні дані або токени для забезпечення максимальної безпеки.

Програмні засоби для резервного копіювання та відновлення даних дозволяють відновити втрачену або пошкоджену інформацію у разі інцидентів, таких як вірусні атаки або технічні збої. Вони гарантують безпеку даних, зберігаючи їх копії на зовнішніх носіях або в хмарних сховищах, що дає можливість швидко відновити роботу ІКС.

Також важливими є системи для моніторингу та аудиту, які дозволяють постійно відстежувати всі дії в ІКС, фіксуючи операції з даними та доступ до них. Це дозволяє своєчасно виявляти будь-які порушення безпеки та здійснювати детальний аналіз інцидентів. Крім того, для захисту від витоків даних використовуються засоби, що контролюють передачу конфіденційної інформації, обмежуючи її несанкціоноване копіювання чи передачу.

Загалом, програмні засоби безпеки ІКС формують багаторівневий захист для інформаційної інфраструктури підприємства, надаючи

можливість ефективно захищати від широкого спектра кіберзагроз, забезпечуючи безперервну і надійну роботу системи та зберігаючи цілісність і конфіденційність даних.

Програмні засоби захисту є найважливішою і необхідною частиною механізму захисту сучасних інформаційних систем і можуть бути як автономними, так і входити до складу різного програмного забезпечення. Програмні засоби можуть виконувати функції виявлення, запобігання та реагування на загрози інформаційній безпеці. Вони забезпечують шифрування даних, контроль доступу, виявлення шкідливого програмного забезпечення та моніторинг мережевої активності. Їх інтеграція в інформаційні системи дозволяє підвищити стійкість до кібератак і мінімізувати ризики витоку даних. Використання сучасних програмних рішень у поєднанні з апаратними засобами створює багаторівневий захист, що відповідає вимогам безпеки підприємств.

По відношенню до загроз, ці заходи можна класифікувати на:

- ❖ *превентивні, що перешкоджають реалізації загроз;*
- ❖ *заходи виявлення порушень безпеки інформації;*
- ❖ *заходи, що локалізують порушення безпеки інформації;*
- ❖ *заходи по виявленню порушника; заходи відновлення безпеки інформації.*

Превентивні заходи

Превентивні заходи спрямовані на недопущення виникнення загроз, що може включати в себе широке коло дій, спрямованих на зменшення ризиків і забезпечення безпеки на всіх етапах функціонування інформаційних та комунікаційних систем. Вони охоплюють низку стратегій і технічних рішень, що мають за мету не тільки реагувати на потенційні загрози, але й попереджати їх, знижуючи ймовірність їх виникнення.

Одним із основних принципів превентивних заходів є випереджаюче виявлення загроз, що дозволяє організаціям швидко реагувати на можливі проблеми до того, як вони призведуть до шкоди. Це може включати використання систем моніторингу, аналізу ризиків, а також прогнозування ймовірних сценаріїв загроз. Створення бар'єрів на шляху реалізації загроз є важливим етапом у забезпеченні захисту. Це може бути здійснено через фізичні заходи, такі як обмеження доступу до важливих ресурсів, або через технологічні методи, як-от застосування засобів шифрування або аутентифікації для запобігання несанкціонованому доступу.

Резервування є ще одним важливим елементом превентивних заходів, що дозволяє забезпечити безперервність діяльності організації в разі виникнення непередбачених обставин, таких як технічні збої чи атаки. Це може включати створення дублюючих систем зберігання даних, впровадження планів відновлення після катастроф і підготовку резервних каналів зв'язку.

Розподіл ролей і використання засобів розмежування доступу є важливими аспектами управління безпекою, оскільки дозволяють обмежити доступ до критичних даних або систем тільки для уповноважених осіб. Також важливим є контроль доступу в приміщення, особливо в зони, де зберігаються конфіденційні дані або де можуть виникати загрози фізичного доступу до систем.

Превентивні заходи також передбачають регулярне навчання співробітників, перевірку безпеки програмного забезпечення, здійснення аудиту і тестування на уразливості для виявлення та усунення потенційних слабких місць до того, як вони будуть використані зловмисниками.

Таким чином, застосування превентивних заходів забезпечує більш високий рівень безпеки та ефективності функціонування системи, мінімізуючи ймовірність виникнення інцидентів і завдаючи мінімальної шкоди в разі їх реалізації.

Заходи виявлення порушень і виявлення порушника

Заходи виявлення порушень і виявлення порушника є важливим елементом системи безпеки та управління ризиками в будь-якій організації. Їх основною метою є оперативне виявлення спроб несанкціонованого доступу, порушень політики безпеки або інших загроз для інформаційних і комунікаційних систем. Виявлення порушень дозволяє вчасно вжити заходи для мінімізації шкоди та попередити подальші інциденти.

1. Моніторинг та аудиторський контроль

Одним з основних заходів виявлення порушень є постійний моніторинг систем і мереж, що включає в себе відстеження активності користувачів, перевірку журналів подій, аналіз з'єднань, виявлення незвичних або підозрілих дій. Використання інструментів для автоматичного збору та аналізу логів допомагає вчасно виявляти аномалії, які можуть бути ознаками порушень.

2. Системи виявлення вторгнень (IDS)

Системи IDS (Intrusion Detection Systems) призначені для виявлення аномальних або зловмисних дій у мережах або комп'ютерних системах.

Вони можуть виявляти спроби вторгнення, несанкціонований доступ або інші порушення політик безпеки, аналізуючи трафік та активність в режимі реального часу.

3. Антивірусні та антишпигунські програми

Для виявлення шкідливого програмного забезпечення, яке може використовуватися для порушення безпеки, необхідно застосовувати антивірусні системи, що перевіряють наявність вірусів, троянів, шпигунських програм, які можуть порушити конфіденційність даних або знизити цілісність системи.

4. Аналіз поведінки користувачів

Використання технологій, що відстежують і аналізують поведінку користувачів, дозволяє виявляти аномалії у звичайному режимі роботи, наприклад, несанкціоновані спроби доступу до заборонених ресурсів, зміни в облікових записах або інші підозрілі дії.

5. Виявлення фізичних порушень

Важливим компонентом безпеки є контроль фізичного доступу до приміщень, де зберігаються критичні дані або обладнання. Використання систем відеоспостереження, контролю доступу та сигналізацій дозволяє виявити порушників на етапі спроби фізичного доступу.

6. Реакція на інциденти та реагування на загрози

Після виявлення порушення важливо здійснити правильну реакцію. Це включає в себе автоматичне або ручне блокування зловмисних дій, повідомлення про інцидент відповідальних осіб або автоматичне зупинення доступу для підозрілих користувачів, а також проведення внутрішнього розслідування.

7. Пошук та виявлення порушника

Якщо порушення вже сталося, важливо виявити, хто саме здійснив порушення. Це може бути досягнуто шляхом детального аналізу логів, відстеження дій у системі, а також використання додаткових методів, таких як відновлення втрачених або змінених даних, аналіз цифрових доказів, встановлення причетності через систему аудиту та ідентифікації.

8. Захист від витоку інформації (DLP-системи)

Виявлення спроб витоку конфіденційної або критичної інформації є важливим аспектом захисту. Впровадження систем DLP (Data Loss Prevention) дозволяє моніторити та обмежувати доступ до чутливих даних, а також виявляти спроби передачі або копіювання таких даних з несанкціонованих пристроїв.

Таким чином, заходи виявлення порушень і виявлення порушників повинні бути інтегрованими і спрямованими на своєчасну ідентифікацію

загроз та порушників безпеки, щоб оперативно вжити заходів для захисту інформаційних ресурсів організації.

Заходи, що локалізують порушення

Заходи, що локалізують порушення, спрямовані на те, щоб обмежити вплив загроз і не допустити їх поширення. Вони передбачають низку дій, які дозволяють ізолювати уражену частину системи та запобігти подальшому поширенню атаки чи витоків інформації. Першим кроком після виявлення порушення є ізоляція уражених систем або компонентів, що включає вимкнення мережевих з'єднань або відключення скомпрометованих серверів та комп'ютерів. Це дозволяє зупинити поширення загрози в мережі і мінімізувати її вплив на інші системи. Наступним важливим етапом є обмеження доступу до ресурсів, таких як зміна паролів або блокування облікових записів користувачів, щоб унеможливити подальше використання скомпрометованих елементів. Для цього можуть використовуватися різні методи, наприклад, додаткові системи контролю доступу та багатофакторна аутентифікація.

Також важливо використовувати мережеві екрани, які можуть фільтрувати і блокувати підозрілі з'єднання, і таким чином локалізувати порушення. Мережеві екрани або інші системи фільтрації трафіку допомагають обмежити доступ зловмисників до внутрішньої мережі та запобігти поширенню атак. Інструменти для моніторингу та виявлення вторгнень (IDS/IPS) дозволяють своєчасно реагувати на несанкціоновану активність і автоматично блокувати підозрілі з'єднання. Вони здатні виявляти аномалії, які свідчать про можливі порушення, і миттєво реагувати, блокуючи відповідні канали.

Ізоляція порушення також може бути досягнута за допомогою сегментації мережі. Коли організація розділяє свою інфраструктуру на окремі сегменти, це дозволяє обмежити вплив порушення в межах одного сегмента та завадити поширенню загрози на всю мережу. Шлюзи безпеки між сегментами допомагають контролювати потік даних і блокувати несанкціоновану активність. Крім того, активуються резервні системи, щоб мінімізувати вплив інциденту на діяльність організації. Ці системи дозволяють забезпечити безперервність роботи організації, навіть якщо одна з частин інфраструктури була уражена.

Окрім цього, важливим заходом є контроль доступу до даних. Обмеження доступу до чутливої інформації, зміна дозволів на файли та ресурси можуть запобігти її несанкціонованому використанню. Відновлення і патчування уразливих компонентів також є невід'ємною

частиною локалізації порушення. Застосування оновлень і виправлень уразливостей гарантує, що зловмисники не зможуть використати виявлені слабкі місця для подальшої атаки. Важливим є також фізичне відключення або ізоляція уражених пристроїв, таких як носії інформації або комп'ютери, для запобігання доступу до даних через фізичні канали.

У разі локалізації порушення важливо провести детальний моніторинг, щоб упевнитись у повному усуненні загрози. Для цього здійснюється повторна перевірка систем на наявність шкідливого програмного забезпечення та аномальної активності. Це дозволяє переконатися, що інцидент був повністю ліквідований і що загроза більше не існує. Таким чином, заходи локалізації порушень дозволяють ефективно зупинити поширення загроз і мінімізувати їх вплив на організацію.

Заходи відновлення безпеки інформації

Заходи відновлення безпеки інформації спрямовані на відновлення нормальної роботи інформаційних систем та ресурсів після інциденту безпеки. Вони охоплюють низку дій, що забезпечують повернення пошкоджених або втрачених даних, відновлення працездатності систем та захист від подальших загроз. Одним із основних етапів є відновлення даних, яке передбачає використання резервних копій, зроблених до інциденту. Це дозволяє мінімізувати втрати інформації та забезпечити стабільність діяльності організації. Поряд із відновленням даних необхідно провести патчинг та оновлення програмного забезпечення, що дозволяє усунути уразливості, які могли бути використані зловмисниками. Оновлення операційних систем і додатків допомагає захистити від подальших атак. Після цього важливо провести ретельний аналіз інциденту, щоб зрозуміти, як саме відбулася атака, які були її наслідки і які системи постраждали. Це дозволяє визначити слабкі місця в системі та усунути їх, попередивши можливі повторні загрози. Відновлення працездатності систем і інфраструктури є наступним кроком, що включає повернення до нормальної роботи серверів, мережевого обладнання та програмного забезпечення. Після цього важливо здійснити моніторинг систем для забезпечення стабільності і виявлення можливих повторних атак. Одночасно з відновленням, варто враховувати нові загрози та вжити заходів для їх нейтралізації, застосовуючи кращі практики безпеки. Наприклад, покращення політики доступу, використання багатоетапної аутентифікації та вдосконалення моніторингу. Після завершення заходів відновлення слід переглянути план дій на випадок надзвичайних ситуацій та адаптувати його з урахуванням нових викликів. Також важливо

провести навчання для персоналу, щоб покращити їх здатність реагувати на можливі загрози в майбутньому. Завершальним етапом є оцінка ефективності вжитих заходів та їх удосконалення на основі отриманого досвіду.

Всі ці заходи формують комплексний підхід до відновлення безпеки інформації, що дозволяє не тільки швидко відновити працездатність системи, але й підвищити її стійкість до майбутніх загроз. Цілі застосування коригувальних механізмів захисту:

- ➔ відновлення системи в разі атаки;
- ➔ страхування ризиків інформаційної безпеки;
- ➔ реагування на порушення безпеки, ліквідація наслідків здійснення загроз і мінімізація шкоди;
- ➔ розробка, впровадження та реалізації плану відновлення після аварії (план забезпечення безперервної роботи та відновлення), резервне копіювання і відновлення даних і т. п.

Основними недоліками використання програмних засобів безпеки є кілька важливих факторів. По-перше, додаткове навантаження на процесор може призводити до зниження швидкості роботи системи. Це може мати особливе значення в умовах високих вимог до продуктивності та оперативного реагування, коли збільшення часу відповіді на запити може негативно впливати на загальну ефективність роботи. По-друге, використання програмних засобів безпеки також може зменшити обсяг доступної оперативної пам'яті, оскільки ці програми потребують певної кількості ресурсів для своєї роботи. Крім того, багато програмних рішень є орієнтованими на конкретні архітектури, що обмежує їх універсальність і можливість використання в різних середовищах. Ця залежність від операційної системи також додає ще один рівень складності, оскільки зміна або оновлення ОС може потребувати коригування або оновлення програмних засобів безпеки, що додатково ускладнює їх адміністрування.

Перелік програмних засобів захисту може бути будь-яким, а виконувані ними функції, що складають сервіси безпеки можуть бути такі:

- ✱ перевірка прав доступу (ідентифікація);
- ✱ розпізнавання користувачів та компонентів ПЗ (аутентифікація);
- ✱ управління доступом до ресурсів системи (авторизація);
- ✱ протоколювання й аудит;
- ✱ шифрування і контроль цілісності;

- ✱ виявлення та знешкодження шкідливого ПЗ;
- ✱ резервування інформації і відновлення систем;
- ✱ надійне знищення інформації після використання;
- ✱ управління оновленнями програмних компонент;
- ✱ сигналізація порушення використання ресурсів (виявлення вторгнень і аномалій);
- ✱ фільтрація трафіку і екранування мереж;
- ✱ тунелювання і створення віртуальних мереж;
- ✱ контроль електронної пошти та вебтрафіку;
- ✱ виявлення і запобігання комп'ютерних атак;
- ✱ аналіз захищеності ІКС;
- ✱ контроль діяльності співробітників;
- ✱ управління безпекою.



На основі різноманітних сервісів безпеки формуються основні компоненти загальної системи забезпечення безпеки інформації, яка організована у вигляді окремих підсистем. Кожна підсистема може включати кілька специфічних сервісів безпеки, що сприяє комплексному підходу до захисту. Замість того, щоб використовувати окремі інструменти, як-от системи екранування, тунелювання, антивірусні рішення чи системи виявлення і запобігання вторгнень, на ринок поставляються інтегровані програмно-апаратні комплекси. Такі рішення дозволяють ефективно поєднувати всі необхідні елементи захисту, оптимізуючи процеси і знижуючи загальну вартість володіння системою безпеки.

Інтеграція різних засобів захисту в єдину структуру компанії не тільки зменшує витрати, але й значно спрощує процес їх установки, адміністрування та оновлення. В результаті цього підвищується рівень захисту інформаційних ресурсів компанії на всіх етапах їх обробки, зберігання і передачі. Крім того, ця інтеграція дозволяє централізовано управляти всіма компонентами системи безпеки, що забезпечує швидшу реакцію на інциденти безпеки і зменшує потенційні ризики для організації.

9.2. ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ В ІКС

Ідентифікація, аутентифікація та авторизація — це три ключових процеси, які забезпечують контроль доступу та безпеку інформаційних і комунікаційних систем (ІКС). Кожен з цих процесів має важливу роль у забезпеченні цілісності, конфіденційності та доступності інформації.

Ідентифікація — це процес визначення, хто саме намагається отримати доступ до системи або ресурсу. Вона передує всім іншим діям і є першою лінією захисту в ІКС. Ідентифікація зазвичай здійснюється за допомогою унікальних ідентифікаторів, таких як ім'я користувача, електронна пошта або інші персональні дані. Мета цього етапу — правильно визначити особу або систему, що намагається отримати доступ. Після ідентифікації здійснюється процес аутентифікації, який підтверджує достовірність заявленої особи або системи. Ефективна ідентифікація дозволяє запобігти несанкціонованому доступу та забезпечити належний рівень безпеки. Сучасні системи використовують багатофакторну ідентифікацію, що поєднує різні методи, наприклад, паролі, біометричні дані та токени. Впровадження таких підходів підвищує надійність захисту інформаційних і інтелектуальних систем.

Аутентифікація є наступним етапом і полягає в перевірці справжності даних, наданих під час ідентифікації. Це процес підтвердження, що користувач або система є тим, за кого вони себе видають. Аутентифікація здійснюється шляхом перевірки одного або кількох факторів, таких як паролі, одноразові коди, біометричні дані чи криптографічні ключі. Сучасні підходи передбачають використання багатофакторної аутентифікації для підвищення рівня безпеки. Важливим аспектом є забезпечення балансу між зручністю для користувача та рівнем захисту даних. Надійна аутентифікація є ключовим елементом інформаційної безпеки, який мінімізує ризики несанкціонованого доступу до ресурсів. Аутентифікація може здійснюватися за допомогою різних методів, таких як:

- Паролі та PIN-коди.
- Біометричні дані (відбитки пальців, розпізнавання обличчя).
- Токени або смарт-карти.
- Одноразові паролі (OTP).
- Двофакторна або багатофакторна аутентифікація (2FA або MFA), що поєднує кілька методів перевірки.

Авторизація є процесом надання дозволу користувачеві чи системі на доступ до певних ресурсів або дій у межах ІКС після успішної аутентифікації. Вона визначає рівень доступу, який має користувач, що може включати доступ до певних файлів, функцій системи або мережевих ресурсів. Авторизація базується на політиках безпеки, які встановлюють права та обмеження для кожного користувача чи групи. Цей процес забезпечує, що кожен суб'єкт має доступ лише до тих ресурсів, які необхідні для виконання його завдань. Реалізація авторизації може здійснюватися за допомогою ролей, списків контролю доступу (ACL) або

атрибутів користувача. Важливим є регулярний перегляд і оновлення політик авторизації, щоб уникнути надмірного доступу чи потенційних вразливостей у системі. Це може бути:

- Ролі (наприклад, адміністратор, користувач, гість).
- Списки контролю доступу (ACL).
- Політики доступу, що визначають, які дії дозволяються певним групам користувачів.

Ці три процеси разом формують основу безпеки ІКС, забезпечуючи ефективний контроль доступу, захист від несанкціонованого доступу та зловмисників, а також гарантують, що лише авторизовані особи мають можливість взаємодіяти з конфіденційними даними та ресурсами.

Застосування відкритих каналів передачі даних, таких як Інтернет, створює потенційні ризики для безпеки інформаційних і комунікаційних систем (ІКС), оскільки ці канали можуть бути використані зловмисниками для перехоплення, модифікації або підміни даних, а також для несанкціонованого доступу до ресурсів системи. Одним із ключових завдань забезпечення безпеки ІКС при взаємодії користувачів є застосування методів і засобів, що дозволяють одній стороні переконатися в достовірності іншої сторони. Це є необхідною умовою для того, щоб забезпечити захист даних і гарантувати, що інформація не буде спотворена або доступна для несанкціонованих осіб.

Методи аутентифікації є важливим інструментом для підтвердження особи користувача. У разі відкритих каналів, особливо в Інтернеті, забезпечення достовірності є важливим елементом захисту від різноманітних атак. Для підвищення рівня безпеки застосовуються двофакторні або багатофакторні методи аутентифікації, які вимагають від користувача не лише введення пароля, але й надання додаткових доказів своєї особи, наприклад, через використання одноразових паролів або біометричних даних.

Шифрування є ще одним критичним елементом для забезпечення безпеки даних під час їх передачі через відкриті канали. Шифрування гарантує, що навіть якщо зловмисники зможуть перехопити дані під час передачі, вони не зможуть отримати доступ до змісту цих даних без відповідного ключа для дешифрування. Протоколи, такі як SSL/TLS, є стандартом для забезпечення захищеного з'єднання між користувачем і сервером, що дозволяє забезпечити конфіденційність і цілісність переданої інформації.

Цифрові підписи також використовуються для підтвердження автентичності переданої інформації. Цей метод дозволяє перевірити, що дані не були змінені після їх підписання і що їх автор є тим, ким він

заявляє. Цифровий підпис дозволяє не тільки забезпечити автентичність інформації, а й її цілісність, що важливо для захисту від атак, які намагаються змінити передану інформацію.

Також важливим елементом безпеки є використання сертифікаційних центрів для видачі цифрових сертифікатів, що дозволяють сторонам підтвердити автентичність один одного. Довіра до таких сертифікатів і самих сертифікаційних центрів є необхідною умовою для безпечної взаємодії в ІКС.

Загалом, застосування цих методів у сукупності дозволяє створити надійну систему захисту даних, що забезпечує високий рівень безпеки в умовах відкритих каналів передачі інформації, дозволяючи сторонам бути впевненими в достовірності один одного і захищеності переданих даних.

Ідентифікація та аутентифікація – це перша лінія оборони, «прохідна» інформаційного простору. З метою забезпечення санкціонованого доступу до ресурсів ІКС кожен суб'єкт (співробітник, користувач, процес) і об'єкт (ресурс ІКС) має бути однозначно визначеним. Для цього спочатку здійснюється попередня реєстрація всіх суб'єктів та об'єктів інформаційної системи і кожному суб'єкту чи об'єкту привласнюється унікальний ідентифікатор (число або рядок символів). Після цього ідентифікатори використовуються для подальшої ідентифікації та забезпечення коректного зіставлення суб'єктів із їхніми правами доступу. Унікальність ідентифікаторів гарантує, що система може точно розпізнати кожного користувача чи ресурс. Ця процедура є ключовою для створення надійної основи безпеки, адже вона виключає плутанину або помилки в управлінні доступом. Завдяки цьому процесу забезпечується цілісність і конфіденційність даних в інформаційно-інтелектуальній системі.

Ідентифікація

Ідентифікація – це процес, що передбачає надання унікального імені (ідентифікатора) об'єктам та суб'єктам ІКС для подальшого розпізнавання їх системою, або порівняння запропонованого ідентифікатора з переліком привласнених ідентифікаторів.

Одні ідентифікатори автоматично генеруються ОС і додатками (ідентифікатори процесів, ідентифікатори логічних мережеских з'єднань), інші призначаються адміністратором (ідентифікатори користувачів, адреси

комп'ютерів, доменні імена мережевих сервісів), треті породжуються самими користувачами (вибір власного імені, призначення імен файлів).

Важливо щоб наданий ідентифікатор зберігався в переліку зареєстрованих ідентифікаторів інформаційної системи. Якщо буде введений неіснуючий ідентифікатор, то очевидно, система не зможе дозволити доступ до інформаційної системи.

Сама процедура ідентифікації пов'язана лише з тим, що користувач вводить якусь інформацію. Ніякої перевірки того, що ця інформація дійсно належить йому, не здійснюється. Приклад ідентифікації без перевірки приналежності цього ідентифікатора – це вибір *«НІКНЕЙМА»* в чаті, де досить просто придумати для себе якесь ім'я і далі під ним діяти. При цьому ніякого взаємозв'язку між реальним фізичною особою і його ідентифікатором, у такому випадку, не відбувається.

Аутентифікація

У більш серйозних системах, де передбачається відповідальність користувача за дії, які він здійснює в системі, йому обов'язково потрібно довести, що введений їм ідентифікатор належить йому. Саме цьому і слугує процедура аутентифікації. Аутентифікація дозволяє підтвердити, що користувач є тим, за кого себе видає, за допомогою одного або кількох факторів: знання (пароль), володіння (токен) або властивостей (біометричні дані). У серйозних системах часто використовується багатофакторна аутентифікація для забезпечення більш високого рівня безпеки. Ця процедура знижує ризик несанкціонованого доступу та підвищує довіру до дій, які виконуються в системі. Крім того, аутентифікація є важливим етапом для забезпечення прозорості та підзвітності операцій у критично важливих інформаційних системах.

Аутентифікація – це процес перевірки достовірності пред'явлених ідентифікаторів суб'єкта або об'єкта інформаційної системи.

Метою аутентифікації суб'єкта є переконатися, що суб'єкт є саме тим, ким він представився (ідентифікувався).

Метою аутентифікації об'єкта є підтвердження, що об'єкт є саме тим, який необхідний для виконання певних операцій або доступу до ресурсів системи.

В якості синоніма слова *«аутентифікація»* іноді використовують словосполучення *«перевірка справжності»*. Для цього в системі повинні зберігатися спеціальні ознаки кожного суб'єкта і об'єкта, за якими їх можна було б однозначно впізнати. Аутентифікація запобігає доступ до системи небажаних осіб і дозволяє вхід для легальних користувачів. Таким чином, ідентифікацію та аутентифікацію можна вважати основним механізмом, який реалізує захист від несанкціонованого доступу (НСД).

За відсутності процедури аутентифікації, доступ до системи нелегальних осіб стає простим завданням – достатньо просто використовувати ідентифікатор легального користувача.

Аутентифікація користувачів є одним із основних механізмів забезпечення безпеки інформаційних систем, оскільки вона не лише захищає від несанкціонованого доступу з боку злоумисників, але й допомагає уникнути ситуацій, коли легітимні користувачі можуть заперечувати свої неправомірні дії. Без належної аутентифікації, навіть якщо користувач вчинив недобросовісні або недбалий вчинок, він може стверджувати, що його ідентифікатор був використаний іншою особою, і тим самим уникнути відповідальності за свої дії. Це створює серйозну проблему для системи безпеки, оскільки без аутентифікації неможливо точно встановити, хто саме здійснив ту чи іншу дію в межах інформаційної системи.

Аутентифікація за допомогою надійних методів (наприклад, багатофакторної аутентифікації або використання біометричних даних) забезпечує можливість точно ідентифікувати користувача та відслідковувати його дії. У разі порушення, система може надати незаперечні докази того, що конкретний користувач здійснив неправомірну дію, що значно ускладнює заперечення його участі в таких діях. Таким чином, аутентифікація не лише обмежує доступ до інформації для сторонніх осіб, але й є важливим елементом для забезпечення відповідальності користувачів за їхні дії в системі.

Авторизація

Авторизація — це процес надання користувачу дозволу на доступ до певних ресурсів або виконання певних дій у рамках інформаційної системи після його успішної аутентифікації. Після того, як система впізнала користувача та підтвердила його ідентичність (аутентифікація), авторизація визначає, що саме цей користувач може робити з системою: чи може він читати, змінювати чи видаляти дані, отримувати доступ до певних функцій або служб.

Авторизація базується на принципі прав доступу, які можуть бути надані користувачам на різних рівнях. Ці права визначають, які ресурси або функції системи доступні для конкретного користувача чи групи користувачів. Авторизація може бути реалізована через ролі, де кожній ролі відповідає набір прав, або через індивідуальні налаштування для кожного користувача. Дотримання принципу мінімальних привілеїв є ключовим для зменшення ризиків, пов'язаних із надмірним доступом. Регулярний моніторинг і перегляд прав доступу дозволяє забезпечити актуальність авторизаційної політики та запобігти потенційним вразливостям. Авторизація зазвичай включає використання таких механізмів, як:

1. **Ролі користувачів** — користувачі отримують ролі (наприклад, адміністратор, користувач, гість), що визначають рівень їх доступу до інформації та функцій системи. Кожна роль має чітко визначений набір прав і обмежень, що забезпечує ефективне управління доступом та мінімізацію ризиків. 3. Такий підхід дозволяє спростити адміністрування системи, забезпечуючи гнучкість і прозорість у розподілі прав доступу.

2. **Списки контролю доступу (ACL)** — це списки, які вказують, який користувач або група користувачів має право на доступ до конкретних ресурсів і в який спосіб. Кожен запис у списку ACL визначає користувача чи групу, ресурс, до якого надається доступ, та тип доступу (читання, запис, виконання тощо). Використання ACL дозволяє точно контролювати доступ до критичних даних і функцій, знижуючи ймовірність несанкціонованих змін чи витоків інформації.

3. **Політики доступу** — набір правил, які можуть включати умови доступу, час доступу, з яких пристроїв і з яких мереж дозволено входити до системи. Ці правила визначають, коли і за яких обставин користувачі можуть отримати доступ до ресурсів, забезпечуючи додатковий рівень безпеки. Політики доступу можуть бути адаптовані для різних типів користувачів і ситуацій, наприклад, для віддалених працівників або у випадку підвищеного ризику доступу.

Процес авторизації є важливим для забезпечення безпеки, оскільки він дозволяє контролювати доступ до чутливої або конфіденційної інформації та забезпечує, що тільки уповноважені користувачі можуть виконувати певні дії, що знижує ризик несанкціонованого доступу або змін. Авторизація реалізується шляхом перевірки прав доступу кожного користувача або системного процесу перед виконанням запитуваної операції. Цей процес може бути динамічним, враховуючи контекст, наприклад, місце перебування, час доступу або використовуваний пристрій. Інтеграція авторизації з іншими заходами безпеки, такими як моніторинг активності або шифрування даних, підвищує загальний рівень захисту системи. Завдяки ефективній авторизації

підприємства можуть забезпечувати відповідність вимогам законодавства та стандартів інформаційної безпеки.

Перед авторизацією здійснюються етапи ідентифікації та аутентифікації. Ідентифікація визначає, хто саме намагається отримати доступ до інформаційної системи, шляхом надання унікального ідентифікатора, такого як ім'я користувача чи електронна адреса. Аутентифікація підтверджує, що цей ідентифікатор дійсно належить суб'єкту, який його використовує, за допомогою пароля, біометричних даних чи інших методів перевірки. Лише після успішного проходження цих етапів суб'єкт допускається до процедури авторизації для визначення рівня його доступу до ресурсів системи.

Авторизація – це процес надання автентифікованому суб'єкту відповідних прав на доступ до об'єктів інформаційної системи. Це включає визначення того, які дані та ресурси суб'єкт може використовувати, які операції з ними виконувати, які програми може запускати, а також встановлення обмежень щодо часу, терміналів та умов доступу. Авторизація забезпечує контроль за тим, хто і в якій мірі може взаємодіяти з системою та її ресурсами після успішної аутентифікації.

Авторизація зазвичай виконується після успішного проходження суб'єктом аутентифікації. Під час цього етапу визначається, які права доступу має аутентифікований користувач, тобто, які об'єкти системи він може використовувати, які операції може виконувати, на яких терміналах може працювати, а також доступ до ресурсів системи та програмного забезпечення.

Процедура авторизації, або управління доступом (access control), полягає в наданні суб'єкту тільки тих прав доступу, які визначені для його ідентифікатора. Це забезпечує контроль над тим, які ресурси та операції доступні конкретному користувачеві в системі.

Це означає, що у випадку, коли фізичний суб'єкт має декілька ідентифікаторів у системі, система може застосовувати різні рівні доступу для кожного з цих ідентифікаторів. Наприклад, один ідентифікатор може мати обмежений доступ до певних даних або функцій, тоді як інший може надавати більш широкий доступ. Такий підхід дозволяє гнучко

налаштовувати рівні доступу в залежності від ролі або контексту використання кожного ідентифікатора.



Аутентифікація відповідає за перевірку ідентифікації користувача, визначаючи, чи є він легальним, тоді як авторизація визначає, які саме ресурси або функції доступні цьому користувачеві після успішного проходження аутентифікації. Якщо користувач отримує доступ до ресурсів або дій без належної авторизації або в обхід системи контролю доступу, такий доступ вважається несанкціонованим і може призвести до порушення безпеки системи. Аутентифікація зазвичай здійснюється за допомогою комбінації імені користувача та пароля, біометричних даних або багатофакторних методів. Авторизація, в свою чергу, може бути реалізована через розподіл прав доступу, де різним користувачам або групам користувачів надаються різні рівні доступу залежно від їхніх ролей і потреб. Правильна реалізація аутентифікації та авторизації є критично важливою для забезпечення належного рівня безпеки та захисту конфіденційної інформації в інформаційних системах.

9.3. Види аутентифікації суб'єктів в ІКС

Аутентифікація суб'єктів в інформаційно-комунікаційних системах (ІКС) є ключовим етапом процесу забезпечення безпеки, оскільки вона підтверджує особу користувача або об'єкта, що намагається отримати доступ до системи. Існують різні види аутентифікації, кожен з яких має свої особливості та рівень безпеки. Одним із найпоширеніших методів є аутентифікація за паролем, коли користувач вводить унікальний пароль для підтвердження своєї особи. Однак цей метод має обмеження, адже паролі можуть бути забуті або зламані за допомогою атак на паролі, що знижує його ефективність.

Щоб підвищити рівень безпеки, аутентифікація часто поєднується з іншими методами, такими як використання унікальних ідентифікаторів, що складаються з логіна або ідентифікаційного номера, що додає додатковий рівень перевірки. Більш складною є аутентифікація за допомогою смарт-карт або токенів, де фізичний носій, наприклад, USB-токен, містить сертифікат або ключ, необхідний для підтвердження особи користувача. Це підвищує рівень захисту, оскільки злоумисник не зможе отримати доступ до системи без фізичного носія.

Іншим ефективним методом є біометрична аутентифікація, яка використовує унікальні біометричні характеристики користувача, такі як відбитки пальців, розпізнавання обличчя чи райдужки ока. Така

аутентифікація забезпечує високий рівень безпеки, оскільки біометричні дані важко підробити, але цей метод потребує спеціального обладнання та може бути менш зручним для користувачів.

Одночасно використовуються методи аутентифікації за допомогою одноразових паролів (ОТР), які генеруються для одного сеансу за допомогою мобільних додатків або через SMS. Це зменшує ризики фішингових атак і підвищує безпеку. Однак цей метод має обмеження, такі як можливість перехоплення кодів через ненадійні канали зв'язку.

Щоб ще більше зміцнити безпеку, активно застосовується двофакторна аутентифікація (2FA), яка поєднує два незалежних фактори — наприклад, пароль і одноразовий код, надісланий на телефон. Це значно ускладнює несанкціонований доступ до системи, навіть якщо зломисник здобуде один із факторів.

І, на останок, є методи, що використовують поведінкові характеристики користувача для аутентифікації. Це може бути стиль набору тексту, рухи миші або інші унікальні параметри взаємодії з пристроєм. Хоча цей метод не потребує додаткових пристроїв, його точність може бути низькою, і він може бути вразливим до змін у поведінці користувача.

Усі ці методи можуть застосовуватися окремо або комбінуватися, в залежності від вимог до безпеки в конкретній інформаційно-комунікаційній системі. Залежно від рівня захисту, що необхідний для кожної системи, організації можуть вибирати оптимальні варіанти аутентифікації, забезпечуючи надійний захист своїх ресурсів і даних.

У процедурі аутентифікації беруть участь дві сторони: одна сторона доводить свою автентичність, пред'являючи деякі докази, а інша — автентифікатор, — перевіряє ці докази і приймає рішення. Як доказ автентичності використовуються найрізноманітніші прийоми:

- ➔ шляхом перевірки знання того, чого не знають інші (паролів, PIN-кодів, ключових слів). Умовно цей фактор позначається як «*Я знаю*»;
- ➔ шляхом перевірки володіння якимось унікальним об'єктом, наприклад, пропуск, смарт-картка, посвідчення особи, якийсь унікальний жетон. Умовно цей фактор позначається як «*Я маю*»;
- ➔ шляхом перевірки унікальних фізичних характеристик (відбитки пальців, особливості райдужної оболонки очей, форма кисті рук і т.п.) і параметрів самих користувачів за допомогою спеціальних біометричних пристроїв. Цей фактор умовно позначається як «*Я є*».

*Якщо використовується тільки один з перерахованих способів аутентифікації, то це називається однофакторною автентифікацією. Для підвищення надійності системи аутентифікації використовують більш одного фактора, тобто використовують **багатофакторну аутентифікацію**, коли користувачеві потрібно пройти процедури перевірки на основі більш ніж одного фактора.*

Однофакторна аутентифікація передбачає використання лише одного елементу для перевірки особи користувача, наприклад, пароля, пін-коду або ідентифікаційного номера. Це простий метод аутентифікації, але він має свої обмеження, зокрема можливість компрометації цього одного елемента через фішинг, підбір паролів або інші методи зловмисників.

Для підвищення рівня безпеки в системах, де доступ до важливої або чутливої інформації потребує додаткового захисту, використовується багатофакторна аутентифікація (MFA). Це процес, коли для підтвердження особи користувача необхідно пройти перевірку за допомогою кількох різних факторів, що належать до різних категорій. Наприклад, користувач може ввести пароль (перша категорія – знання), отримати одноразовий код на мобільний телефон або електронну пошту (друга категорія – володіння) або пройти біометричну перевірку (третья категорія – біометрія).

Багатофакторна аутентифікація значно ускладнює можливість несанкціонованого доступу, оскільки для успішного проходження всіх етапів перевірки зловмисник повинен отримати доступ до кількох елементів, які значно важче зламати або підробити. Таким чином, багатофакторна аутентифікація є потужним механізмом захисту, що дозволяє забезпечити більш високий рівень безпеки в інформаційно-комунікаційних системах.

Багатофакторна аутентифікація – це метод перевірки особи користувача, що передбачає використання кількох різних факторів для забезпечення надійності процесу. Основними типами факторів є знання (щось, що знає тільки користувач, наприклад, пароль або PIN-код), володіння (щось, чим користувач володіє, наприклад, електронний ключ або платіжна картка) і біометрія (щось, що є фізичною характеристикою користувача, наприклад, відбиток пальця або скан обличчя).

Приклади багатофакторної аутентифікації включають комбінацію різних факторів. Наприклад, користувач може одночасно підтвердити знання секрету і пред'явити об'єкт, що належить йому. Типовими варіантами є електронний ключ у

поєднанні з паролем, де електронний ключ є фактором володіння, а пароль – фактором знання. Інший приклад – відбиток пальця і пароль, що поєднує фізичну ознаку користувача з його знанням.

Одним із найпоширеніших прикладів двофакторної аутентифікації є використання банкомату. Користувач вставляє платіжну картку, яка підтверджує, що він володіє необхідним об'єктом, і вводить PIN-код, який свідчить про знання секретної інформації. Лише після цього користувач отримує доступ до свого банківського рахунку.

Багатофакторна аутентифікація значно підвищує рівень безпеки інформаційних систем, оскільки зломиснику необхідно отримати доступ до декількох факторів одночасно, що ускладнює здійснення несанкціонованого доступу і забезпечує надійний захист даних.

Для реалізації способів аутентифікації необхідний первинний контакт між суб'єктом і об'єктом, під час якого відбувається обмін автентифікаторами. Такий обмін забезпечує взаємне підтвердження достовірності сторін. Проте в ряді випадків цей контакт може бути ускладнений або неможливий. Наприклад, у системах електронного бізнесу B2C (business-to-consumer) фізична взаємодія між клієнтом і постачальником послуг або товарів часто відсутня.

У таких ситуаціях найбільш ефективним є застосування аутентифікації на основі рекомендацій або гарантій від довіреного посередника. Одним із поширених прикладів є використання сертифікатів або квитків, які надають додатковий рівень довіри. Найбільш відомими в цій сфері є сертифікати формату X.509. Ці сертифікати зв'язують клієнта з його ідентифікатором і підтверджують його достовірність за допомогою цифрового підпису, що належить довіреному центру сертифікації.

Центр сертифікації виступає як авторитетна третя сторона, яка гарантує, що наданий сертифікат є справжнім і належить конкретному суб'єкту. Це дозволяє сторонам у системі електронного бізнесу встановити довіру без прямого контакту, забезпечуючи при цьому високий рівень безпеки та надійності. Використання таких механізмів є невід'ємною частиною сучасних інформаційно-комунікаційних систем, особливо у сфері електронної комерції, де необхідно гарантувати ідентичність клієнтів і захист їхніх даних.

Система аутентифікації, хоч і є важливою складовою забезпечення інформаційної безпеки, не позбавлена уразливостей. Однією з найбільших загроз є внутрішній порушник — суб'єкт, який вже успішно пройшов процедури аутентифікації та авторизації. Такий порушник, маючи законний доступ до системи, може здійснювати дії, що порушують правила безпеки або навіть шкодять інформаційним ресурсам підприємства.

Ще однією серйозною загрозою є можливість присвоєння порушниками чужих засобів аутентифікації, таких як паролі, токени чи інші автентифікатори. Заволодіння цими засобами дозволяє зловмиснику видавати себе за іншого користувача, обходячи систему аутентифікації. Це може статися через соціальну інженерію, фізичний доступ до пристроїв користувача, витік інформації або технічні уразливості системи.

Тому для підвищення ефективності аутентифікації важливо впроваджувати додаткові заходи захисту. До них належать багатофакторна аутентифікація, контроль поведінкових характеристик користувачів, моніторинг доступу в реальному часі, а також постійне оновлення та удосконалення систем захисту від кібератак. Такі заходи допомагають значно зменшити ризики, пов'язані з внутрішніми та зовнішніми загрозами, і забезпечити більш високий рівень безпеки інформаційних систем.



Система аутентифікації, хоча і є важливою складовою інформаційної безпеки, має свої обмеження. Паролі можуть бути підглянуті, викрадені або перехоплені під час передачі. Унікальні об'єкти аутентифікації, такі як електронні ключі чи токени, також можуть бути вкрадені або навіть відібрані силою. Абсолютно надійна аутентифікація людини залишається теоретично недосяжною метою, адже не існує автентифікатора, який зі стовідсотковою надійністю підтверджував би автентичність особи. Наприклад, паролі можна перехопити, електронні ключі — вкрати, а біометричні дані, такі як відбитки пальців, підробити.

Через ці обмеження аутентифікація сама по собі не може повністю захистити інформаційну систему від дій порушника. Тому її ефективність має бути підкріплена іншими заходами, такими як багатофакторна аутентифікація, моніторинг активності користувачів, обмеження прав доступу та регулярне оновлення засобів захисту.

У багатьох випадках односторонньої аутентифікації недостатньо, і тоді використовують двосторонню (взаємну) аутентифікацію. Наприклад, користувач, який надсилає запит до корпоративного вебсервера, повинен довести свою легальність, але також переконатися, що має справу саме з

офіційним сервером свого підприємства, а не зі шкідливим ресурсом. У такій взаємодії як сервер, так і клієнт проходять процедуру взаємної аутентифікації.

Подібний підхід застосовується і в комунікаціях між пристроями. Наприклад, під час встановлення сеансу зв'язку між двома пристроями передбачаються процедури взаємної аутентифікації, що дозволяє гарантувати безпечний обмін даними і виключити підробку або підміну одного з учасників сеансу. Це особливо важливо в умовах використання відкритих або незахищених каналів зв'язку, де загрози перехоплення чи підміни інформації є найбільш актуальними.

9.4. ПАРОЛЬНА АУТЕНТИФІКАЦІЯ

Парольна аутентифікація є одним із найпоширеніших методів перевірки автентичності суб'єктів в інформаційно-комунікаційних системах. Вона базується на використанні секретного коду (пароля), який відомий лише користувачу і системі. Пароль слугує ключем, що підтверджує, що користувач має право доступу до відповідних ресурсів.

Процес паролльної аутентифікації включає кілька етапів. Спочатку користувач вводить свій ідентифікатор (наприклад, ім'я користувача) і пароль. Система перевіряє відповідність введених даних збереженим у базі даних. Якщо пароль збігається з тим, що асоційований із цим ідентифікатором, користувач отримує доступ до системи. У протилежному випадку доступ забороняється. Парольна аутентифікація залишається актуальним методом, але для підвищення безпеки часто поєднується з іншими механізмами, такими як багатофакторна аутентифікація або використання апаратних токенів. У разі використання багатофакторної аутентифікації, після введення правильного пароля користувач повинен надати додатковий фактор, наприклад, код, надісланий на мобільний пристрій або біометричні дані. Це дозволяє значно підвищити рівень безпеки, оскільки навіть у разі компрометації пароля доступ до системи буде заблоковано. Такі додаткові методи підтвердження значно знижують ймовірність несанкціонованого доступу. З часом парольна аутентифікація може бути замінена або доповнена більш сучасними методами, такими як використання біометрії або апаратних пристроїв для аутентифікації.

Парольна аутентифікація є найпростішою формою аутентифікації. Вона побудована на порівнянні *еталонного зразка аутентифікаційної інформації*, що зберігається в системі з тією інформацією, що надається користувачем при вході в систему. Якщо дані збігаються, то робиться висновок про справжність користувача. Якщо ж

вони розрізняються, то робиться висновок про те, що пароль введений невірно, і отже, процедура аутентифікації не пройдена.

Прийнята в організації політика безпеки, як правило, передбачає такі обов'язкові параметри використання паролів аутентифікації:

- ❖ складність і мінімальна довжина пароля;
- ❖ максимальний термін дії пароля (секрет не може зберігатися таємно вічно);
- ❖ розбіжність пароля з ідентифікатором та ім'ям користувача, під яким він зареєстрований в системі;
- ❖ неповторюємість паролів одного користувача.

При правильному використанні паролів аутентифікація може забезпечити прийнятний рівень безпеки. Однак ефективність паролів залежить від їх складності та регулярного оновлення. Слабкі паролі, такі як прості комбінації або ті, що використовують особисту інформацію, можуть стати вразливими до атак, таких як брутфорс або фішинг. Для покращення безпеки важливо впроваджувати політики, що вимагають використання складних паролів, а також періодичної їх зміни. Крім того, інтеграція додаткових методів аутентифікації, таких як двоетапна перевірка або біометрія, може значно підвищити надійність системи.



Однак завжди слід пам'ятати, що це найслабший засіб перевірки автентичності:

1. Паролі з самого початку можуть не зберігатися в таємниці, оскільки мають стандартні значення, вказані в документації, і далеко не завжди після установки системи проводиться їх зміна (administrator, root, system, supervisor).

2. Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на якийсь час власника пароля, а таємниця, яку знають двоє, це вже не таємниця.

3. Введення пароля можна підглянути візуально або перехопити, використовуючи клавіатурні шпигуни.

4. Пароль можна підібрати «методом грубої сили»- повним перебором можливих паролів.

5. Пароль можна вгадати, добре знаючи користувача.

6. Пароль також можна перехопити, використовуючи програму-аналізатор пакетів мережі.

Наступні заходи дозволяють значно підвищити надійність захисту пароля:

- ➔ накладення обмежень на складність і довжину пароля (пароль повинен бути не менше 6–8 символів і повинен містити літери, цифри, знаки пунктуації і т. п.);
- ➔ управління терміном дії пароля, його періодична зміна;
- ➔ обмеження числа невдалих спроб введення пароля (це ускладнює застосування «методу грубої сили»);
- ➔ обмеження доступу до файла пароля;
- ➔ зберігання і передавання пароля у зашифрованому вигляді.

У більшості випадків для пароліної аутентифікації використовуються багаторазові паролі.

Для підвищення безпеки пароліної системи аутентифікації на противагу багаторазовим пароліам, використовуються так звані **одноразові паролі**, тобто паролі, що дійсні тільки для одного сеансу аутентифікації.

Їх основна перевага – це даремність для порушника перехоплення або викрадення вже використаного пароля. Такий пароль діє тільки для одного сеансу аутентифікації, і його не можна застосувати колись потім, якщо його випадково підслухати, підглянути, перехопити. Одноразові паролі використовуються для забезпечення безпеки електронних платежів, доступу в інтернет-банк, доступу, наприклад, в особистий кабінет на сайтах різних організацій, а також можуть використовуватися для посилення аутентифікації на основі багаторазового пароля.

Наприклад, на багатьох популярних сайтах зараз введена система прив'язки облікового запису до мобільного телефону, на який висилається одноразовий пароль у разі, якщо, наприклад, вхід у систему відбувається з нового фізичного пристрою. В цьому випадку аутентифікація на основі багаторазового пароля може бути посилена. Одноразові паролі, як правило, надаються користувачеві або за допомогою коротких повідомлень на мобільний телефон, або друкуються на чеках в банкоматах.

Для забезпечення надійності одноразових паролів можна використовувати такий прийом: кожний наступний одноразовий пароль може залежати від попередніх, і в цьому випадку тільки правильна їх послідовність дозволяє користувачеві успішно пройти їх аутентифікацію. Якщо хоча б один з одноразових паролів буде перехоплений, то порушник вже не зможе пройти аутентифікацію від імені легального користувача.

Іншим варіантом забезпечення надійності одноразових паролів є синхронізація вироблення паролів з системою аутентифікації. У цьому випадку разом з одноразовим паролем передається значення часу, коли цей пароль був вироблений. Еталонний зразок виробляється залежно від того ж часу. Якщо синхронізація вірна, то паролі повинні збігтися, пароль і його еталонне значення.



Перевагою пароліної аутентифікації є її інтелектуальна складова, адже процес вибору та запам'ятовування пароля безпосередньо пов'язаний з розумовими здібностями та свідомістю користувача. Це робить пароліний механізм зручним у випадках, коли потрібно підтвердити ідентифікацію людини, оскільки пароль є чимось унікальним для кожного користувача і створюється з урахуванням особистих уподобань або значущих даних. Однак важливо, щоб паролі зберігалися виключно в «людській» пам'яті користувачів, оскільки запис паролів на матеріальних носіях може призвести до їх викрадення або втрати, що створює додаткові ризики для безпеки. Таким чином, захист паролем покладається на здатність користувача тримати його в пам'яті, що дозволяє зберігати певний рівень безпеки, якщо користувач уважно ставиться до його збереження.

9.5. АУТЕНТИФІКАЦІЯ НА ОСНОВІ PIN-КОДУ

Аутентифікація на основі PIN-коду є одним із найпоширеніших способів підтвердження ідентичності користувача в інформаційно-комунікаційних системах. PIN-код (персональний ідентифікаційний номер) являє собою короткий набір цифр, який користувач має ввести для отримання доступу до системи або ресурсу. Цей метод є зручним, оскільки PIN-коди зазвичай прості для запам'ятовування та швидкого введення. Однак його безпека може бути знижена, якщо PIN-код є занадто простим або вразливим до атак, таких як спроби перебору. Щоб підвищити рівень безпеки, багато систем використовують додаткові механізми, наприклад, обмеження кількості спроб введення неправильного PIN-коду або поєднання з іншими методами аутентифікації. Інтеграція PIN-коду з біометричними даними чи паролями може зробити цей метод ще більш надійним.

Найбільш поширеним методом аутентифікації власника пластикової картки є введення секретного числа, яке зазвичай називають **PIN-кодом** (*Personal Identification Number – персональний ідентифікаційний код*) або іноді CHV (*CardHolder Verification*).

Картки можуть бути втрачені, вкрадені або підроблені, що створює ризики для безпеки користувачів. У таких випадках захист від несанкціонованого доступу забезпечується завдяки секретному значенню PIN-коду, яке використовується для аутентифікації користувача. Важливо, щоб PIN-код залишався відомим тільки законному власнику картки, оскільки доступ до системи або рахунку може бути отриманий тільки за умови правильного введення цього секретного значення. Тому важливо, щоб користувачі уважно ставилися до збереження свого PIN-коду, а також регулярно його змінювали, щоб зменшити ризики витоку або крадіжки цього секрету.

Значення PIN-коду повинно бути надійно захищене протягом усього терміну дії картки. Для цього користувачам рекомендується не записувати PIN на самій картці або в легкодоступних місцях. Водночас системи можуть запроваджувати додаткові заходи безпеки, такі як ліміти на кількість неправильних спроб введення PIN-коду, блокування картки після певної кількості помилок або використання багатофакторної аутентифікації для підвищення рівня захисту.

Довжина **PIN-коду** повинна бути досить великою, щоб мінімізувати ймовірність визначення правильного **PIN-коду** методом проб і помилок. З іншого боку, довжина **PIN-коду** повинна бути досить короткою, щоб дати можливість власникам карток запам'ятати його значення. Згідно з рекомендацією стандартів безпеки, **PIN-код** повинен містити від 4 до 12 буквено-цифрових символів. Однак в більшості випадків введення нецифрових символів технічно неможливо, оскільки доступна тільки цифрова клавіатура. Тому, зазвичай, **PIN-код** являє собою чотирирозрядне число, кожна цифра якого може приймати значення від 0 до 9. Попри це, для підвищення безпеки, рекомендується використовувати максимально складні та непередбачувані комбінації цифр, уникати простих шаблонів, таких як "1234" або "0000". Щоб уникнути несанкціонованого доступу, також важливо обмежити кількість спроб введення неправильного PIN-коду, після чого доступ до системи може бути тимчасово заблокований або вимагати додаткової аутентифікації. Крім того, регулярна зміна PIN-коду є важливою практикою для забезпечення довготривалої безпеки. Для додаткової надійності рекомендується поєднувати PIN-код з іншими методами аутентифікації, такими як двоетапна перевірка або біометрія.

PIN-код вводиться за допомогою клавіатури термінала або комп'ютера і потім відправляється на картку. Картка порівнює отримане значення **PIN-коду** з еталонним значенням, збереженим в картці, і відправляє результат порівняння на термінал.

Використовуються два основні способи перевірки PIN-коду: *неалгоритмічний і алгоритмічний*.

Неалгоритмічний спосіб перевірки PIN-коду

Неалгоритмічний спосіб перевірки PIN-коду полягає у використанні простого механізму порівняння введеного коду з попередньо збереженим значенням у захищеній базі даних. На відміну від алгоритмічних методів, тут не застосовуються складні математичні обчислення чи генерація кодів за допомогою формул. У цьому способі PIN-код зберігається у вигляді хешу або іншого захищеного формату, і під час перевірки система порівнює отримане хеш-значення з тим, яке було попередньо збережене.

Цей метод має кілька важливих переваг. По-перше, він є простим у реалізації, що робить його популярним для впровадження у багатьох інформаційних системах. По-друге, відсутність складних алгоритмів знижує ризик виникнення уразливостей через помилки в їх реалізації. По-третє, метод є універсальним і може працювати з будь-якими типами PIN-кодів, незалежно від їх довжини чи формату.

Однак, неалгоритмічний спосіб перевірки також має свої недоліки. Одним із головних є необхідність безпечного зберігання PIN-кодів у базі даних. Навіть якщо коди зберігаються у хешованому вигляді, у разі компрометації бази даних зломисники можуть отримати ці хеші та спробувати підібрати коди, використовуючи атаки типу brute force. Крім того, для кожного користувача потрібне окреме збереження хешу його PIN-коду, що може збільшувати навантаження на базу даних у великих системах.

Наприклад, у процесі аутентифікації користувач вводить свій PIN-код, який система хешує (наприклад, використовуючи алгоритм SHA-256). Отриманий хеш порівнюється зі значенням у базі даних. Якщо хеші співпадають, користувач отримує доступ до системи; якщо ні – доступ блокується. Для підвищення безпеки рекомендується використовувати сучасні алгоритми хешування з додаванням сілових значень (salt), які ускладнюють підбір хешу навіть за умов компрометації бази.

Таким чином, неалгоритмічний спосіб перевірки PIN-коду є ефективним для багатьох практичних задач, але потребує додаткових заходів безпеки для захисту бази даних та зменшення ризиків компрометації. Для підвищення безпеки такі системи повинні включати шифрування PIN-кодів у базах даних, а також використання методів детекції несанкціонованого доступу. Крім того, регулярні аудити та перевірка вразливостей можуть допомогти виявити потенційні загрози та своєчасно вжити заходів щодо їх усунення.

Алгоритмічний спосіб перевірки PIN-коду

Алгоритмічний спосіб перевірки PIN-коду полягає в використанні спеціальних математичних операцій або криптографічних алгоритмів для перевірки коректності введеного коду без необхідності зберігання самого коду в системі. Такий підхід дозволяє значно підвищити рівень безпеки, оскільки система працює не з фактичним PIN-кодом, а з його хешованим або зашифрованим значенням. Цей метод знижує ймовірність компрометації даних, оскільки навіть у разі витоку даних з бази не можна буде отримати сам PIN-код.

Принцип роботи алгоритмічного методу полягає в тому, що при введенні користувачем PIN-коду система використовує певний алгоритм хешування або шифрування, щоб перетворити введену послідовність цифр на унікальне значення, яке не є прямим відображенням самого коду. Наприклад, один з найбільш поширених способів — це хешування, при якому PIN-код перетворюється в унікальний хеш-код за допомогою алгоритму, наприклад SHA-256 або bcrypt. Цей хеш зберігається в базі даних, замість того щоб зберігати сам PIN-код. Коли користувач намагається зайти в систему, він вводить свій PIN-код, система знову його хешує і порівнює з збереженим хешем. Якщо значення співпадають, користувач отримує доступ.

Для додаткового підвищення безпеки часто використовується метод додавання солі (salt) до PIN-коду перед його хешуванням. Сіль — це випадкові дані, які додаються до коду перед його хешуванням, що ускладнює зломисникам створення таблиць для зламу. Крім того, в деяких випадках можуть використовуватися комбіновані алгоритми, що дозволяють підвищити рівень захисту.

Однією з головних переваг цього методу є те, що система не зберігає сам PIN-код, а лише його зашифровану або хешовану версію. Це робить систему більш стійкою до атак, оскільки навіть якщо зломисник отримає доступ до бази даних, він не зможе відновити справжні PIN-коди. Крім того, алгоритмічний метод перевірки дозволяє швидко обробляти великі обсяги запитів, не знижуючи продуктивності системи.

Проте цей метод має й свої недоліки. Якщо криптографічні алгоритми реалізовані некоректно, то система може бути вразливою до атак, таких як атаки на слабкі алгоритми хешування або на реалізацію самого алгоритму. Крім того, використання складних алгоритмів може призвести до підвищених вимог до обчислювальних ресурсів, що може негативно вплинути на продуктивність системи.

Загалом, алгоритмічний метод перевірки PIN-коду є одним з найбільш ефективних способів захисту даних, оскільки він дозволяє значно

зменшити ризики їх компрометації. Однак важливо правильно реалізувати криптографічні алгоритми і впроваджувати додаткові механізми захисту, щоб забезпечити належний рівень безпеки.



Перевагою аутентифікації на основі PIN-коду є її простота та швидкість використання. PIN-код є коротким числовим кодом, який легко запам'ятовується, але при цьому забезпечує базовий рівень захисту при доступі до різних систем або об'єктів. Важливою перевагою є те, що цей метод є надійним за умови використання достатньо складних кодів та обмежень на кількість спроб введення неправильного PIN-коду, що унеможливорює злом системи за допомогою брутфорс-атак.

Аутентифікація за допомогою PIN-коду зручна для користувачів, оскільки їй не потрібно спеціального обладнання чи складних налаштувань, що робить цей метод широко доступним для використання в банківських картках, мобільних пристроях та інших системах. У разі втрати картки або її крадіжки, без PIN-коду доступ до ресурсів залишається неможливим, що додає додатковий рівень захисту.

Завдяки використанню PIN-коду можна поєднати простоту запам'ятовування з достатнім рівнем безпеки, що робить цей метод зручним та доступним для багатьох користувачів.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 9

1. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
3. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
4. V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

5. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.
6. F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021).
7. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 374–391.
8. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.
9. Довженко, Н., Мазур, Н., Костюк, Ю., & Рзаєва, С. (2024). Інтеграція iot та штучного інтелекту в інтелектуальні транспортні системи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 430–444
10. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.
11. H. Shevchenko, et al., Information Security Risk Analysis SWOT, Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021) 309-317.
12. Жданова, Ю., Шевченко, С., Спасітелева, С., & Сокульский, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.
13. O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.
14. Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 468–486.

15. A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.Крючкова, Л., & Стеблина, О. (2024).
16. Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 338–347.
17. D. Virovets, et al., Ways of Interaction of Autonomous Economic Agents in Decentralized Autonomous Organizations, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 182–190.
18. Марценюк, М., Козачок, В., Богданов, О., Іосіфов, Є., & Бржевська, З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 148–155.
19. A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.
20. D. Shevchuk, et al., Designing Secured Services for Authentication, Authori-zation, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.
21. M. TajDini, et al., Brainwave-based Authentication using Features Fusion, Comput. Secur. 129, no. 103198 (2023) 1–11.

РОЗДІЛ 10 ВИДИ АУТЕНТИФІКАЦІЇ



10.1. Апаратна аутентифікація

10.2. Аутентифікація за допомогою біометричних даних

10.3. Аутентифікація на основі цифрових сертифікатів

10.4. Централізовані системи аутентифікації. Концепція єдиного логічного входу

10.5. Система Kerberos

10.6. Централізований контроль віддаленого доступу

10.1. АПАРАТНА АУТЕНТИФІКАЦІЯ

Апаратна аутентифікація є одним із найефективніших способів підтвердження особи користувача, який базується на використанні фізичних пристроїв або спеціалізованого обладнання, що зберігають або генерують унікальні дані для перевірки особи. Цей метод аутентифікації відзначається високою надійністю, оскільки він залежить від фізичних елементів, таких як смарт-карти, USB-токени або біометричні пристрої, що важко підробити або викрасти без фізичного доступу до них.

Один із найпоширеніших варіантів апаратної аутентифікації — це смарт-карти, які містять вбудовані чіпи з криптографічними ключами для підтвердження особи користувача. Для аутентифікації користувач вставляє картку в спеціальний зчитувальний пристрій, що дозволяє перевірити її дійсність і доступ. Ще одним популярним пристроєм є USB-токени, які підключаються до USB-порту комп'ютера або мобільного пристрою, генеруючи одноразові паролі або містять криптографічні ключі для підтвердження аутентифікації. Крім того, біометричні пристрої, такі як

зчитувачі відбитків пальців, сітківки ока чи розпізнавання обличчя, також використовуються для апаратної аутентифікації. Ці пристрої дозволяють зчитувати унікальні фізіологічні ознаки, що гарантує високу ступінь захисту і унікальність кожної особи.

Окрім того, використання RFID-чипів для безконтактної аутентифікації є ще одним прикладом апаратної аутентифікації, де користувач має спеціальну картку або мітку, яка передає дані на зчитувальний пристрій. Апаратна аутентифікація забезпечує високий рівень безпеки, оскільки фізичні пристрої важко підробити, і часто поєднується з іншими методами аутентифікації для створення багатофакторних систем, що дає додатковий рівень захисту.

В інформаційно-комунікаційних системах (ІКС) з високими вимогами до захищеності інформації проблеми, пов'язані з недоліками пароліної аутентифікації, можуть бути ефективно усунені шляхом використання апаратних пристроїв аутентифікації. Ці пристрої, такі як смарт-карти, USB-токени, біометричні зчитувачі або інші засоби апаратної аутентифікації, відносяться до категорії персональних засобів аутентифікації. Вони надають можливість однозначної ідентифікації суб'єкта за принципом володіння автентифікатором, що істотно підвищує рівень безпеки в порівнянні з традиційними паролями. Відсутність фізичного доступу до таких пристроїв або їх підробка є складним завданням для зловмисників, що робить ці засоби аутентифікації важливим компонентом для захисту інформації в середовищах, де безпека є критично важливою. Апаратні пристрої аутентифікації, як правило, використовуються в комбінації з іншими методами захисту, забезпечуючи додатковий рівень безпеки завдяки багатофакторній аутентифікації.

Апаратні автентифікатори, звані також апаратними ключами, належать до фактора аутентифікації «Я маю».

Пристрої апаратної аутентифікації діляться на дві групи:

- 1) пасивні (зберігається один фіксований автентифікатор);
- 2) активні (можуть генерувати різні автентифікатори).

Пасивні пристрої аутентифікації

Пасивні пристрої аутентифікації — це тип пристроїв, які не вимагають активних дій від користувача для здійснення аутентифікації. Ці пристрої не мають власного джерела енергії та не потребують фізичного контакту для обміну інформацією з системою. Зазвичай вони відправляють дані лише у відповідь на запит або при наближенні до відповідного зчитувального пристрою. Такі пристрої широко застосовуються в системах

контролю доступу і використовують технології безконтактної передачі даних. До пасивних пристроїв аутентифікації належать, наприклад, RFID-картки, які працюють на основі радіочастотної ідентифікації, а також безконтактні картки, що використовують радіохвилі для передачі даних. Такі картки не потребують контакту з зчитувальним пристроєм, достатньо просто наблизити їх до нього для підтвердження особи користувача. Крім того, існують біометричні карти, які не містять джерела енергії і передають необхідну інформацію через електричні сигнали при наближенні до зчитувача. Пасивні пристрої мають значну перевагу в зручності використання, оскільки вони не вимагають великих зусиль від користувача та знижують ймовірність помилок через людський фактор. Проте вони можуть мати меншу безпеку в порівнянні з активними пристроями, оскільки не мають додаткових засобів захисту, таких як шифрування чи перевірка на рівні самого пристрою.

Приклади пасивних пристроїв аутентифікації:

- ➔ механічні ключі;
- ➔ пластикові картки з магнітною смугою;
- ➔ елементи Touch Memory (iButton);
- ➔ безконтактні картки Proximity і RFID-брелоки.



Рис. 10.1. Елемент (а) та пристрій для читання TouchMemory (б)
Джерело: [1-7]



Рис. 10.2. RFID-брелок (а), програматор (б) та пристрій для читання (в)
Джерело: [1-7]

Для аутентифікації користувача за допомогою картки пам'яті достатньо надати картку зчитувачу та ввести свій PIN-код. Якщо введений PIN-код співпадає з даними, що зберігаються на магнітній смужі картки, користувач буде успішно автентифікований. Це забезпечує зручний і швидкий процес аутентифікації, де картка служить ідентифікатором, а PIN-код додає рівень безпеки.

Однак існують певні недоліки такої системи. Один з головних мінусів — необхідність спеціального зчитувача для обробки картки, що збільшує вартість рішення. Встановлення зчитувачів на кожен комп'ютер в компанії може бути економічно не вигідним, особливо якщо мережа великої організації має багато робочих станцій. Крім того, процес виготовлення карток пам'яті також не є дешевим, оскільки включає необхідність «прошивки» кожної картки, що додає витрати як на виробництво, так і на адміністрування системи.

Автентифікатори *iButton* мають ПЗУ, що містить 64-розрядний код, однопровідний порт і схему, яка реалізує логіку управління. При зіткненні зі зчитувачем ідентифікатор *iButton* передає йому унікальний номер, зчитувач перевіряє його і ініціює сеанс обміну даними з ідентифікатором.

Радіочастотні ідентифікатори, або *RFID-ідентифікатори* (*radio-frequency identification, RFID*), виготовляються у вигляді пластикового брелока, або картки що не мають ніяких зовнішніх інформаційних виходів-входів. Всередині пластикового корпусу знаходиться інтегральна схема, а також антена, призначена для передачі і прийому радіосигналів. Зчитувач радіочастотних сигналів вбудовується в електронні замки і постійно випромінює радіочастотний сигнал, який приймається антеною брелока і передається інтегральній схемі для випромінювання автентифікаційних даних в напрямку зчитувача. Крім того, *RFID-ідентифікатор* дозволяє службі безпеки відслідковувати переміщення його власника по всіх приміщеннях, оснащених відповідними датчиками

Недолік пасивних пристроїв аутентифікації полягає в більшій простоті копіювання автентифікаційної інформації, що зберігається на них (в порівнянні з активними пристроями).

Активні пристрої аутентифікації

Активні пристрої аутентифікації — це апаратні засоби, які не лише зберігають інформацію для ідентифікації, але й активно взаємодіють з системою під час процесу аутентифікації. Ці пристрої зазвичай використовують криптографічні методи для захисту переданих даних і для підтвердження особистості користувача. Вони забезпечують високий

рівень безпеки, оскільки інформація зберігається не просто на пристрої, а й використовується для створення одноразових паролів або цифрових підписів.

Типовими прикладами активних пристроїв є смарт-картки, USB-токени та криптографічні ключі. Смарт-картки можуть містити вбудовані чіпи, які генерують одноразові паролі (OTP) або зберігають сертифікати для цифрового підпису. USB-токени зазвичай використовуються для двофакторної аутентифікації, де користувач підтверджує свою особистість, вставляючи пристрій у комп'ютер і вводячи PIN-код або пароль.

Перевагою активних пристроїв є високий рівень безпеки, оскільки вони складніші для підробки чи викрадення, ніж пасивні пристрої, і часто використовують додаткові криптографічні механізми для захисту даних. Водночас їх використання може бути зручним для користувачів, які часто працюють з важливими або конфіденційними даними, оскільки ці пристрої забезпечують більш складну аутентифікацію, яка значно ускладнює злоумисникам доступ до системи.

Приклади активних пристроїв аутентифікації:

- ➔ смарт-картки (пластикові картки з мікропроцесором);
- ➔ USB-токени (USB-ключі);
- ➔ OTP-токени (генератори одноразових паролів);
- ➔ гібридні токени (генератори одноразових паролів).



Рис. 10.3. Смарт-картка (а) і пристрій для читання (б, в)
Джерело: [1-7]



Рис. 10.4. USB-токен аутентифікації
Джерело: [1-7]

Основною відмінністю смарт-карток від звичайних карт пам'яті є їх здатність до обробки інформації. Якщо звичайна карта пам'яті лише зберігає дані, без можливості їх обробки, то смарт-картка має вбудоване апаратне і програмне забезпечення, яке дозволяє не тільки зберігати, але й виконувати певні операції з інформацією. Це може включати криптографічну обробку даних, генерацію одноразових паролів, перевірку підписів чи інші операції, що забезпечують більш високий рівень безпеки.

Завдяки своїй інтеграції з оброблювальними чіпами та можливості виконувати складні обчислення, смарт-картки можуть забезпечувати захист даних через використання криптографії для збереження та передачі конфіденційної інформації. Крім того, вони забезпечують більш високий рівень захисту від підробки та несанкціонованого доступу порівняно з картами пам'яті, оскільки обробка інформації здійснюється безпосередньо на самій картці, а не на сторонньому обладнанні.



Рис. 10.5. OTP-токени. Генератори одноразових паролів
Джерело: [1-7]

Це робить смарт-картки особливо корисними в таких сферах, як фінансові послуги, доступ до захищених інформаційних систем та використання в державних і корпоративних середовищах, де важливий високий рівень безпеки та конфіденційності.

Смарт-картки можуть бути як **контактними**, так і **безконтактними**.

Контактні смарт-картки

Контактна смарт-картка має золоті контактні площадки на лицьовій стороні, і коли така картка вставлена в зчитувач, ці контактні площадки стикаються з відповідними електричними контактами в зчитувачі, які призначені для електричного живлення компонентів смарт-картки і передачі необхідної для аутентифікації інформації. Зазвичай контактні смарт-картки використовуються для зберігання особистих даних

користувача, таких як шифрувальні ключі, паролі або цифрові сертифікати, що дозволяє забезпечити високий рівень безпеки при доступі до захищених систем. Після встановлення з'єднання між картою і зчитувачем, дані з картки можуть бути використані для аутентифікації користувача, а також для здійснення операцій, що вимагають додаткового підтвердження ідентичності. Важливим аспектом є те, що контактні смарт-картки є відносно вразливими до фізичних пошкоджень або несанкціонованого доступу, тому часто використовуються разом з додатковими заходами безпеки, такими як PIN-коди або біометричні технології.

Безконтактні смарт-картки

У *безконтактних смарт-картках* передбачається радіочастотний блок із вбудованою антеною, яка прокладена по периметру картки. Антена слугує як для передачі автентифікаційних даних, так і для добування енергії з електромагнітного поля, випромінюваного зчитувачем. Смарт-картка містить процесор, ПЗП, в якому зберігається криптографічна програма, ОЗП, а також програмований ПЗП, що містить змінювані дані власника картки. Наявність у них пам'яті й інтегральних схем дозволяє організувати роботу алгоритмів шифрування безпосередньо в самій картці для безпечної аутентифікації, що використовується в масштабах всієї компанії. Зчитувачі таких карток можуть мати найрізноманітніше конструктивне виконання: наприклад, вони можуть бути вбудовані в клавіатуру або в корпус комп'ютера.

Токени

USB-ключі, або *USB-токени*, підключаються безпосередньо до USB-порту комп'ютера, виключаючи необхідність використання дорогих зчитувальних пристроїв.



Рис. 10.6. Гібридні токени

Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity>

Кожен USB-ключ має унікальний номер, присвоєний виробником, має захист від зламу, а деякі і мініклавіатуру для вводу PIN-коду, що

дозволить реалізувати вже двофакторну аутентифікацію. **ОТР-токени (One-Time Password tokens)** призначені для забезпечення додаткового рівня безпеки через використання одноразових паролів. Вони активно використовуються в інформаційно-комунікаційних системах (ІКС) з автономним сервером аутентифікації. Основним принципом роботи таких токенів є генерування паролів, які можна використовувати лише один раз, що значно знижує ймовірність несанкціонованого доступу до системи.

У пристрої ОТР-токена зберігається таємний ключ користувача, копія якого зберігається на сервері аутентифікації. Коли користувач хоче отримати доступ до системи, він вводить одноразовий пароль, згенерований ОТР-токеном. Сервер аутентифікації, використовуючи збережений таємний ключ і ту ж схему генерації паролів, генерує одноразовий пароль і порівнює його з тим, що ввів користувач. Якщо паролі співпадають, доступ до системи надається.

ОТР-токени використовують складні алгоритми для генерації паролів, що забезпечує високий рівень безпеки. Крім того, оскільки паролі використовуються лише один раз, навіть якщо зломисник перехопить одноразовий пароль, він не зможе його повторно використати. Це робить ОТР-токени ефективним засобом захисту від атак, що спираються на зловживання паролями, таких як фішинг або перехоплення даних при передаванні.

Гібридні токени є поєднанням кількох методів аутентифікації, що дозволяє забезпечити більш високий рівень безпеки при підтвердженні особи користувача в інформаційно-комунікаційних системах (ІКС). Вони поєднують різні механізми аутентифікації, такі як одноразові паролі, біометричні дані, криптографічні ключі чи інші методи, що підвищують ефективність та надійність перевірки користувача. Одним із типових прикладів гібридних токенів є комбінація смарт-картки з біометрією або PIN-коду з одноразовими паролями, які генеруються за допомогою ОТР-токенів. Це дозволяє знизити уразливості, властиві кожному окремому методу, і значно покращити рівень захисту. Наприклад, гібридні токени можуть включати комбінацію смарт-картки та PIN-коду, де смарт-картка містить криптографічний ключ, а для її використання необхідно ввести PIN-код. Це підвищує безпеку, оскільки навіть у разі втрати картки без правильного PIN-коду доступ неможливий. Іншим прикладом є поєднання біометрії та одноразових паролів, де для доступу користувач вводить одноразовий пароль, що генерується ОТР-токеном, а також проходить перевірку через біометричні дані, наприклад, відбиток пальця або розпізнавання обличчя. Також може використовуватися поєднання смарт-картки з біометрією, де для підтвердження особи перевіряється не тільки картка, а й біометричні параметри користувача. Гібридні токени

забезпечують високий рівень захисту, оскільки зломисникам набагато складніше подолати декілька рівнів перевірки одночасно. Ці системи є популярними у сферах, де необхідно забезпечити високу ступінь безпеки, таких як фінансові установи, державні органи та корпоративні мережі з чутливими даними.

Переваги застосування апаратної ідентифікації

Головною перевагою застосування апаратної ідентифікації є досить висока надійність, можливість використання пристроїв аутентифікації для вирішення додаткових завдань (активні пристрої аутентифікації – це мінікомп'ютери). Завдяки їх конструкції і можливості інтеграції з іншими системами безпеки, такі пристрої можуть використовуватися для комплексного контролю доступу та моніторингу. Вони також можуть забезпечити значно більший рівень захисту, ніж звичайні паролі або ПІН-коди, оскільки кожен пристрій має унікальні характеристики, які неможливо легко підробити. Крім того, апаратні пристрої аутентифікації можуть забезпечувати високий рівень захисту від атак на основі соціальної інженерії або фішингу, оскільки зломисники не можуть безпосередньо отримати доступ до фізичного пристрою. Однак, для досягнення оптимального рівня безпеки важливо комбінувати апаратну аутентифікацію з іншими методами, такими як біометрія або додаткові програмні засоби захисту. Це дозволяє створити багаторівневу систему, яка ефективно протистоїть різноманітним загрозам.

Недоліки застосування апаратної ідентифікації

Загальна проблема використання апаратних пристроїв аутентифікації – це втрата, або незаконне привласнення пристрою і відповідно застосування його зломисником. Вирішення цієї проблеми може бути в використанні другого фактора для аутентифікації, наприклад, PIN-коду. Іншим підходом є застосування біометричних даних як додаткового рівня перевірки, що значно ускладнює несанкціоноване використання пристрою. Крім того, для зниження ризиків важливою є постійна зміна паролів та PIN-кодів, а також їх зберігання в зашифрованому вигляді. Також ефективним заходом є активне використання механізмів відстеження та блокування пристроїв у разі їх втрати або викрадення. Ці заходи разом забезпечують більш високий рівень захисту в системах, де застосовуються апаратні засоби аутентифікації.

Другим недоліком апаратної аутентифікації є висока ціна пристроїв для її реалізації. Альтернативою слугують біометричні технології, які характеризуються відносними труднощами втрати автентифікатора. Проте, біометричні технології мають свої обмеження, такі як можливість помилкових спрацьовувань або відмови в аутентифікації через фізичні зміни у користувача (наприклад, травми або старіння). Вартість біометричних пристроїв також може бути високою, хоча вона поступово знижується зі збільшенням доступності технології. Крім того, біометрія не гарантує 100% захисту, оскільки зловмисники можуть використовувати різні методи для підробки біометричних даних. Таким чином, необхідно впроваджувати багаторівневу систему аутентифікації, що поєднує кілька технологій для забезпечення більш високого рівня безпеки.



На основі апаратних автентифікаторів створюються програмно-апаратні комплекси, що забезпечують захист від несанкціонованого доступу до комп'ютерів. Вони зазвичай складаються з апаратних засобів, таких як смарт-картки або токени, і програмного забезпечення, яке управляє процесом аутентифікації та авторизації користувачів. Одним із основних компонентів таких комплексів є апаратний контролер, який виконує функцію блокування завантаження операційної системи з зовнішніх пристроїв. Це забезпечує додатковий рівень безпеки, оскільки навіть якщо зловмисник має фізичний доступ до комп'ютера, він не зможе завантажити операційну систему або виконати шкідливі програми з зовнішнього носія (наприклад, USB-флешки), поки не пройде процедуру аутентифікації через відповідний апаратний автентифікатор. Такий підхід значно ускладнює можливість несанкціонованого доступу, оскільки для завантаження операційної системи і отримання доступу до системи необхідно пройти багатоетапну перевірку за допомогою апаратних і програмних засобів. Цей метод часто використовується в корпоративних середовищах, де важливо зберегти цілісність і конфіденційність інформації, а також у високоризикових ситуаціях, де фізичний захист комп'ютерів має вирішальне значення.

Процедура введення двофакторної аутентифікації передбачає використання двох різних факторів для підтвердження ідентичності користувача. Це підвищує рівень безпеки порівняно з однофакторною аутентифікацією, де для доступу достатньо одного елементу (наприклад, пароля). Перший фактор зазвичай є чимось, що користувач знає, наприклад, пароль або PIN-код, тоді як другий фактор може бути чимось, що користувач має, наприклад, смартфон для отримання одноразового коду, або чимось, що користувач є, як біометричні дані (відбитки пальців

або сканування обличчя). Це значно знижує ймовірність несанкціонованого доступу, оскільки зломисник повинен мати доступ до двох різних елементів для успішного обходу системи захисту. Використання двофакторної аутентифікації є рекомендованим для всіх важливих або конфіденційних систем, таких як банківські рахунки або корпоративні ресурси.



Рис. 10.7. Процедура введення двофакторної аутентифікації

Джерело: URL:

<https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Типова послідовність дій для введення двофакторної аутентифікації:

1. Введення першого фактору – пароля або PIN-коду

Користувач спочатку вводить свій стандартний пароль або PIN-код, який є першим фактором. Це може бути секретний код, збережений в пам'яті користувача або на картці пам'яті, або навіть біометричні дані, якщо вони є частиною системи.

2. Перевірка першого фактора

Система перевіряє введений пароль або PIN-код, щоб переконатися, що він відповідає зареєстрованому даним користувача в системі. Якщо пароль вірний, процес переходить до наступного етапу.

3. Введення другого фактору – одноразового пароля (ОТР) або підтвердження через мобільний додаток

Після перевірки першого фактора система надає користувачеві можливість ввести другий фактор. Це може бути одноразовий пароль (ОТР), що генерується апаратним або програмним токеном (наприклад, через мобільний додаток або спеціальний пристрій), або підтвердження через мобільний додаток, SMS, або інші канали зв'язку.

4. Перевірка другого фактора

Після того як користувач введе одноразовий пароль або надасть інші дані для підтвердження, система перевіряє, чи співпадає введений код з тим, що був згенерований у момент запиту. Якщо другий фактор підтверджено, доступ до системи надається.

5. Вхід у систему

Якщо обидва фактори (перший і другий) виявилися вірними, користувач отримує доступ до системи чи сервісу. У разі невідповідності будь-якого з факторів доступ блокується, і користувач може бути запитаний для повторного введення даних.

Цей процес забезпечує більш високий рівень безпеки, оскільки навіть якщо один фактор (наприклад, пароль) буде скомпрометований, зломисник не зможе отримати доступ до системи без другого фактору.

Основними можливостями такого електронного замка є:

- ✱ ***ідентифікація та аутентифікація користувачів за допомогою ідентифікаторів Touch Memory і пароля*** (операційна система завантажується з жорсткого диска тільки після успішної аутентифікації, якщо користувач не пройшов аутентифікацію протягом короткого інтервалу часу, то електронний замок вимикає комп'ютер);
- ✱ ***блокування доступу до зовнішніх носіїв***, що виключає несанкціонований доступ завантаження позаштатної операційної системи;
- ✱ ***перевірка цілісності файлів операційної системи***, програм і даних користувачів на жорсткому диску після включення комп'ютера і до завантаження операційної системи (в разі порушення цілісності контрольованих файлів комплекс блокує доступ до комп'ютера всіх користувачів, крім адміністратора).

10.2. АУТЕНТИФІКАЦІЯ ЗА ДОПОМОГОЮ БІОМЕТРИЧНИХ ДАНИХ

Аутентифікація за допомогою біометричних даних є процесом підтвердження ідентичності користувача на основі унікальних фізіологічних або поведінкових характеристик, які притаманні тільки йому. Це один з найбільш надійних і зручних способів аутентифікації, оскільки біометричні дані, такі як відбитки пальців, райдужна оболонка ока чи розпізнавання обличчя, є важко підроблюваними і неможливо змінити, на відміну від паролів чи PIN-кодів.

Процес аутентифікації за допомогою біометрії починається з реєстрації користувача, в ході якої система зчитує унікальні характеристики людини, наприклад, відбитки пальців, образи обличчя чи зразки голосу. Зібрані біометричні дані обробляються спеціальними алгоритмами, що дозволяють створити шаблон або цифрове представлення цих характеристик. Шаблон зберігається в базі даних і використовується для порівняння під час подальших спроб аутентифікації.

Коли користувач намагається отримати доступ до системи, він надає свої біометричні дані, наприклад, прикладаючи палець до сканера або поглядаючи в камеру для розпізнавання обличчя. Зібрані дані порівнюються з шаблоном, збереженим у системі. Якщо дані співпадають, користувач отримує доступ, інакше процес аутентифікації не проходить. У разі необхідності можуть бути використані додаткові фактори аутентифікації.

Основними перевагами біометричної аутентифікації є її висока надійність, оскільки біометричні дані є унікальними для кожної людини і майже неможливо їх підробити, а також зручність, оскільки користувачам не потрібно запам'ятовувати паролі або носити додаткові пристрої, такі як карти чи ключі. Процес аутентифікації займає кілька секунд, що робить систему швидкою і ефективною.

Проте є й недоліки. По-перше, біометричні дані, на відміну від паролів, неможливо змінити, що підвищує ризики в разі їх компрометації. По-друге, для коректної роботи цієї системи необхідно спеціалізоване обладнання, наприклад, сканери відбитків пальців або камери для розпізнавання обличчя, що може підвищити вартість впровадження такої системи. Крім того, через високу вартість обладнання та можливі питання конфіденційності, біометрична аутентифікація може бути недоступною для невеликих підприємств або користувачів.

Незважаючи на ці недоліки, біометрична аутентифікація активно використовується в різних сферах, таких як мобільні пристрої, фінансові послуги, контроль доступу до захищених приміщень і корпоративних

мереж, оскільки вона забезпечує високу ступінь захисту і зручність користування.

Біометрія являє собою сукупність автоматизованих методів аутентифікації людей на основі їх фізіологічних і поведінкових характеристик. В основі роботи цих методів лежить біометричне порівняння особливостей суб'єкта з його аналогічними характеристиками, що зберігаються в базі даних. Це дозволяє забезпечити високий рівень точності і безпеки при підтвердженні особистості користувача.

Фізіологічні характеристики включають унікальні ознаки, такі як відбитки пальців, райдужна оболонка ока, форма обличчя, лінії на долоні та інші фізичні особливості, які є постійними і важко підроблюваними. Поведінкові характеристики, в свою чергу, пов'язані з індивідуальними звичками або манерою поведінки, такими як малюнок підпису, манера набору тексту на клавіатурі чи спосіб ходьби.

Процес біометричної аутентифікації полягає в зчитуванні цих характеристик з допомогою спеціальних сенсорів або сканерів, а потім їх обробці і порівнянні з інформацією, що зберігається в базі даних. Якщо порівняння виявляє збіг, користувач отримує доступ до системи або ресурсу. Важливою особливістю є те, що біометричні дані унікальні для кожної людини, що робить їх ідеальними для ідентифікації.

Біометрія є одним з найбільш надійних способів аутентифікації, оскільки важко підробити або змінити біометричні дані. Однак система вимагає високоякісного обладнання для зчитування цих даних та обробки, що може збільшити вартість впровадження біометричних систем, а також викликає певні питання з точки зору конфіденційності і захисту особистих даних.

До числа фізіологічних характеристик, які носять індивідуальний характер і зберігаються протягом усього життя людини, належать:

- ➔ форма і геометрія обличчя;
- ➔ форма і будова черепа;
- ➔ відбитки пальців;
- ➔ сітківка ока – рисунок кровоносних судин на задній стінці очного яблука;
- ➔ райдужна оболонка ока;
- ➔ геометрія долоні, кисті руки або пальця;
- ➔ термографія особи, термографія руки;
- ➔ ІЧ малюнок вен на долоні (Альфа-банк) або пальці руки;
- ➔ ДНК;

- форма вуха;
- резонанс черепа.

Процедури біометричної аутентифікації використовують унікальні фізичні або поведінкові характеристики особи для перевірки її ідентичності. Ці характеристики можуть включати відбитки пальців, розпізнавання обличчя, райдужку ока, голосовий зразок, або навіть манеру поведінки під час введення паролів (динамічна біометрія).



Рис. 10.8. Процедури біометричної аутентифікації
Джерело: [1-7]

До поведінкових характеристик відносяться параметри особистості, які виникли в процесі відтворення однієї і тієї ж регулярної дії, таких як голос, динаміка підпису або клавіатурний почерк. Ці характеристики є індивідуальними для кожної людини та можуть використовуватися для аутентифікації у різних системах.



Рис. 10.9. Прилад для проведення біометричної аутентифікації за аналізом динаміки підпису

Джерело: [1-7]

Наприклад, аналіз підпису може здійснюватися за допомогою спеціальної ручки з перетворювачем прискорення по осях X і Y. У процесі цього аналізу враховується не тільки сам процес написання літер, а й інші аспекти, як-от швидкість написання, ступінь натискування на поверхню та інші динамічні характеристики. Такий підхід дозволяє забезпечити високий рівень точності в процесі верифікації особи.

Подібні методи часто використовуються в системах, де важливо підтвердити особистість користувача без необхідності в запам'ятовуванні паролів або використанні фізичних носіїв. Їх перевагою є те, що поведінкові характеристики можуть бути унікальними і практично неможливими для підробки, що значно підвищує рівень безпеки системи.

Під розпізнаванням стилю роботи на клавіатурі розуміється швидкість натискання на клавіші (час між натиснутими клавішами), ритм ударів (час утримання клавіша) і тиск, який здійснюється на клавіші. Визначаються вони при введенні з клавіатури контрольної фрази.

Недоліком біометричних систем за поведінковою характеристикою є те, що на їх роботу впливає психофізичний стан особистості. У деяких випадках залежність поведінкових характеристик від стану людини є перевагою (допуск до виконання відповідальних дій, виявлення порушників).

Для роботи системи біометричної аутентифікації спочатку створюється база даних характеристик користувачів. Для цього біометричні характеристики користувача знімаються, обробляються (значення шифруються, або хешуються), і результат обробки (**так званий біометричний еталон**) заноситься в базу даних облікових записів користувачів. Потім, коли користувачу буде потрібно пройти процедуру аутентифікації, пред'явлені їм біометричні дані будуть порівнюватися з еталоном, що зберігаються в базі даних. Якщо вони збігаються, вважається, що аутентифікація пройдена. Якщо ні, відповідно, йде відмова.

В деяких галузях (криміналістика, розпізнавання образів) процедуру порівняння біометричних параметрів особистості з біометричним еталоном називають біометричною ідентифікацією. Треба звернути увагу на відмінність цієї процедури від процедури біометричної аутентифікації.

Мета аутентифікації надати доступ до ресурсів ІКС обмеженому числу користувачів, біометричні еталони яких зберігаються в базі даних для цієї ІКС.

Мета ідентифікації визначити особистість, маючи її біометричні параметри і базу даних з великою кількістю біометричних еталонів.

Ще один термін, що використовується в біометрії для перевірки – це **верифікація**.

Верифікація – це процедура аутентифікації за біометричними параметрами, що доповнюється додатковим унікальним ідентифікатором. Спочатку система запитує додатковий ідентифікатор, за яким вона вибирає відповідний біометричний еталон з бази даних. Потім надані біометричні параметри користувача порівнюються з еталоном. Якщо ці параметри збігаються, це свідчить про те, що людина є тією, за кого себе видає, і, таким чином, верифікація пройдена успішно.

Цей процес можна розглядати як форму двофакторної аутентифікації, де першим фактором є традиційний ідентифікатор (наприклад, логін або інший унікальний код), а другим — біометричні параметри. Верифікація таким чином забезпечує більш високий рівень безпеки, оскільки для доступу до системи необхідно одночасно підтвердити два фактори: знання ідентифікатора та біометричні дані, що є унікальними для кожної людини.

У роботі біометричних систем можуть виникати помилки двох видів:

Помилковий дозвіл – ймовірність того, що стороння людина може бути помилково прийнята за легального користувача і помилкова відмова – ймовірність того, що легальний користувач буде не допущений через якийсь помилки системи.

Наприклад, через те, що користувач інакше приклав палець до сканера, моргнув в процесі сканування його очей, інакше повернувся до камери, яка знімає його обличчя, і щось подібне. У порівнянні з можливістю пропуску порушника це часто сприймається як менше зло і як більш допустиме явище.

Біометрія

Біометрія, як наука про автоматизовану ідентифікацію особи за фізіологічними та поведінковими характеристиками, зазнала значних змін у останні роки. Раніше біометричні системи були складними та дорогими, однак з розвитком технологій та зростанням попиту на безпечні методи

аутентифікації, зокрема в електронній комерції, спостерігається тенденція до зниження вартості та підвищення доступності біометричних рішень.

Однією з найбільш поширених біометричних технологій є розпізнавання відбитків пальців. Цей метод став доступним завдяки зниженню вартості апаратно-програмних продуктів, що орієнтовані на розпізнавання відбитків пальців. Він широко використовується в мобільних пристроях, системах контролю доступу та інших сферах.

Ідентифікація за рисами обличчя також набуває популярності завдяки поширенню мультимедійних технологій та встановленню відеокамер у громадських місцях, таких як вулиці, вокзали та аеропорти. Цей метод дозволяє здійснювати безконтактну ідентифікацію та має широкий спектр застосувань, від систем безпеки до персоналізованих сервісів.

У 2024 році Європейський Союз запровадив нові правила перетину кордону, які включають використання біометричних даних, таких як сканування обличчя та відбитків пальців, замість традиційних штампів у паспорті. Це дозволяє автоматично фіксувати в'їзд усіх іноземців до країн Шенгенської зони та зберігати ці дані протягом трьох років. Такі зміни сприяють підвищенню безпеки та спрощенню процесу перетину кордону.

Загалом, біометрія продовжує розвиватися, пропонуючи нові можливості для безпечної та зручної ідентифікації в різних сферах життя.

Переваги біометричних систем

Переваги біометричних систем безпеки очевидні:

- ➔ біометрію важко підробити. Для виявлення імітації можна застосовувати такі технології, як контроль температури, наявності пульсу, контроль опору матеріалу, який прикладений до сенсора;
- ➔ біометричні характеристики неможливо забути або втратити на відміну від паперових і апаратних ідентифікаторів.

Недоліки біометричних систем

Небезпека використання біометрії полягає в тому, що будь-яка компрометація для біометрії виявляється фатальною. Паролі, при всій їх ненадійності, можна змінити, загублену картку анулювати і завести нову. Пальці, очі або голос змінити не можна. Якщо біометричні дані виявляться скомпрометовані, доведеться істотно модернізувати всю систему.

Зазначимо декілька з існуючих на даний момент проблем, які все ж, поступово вирішуються:

▲ Ціна.

Дана проблема актуальна для нових біометричних технологій і для всіх нових технологій взагалі.

▲ Не універсальність

Дана проблема пов'язана з тим, що деякі характеристики погано виражені в окремих людей. Відомо, що приблизно у 2 % людей папілярні візерунки знаходяться в такому стані, що не піддаються автоматичному розпізнаванню. Дана проблема виникає і при спробі застосування біометричних технологій для людей, які мають фізичні вади (ампутації рук або пальців, шрами на обличчі, проблеми з очима і т. п.). У цьому випадку, на відміну від помилок першого (помилковий відказ) *FRR (false rejection rate)* і другого роду (помилковий допуск) *FAR (false acceptance rate)* говорять про так звану «помилку третього роду» – відмову системи приймати біометричну характеристику. Шляхом вирішення цієї проблеми є комплексність підходу, що використовує відразу кілька біометричних характеристик, що дозволяє на порядок знизити кількість людей, біометрична ідентифікація яких неможлива. Іншим шляхом вирішення даної проблеми є використання біометричної ідентифікації спільно з іншими методами (наприклад, з автентифікацією по смарт-картці).

Щодо комплексного застосування декількох біометричних технологій слід підкреслити, крім вирішення проблеми помилки третього роду, таке застосування дозволяє істотно поліпшити і характеристики, пов'язані з помилковою відмовою і помилковим допуском. Саме тому даний напрям, званий **мультибіометричною ідентифікацією**, є одним з найбільш перспективних в області біометрії;

▲ Чутливість до обману

Проблема найбільш виражена для традиційних технологій (палець, обличчя), що пов'язано з їх давньою появою. Існують і успішно застосовуються різні методи боротьби з цією проблемою, засновані на різних фізичних характеристиках муляжів і живих тканин. Наприклад, для відбитків пальців може застосовуватися методика вимірювання пульсу або електропровідності;

▲ Відсутність стандартів

Прийняті або перебувають на виході стандарти, що стосуються даних відбитка пальця, двовимірного зображення особи, біометричного програмного інтерфейсу, тестування біометричних технологій та обміну біометричними даними;

▲ Відсутність нормативної бази

Проблема відсутності нормативної бази є на даний момент найбільш важливою: отримання і використання біометричних характеристик може

регулюватися тільки на основі законодавства. Існуючі на даний момент закони вимагають серйозних доповнень і коригувань, без яких, з одного боку, не будуть захищені права людини, а з іншого – не можуть нормально розвиватися біометричні технології.

10.3. АУТЕНТИФІКАЦІЯ НА ОСНОВІ ЦИФРОВИХ СЕРТИФІКАТІВ

Аутентифікація на основі цифрових сертифікатів є одним із найбільш ефективних та безпечних методів підтвердження особи, що використовує криптографічні технології для захисту даних. Цей метод здобуває все більшу популярність, зокрема у сферах, де необхідно забезпечити високу довіру, захист від підробки і конфіденційність, таких як банківські транзакції, електронний підпис, доступ до критичної інформації тощо. Цифровий сертифікат — це криптографічний документ, який підтверджує зв'язок між публічним ключем користувача та його особою, організацією або іншою сутністю, що цей ключ використовує. Сертифікат містить публічний ключ, інформацію про власника сертифіката, а також цифровий підпис сертифікаційного центру (ЦС), який видає сертифікат.

Основний процес аутентифікації за допомогою цифрових сертифікатів включає кілька етапів. Спочатку користувач генерує пару криптографічних ключів — публічний та приватний. Приватний ключ зберігається в захищеному місці, наприклад, на спеціальному носії або в апаратному модулі, а публічний ключ включається в сертифікат. Після цього користувач подає запит на отримання сертифіката до сертифікаційного центру, який перевіряє достовірність інформації про користувача. Якщо перевірка пройшла успішно, сертифікаційний центр підписує сертифікат своїм приватним ключем, що підтверджує його автентичність.

Під час аутентифікації користувач надає свій цифровий сертифікат серверу або системі, які перевіряють його підпис, порівнюючи його з публічним ключем сертифікаційного центру. Якщо підпис правильний і сертифікат не протермінований, система дозволяє користувачу доступ до необхідних ресурсів, підтверджуючи його особу. Переваги цього методу включають високу надійність, оскільки завдяки використанню криптографії підробити цифровий сертифікат практично неможливо. Також забезпечується цілісність даних, адже підпис підтверджує, що інформація не була змінена після її підписання сертифікаційним центром.

Проте для досягнення максимальної безпеки, цифрові сертифікати часто комбінуються з іншими методами аутентифікації, такими як PIN-

коди, токени або двофакторна аутентифікація. Таким чином, цей метод аутентифікації стає важливим елементом систем захисту в багатьох сферах, забезпечуючи надійний доступ до критично важливої інформації та електронних послуг.

Аутентифікація з застосуванням цифрових сертифікатів є альтернативою застосуванню паролів і є кращим рішенням в умовах, коли число користувачів (нехай і потенційних) вимірюється мільйонами.

У таких обставинах процедура попередньої реєстрації користувачів, пов'язана з призначенням і зберіганням їх паролів, стає просто нездійсненною. При наявності сертифікатів ІКС, яка дає користувачеві доступ до своїх ресурсів, не зберігає ніякої інформації про своїх користувачів – вони самі її надають в своїх запитах у вигляді сертифікатів, що засвідчують особу користувачів. Можна розглядати це як четвертий фактор аутентифікації – мати рекомендації від довіреного посередника, якому вірить перевіряючий.

Сертифікати, що використовуються для аутентифікації в системах на основі криптографії, видаються спеціальними уповноваженими організаціями, відомими як **центри сертифікації** (*Certificate Authority, CA*). Центр сертифікації (CA) є основним компонентом інфраструктури відкритих ключів (PKI) і виконує важливу роль у забезпеченні довіри та безпеки в системах, де застосовуються цифрові підписи та шифрування. Однією з основних функцій центру сертифікації є видача цифрових сертифікатів, які містять публічний ключ користувача, його ідентифікаційні дані та іншу важливу інформацію, таку як термін дії сертифіката і відомості про самого центру сертифікації.

Перед тим як видати сертифікат, центр сертифікації проводить ретельну перевірку ідентичності заявника. Це може включати перевірку документів, проведення аутентифікації або інші методи для підтвердження особи, що дозволяє мінімізувати ризик видачі сертифікатів недостовірним особам. Після цього сертифікат підписується закритим ключем центру сертифікації, що забезпечує його автентичність та цілісність. Завдяки підпису СА інші сторони можуть перевірити, що сертифікат дійсно належить вказаному користувачу або організації.

Центр сертифікації також відповідає за управління статусом сертифікатів, включаючи їх оновлення, скасування або відміну у разі закінчення терміну дії або зміни ключів користувача. Для цього СА публікує списки відкликаних сертифікатів (CRL) або інші методи перевірки статусу сертифікатів, що дозволяють користувачам перевіряти актуальність сертифікатів.

Завдяки централізованому управлінню сертифікатами, система сертифікацій забезпечує високий рівень безпеки та довіри в електронних транзакціях, зокрема під час шифрування даних або аутентифікації користувачів, адже не потрібно зберігати паролі на серверах. Замість цього достатньо мати в базі даних тільки імена користувачів та їх відкриті ключі, що спрощує та підвищує ефективність управління доступом до ресурсів.

Сертифікат являє собою електронну форму, в якій міститься наступна інформація:

- ✱ відкритий ключ власника даного сертифіката;
- ✱ відомості про власника сертифіката (ім'я, адреса електронної пошти, найменування організації, в якій він працює, і т. п.);
- ✱ найменування організації, що видала цей сертифікат;
- ✱ електронний підпис організації, тобто зашифровані закритим ключем цієї організації дані, що містяться в сертифікаті.

Використання сертифікатів засноване на припущенні, що центрів сертифікації небагато і їх відкриті ключі широко доступні, наприклад, з публікацій у журналах.



Коли користувач хоче підтвердити свою особистість, він пред'являє свій сертифікат у двох формах: відкритій та зашифрованій. Відкритий сертифікат є тим, який користувач отримав від центру сертифікації (ЦС), і він містить публічний ключ користувача, а також інші дані, які підтверджують його особу. Зашифрований сертифікат створюється за допомогою закритого ключа користувача. Цей процес є частиною процедури аутентифікації, і важливою його метою є підтвердження того, що користувач є власником закритого ключа, який відповідає його публічному ключу в сертифікаті.

Процедура аутентифікації полягає в тому, що сторона, яка проводить перевірку, бере відкритий ключ з незашифрованого сертифіката та використовує його для розшифровки зашифрованого сертифіката. Якщо результат розшифровки збігається з відкритим сертифікатом, це означає, що користувач дійсно є власником закритого ключа, яким був зашифрований сертифікат. Потім перевіряється підпис сертифікаційного центру, зазначений у сертифікаті. Для цього використовують публічний ключ ЦС, що дозволяє розшифрувати підпис і порівняти його з оригінальним сертифікатом. Якщо сертифікат зберігається без змін, і він містить правильну інформацію, це означає, що він був виданий на основі

перевірки в сертифікаційному центрі та належить зазначеному користувачу.

Однією з основних переваг використання цифрових сертифікатів є те, що вони знижують потребу в зберіганні паролів користувачів на сервері. Замість того, щоб мати на сервері базу даних з іменами користувачів та їх паролями, достатньо зберігати лише список імен і відкритих ключів. Це значно підвищує безпеку системи, оскільки паролі не зберігаються в відкритому вигляді, і немає ризику їх компрометації. Вся інформація, що стосується користувача, міститься у сертифікаті, який підлягає криптографічній перевірці, що робить цей метод дуже ефективним для захисту інформації.

10.4. ЦЕНТРАЛІЗОВАНІ СИСТЕМИ АУТЕНТИФІКАЦІЇ. КОНЦЕПЦІЯ ЄДИНОГО ЛОГІЧНОГО ВХОДУ

Централізовані системи аутентифікації є механізмами, які забезпечують централізоване управління процесами перевірки автентичності користувачів в інформаційних системах. Вони дозволяють централізовано зберігати, управляти та перевіряти дані про користувачів, знижуючи складність адміністрування безпеки в організації.

Основною перевагою централізованої аутентифікації є єдиний контроль за доступом до всіх ресурсів організації. Користувачеві достатньо один раз ввести свої аутентифікаційні дані (пароль, PIN-код, біометричні дані або сертифікат) для отримання доступу до різних систем і ресурсів, що використовуються в організації. Такий підхід зменшує потребу в управлінні кількома обліковими записами та паролями для кожної системи окремо, що значно спрощує адміністрування.

Одним із прикладів централізованої аутентифікації є використання технології LDAP (Lightweight Directory Access Protocol). LDAP дозволяє зберігати інформацію про користувачів, їхні права доступу та інші атрибути в централізованій базі даних. Через цей протокол різні системи можуть отримувати і перевіряти дані про користувачів, що дозволяє централізовано управляти доступом до мережі та системи.

Іншим популярним рішенням є використання системи аутентифікації через Active Directory (AD), яка є однією з найбільш широко використовуваних технологій для централізованого керування користувачами та доступом в середовищі Windows. Active Directory дозволяє зберігати інформацію про облікові записи користувачів,

комп'ютери, групи та інші ресурси, а також забезпечує єдиний процес аутентифікації для всіх користувачів та пристроїв в мережі.

Централізовані системи аутентифікації можуть також включати використання одноразових паролів (ОТР) або двофакторної аутентифікації (2FA), де для підтвердження особи користувача необхідно ввести не лише пароль, а й додатковий код, який може бути надісланий на мобільний пристрій або згенерований за допомогою спеціального токена. Це підвищує рівень безпеки, оскільки навіть у разі компрометації пароля, доступ до системи можна отримати лише за наявності другого фактора аутентифікації.

Централізовані системи аутентифікації також можуть бути інтегровані з іншими службами безпеки, такими як системи управління правами доступу (RBAC) або системи моніторингу безпеки, що дозволяють забезпечити комплексний захист інформаційних ресурсів організації.

Одним з важливих аспектів централізованої аутентифікації є те, що вона дозволяє зменшити адміністративні витрати на управління паролями і забезпечує більшу надійність через зосередження інформації в одному місці, що полегшує її захист і аудит.

Традиційний спосіб аутентифікації за допомогою багаторазових паролів підходить для випадку, коли користувач весь час працює з єдиним комп'ютером, звертаючись тільки до його ресурсів. Такому користувачеві потрібно запам'ятовувати і періодично міняти тільки один пароль.

Більш типовим є випадок, коли користувачеві доводиться працювати на різних, розосереджених комп'ютерах: стаціонарному комп'ютері, особистому планшеті, гостьовому комп'ютері підприємства-партнера – і при цьому отримувати доступ до різних серверів, наприклад серверів свого підприємства, серверів підприємства-партнера, до захищених вебсайтів Інтернету. У тому випадку, коли кожен комп'ютер і кожен сервер вимагають окремої аутентифікації за допомогою багаторазового пароля, користувачеві доводиться пам'ятати і оновлювати досить багато паролів.

У цьому випадку на допомогу користувача приходять **технологія єдиного логічного входу (*Single Sign On, SSO*)**. Технологія SSO дозволяє користувачу автентифікуватися через сервер аутентифікації один раз, доводячи свою автентичність за допомогою будь-якого способу аутентифікації, і тепер використовувати різні ресурси одного і того ж домену безпеки без необхідності повторної аутентифікації на кожному з ресурсів.

Концепція єдиного логічного входу (Single Sign-On, SSO) передбачає, що користувач може здійснити аутентифікацію лише один раз

і отримати доступ до всіх необхідних інформаційних систем та ресурсів без необхідності повторно вводити свої дані для кожної з систем. Це значно спрощує управління доступом і знижує кількість паролів, які користувачі повинні запам'ятовувати, тим самим полегшуючи процес аутентифікації. Основною метою SSO є спрощення процесу доступу до різних систем, зменшуючи необхідність введення пароля для кожного ресурсу окремо, що підвищує зручність використання і зменшує ризик безпеки через збереження лише одного набору облікових даних.

При використанні SSO, користувач спочатку вводить свої облікові дані (наприклад, логін та пароль) на сервері, що відповідає за аутентифікацію. Після того як ці дані перевіряються, сервер генерує сесію або токен, який зберігається на пристрої користувача. З цим токеном користувач може отримати доступ до інших систем або ресурсів без необхідності повторної аутентифікації. Кожен ресурс, до якого намагається звернутися користувач, перевіряє цей токен, і якщо він дійсний, надає доступ без нової перевірки облікових даних.

Один із основних компонентів цієї системи — це сервер SSO, який забезпечує централізовану перевірку аутентифікації та генерує токени доступу. Цей сервер може використовувати різні технології для верифікації, зокрема протоколи, такі як OAuth, SAML або OpenID Connect, для передачі даних про аутентифікацію між різними сервісами.

Основна ідея полягає в централізованому управлінні аутентифікацією, де користувач після першого входу отримує спеціальний токен, який використовується для авторизації в інших системах, що підтримують цей механізм. Цей токен передається від однієї системи до іншої, дозволяючи користувачу отримати доступ без необхідності вводити пароль кожного разу.

Технологічно SSO ґрунтується на довірі між різними системами, які взаємодіють з єдиним центром аутентифікації. Для забезпечення безпеки аутентифікації використовуються різні протоколи, такі як SAML (Security Assertion Markup Language), OpenID Connect або OAuth 2.0, що дозволяють безпечно передавати дані про користувача між системами без розкриття паролів.

Основні переваги SSO включають зручність для користувачів, оскільки вони можуть використовувати єдиний набір аутентифікаційних даних для доступу до всіх ресурсів без запам'ятовування численних паролів для різних систем. Це також сприяє зниженню ризику компрометації паролів, оскільки користувач вводить свої дані тільки один раз, зменшуючи ймовірність того, що ці дані можуть бути перехоплені. Для адміністраторів організацій централізоване управління доступом

дозволяє знижувати витрати часу на моніторинг прав доступу, а також забезпечує більш ефективний контроль за політиками безпеки.

Однак єдиний логічний вхід також має свої недоліки. Одним з основних ризиків є точка відмови: якщо система SSO зазнає збоїв, користувачі можуть втратити доступ до всіх підключених систем. Крім того, якщо аутентифікаційні дані користувача будуть викрадені, злоумисник може отримати доступ до всіх ресурсів, що знаходяться під його контролем, що значно збільшує потенційний масштаб пошкоджень. Тому важливо забезпечити належний рівень захисту для системи SSO, застосовуючи додаткові механізми безпеки, такі як двофакторна аутентифікація. Отже, SSO дозволяє забезпечити одноразову аутентифікацію для доступу до кількох ресурсів і підвищує як зручність для користувачів, так і безпеку інформаційних систем завдяки зменшенню кількості введення паролів і централізованому управлінню доступами.

Таким чином, хоча концепція єдиного логічного входу дає безліч переваг у вигляді зручності та підвищення безпеки для користувачів і адміністраторів, її ефективність і безпека безпосередньо залежать від надійності та правильної реалізації централізованої аутентифікаційної системи.

Домен безпеки (security domain) — це логічна структура, в межах якої всі ресурси підпорядковуються єдиній політиці безпеки та управляються спільним контролером. У контексті інформаційних систем і мереж домен безпеки визначає межі, в яких реалізується управління доступом, авторизацією та моніторингом діяльності користувачів. У такому домені всі користувачі, пристрої, та інші ресурси об'єднуються спільною політикою безпеки, що визначає правила і механізми доступу, а також забезпечення конфіденційності, цілісності та доступності інформації.

Основною характеристикою домену безпеки є наявність єдиного контролера домену, який відповідає за централізоване управління безпекою в межах цього домену. Це дозволяє застосовувати одні й ті самі правила доступу, а також здійснювати аудит і контроль за всіма подіями, що відбуваються в межах домену. Такі домени можуть охоплювати фізичні та логічні ресурси, включаючи сервери, робочі станції, бази даних, а також мережеві пристрої та додатки.

Домен безпеки допомагає організувати і підтримувати єдину політику безпеки в межах організації або мережі, спрощуючи адміністрування і знижуючи ризики, пов'язані з несанкціонованим доступом до критичних ресурсів. Використання доменів безпеки особливо важливе в великих організаціях, де зберігаються великі обсяги даних і де

необхідна централізована система управління доступом для ефективного захисту інформації.

В даний час не існує системи аутентифікації, що реалізує концепцію єдиного логічного входу, яка б працювала з усіма типами операційних систем, додатків і при цьому враховувала б різноманітні відносини між організаціями, до яких належать користувачі та інформаційні ресурси. Однак є системи, що дозволяють організувати єдиний логічний вхід для однорідної інформаційної системи, наприклад для мережі, що використовує тільки одну певну ОС або один певний протокол аутентифікації, або для групи організацій, які довіряють один одному при аутентифікації своїх користувачів. Так, наприклад, властивість однорідності операційних систем є умовою застосування системи єдиного входу на основі довідкової служби Microsoft Active Directory.

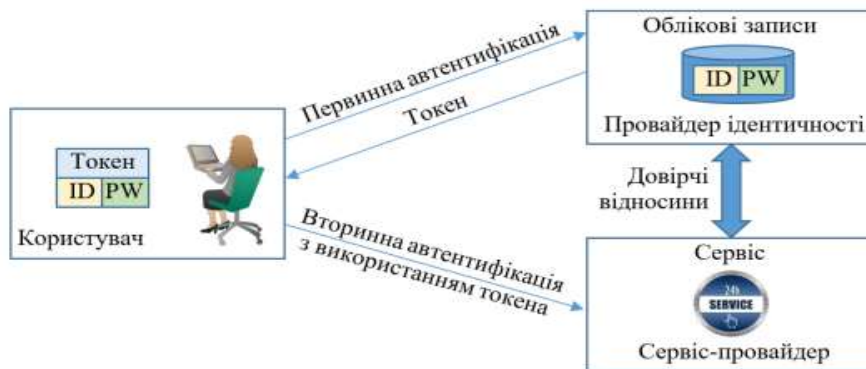


Рис. 10.10. Схема єдиного логічного входу

Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity>

У цій схемі є три важливих елемента:

- ✱ **Користувач**, що має ID-ідентифікатор, PW – багаторазовий пароль.
- ✱ **Провайдер ідентичності (Identity Provider)** – це система, яка може автентифікувати користувача на основі бази даних облікових записів користувачів. Цей елемент може мати й інші назви, наприклад сервер аутентифікації.
- ✱ **Сервіс-провайдер (Service Provider)**, або ресурсний сервер, – це система, що надає сервіси (файловий сервіс, поштовий сервіс, вебсервіс, сервіс баз даних тощо).

Особливістю цієї схеми є те, що провайдер сервісів не підтримує базу облікових даних користувачів. База облікових даних є тільки у провайдера ідентичності, а провайдер сервісів довіряє результатам

аутентифікації користувачів, виконаної провайдером ідентичності. Тобто існують довірчі відносини (trust relationships) між провайдером ідентичності та провайдером сервісів.

Користувач виконує логічний вхід в систему, звертаючись до провайдера ідентичності. Якщо користувач зміг підтвердити свою автентичність, то провайдер ідентичності надає користувачеві деяку інформаційну структуру – токен доступу, який користувач зберігає у своїй базі даних.

При необхідності отримання доступу до деякого сервісу користувач пред'являє токен доступу ресурсному серверу. Токен доступу повинен бути захищений таким чином, щоб ресурсний сервер мав можливість перевірити, що токен був дійсно виданий користувачеві сервером аутентифікації, яким ресурсний сервер довіряє автентифікувати користувачів. У цьому випадку відбувається вторинна аутентифікація користувача, але для самого користувача вона прозора, оскільки пред'явленням токена доступу займається програмне забезпечення комп'ютера.

Токен доступу зазвичай має обмежений час дії, наприклад добу, тому користувач повинен його відновлювати, повторюючи процедуру з сервером аутентифікації.

SSO дозволяє користувачам вводити свої облікові дані тільки один раз для отримання можливості доступу до всіх ресурсів, що зменшує час, який користувачі витрачають на процес аутентифікації. Також це дозволяє адміністраторам раціоналізувати використання облікових записів і краще керувати розподілом прав доступу. **SSO** підвищує безпеку, знижуючи ймовірність того, що користувач буде зберігати свій пароль під клавіатурою – адже тепер йому потрібно запам'ятати набагато менше паролів (в ідеалі – один).

Single Sign-On (SSO) також сприяє покращенню досвіду користувачів, оскільки зменшує кількість переривань у роботі через необхідність повторної аутентифікації. Завдяки цьому користувачі можуть зосередитися на своїх завданнях, не витрачаючи час на повторне введення облікових даних при переході між різними системами.

З точки зору адміністративного управління, SSO спрощує процедури надання та відкликання доступу. Адміністратори можуть централізовано керувати доступом до різних ресурсів, що зменшує ризик помилок і забезпечує більшу відповідність політикам безпеки підприємства. Крім того, централізоване управління дозволяє швидко відключати доступ для співробітників, які залишили компанію, або для облікових записів, які вважаються скомпрометованими.

Однак впровадження SSO має і свої виклики. Наприклад, компрометація єдиного набору облікових даних може дати зловмисникам доступ до всіх ресурсів користувача. Для зменшення цього ризику важливо інтегрувати додаткові механізми захисту, такі як:

- **Двофакторна аутентифікація (2FA)**

Поєднання пароля з одноразовим кодом або біометричними даними підвищує рівень безпеки.

- **Моніторинг і аудит**

Постійний контроль за спробами входу дозволяє виявляти аномалії, такі як спроби доступу з незвичних місць або пристроїв.

- **Політики складних паролів**

Забезпечують додатковий рівень захисту, знижуючи ймовірність успішної атаки методом перебору.

SSO також може інтегруватися з протоколами та стандартами, такими як OAuth, OpenID Connect та SAML (Security Assertion Markup Language). Ці стандарти дозволяють безпечно передавати автентифікаційні дані між різними додатками та платформами, забезпечуючи сумісність із хмарними сервісами та сучасними корпоративними інфраструктурами.

Застосування SSO є особливо актуальним у великих підприємствах, де користувачам необхідно працювати з багатьма програмами та сервісами. У таких випадках інтеграція SSO з корпоративними системами управління ідентичністю (IDM) забезпечує повну синхронізацію доступу, покращує ефективність роботи та знижує адміністративні витрати.

Незважаючи на ризики, правильне впровадження та налаштування SSO робить цей підхід ефективним інструментом для підвищення зручності, безпеки та продуктивності в інформаційних системах підприємства.

10.5. СИСТЕМА KERBEROS

Система централізованої аутентифікації тісно пов'язана з системою централізованого керування доступом, так як остання повинна базуватись на результатах аутентифікації кожен раз, коли обчислювальний процес, який представляє користувача, намагається отримати доступ до ресурсу комп'ютера, що входить в деякий домен. Система Kerberos може працювати в середовищі багатьох популярних ОС, наприклад в ОС Windows система Kerberos вбудована як основний компонент безпеки. Існують реалізації Kerberos для сімейства Unix, включаючи Red Hat Linux, Fedora, CentOS, і для Mac OS X. Поточною версією є версія 5, яка стандартизована IETF в RFC 4120.

В основі функціонування цієї досить громіздкої системи лежить кілька простих принципів:

- в мережах, що використовують систему безпеки Kerberos, всі процедури аутентифікації між клієнтами і серверами мережі виконуються через посередника, якому довіряють обидві сторони процесу аутентифікації, причому таким авторитетним арбітром є сама система Kerberos;
- в системі Kerberos клієнт повинен доводити свою автентичність для доступу до кожної служби, послуги якої він запитує;
- усі обміни даними в мережі виконуються в захищеному вигляді із застосуванням симетричного алгоритму шифрування AES (або DES в ранніх реалізаціях Kerberos).

Прикладом системи, що реалізує процедуру єдиного логічного входу, є *мережева служба Kerberos*.

Kerberos – це технологія безпеки, яка реалізує функції аутентифікації. Програма працює на базі моделі клієнт-сервер і клієнтські компоненти цього програмного продукту присутні в більшості серверних операційних систем.

Kerberos — це мережевий протокол аутентифікації, який реалізує процедуру єдиного логічного входу (SSO) в комп'ютерних мережах. Цей протокол дозволяє користувачам отримувати доступ до різних ресурсів мережі без необхідності повторно вводити свої облікові дані для кожного сервісу. Основна ідея протоколу полягає в централізації аутентифікації, що дозволяє безпечно перевіряти особу користувача лише один раз, після чого йому надається доступ до всіх ресурсів в рамках системи, що підтримує Kerberos.

Kerberos працює за допомогою трьох основних компонентів: клієнта, сервера та сервера аутентифікації, який називається Key Distribution Center (KDC). Клієнт — це кінцевий користувач або програма, що хоче отримати доступ до ресурсу в мережі. Сервер — це комп'ютер або служба, до якої клієнт хоче підключитися. KDC є центральною ланкою, що відповідає за перевірку даних користувачів і видачу квитків доступу.

Коли користувач хоче підключитися до мережі, він спочатку звертається до KDC, передаючи свої облікові дані. KDC перевіряє ці дані, а потім видає користувачу Ticket-Granting Ticket (TGT), який є доказом того, що користувач пройшов аутентифікацію. Цей квиток містить криптографічно захищену інформацію, зокрема ідентифікацію користувача та час, до якого він може використовувати цей квиток.

Після отримання TGT клієнт може використовувати його для отримання доступу до конкретних ресурсів. Клієнт звертається до KDC, щоб отримати service ticket для конкретного ресурсу або сервера, до якого він хоче підключитися. Після отримання сервісного квитка клієнт може використовувати його для доступу до сервера, причому сервер перевіряє квиток, не запитуючи пароль користувача, що значно підвищує зручність і безпеку процесу.

Однією з ключових переваг Kerberos є його здатність підтримувати централізовану систему аутентифікації, що дозволяє організаціям зменшити кількість облікових записів і паролів, які потрібно зберігати та захищати. Оскільки аутентифікація відбувається через квитки, знижуються ризики, пов'язані з зберіганням паролів на різних серверах, і збільшується безпека доступу.

Система Kerberos активно використовується в багатьох корпоративних мережах, зокрема в операційних системах Windows (через Active Directory) та в Unix-подібних системах для забезпечення безпечного доступу до ресурсів і зниження витрат на управління аутентифікацією.

Основні компоненти Kerberos

Мережева служба Kerberos побудована в архітектурі клієнт-сервер, що дозволяє їй працювати в найскладніших мережах. Kerberos-клієнт встановлюється на всіх комп'ютерах мережі, які можуть звернутися до будь-якої мережевої служби.

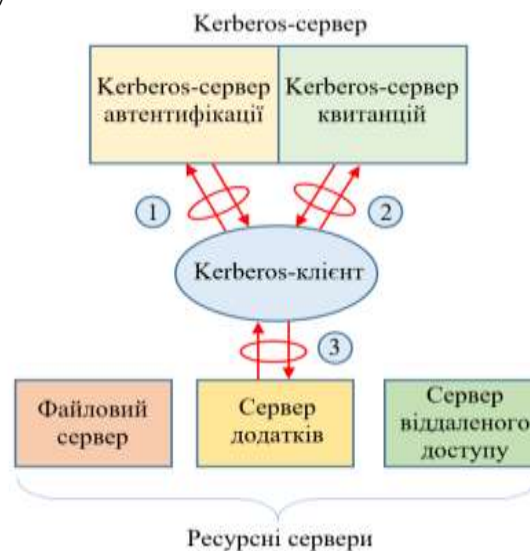


Рис. 10.11. Три етапи роботи системи Kerberos

Джерело: URL: <https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity>

У таких випадках Kerberos-клієнт від імені користувача передає запит на Kerberos-сервер і підтримує з ним діалог, необхідний для виконання функції системи Kerberos. Отже, в системі Kerberos є наступні учасники: Kerberos-сервер, Kerberosклієнти, ресурсні сервери. Kerberos-клієнти намагаються отримати доступ до мережеских ресурсів – файлів, додатків, принтеру і т. д., які знаходяться на ресурсних серверах. Цей доступ може бути наданий, по-перше, тільки легальним користувачам, а по-друге, при наявності у них достатніх повноважень, визначених службами авторизації відповідних ресурсних серверів – файловим сервером, сервером додатків, сервером друку. Однак в системі Kerberos ресурсним серверам забороняється «безпосередньо» приймати запити від клієнтів, їм дозволяється починати розгляд запиту клієнта тільки тоді, коли на це надходить дозвіл від Kerberos-сервера.

Центр поширення ключів (KDC – Key Distribution Center) – центр поширення ключів є основним елементом системи Kerberos, який відповідає за зберігання секретних ключів усіх користувачів і служб в мережі. KDC реалізує службу аутентифікації та функції поширення ключів. Кожен системний об'єкт має свій обліковий запис у KDC і використовує секретний ключ для аутентифікації та передачі критичної інформації. Для користувачів паролі перетворюються в секретні ключі, які використовуються для аутентифікації. Завдяки KDC, усі компоненти в системі можуть безпечно здійснювати аутентифікацію через ключі, не зберігаючи паролі в відкритому вигляді. KDC є довіреним сервером аутентифікації для всіх користувачів, додатків і служб у межах домену безпеки.

Служба надання білетів (TGS – Ticket Granting Service) TGS є частиною KDC, що відповідає за генерацію та видачу білетів (tickets) користувачам або системним об'єктам, які потребують доступу до інших служб або ресурсів у мережі. Коли користувач або система потребує аутентифікації на іншому об'єкті, наприклад, на сервері друку чи іншому сервісі, TGS видає білет, що дозволяє отримати доступ до цього ресурсу. Білет є зашифрованим документом, який містить інформацію про користувача, дозволи на доступ та інші дані, що потрібні для авторизації на конкретному сервері.

Клієнт (Client) — це комп'ютер або користувач, який хоче отримати доступ до ресурсів мережі. Клієнт відправляє запит до KDC для отримання Ticket-Granting Ticket (TGT) — квитка, який підтверджує, що він пройшов аутентифікацію. TGT дозволяє клієнту далі отримувати доступ до конкретних ресурсів через TGS.

Сервери (Services) — це системні об'єкти або служби, до яких користувач хоче отримати доступ. Вони можуть включати в себе сервери файлів, сервери баз даних, сервери друку та інші ресурси мережі. Сервери вимагають наявності аутентифікації через використання білетів, отриманих від TGS, для підтвердження того, що користувач має право доступу до їхніх ресурсів.

У загальному, процес роботи Kerberos виглядає так: спочатку клієнт аутентифікується в KDC, отримує TGT. Далі, коли клієнт хоче доступ до конкретного ресурсу, він відправляє запит до TGS для отримання сервісного білету, який потім використовується для отримання доступу до сервера. Завдяки цьому процесу користувач може безпечно і зручно отримувати доступ до різних ресурсів, при цьому мінімізуючи ризик крадіжки паролів і забезпечуючи високий рівень безпеки в мережі.

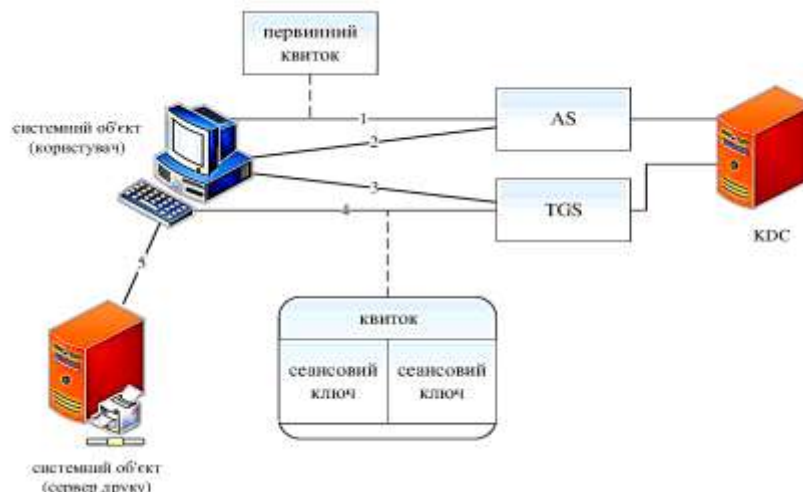


Рис. 10.12. Служба надання білетів (TGS – Ticket Granting Service) на KDC (центр поширення ключів)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Призначення Kerberos

Kerberos призначений для вирішення важливого завдання забезпечення безпечної аутентифікації в відкритих або незахищених мережах. У такій мережі користувачі та інші об'єкти — ресурси системи — є суб'єктами, які мають свої секретні ключі для підтвердження ідентичності. Проблема, яку вирішує Kerberos, полягає в тому, як безпечно довести справжність суб'єкта, коли мережа доступна для активного і пасивного прослуховування, а безпечне передавання секретного ключа через відкриті канали є небажаним.

Kerberos забезпечує безпечну аутентифікацію лише на початковому етапі сеансу. Подальший захист даних — їхня конфіденційність, автентичність і цілісність — має бути забезпечений за допомогою механізмів клієнта і ресурсного сервера. Це може включати використання протоколів шифрування, таких як TLS або IPsec, залежно від потреб мережі.

У класичному випадку, щоб суб'єкт С міг довести свою автентичність об'єкту S (наприклад, серверу), він повинен не тільки назвати своє ім'я, але й продемонструвати знання свого секретного ключа. Однак, просте передавання секретного ключа через мережу не є безпечним — він може бути перехоплений зловмисником під час передачі через незахищену мережу. Крім того, об'єкт S не має доступу до секретного ключа суб'єкта С, і, відповідно, не повинен зберігати цю інформацію.

Задача, яку вирішує Kerberos, полягає в створенні механізму, який дозволяє суб'єкту довести свою автентичність без необхідності прямого передавання секретного ключа. Це досягається шляхом використання принципу білетів (tickets).

Kerberos використовує централізовану службу аутентифікації (KDC), яка зберігає секретні ключі усіх учасників. Коли суб'єкт С хоче підтвердити свою ідентичність об'єкту S, він не передає свій секретний ключ безпосередньо. Замість цього, суб'єкт С аутентифікується через KDC, отримуючи білет для доступу до сервісу або об'єкта. Білет містить зашифровану інформацію, яку об'єкт S може розшифрувати, знаючи певний ключ для цього ресурсу. Таким чином, через сервіси аутентифікації Kerberos, суб'єкт С може довести свою автентичність без передачі секретного ключа, а об'єкт S може впевнитися в тому, що суб'єкт має право на доступ, використовуючи білети, видані централізованим KDC. Це забезпечує захищену і ефективну систему для аутентифікації в умовах відкритих мереж.

Система Kerberos виступає як довірена третя сторона, яка володіє секретними ключами всіх суб'єктів і забезпечує їх взаємну аутентифікацію. Вона допомагає здійснювати попарну перевірку справжності суб'єктів без необхідності прямого передавання секретних ключів по мережі. Це дозволяє захистити ключову інформацію та забезпечити безпечний доступ до ресурсів.

Коли суб'єкт С (клієнт) хоче отримати доступ до об'єкта S (зазвичай це сервер), він відправляє запит до Kerberos, в якому містяться дані про клієнта та запитувану послугу. У відповідь Kerberos генерує квиток (ticket), який зашифровується за допомогою особистого ключа сервера. Крім цього, частина інформації з квитка також зашифровується секретним ключем клієнта. Такий механізм дозволяє гарантувати, що тільки клієнт, що

володіє відповідним секретним ключем, зможе отримати і правильно розшифрувати частину даних у квитку.

Клієнт розшифровує отриману частину даних та пересилає її разом з квитком на сервер. Сервер, отримавши ці дані, розшифровує квиток за допомогою свого ключа і перевіряє, чи збігається вміст з інформацією, яку клієнт передав разом із квитком. Якщо перевірка успішна, сервер підтверджує автентичність клієнта, оскільки той зміг правильно розшифрувати інформацію, яка була зашифрована за допомогою його секретного ключа. Таким чином, клієнт доводить свою ідентичність без передачі секретних ключів по мережі, і доступ до сервера стає можливим лише у разі успішної перевірки автентичності.

Цей процес гарантує, що секретні ключі не передаються по мережі, навіть у зашифрованому вигляді, а лише використовуються для шифрування та дешифрування даних, що робить систему Kerberos безпечною та ефективною для аутентифікації в відкритих мережах. Kerberos — це надійна та перевірена часом система, яка залишається актуальною в сучасних мережових середовищах. Її використання забезпечує захист аутентифікації та доступу до ресурсів, знижуючи ризики компрометації даних. Однак для забезпечення повного захисту даних рекомендується доповнювати систему Kerberos іншими механізмами безпеки.

10.6. ЦЕНТРАЛІЗОВАНИЙ КОНТРОЛЬ ВІДДАЛЕНОГО ДОСТУПУ

Для управління віддаленими з'єднаннями в мережах різних масштабів необхідне використання серверів віддаленого доступу, зокрема, при підключенні до великих локальних мереж, де кількість віддалених користувачів істотно зростає. В таких умовах один сервер віддаленого доступу вже не може виконувати всі функції керування підключеннями, що потребує впровадження централізованого контролю доступу. Центральне управління доступом до мережових ресурсів можна здійснити через сервер аутентифікації, який здійснює перевірку автентичності користувачів і керує їх доступом до різних сегментів мережі.

Стандартна схема контролю доступу включає в себе кілька етапів: користувач з'єднується із сервером віддаленого доступу (RAS), який здійснює першу аутентифікацію (наприклад, через протокол CHAP). Після цього користувач може отримати доступ до внутрішніх ресурсів, проходячи повторну аутентифікацію на серверах цих ресурсів. Така багаторівнева аутентифікація є незручною для користувача, оскільки кожен раз потрібно вводити різні паролі для кожного серверу, а адміністрування мережі стає складнішим через необхідність підтримки множинних баз

даних для кожного з серверів. Щоб вирішити ці проблеми, часто використовують систему єдиної аутентифікації (Single Sign-On, SSO), яка дозволяє користувачу увійти лише один раз, після чого доступ до всіх внутрішніх ресурсів стає можливим без повторного введення паролів. Цей підхід значно спрощує роботу як для користувачів, так і для адміністраторів, знижуючи ймовірність помилок і підвищуючи зручність використання. Водночас, для забезпечення високого рівня безпеки, система SSO повинна бути ретельно налаштована та інтегрована з усіма необхідними системами аутентифікації та авторизації. Це також дозволяє централізовано контролювати доступ до різноманітних ресурсів і моніторити користувацькі сесії для виявлення можливих порушень безпеки.

Також такі проблеми можна вирішити за допомогою централізованої служби аутентифікації, що дозволяє зберігати єдину базу даних для всіх серверів віддаленого доступу та керувати користувачами централізовано. Сервер аутентифікації не лише здійснює перевірку користувачів, а й виконує авторизацію їх доступу, а також веде облік всіх з'єднань, реєструючи дії користувачів. Важливою особливістю такої системи є те, що сервер аутентифікації може взаємодіяти із сучасними службами каталогів, такими як Microsoft Active Directory або Novell Directory Services, що дозволяє забезпечити інтеграцію з іншими системами аутентифікації та доступу до інформаційних ресурсів.

Для централізованого контролю віддаленого доступу використовуються спеціалізовані протоколи, серед яких найбільш поширеними є TACACS (Terminal Access Controller Access Control System) і RADIUS (Remote Authentication Dial-In User Service). Ці протоколи дозволяють створювати єдину систему управління для всіх серверів віддаленого доступу в мережі. Вони також надають адміністратору можливість централізовано управляти базами даних користувачів, привілеями доступу, а також моніторити використання ресурсів мережі. Завдяки централізованому управлінню, адміністратор може швидко змінювати політики доступу, оновлювати паролі або видаляти облікові записи користувачів без необхідності оновлювати конфігурації на кожному окремому сервері. Це дозволяє знижувати адміністративні витрати та підвищувати ефективність управління доступом. Крім того, зручність таких протоколів у забезпеченні зручного моніторингу всіх операцій робить їх важливими інструментами для забезпечення безпеки на великих підприємствах. Однак правильна конфігурація і регулярний аудит є важливими умовами для забезпечення належного рівня безпеки в таких системах.

Загальний опис протоколів RADIUS і TACACS+

Протоколи RADIUS (Remote Authentication Dial-In User Service) та TACACS+ (Terminal Access Controller Access-Control System Plus) широко використовуються для забезпечення аутентифікації, авторизації та обліку (AAA) доступу користувачів у сучасних мережах. Їх особливості визначаються різними цілями, для яких вони були створені, а також архітектурними підходами до безпеки та функціональності. RADIUS є більш орієнтованим на обробку аутентифікації та авторизації, здебільшого використовується для доступу до мереж, таких як VPN або Wi-Fi. Він підтримує шифрування лише паролів, що робить його менш безпечним у порівнянні з TACACS+, який надає розширені можливості для контролю доступу та детального обліку дій користувачів. TACACS+ забезпечує окрему обробку аутентифікації, авторизації та обліку, що дозволяє більш гнучко управляти доступом на різних рівнях. Крім того, TACACS+ використовує більш сильне шифрування, що робить його більш безпечним для використання в середовищах з підвищеними вимогами до захисту даних.

Протокол RADIUS

RADIUS був розроблений як легкий і масштабований протокол для підтримки доступу до мережевих ресурсів. Його специфікація описана в документах RFC-2138 та RFC-2139. Протокол підтримує аутентифікацію користувачів за допомогою обміну пакетами, що дозволяють перевірити правильність введених даних, а також надати або обмежити доступ до мережі. RADIUS працює на основі запитів і відповідей, де сервер здійснює перевірку наданих користувачем даних, таких як ім'я користувача і пароль. Завдяки своїй простоті та ефективності, протокол часто використовується для управління доступом в бездротових мережах та VPN-сервісах. Однак, незважаючи на свою популярність, він має деякі обмеження в плані безпеки, особливо коли йдеться про захист переданих даних. Для покращення безпеки в RADIUS використовується шифрування паролів користувачів, однак самі дані пакету, окрім паролів, передаються без шифрування, що може зробити протокол вразливим до атак типу "перехоплення". Оскільки RADIUS працює за допомогою UDP, він може бути менш надійним в умовах нестабільних мереж, де можливі втрати пакетів. У випадку необхідності більш високого рівня безпеки і надійності, часто використовують альтернативи, такі як TACACS+ або інші методи багатфакторної аутентифікації. Незважаючи на ці обмеження, RADIUS залишається ефективним і популярним вибором для управління доступом

у великих організаціях та для інтеграції з різними мережевими пристроями.



Рис. 10.13. Схема централізованого контролю віддаленого доступу з використанням протоколу RADIUS

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Схема централізованого контролю віддаленого доступу з використанням протоколу RADIUS передбачає централізовану аутентифікацію, авторизацію та облік для користувачів, які намагаються підключитися до мережесих ресурсів. Коли користувач ініціює з'єднання з віддаленим сервером або мережевим пристроєм, таким як маршрутизатор або точка доступу Wi-Fi, пристрій, що обробляє запит, виступає в ролі клієнта RADIUS і надсилає запит на аутентифікацію до RADIUS сервера. На сервері RADIUS відбувається перевірка наданих користувачем даних, таких як ім'я користувача та пароль, які порівнюються з базою даних, що зберігає інформацію про користувачів. Якщо дані є коректними, сервер надає підтвердження аутентифікації і визначає рівень доступу користувача до ресурсів мережі, після чого передає команду авторизації назад до клієнта. Авторизація, у свою чергу, може включати в себе не лише доступ до певних ресурсів, але й обмеження за протоколами, швидкістю з'єднання або іншими параметрами. Крім того, у процесі підключення на сервер також реєструються дії користувача, що забезпечує облік використання мережесих ресурсів. Основною перевагою протоколу RADIUS є його

масштабованість і простота, що робить його ідеальним для використання в бездротових мережах, VPN і для інших типів віддаленого доступу. Однак, незважаючи на свою ефективність, RADIUS має деякі обмеження в безпеці, оскільки дані, зокрема паролі, передаються у вигляді, що підлягає дешифруванню, і використовує менш надійний протокол UDP для передачі даних, що може призводити до втрат пакетів у випадку нестабільних мереж. Попри це, RADIUS залишається популярним вибором для реалізації централізованого контролю доступу завдяки своїй ефективності та можливості інтегруватися з різними системами управління доступом в мережах.

Основні характеристики протоколу:

Основні функції

RADIUS забезпечує базові процеси аутентифікації та авторизації, інтегруючи їх у спільний механізм. У разі успішної аутентифікації користувач отримує доступ до визначених ресурсів. Ця інтеграція зменшує гнучкість у створенні складних політик доступу. Проте, таке спрощене управління дозволами може бути достатнім для багатьох організацій, де вимоги до безпеки не є надмірно складними. RADIUS зручний для середовищ, де основна мета — швидка і проста аутентифікація користувачів, наприклад, у бездротових мережах або VPN. Однак в умовах, коли потрібне детальне налаштування доступу до різних ресурсів і виконання складних політик, таких як в корпоративних мережах, його можливості можуть виявитися обмеженими. У таких випадках TACACS+ буде кращим вибором через здатність розділяти аутентифікацію, авторизацію та облік, що забезпечує більшу гнучкість та контроль.

Протокол передачі

RADIUS використовує UDP, що забезпечує високу швидкість передачі даних. Однак цей транспортний протокол менш надійний через відсутність механізмів підтвердження доставки пакетів, що може призводити до втрат даних у великих або нестабільних мережах. Це обмеження може стати проблемою в ситуаціях, де важлива висока точність і надійність передачі даних, таких як у критичних інфраструктурах або при роботі з чутливою інформацією. Однак для більшості стандартних мережевих середовищ, де вимоги до надійності не є надмірно високими, RADIUS залишається ефективним і швидким рішенням. Враховуючи це, для організацій, що потребують високої надійності, RADIUS може бути комбінований з іншими механізмами відновлення чи фільтрації помилок. Незважаючи на обмеження, цей протокол досі є популярним завдяки простоті і швидкості роботи в менш вимогливих мережах.

Методи аутентифікації

Протокол підтримує PAP (Password Authentication Protocol) і CHAP (Challenge Handshake Authentication Protocol). Для складніших методів, таких як EAP (Extensible Authentication Protocol), потрібні спеціальні налаштування. PAP є простим і менш безпечним методом, оскільки пароль передається в незашифрованому вигляді, що робить його вразливим до перехоплення. З іншого боку, CHAP використовує механізм хешування для захисту пароля, що робить його більш безпечним, оскільки сам пароль не передається по мережі. EAP є більш гнучким і дозволяє використовувати різноманітні методи аутентифікації, зокрема сертифікати, смарт-карти чи біометричні дані. Проте для налаштування EAP необхідні додаткові ресурси та спеціалізовані налаштування на сервері та клієнтських пристроях.

Безпека

Шифрування обмежується лише паролями користувачів, що захищаються за допомогою MD5. Інші дані пакета передаються у відкритому вигляді, що робить RADIUS вразливим до атак перехоплення. Це означає, що атакуючий, маючи доступ до мережі, може легко отримати інформацію, що передається без шифрування, зокрема ідентифікатори користувачів та інші чутливі дані. Для захисту від таких атак можна використовувати додаткові механізми, такі як VPN або тунелювання, щоб забезпечити більший рівень безпеки. Однак на практиці, навіть з цією уразливістю, RADIUS залишається популярним завдяки своїй простоті та ефективності в умовах менш критичних середовищ. Для покращення безпеки часто комбінують RADIUS з іншими протоколами чи засобами шифрування, щоб компенсувати його недоліки.

Масштабованість і сумісність

Простота реалізації зробила RADIUS популярним серед сторонніх розробників і виробників мережевого обладнання. Протокол часто використовується для аутентифікації у Wi-Fi мережах, зокрема у рамках WPA2-Enterprise і WPA3-Enterprise. Ці стандарти забезпечують безпечний доступ до бездротових мереж, де кожен користувач має свій унікальний логін і пароль. Використання RADIUS у таких системах дозволяє централізовано керувати доступом до мережі та швидко змінювати політики безпеки. Протокол також підтримує інтеграцію з іншими системами обліку та контролю доступу, що робить його універсальним для різноманітних застосувань. Водночас, для високих вимог безпеки, таких як у фінансових установах, часто застосовують більш складні протоколи, зокрема TACACS+.

Протокол TACACS та TACACS+ TACACS

Протокол TACACS є більш складним і забезпечує роздільне зберігання облікових, автентифікаційних та авторизаційних даних, що покращує безпеку і гнучкість в управлінні доступом.

Протокол використовує архітектуру "клієнт-сервер", де сервер автентифікації (TACACS-сервер) здійснює перевірку і автентифікацію користувачів на основі наявної бази даних. При цьому всі запити від серверів віддаленого доступу передаються серверу TACACS, який в залежності від запиту, здійснює автентифікацію або авторизацію користувача. Кожен запит, що надходить від клієнта, містить ідентифікаційні дані користувача, які сервер TACACS використовує для перевірки в базі даних. Після успішної автентифікації сервер TACACS може визначити, які саме ресурси та команди користувач може використовувати. Авторизація здійснюється шляхом перевірки прав доступу користувача, визначених політиками. Це дозволяє забезпечити ефективно і точно управління доступом у мережах з різними рівнями безпеки.

Протокол RADIUS, в свою чергу, є простішим в реалізації і став більш популярним завдяки безкоштовним серверним програмам та меншій складності в налаштуванні. Протокол RADIUS також дозволяє ефективно інтегруватися із сучасними системами автентифікації та безпеки, такими як Kerberos. Хоча обидва протоколи (TACACS і RADIUS) мають схожі функціональні можливості, вибір між ними часто залежить від специфіки мережі і вимог до безпеки.

У сучасних реалізаціях TACACS і RADIUS можуть застосовуватися разом, де один з протоколів виступає як основна система для контролю доступу, а інший використовується для інтеграції з зовнішніми системами автентифікації. Протокол TACACS+, який є покращеною версією TACACS, забезпечує шифрування паролів при їх передачі і підтримує більш гнучку архітектуру для зберігання та управління даними користувачів. TACACS+ використовує алгоритм MD5 для шифрування паролів, що значно підвищує безпеку передачі даних по мережі.

Отже, використання централізованої системи автентифікації на базі протоколів TACACS або RADIUS дозволяє значно спростити адміністрування мережі, підвищити її безпеку і зменшити ймовірність виникнення помилок в процесі управління віддаленими з'єднаннями. Це особливо важливо для великих організацій, де використовується кілька серверів віддаленого доступу, що потребують інтеграції і централізованого

контролю доступу. Централізоване управління дозволяє зберігати всі облікові записи та політики доступу в одному місці, що спрощує оновлення та моніторинг. Крім того, зменшується ризик неконтрольованого доступу, оскільки всі аутентифікаційні та авторизаційні процеси проходять через єдиний точку перевірки. Такий підхід забезпечує гнучкість у налаштуванні рівнів доступу для різних категорій користувачів. В кінцевому результаті це сприяє оптимізації безпеки і більш ефективному використанню мережевих ресурсів.

TACACS+

Загалом, TACACS+ є сучасною розробкою компанії Cisco Systems, що є еволюцією попередніх версій TACACS і XTACACS. Цей протокол був розроблений з акцентом на підвищення безпеки та гнучкості налаштувань. TACACS+ дозволяє відокремлену обробку аутентифікації, авторизації та обліку, що дає змогу більш точно контролювати доступ до різних рівнів системи. Він використовує повне шифрування для всіх обміну даними між клієнтом і сервером, що забезпечує вищий рівень захисту порівняно з RADIUS. TACACS+ підтримує більш детальну та складну конфігурацію політик доступу, дозволяючи адміністраторам визначати точні правила для кожного користувача чи пристрою. Крім того, протокол пропонує підтримку багатьох типів аутентифікації, що дає можливість інтеграції з різноманітними системами та пристроями для управління доступом.

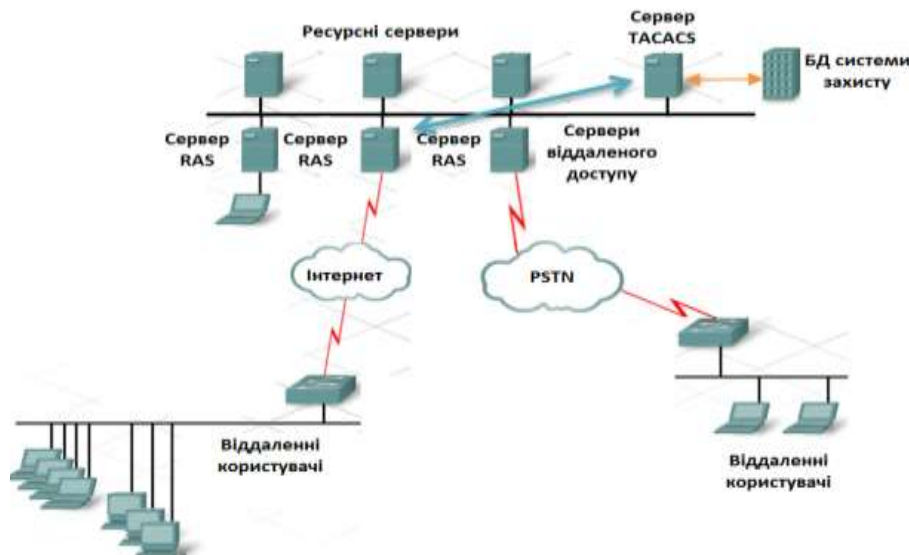


Рис. 10.14. Схема централізованого контролю віддаленого доступу з використанням протоколу TACACS

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Схема централізованого контролю віддаленого доступу з використанням протоколу TACACS+ передбачає централізовану аутентифікацію, авторизацію та облік доступу для користувачів через мережеві ресурси. У цьому випадку, коли користувач намагається підключитися до віддаленого сервера або пристрою, він спочатку ініціює з'єднання з мережевим пристроєм, таким як маршрутизатор чи комутатор, що підтримує протокол TACACS+. Цей пристрій виступає в ролі клієнта і передає запит на аутентифікацію до TACACS+ сервера, який обробляє перевірку даних користувача. Сервер перевіряє надані дані (наприклад, ім'я користувача та пароль) за допомогою своєї бази даних, визначаючи, чи має цей користувач право на доступ до мережевих ресурсів. Якщо аутентифікація є успішною, сервер TACACS+ може також виконати авторизацію, тобто визначити, які саме ресурси користувач може використовувати і які команди має право виконувати на мережевих пристроях. Крім того, кожна дія користувача, така як підключення або використання ресурсів, реєструється у спеціальній обліковій системі, що дозволяє адміністратору здійснювати моніторинг і контроль використання мережевих ресурсів. Завдяки своїй архітектурі, яка дозволяє розділяти функції аутентифікації, авторизації та обліку, протокол TACACS+ забезпечує більш гнучке і детальне управління доступом, що є важливим для великих організацій із складними вимогами до безпеки. Водночас TACACS+ використовує TCP для забезпечення надійності передачі даних, що дозволяє уникнути втрат пакетів, характерних для протоколів на основі UDP, таких як RADIUS. Всі дані, що передаються між клієнтом і сервером, включаючи паролі, шифруються, що підвищує рівень безпеки порівняно з іншими протоколами. Таким чином, централізоване використання протоколу TACACS+ забезпечує не тільки високий рівень безпеки, але й спрощує адміністрування мережі, дозволяючи централізовано керувати доступом та моніторити всі дії користувачів у реальному часі.

Основні особливості TACACS+:

Розподіл функцій

На відміну від RADIUS, TACACS+ розділяє процеси аутентифікації, авторизації та обліку. Це дозволяє створювати складні політики доступу, визначаючи, які ресурси або команди можуть використовувати окремі користувачі. Завдяки такій архітектурі TACACS+ дозволяє адміністраторам мережі точніше налаштовувати права доступу для кожного користувача, надаючи можливість контролювати доступ не тільки до мережевих ресурсів, але й до конкретних команд на пристроях. Це особливо корисно в середовищах, де є необхідність у наданні доступу до специфічних функцій або пристроїв лише певним групам користувачів,

наприклад, адміністраторам або технічному персоналу. Крім того, розділення цих процесів дозволяє знижувати ризики помилок, адже кожен етап можна налаштувати окремо, вносячи зміни лише в необхідні частини системи. Завдяки такій гнучкості TACACS+ забезпечує високий рівень контролю доступу та безпеки в складних мережевих середовищах.

Протокол передачі

TACACS+ базується на TCP, що забезпечує надійну передачу даних завдяки підтвердженню доставки та повторній передачі в разі помилок. Це робить протокол більш стійким до втрат даних у складних мережах. Завдяки використанню TCP, TACACS+ гарантує, що повідомлення досягне кінцевого пункту призначення без втрат, що є важливим у високонавантажених або ненадійних мережах. Така надійність забезпечує стабільність і безпеку протоколу, що є критично важливим для мереж з високими вимогами до аутентифікації та авторизації. Водночас, на відміну від RADIUS, який працює на основі UDP і може бути менш надійним в умовах нестабільного з'єднання, TACACS+ пропонує більш стабільну і безпечну передачу даних. Це дозволяє організаціям з високими вимогами до безпеки забезпечити більш надійний контроль доступу в мережах з різними рівнями інфраструктури.

Безпека

У TACACS+ шифрується весь пакет даних, включаючи паролі, що значно підвищує рівень захисту порівняно з RADIUS. Це особливо важливо для чутливих мереж, які потребують високого рівня конфіденційності. Шифрування всього пакету даних у TACACS+ гарантує, що навіть у разі перехоплення пакету сторонніми особами, вони не зможуть отримати доступ до важливих даних, таких як паролі або інші конфіденційні дані користувачів. Це додає ще один рівень захисту для мереж, де інформація повинна бути захищена від потенційних загроз. TACACS+ також забезпечує кращу гнучкість в управлінні політиками доступу, дозволяючи чітко визначати, хто і до яких саме ресурсів має доступ, а не просто загальний доступ до мережі. Завдяки цим перевагам протокол є ідеальним вибором для корпоративних і державних структур, які мають справу з чутливою інформацією і вимагають високого рівня безпеки.

Мультипроцесна обробка

TACACS+ дозволяє обслуговувати одночасно кілька користувачів завдяки мультипроцесній архітектурі. Це підвищує ефективність роботи у великих корпоративних мережах. Мультипроцесна архітектура дозволяє TACACS+ ефективно обробляти запити від численних користувачів одночасно, знижуючи навантаження на сервери і забезпечуючи швидку обробку аутентифікації та авторизації. Це важливо для великих організацій, де

кількість користувачів і пристроїв може бути значною, і забезпечення швидкого доступу до ресурсів є критичним для бізнес-процесів. Крім того, така архітектура дозволяє гнучко масштабувати систему, додаючи нові сервери без значних змін в існуючій інфраструктурі. Завдяки цьому TACACS+ добре підходить для середовищ, які вимагають високої продуктивності та масштабованості, зокрема в умовах зростаючої кількості користувачів та пристроїв.

Гнучкість і налаштування

Протокол дозволяє детально налаштовувати доступ до ресурсів аж до рівня команд, які користувачі можуть виконувати на мережевих пристроях. Це є ключовою перевагою TACACS+ для мереж із суворими вимогами до безпеки. TACACS+ дає змогу розділяти функції аутентифікації, авторизації та обліку, що забезпечує більшу гнучкість у створенні політик доступу. Це дозволяє адміністраторам точніше визначати, хто і які дії може виконувати в системі, що знижує ризики помилок або зловживань. Протокол також підтримує централізоване управління доступом, що спрощує адміністрування у великих організаціях. З цієї причини TACACS+ є популярним вибором для мереж, що потребують високого рівня контролю та безпеки.

Вибір протоколу

Вибір між RADIUS і TACACS+ залежить від потреб мережі. RADIUS зазвичай використовується для простих і масштабованих систем, таких як Wi-Fi мережі або VPN, де вимоги до складних політик доступу невисокі. TACACS+ більше підходить для великих корпоративних середовищ із високими вимогами до безпеки та детального управління доступом. Для мереж з великою кількістю користувачів і необхідністю забезпечення високої гнучкості у визначенні політик доступу TACACS+ є кращим вибором завдяки своїй здатності точно налаштовувати права доступу для кожного користувача. Крім того, TACACS+ часто застосовується в ситуаціях, де потрібен детальний облік всіх дій користувачів для подальшого аналізу або аудиту. RADIUS, завдяки своїй простоті і швидкості обробки запитів, може бути кращим вибором для середовищ, де пріоритетом є ефективність і швидкість обробки аутентифікації. Однак у середовищах з високими вимогами до захисту даних або контролю доступу, TACACS+ забезпечує значно більшу безпеку і можливості для детальної настройки.

Обидва протоколи залишаються актуальними у сучасному світі, але їхнє використання залежить від конкретних завдань, з якими стикається організація. RADIUS залишається популярним вибором для мережевих інфраструктур, де пріоритетом є швидка і масштабована аутентифікація,

наприклад, у бездротових мережах або підключеннях через VPN. TACACS+, зі своєю розширеною гнучкістю і можливостями для налаштування доступу, ідеально підходить для організацій, що потребують детальної та безпечної перевірки доступу в середовищах з високими вимогами до безпеки, таких як дата-центри чи управління корпоративними пристроями. Вибір між ними може також залежати від наявних інфраструктурних вимог, таких як підтримка мережевих пристроїв або наявність конкретних стандартів безпеки. Обидва протоколи можуть бути успішно інтегровані в різні архітектури, забезпечуючи надійний контроль доступу та моніторинг користувачів в організаціях різного розміру.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 10

1. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.
2. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
3. Лахно В. А., Васіліу Є. В., Гладких В. М., Домрачев В. М., Сивкова Н. М. (2020) Методи та засоби захисту інформації: навч. посіб. Київ: Компринт О. В. 444 с.
4. Сунь-Цзи. (2014) Мистецтво війни: переклад Г. Латника. Київ: Арій. 128 с.
5. Гришук Р.В. Основи кібернетичної безпеки : Монографія / Ю.Г. Даник, Р.В. Гришук ; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2019. – 636 с.
6. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.
7. Костюк Ю.В., Ковальова Л.І., Повна Н.І. Захист інформації у сегменті інформаційної системи на основі інтелектуальних технологій // Збірник тез VI Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2023. – с. 77-79.

8. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Порівняльний аналіз рішень для забезпечення контролю та управління привілейованим доступом в іт-середовищі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 98–112.
9. Костюк Ю.В. Математичне моделювання захищених інформаційних систем // Інноваційний потенціал сучасної науки: зб. наук. праць IV Всеукраїнської наук.-практ. інтернет-конф., (18 травня 2023 року. Кам'янець-Подільський). - Кам'янець-Подільський Заклад вищої освіти «Подільський державний університет», 2023. с. 171-174.
10. Z. B. Hu, V. Buriachok, V. Sokolov, Implementation of Social Engineering Attack at Institution of Higher Education, in: 1th International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), vol. 2654 (2020) pp. 155–164.
11. Костюк Ю.В., Кравченко Д.В. Методи захисту даних на підприємствах соціальної сфери. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1033-1047.
12. O. Deineka, et al., Designing Data Classification and Secure Store Policy According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 398409.
13. Костюк Ю.В., Самойленко Ю.О. Спеціалізовані моделі для проектування, розробки та реалізації інформаційних систем // Матеріали IX Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами», 25 листопада 2022 [Електронний ресурс]. – К: НУХТ, 2022. – с. 206-207.
14. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроектні рішення щодо побудови системи авторизації на основі концепції ZERO TRUST. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242.
15. R. Marusenko, V. Sokolov, I. Bogachuk, Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation, Advances in Artificial Systems for Logistics Engineering, vol. 135 (2022) 583–594.
16. Костюк Ю. В Впровадження інтелектуальних систем у процес оцінки ризиків інформаційної безпеки в безпроводових мережах // Сьомі Геретівські читання: наукові статті, тези доповідей та інші матеріали Всеукраїнської науково-практичної конференції (м. Тернопіль, Україна, 22 вересня 2023 року). Науковий, методичний, інформаційний збірник

Тернопільського обласного комунального інституту післядипломної педагогічної освіти / Редколегія: О. М. Петровський, В. С. Мисик, І. М. Вітенко, О. І. Когут, Ю. Ч. Шайнюк, Т. В. Магера, Ф. І. Полянський, Н. Б. Стрийвус, Г. І. Герасимчук. Тернопіль: ТОКІППО, 2023. С. 162-168.

17. S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.

18. Костюк Ю.В., Войткевич А.А. Дослідження технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1017-1032.

19. O. Romanovskyi, et al., Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition, Advances in Computer Science for Engineering and Education IV, vol. 83 (2021) 25–36.

20. Костюк Ю.В., Шапран В.О. Технології виявлення аномальних подій та сигнатур в реальному часі. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1069-1084.

21. S. Kulibaba, Advanced Communication Model with the Voice Control and the Increased Security Level, CEUR Workshop, 3288 (2022) 64–72.

22. Y. Dreis, et al., Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 277–289.

23. M. TajDini, et al., Brainwave-based Authentication using Features Fusion, Comput. Secur. 129, no. 103198 (2023) 1–11.

24. D. Shevchuk, et al., Designing Secured Services for Authentication, Authori-zation, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.

РОЗДІЛ 11

ВИКОРИСТАННЯ СПИСКІВ КОНТРОЛЮ ДОСТУПУ



- 11.1. Типи і використання списків контролю доступу**
- 11.2. Використання шаблонних масок**
- 11.3. Стандартні списки контролю доступу**
- 11.4. Розширені списки контролю доступу**
- 11.5. Іменовані списки контролю доступу**
- 11.6. Розміщення стандартних і розширених списків контролю доступу**
- 11.7. Перевірка списків контролю доступу**

" Списки контролю доступу є серцем управління інформаційною безпекою: вони встановлюють чіткі правила гри, забезпечуючи рівновагу між доступністю та захищеністю ресурсів."

Джон Максвелл, експерт з інформаційної безпеки

11.1. Типи і використання списків контролю доступу

Списки контролю доступу (ACL, Access Control Lists) використовуються для визначення прав доступу користувачів до ресурсів в інформаційних системах. Існують різні типи ACL, залежно від того, як вони реалізуються та яким чином контролюють доступ до системних ресурсів. Одним з типів є списки контролю доступу на основі файлів (File ACL), які контролюють доступ до файлів і папок у файлових системах,

визначаючи, хто може читати, записувати або виконувати файли. Зазвичай вони використовуються в операційних системах, таких як Windows, Linux і Unix. Інший тип - списки контролю доступу для мережевих ресурсів (Network ACL), які застосовуються до мережевих маршрутизаторів або брандмауерів, щоб контролювати доступ до мережевих ресурсів або блокувати певний трафік. Вони дозволяють або відмовляють у доступі до мережі залежно від IP-адреси, порту або протоколу.

Списки контролю доступу до об'єктів (Object ACL) застосовуються до різних об'єктів в інформаційних системах, таких як бази даних або сервісні додатки, дозволяючи визначити, хто має право доступу до конкретних записів, таблиць або інших ресурсів. Динамічні списки контролю доступу (Dynamic ACL) дозволяють змінювати права доступу в реальному часі на основі певних умов або подій. Це може бути корисно в ситуаціях, де доступ необхідно змінювати в залежності від часу доби або поточного стану системи.

Списки контролю доступу на основі ролей (Role-Based Access Control, RBAC) надають доступ на основі ролей, які мають користувачі в організації, що визначає, які ресурси можна використовувати і що з ними можна робити. У великих організаціях для кожного співробітника встановлюється певна роль, наприклад, адміністратор, користувач або гість, що визначає рівень доступу до корпоративних систем або документів.

Списки контролю доступу на основі атрибутів (Attribute-Based Access Control, ABAC) надають доступ на основі атрибутів користувачів або ресурсів, таких як вік, місцезнаходження, група, статус тощо. Вони застосовуються, наприклад, у медичних установах, де доступ до пацієнтських записів може бути надано залежно від атрибутів медичного працівника або в залежності від місця роботи.

Використання ACL включає контроль доступу до файлів і директорій, забезпечення безпеки мережі через обмеження доступу до ресурсів мережі та управління доступом у додатках для визначення прав доступу користувачів до певних функцій чи інформації. Загалом, ефективне використання списків контролю доступу дозволяє зменшити ризик несанкціонованого доступу до ресурсів і забезпечити контроль за правами доступу в інформаційних системах.

Фільтрування трафіку

Фільтрація трафіку є важливим інструментом забезпечення безпеки сучасних мереж. Вона передбачає обробку IP-пакетів маршрутизаторами та фаєрволами, що дозволяє блокувати небажані пакети або змінювати їх маршрутизацію. Це дозволяє не лише запобігати атакам на мережу,

заздалегідь блокуючи доступ до неї для потенційно небезпечних зовнішніх джерел, а й зупиняти атаки, якщо їх джерело не було виявлено заздалегідь. Крім того, фільтрація трафіку надає адміністраторам можливість контролювати потоки даних у різних сегментах мережі, аналізуючи вміст пакетів і приймаючи рішення щодо їх дозволу або блокування.

Сучасні технології фільтрації трафіку використовують як базові критерії, такі як IP-адреси, MAC-адреси, протоколи та типи програм, так і складніші механізми, зокрема глибокий аналіз пакетів (DPI), аналіз поведінки трафіку, контекстний аналіз і методи штучного інтелекту. Це дозволяє виявляти аномалії, аналізувати вміст даних у пакетах і динамічно адаптуватися до нових загроз. Наприклад, використання AI дозволяє системам фільтрації прогнозувати можливі атаки та ефективніше захищати мережу.

Однією з ключових переваг фільтрації трафіку є захист від атак, таких як DDoS, фішинг чи спроби сканування портів. Відхиляючи небажаний трафік на ранньому етапі, система не лише підвищує безпеку мережі, а й оптимізує її продуктивність, зменшуючи навантаження на інфраструктуру та звільняючи ресурси для легітимних користувачів. Крім того, фільтрація забезпечує гнучкий контроль доступу, дозволяючи адміністраторам налаштовувати політики безпеки відповідно до конкретних потреб підприємства.

Для реалізації фільтрації трафіку використовуються різні пристрої, такі як маршрутизатори з вбудованими міжмережевими екранами, апаратні фаєрволи, системи запобігання вторгнень (IPS) та хмарні служби безпеки. Більш складні системи безпеки здатні розпізнавати та блокувати відомі типи атак із зовнішніх джерел, а також інтегруватися з іншими сучасними рішеннями, такими як Zero Trust Architecture (ZTA) чи мережеві системи SD-WAN.

Однак фільтрація трафіку стикається з певними викликами. Зростання обсягу зашифрованого трафіку ускладнює його аналіз, а поява нових видів атак вимагає постійного оновлення алгоритмів і сигнатур. До того ж необхідно забезпечити високу продуктивність пристроїв фільтрації, щоб уникнути затримок у високонавантажених мережах.

У майбутньому очікується впровадження квантових алгоритмів для покращення криптоаналізу, подальший розвиток технологій DPI та інтеграція штучного інтелекту для передбачення загроз. Фільтрація трафіку залишається одним із ключових механізмів забезпечення кібербезпеки, що постійно вдосконалюється, адаптуючись до нових умов і викликів цифрового середовища.

Списки контролю доступу (ACL): принципи роботи, типи та сучасні виклики

Списки контролю доступу (Access Control Lists, ACL) є одним із ключових інструментів для управління трафіком і забезпечення безпеки мережі. Вони дозволяють адміністраторам мережі здійснювати фільтрацію трафіку, регулювати доступ до внутрішніх та зовнішніх ресурсів і створювати індивідуальні стратегії безпеки. Використання ACL дає змогу мінімізувати ризики несанкціонованого доступу, контролювати потік даних через інтерфейси маршрутизаторів і забезпечувати загальний захист мережевої інфраструктури.

ACL виконують низку функцій, серед яких основними є фільтрація внутрішніх пакетів, захист мережі від несанкціонованого доступу та контроль доступу до портів віртуальних терміналів. Їх застосування базується на порівнянні кожного пакета із заданими правилами, що дозволяють або блокують його передачу. Однак ефективність роботи ACL залежить від правильної конфігурації, адже неправильно організовані або некоректно розміщені списки можуть призвести до втрати продуктивності мережі, надмірного навантаження на маршрутизатори або навіть створення уразливостей.

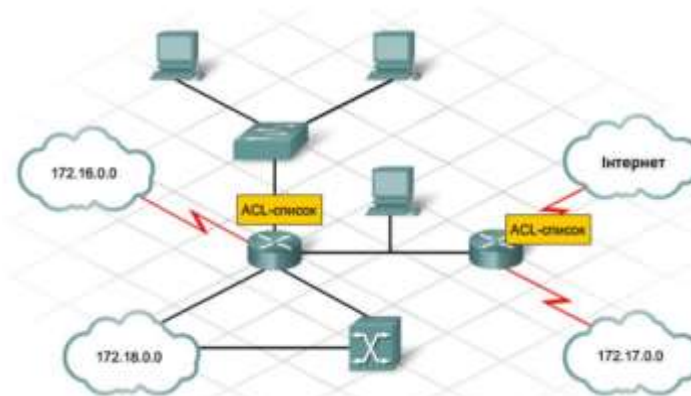


Рис. 11.1. Приклад використання ACL-списків
Джерело: Джерело: [1-6]

Принцип роботи ACL базується на аналізі кожного пакета, що проходить через маршрутизатор. Кожен список контролю доступу складається з набору правил, які маршрутизатор перевіряє у послідовному порядку. Якщо пакет відповідає одному з правил, обробка завершується відповідно до цього правила. У разі, якщо пакет не задовольняє жодному з умов, спрацьовує неявна інструкція заборони всього трафіку, яка автоматично додається в кінець кожного списку. Ця логіка забезпечує високу надійність у фільтрації небажаного трафіку.

ACL поділяються на три основні типи: стандартні, розширені та іменовані. Стандартні ACL є найпростішими і забезпечують фільтрацію за вихідною IP-адресою пакета. Вони застосовуються у випадках, коли потрібна проста заборона або дозвіл доступу до мережі на основі IP-адрес. Розширені ACL, у свою чергу, дозволяють здійснювати більш детальну фільтрацію, враховуючи такі параметри, як вихідна і кінцева IP-адреси, протоколи і номери портів. Вони забезпечують більшу гнучкість і використовуються для складних мережевих сценаріїв. Іменовані ACL є сучасним підходом, що забезпечує зручність управління за рахунок використання описових назв замість числових ідентифікаторів.

Процес налаштування ACL складається з двох етапів: створення списку доступу та його прив'язки до певного інтерфейсу маршрутизатора. Адміністратор може застосовувати ACL до вхідного або вихідного трафіку. Вхідний трафік аналізується під час його надходження на інтерфейс маршрутизатора, тоді як вихідний перевіряється перед передачею даних до наступного вузла мережі.

Сучасні виклики у використанні ACL пов'язані із зростанням складності мереж та обсягів зашифрованого трафіку. Підприємства стикаються з необхідністю адаптувати ACL до високошвидкісних мереж, забезпечуючи мінімальні затримки при фільтрації. Крім того, сучасні кібератаки, такі як DDoS або багаторівневі атаки, потребують інтеграції ACL із системами глибокого аналізу трафіку (DPI) та використання технологій штучного інтелекту для автоматизованого виявлення аномалій.

Для вирішення цих проблем розробляються автоматизовані системи управління ACL, які дозволяють зменшити вплив людського фактору, інтегруються із хмарними платформами безпеки та підтримують принципи Zero Trust. Завдяки цьому ACL залишаються невід'ємною частиною сучасної мережевої інфраструктури, забезпечуючи баланс між безпекою та продуктивністю.

11.2. ВИКОРИСТАННЯ ШАБЛОННИХ МАСОК

Шаблонні маски (или шаблони) в контексті безпеки інформаційних систем використовуються для визначення та контролю доступу до певних даних, ресурсів або функцій на основі заданих параметрів. Вони є потужним інструментом для управління доступом і дозволяють створювати правила, які обмежують чи дозволяють доступ у залежності від шаблонів, що визначають умови доступу.

Один з основних типів шаблонів — шаблони для аутентифікації та авторизації користувачів, які використовуються для верифікації та надання прав доступу до ресурсів. Наприклад, шаблон може визначати, що лише користувачі з певними атрибутами (наприклад, певною роллю або групою) мають доступ до конфіденційних даних.

Шаблонні маски для пошуку та фільтрації використовуються для обробки та аналізу великих обсягів даних. Це дозволяє здійснювати пошук за заданими критеріями, що відповідають певному шаблону, для виявлення потенційно небезпечної або порушуючої політику інформації. Ці шаблони можуть включати регулярні вирази або інші типи фільтрації, що дозволяють знаходити чутливі дані, такі як номери кредитних карт, паролі або інші персональні відомості.

Шаблони для моніторингу та аудиту використовуються для відстеження діяльності в інформаційних системах. Вони допомагають створити специфічні правила, що визначають, які події повинні бути записані для подальшого аналізу. Наприклад, шаблон може відслідковувати спроби доступу до важливих файлів або неправомірні спроби увійти в систему.

Шаблони для автоматизації процесів захисту дозволяють створювати політики та процедури для автоматичного реагування на певні події, що можуть свідчити про порушення безпеки. Це включає автоматичне блокування доступу або повідомлення відповідних осіб про можливу загрозу на основі заданих шаблонів.

Загалом, використання шаблонних масок є важливим інструментом для посилення безпеки інформаційних систем і зменшення ризику витоку або несанкціонованого доступу до чутливої інформації. Вони дозволяють ефективно управляти доступом і реалізувати заходи з моніторингу та захисту на основі чітко визначених умов та шаблонів.

У простих ACL-списках зазвичай вказується тільки одна конкретна IP-адреса, яка або дозволена, або заблокована. Це підходить для простих сценаріїв, коли потрібно фільтрувати доступ до конкретних хостів. Однак, коли необхідно блокувати кілька адрес або цілий діапазон адрес, одного рядка не достатньо. В таких випадках використовуються шаблонні маски (Wildcard Mask), що дозволяють значно розширити можливості фільтрації. Замість численних інструкцій для блокування кожної адреси чи діапазону можна застосувати одну маску, яка надасть більшу гнучкість і спростить конфігурацію ACL.

Шаблонна маска є 32-розрядним двійковим кодом, розбитим на чотири октети, записаними в десятковому форматі. Цей формат маски дає змогу вказувати, які частини IP-адреси повинні бути перевірені, а які

можуть бути ігноровані. В шаблонній масці одиниці означають, що відповідні біти в адресі можуть бути будь-якими (тобто не перевіряються), а нулі вказують, що відповідні біти адреси повинні точно співпадати з заданими значеннями.

Наприклад, запис 219.17.100.2 0.0.0.0 в ACL вказує на конкретний хост з IP-адресою 219.17.100.2, оскільки шаблонна маска 0.0.0.0 не дозволяє жодної варіації в адресі. У той же час запис 219.17.100.2 0.0.0.255 вказує на всі хости, що належать до мережі 219.17.100.0, оскільки маска дозволяє будь-які значення в останньому октеті IP-адреси.

Для більш складних мереж, як, наприклад, підмережа 192.168.77.32/27 (маска 255.255.255.224), шаблонна маска для ACL буде 0.0.0.31. Це означає, що лише останні 5 біт в адресі будуть перевірятися, дозволяючи фільтрувати всі хости, що належать до цієї підмережі.

Крім того, для спрощення налаштування існують спеціальні ключові слова `host` та `any`, які використовуються для вираження стандартних шаблонів. Ключове слово `host` еквівалентно масці 0.0.0.0, що означає точну відповідність одній IP-адресі. Наприклад, запис `host 219.17.100.2` має такий самий ефект, що і запис `219.17.100.2 0.0.0.0`.

Використання ключового слова `any` дає змогу позначити, що адреса може бути будь-якою в межах цієї маски. Це еквівалентно масці 0.0.0.0 255.255.255.255, що означає, що жоден біт адреси не буде аналізуватися і всі адреси будуть вважатися допустимими.

Така гнучкість шаблонних масок в ACL дозволяє адміністраторам точно контролювати доступ до мережі, блокуючи або дозволяючи певні діапазони адрес або окремі хости за допомогою простих та ефективних налаштувань. З урахуванням сучасних вимог до безпеки мереж і значного збільшення обсягів трафіку, шаблонні маски є важливим інструментом для оптимізації конфігурації ACL, дозволяючи реалізовувати складні стратегії фільтрації з мінімальними витратами ресурсів.

11.3. СТАНДАРТНІ СПИСКИ КОНТРОЛЮ ДОСТУПУ

Стандартні списки доступу (ACL) є важливим інструментом для контролю доступу в мережах TCP/IP. Вони дозволяють здійснювати фільтрацію трафіку, відкидаючи або пропускаючи пакети на основі їх вихідної IP-адреси. Стандартні ACL-списки зазвичай використовуються для базового контролю, коли необхідно перевіряти тільки вихідну адресу пакета, не звертаючи уваги на інші його характеристики, такі як порти чи протоколи.

Щоб створити стандартний ACL-список, необхідно увійти в режим глобальної конфігурації маршрутизатора або комутатора та використати команду `access-list`, яка дозволяє визначити набір інструкцій для фільтрації трафіку. Команда має такий синтаксис: `access-list номер списку доступу {permit | deny} [вихідна адреса] [шаблонна маска]`. У цій команді ключове слово `permit` або `deny` визначає, чи дозволяється, чи забороняється пакет, що відповідає зазначеному шаблону. Параметр "вихідна адреса" вказує на IP-адресу, яку слід перевірити, а шаблонна маска дозволяє визначити, які біти цієї адреси будуть перевірятися.

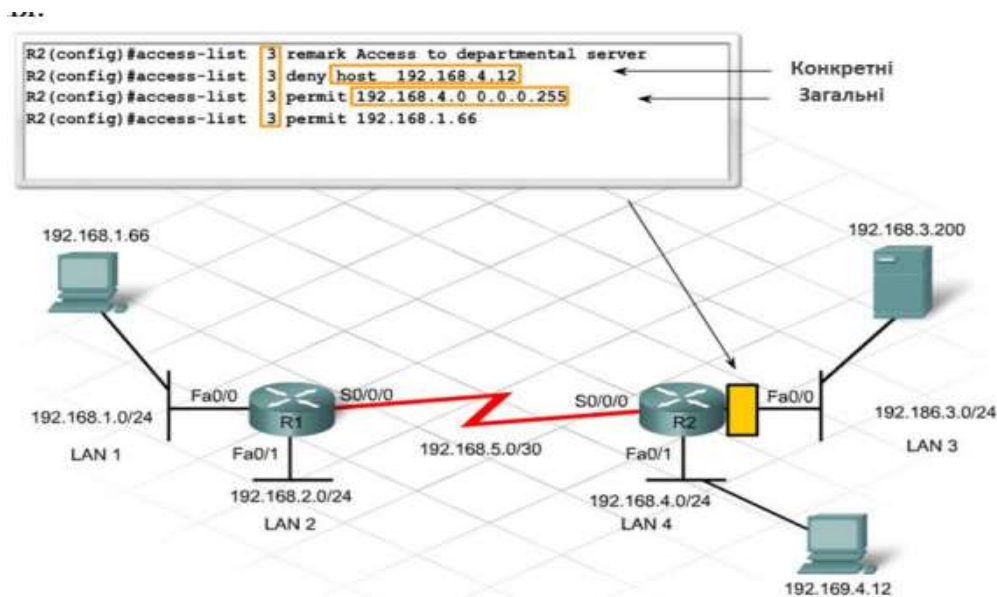


Рис. 11.2. Приклад використання стандартного ACL-списку
Джерело: [1-6]

Приклад конфігурації стандартного ACL може виглядати так: якщо необхідно заблокувати доступ з конкретного хоста в мережі, при цьому дозволивши доступ усім іншим хостам з цієї ж мережі, це можна зробити за допомогою таких інструкцій:

```
R2# conf t
R2(config)# access-list 3 deny host 192.168.4.12
R2(config)# access-list 3 permit 192.168.4.0 0.0.0.255
R2(config)# access-list 3 permit 192.168.1.66 0.0.0.0
```

У цьому випадку забороняється доступ до хоста 192.168.4.12, а також дозволяється доступ для всіх хостів з підмережі 192.168.4.0/24 та для хоста 192.168.1.66 з іншої мережі.

Один з важливих моментів при налаштуванні ACL — це правильний порядок інструкцій. Оскільки пакети порівнюються з інструкцією в списку

доступу до того, як буде знайдено відповідність, важливо, щоб більш специфічні інструкції знаходились перед більш загальними. Якщо перша інструкція дозволяє пакет, а наступна його забороняє, пакет буде дозволений. Тому порядок інструкцій має вирішальне значення для налаштування ACL-списку.

Для кращої документації та зручності адміністрування ACL можна додавати коментарі, використовуючи команду `remark`. Це дозволяє пояснити функцію кожної інструкції, що допомагає при підтримці списків доступу в майбутньому.

Фільтрація за допомогою ACL-списку не буде працювати, поки цей список не буде застосований до інтерфейсу маршрутизатора або комутатора. Для цього необхідно перейти в режим конфігурації інтерфейсу та використовувати команду `ip access-group`. Вказуючи параметри `in` чи `out`, можна налаштувати фільтрацію для вхідних або вихідних пакетів:

```
R2(config)# interface fastethernet 0/0
```

```
R2(config-if)# ip access-group 3 out
```

Це дозволить маршрутизатору фільтрувати вихідний трафік через інтерфейс FastEthernet0/0.

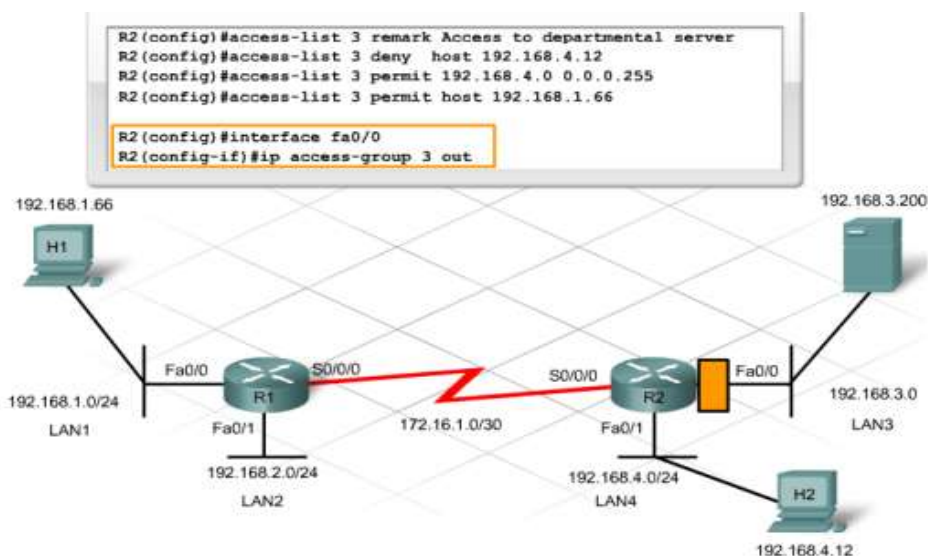


Рис. 11.3. Приклад зв'язування стандартного ACL-списку
Джерело: [1-6]

Крім того, важливо знати, що ACL-список можна видалити повністю, використовуючи команду `no access-list` номер списку доступу. При цьому неможливо видалити окремі рядки зі списку, тому при необхідності змінити ACL потрібно повністю створити новий список.

Таким чином, стандартні ACL-списки є потужним інструментом для базової фільтрації трафіку, що дозволяє контролювати доступ до мережі. Вони використовуються для перевірки вихідних IP-адрес пакета, дозволяючи або забороняючи його проходження. Важливими аспектами їх налаштування є правильний порядок інструкцій, використання коментарів для полегшення адміністрування та правильне застосування ACL до інтерфейсів маршрутизатора.

11.4. РОЗШИРЕНІ СПИСКИ КОНТРОЛЮ ДОСТУПУ

Розширені списки контролю доступу (ACL) мають схожу функцію з стандартними списками контролю доступу, але значно розширюють можливості фільтрації трафіку завдяки більш гнучким критеріям. У стандартних ACL фільтрація пакету відбувається лише на основі вихідної IP-адреси, що обмежує їх застосування до простих сценаріїв. Натомість розширені ACL дозволяють здійснювати фільтрацію за декількома критеріями, такими як вихідна та призначена IP-адреса, тип протоколу (TCP, UDP, ICMP тощо), а також порти, що дає змогу більш детально регулювати доступ до ресурсів мережі. Така можливість значно розширює функціонал ACL, дозволяючи створювати більш складні й точні механізми контролю доступу.

Формат рядків розширеного ACL включає в себе кілька додаткових параметрів, що дозволяють точно налаштувати доступ до конкретних IP-адрес і портів, а також застосовувати фільтрацію за протоколами. Стандартний синтаксис для створення інструкцій ACL виглядає таким чином:

access-list номер ACL-списку {permit | deny} [протокол] [вихідна адреса] [шаблонна маска] [адреса призначення] [шаблонна маска] [умова відповідності порту] [порт]

У цьому рядку протокол (наприклад, IP, TCP, UDP) визначає тип трафіку, що фільтрується. Далі вказуються вихідна та призначена IP-адреси, а також порти, якщо необхідно фільтрувати за ними. Залежно від потреб можна детально налаштовувати доступ, наприклад, дозволити або заборонити з'єднання з конкретними адресами чи портами.

Наприклад, для мережі, де сервер з IP-адресою 192.168.3.75, можна створити розширений ACL для фільтрації трафіку таким чином: дозволити доступ до цього сервера з мережі 192.168.2.0, дозволити доступ з конкретного хоста 192.168.1.66, заборонити доступ з мережі 192.168.4.0 та дозволити доступ з усіх інших адрес в компанії. У такому випадку відповідні команди для налаштування ACL будуть наступними:

```
R2# conf t
R2(config)# access-list 103 permit ip 192.168.2.0 0.0.0.255 host
192.168.3.75
R2(config)# access-list 103 permit ip host 192.168.1.66 host 192.168.3.75
R2(config)# access-list 103 deny ip 192.168.4.0 0.0.0.255 host
192.168.3.75
R2(config)# interface fastethernet 0/0
R2(config-if)# ip access-group 103 out
```

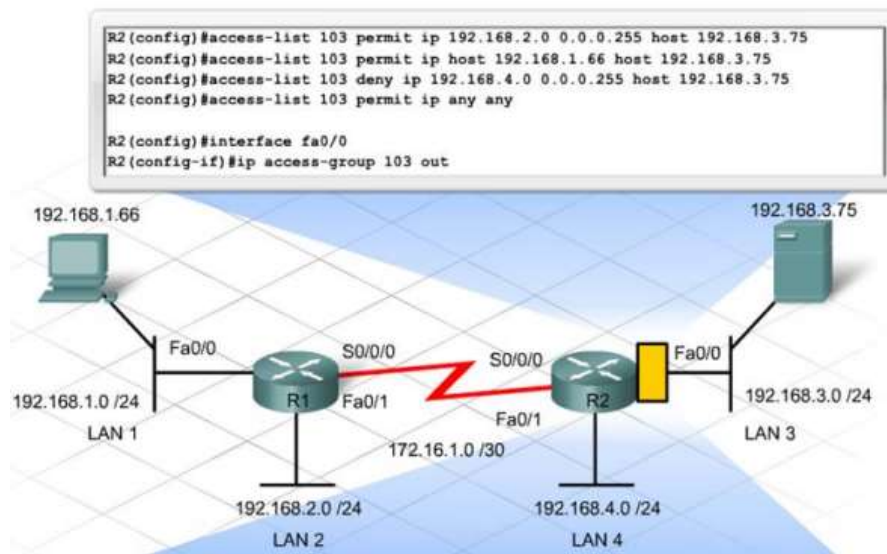


Рис. 11.4. Приклад використання розширеного ACL-списку
Джерело: [1-6]

Ці команди створюють розширений список контролю доступу з номером 103, який фільтрує трафік до сервера 192.168.3.75 на основі заданих умов. Важливо, що в розширених ACL можна не вказувати порт, що дозволяє пропускати трафік через усі порти, або можна налаштувати фільтрацію за конкретними портами, використовуючи різні оператори. Наприклад, якщо необхідно дозволити доступ тільки до порту 80 (HTTP) для веб-сервера, можна застосувати такий запис:

```
R1(config)# access-list 122 permit tcp 192.168.1.0 0.0.0.255 host
192.168.2.89 eq 80
```

Ця інструкція дозволяє трафік на порт 80 для сервера 192.168.2.89, що знаходиться в компанії, при цьому всі інші з'єднання (наприклад, через Telnet або FTP) будуть заблоковані.

Що стосується використання портів, то для точнішого налаштування можна застосовувати різні оператори відповідності портам, такі як eq для точного порту, gt для більших портів, lt для менших, neq для всіх, крім

вказаного порту, і range для діапазону портів. Це дозволяє контролювати доступ до конкретних сервісів або обмежувати доступ до певних типів трафіку на основі порту.

Таким чином, розширені ACL надають набагато більше можливостей для точного контролю доступу в порівнянні зі стандартними списками, завдяки чому вони є потужним інструментом для забезпечення безпеки в мережах і надають адміністраторам більше гнучкості у фільтрації трафіку на основі різних параметрів.

11.5. ІМЕНОВАНІ СПИСКИ КОНТРОЛЮ ДОСТУПУ

Іменовані списки контролю доступу (ACL, Access Control Lists) — це механізм управління доступом, який дозволяє визначати, які користувачі або групи користувачів мають доступ до певних ресурсів в інформаційних системах, а також які дії вони можуть виконувати з цими ресурсами. У контексті ACL кожен об'єкт (наприклад, файл, каталог, або мережевий ресурс) має асоційований список, що містить правила або записи про доступ. Іменовані списки контролю доступу зазвичай включають такі елементи: ідентифікацію суб'єктів доступу, визначення типів дій та іменування списку. Ідентифікація суб'єктів доступу вказує на користувачів або групи, які можуть або не можуть виконувати певні операції на ресурсах. Типи дій визначають, які саме операції можуть бути виконані на ресурсі, такі як читання, запис або виконання файлів або мережевих операцій. Іменування списку дозволяє організувати правила в зручні групи або категорії, що спрощує їхнє адміністрування і використання. Іменовані ACL мають кілька переваг, таких як гнучкість, зручність в адмініструванні та масштабованість. Вони дозволяють централізовано керувати доступом до кількох ресурсів одночасно, що зменшує ймовірність помилок і спрощує зміну політик доступу. Проте іменовані ACL можуть мати й певні недоліки, зокрема складність у підтримці та моніторингу великої кількості правил доступу в умовах постійного змінювання політик безпеки.

Програмне забезпечення Cisco IOS версії 11.2 та вище підтримує створення іменованих списків контролю доступу (NACL, Named Access Control Lists), які є сучасним та ефективним інструментом для управління доступом у мережах. Основна відмінність іменованих ACL від стандартних та розширених полягає в тому, що замість числових діапазонів використовуються описові імена, які значно спрощують адміністрування та організацію списків доступу. Іменовані ACL володіють усіма можливостями стандартних і розширених ACL, однак їх конфігурація стає більш зрозумілою завдяки унікальним іменам.

Процес створення іменованого ACL починається з команди: `ip access-list {standard | extended} ім'я`.

Ця команда переводить маршрутизатор у режим конфігурації іменованого списку доступу, де адміністратор може вводити всі необхідні правила дозволу або заборони доступу. Іменований ACL може містити інструкції, аналогічні тим, що використовуються у стандартних або розширених ACL. Наприклад:

```
R1(config)# ip access-list extended cisco
```

```
R1(config-ext-nacl)# permit ip 192.168.1.66 0.0.0.0 any
```

```
R1(config-ext-nacl)# permit ip 192.168.1.77 0.0.0.0 any
```

У цьому прикладі створюється іменований розширений ACL з назвою `cisco`, який дозволяє трафік з IP-адрес 192.168.1.66 та 192.168.1.77 до будь-яких цільових адрес (вказано як `any`). Кожна інструкція вводиться окремо, що робить процес гнучким і зрозумілим.

Після створення списку доступу він прив'язується до певного інтерфейсу маршрутизатора за допомогою команди `ip access-group`. Наприклад:

```
R1(config)# interface fa0/0
```

```
R1(config-if)# ip access-group cisco out
```

У цьому випадку іменований ACL `cisco` застосовується до інтерфейсу `FastEthernet0/0` для фільтрації вихідного трафіку (`out`). Така прив'язка здійснюється аналогічно стандартним та розширеним ACL, що дозволяє використовувати знайомі принципи налаштування.

Іменовані ACL мають численні переваги. По-перше, використання описових імен замість числових діапазонів значно полегшує адміністрування. Наприклад, ім'я `"web-filter"` або `"vpn-restrictions"` відразу вказує на призначення списку доступу, тоді як числові діапазони не надають такої інформації. По-друге, іменовані ACL забезпечують більшу гнучкість при внесенні змін. Додавання нових правил чи редагування існуючих інструкцій є простішим і не потребує повного перезавантаження списку, як у випадку числових ACL.

Також важливим є те, що іменовані ACL сприяють зменшенню помилок у конфігурації, оскільки адміністратори можуть чіткіше структурувати політики доступу. Наприклад, у складних мережах із великою кількістю пристроїв іменовані ACL полегшують діагностику та усунення неполадок, оскільки правила доступу легко ідентифікуються за їхнім ім'ям.

Отже, іменовані ACL є сучасним стандартом у конфігурації мереж Cisco, що забезпечує зручність, гнучкість та прозорість управління доступом. Вони особливо корисні в масштабних і складних мережах, де

потрібна чітка структура правил безпеки для забезпечення стабільної та захищеної роботи інформаційних систем.

11.6. Розміщення стандартних і розширених списків контролю доступу

Розміщення стандартних і розширених списків контролю доступу (ACL) залежить від конкретних потреб інформаційної системи, її структури та вимог до безпеки. Стандартні ACL зазвичай використовуються для базового контролю доступу, де кожен запис в списку визначає право доступу для певного користувача або групи користувачів до конкретного ресурсу. У таких списках можуть бути лише записи про типи доступу (наприклад, доступ на читання або запис) для певних користувачів. Розширені ACL пропонують більше можливостей для детального налаштування доступу, включаючи специфікацію як джерела та призначення трафіку, так і конкретних типів операцій з ресурсами.

Стандартні ACL зазвичай розміщуються на рівні окремих ресурсів, таких як файли, каталоги або пристрої в інформаційних системах, і визначають доступ для кожного користувача або групи. Вони зберігаються локально в ресурсах, що дозволяє швидко і ефективно контролювати доступ до окремих об'єктів. Розширені ACL, навпаки, часто використовуються на рівні мережевих пристроїв або серверів і дозволяють вказувати детальні умови доступу до ресурсів, включаючи параметри IP-адрес, порти, протоколи і інші мережеві атрибути.

У більш складних і масштабованих інформаційних системах, розширені ACL часто розміщуються на центральних серверах або мережевих пристроях, де можуть бути застосовані до декількох ресурсів одночасно. Це дозволяє зменшити кількість окремих списків, підвищити зручність адміністрування та забезпечити централізований контроль доступу. Важливо, що розміщення ACL має бути налаштоване так, щоб мінімізувати ризики несанкціонованого доступу або помилок в конфігураціях.

Вибір між стандартними та розширеними списками контролю доступу (ACL) є важливим етапом у налаштуванні мережевої безпеки, адже він впливає як на гнучкість фільтрації, так і на продуктивність маршрутизатора та пропускну здатність мережі. Ці два типи ACL мають різні особливості, які слід враховувати залежно від вимог до фільтрації трафіку.

Стандартні ACL-списки відзначаються простотою у створенні та впровадженні. Вони дозволяють фільтрувати трафік лише за вихідною IP-адресою, не враховуючи типу трафіку чи його призначення. Наприклад, стандартні ACL можуть використовуватися для блокування всіх пакетів із певного джерела незалежно від того, куди ці пакети направляються. Однак така базова фільтрація має свої обмеження. Неправильне розташування стандартного ACL у мережі, наприклад, занадто близько до джерела, може призвести до ненавмисного блокування дозволеного трафіку. Тому стандартні ACL рекомендується розміщувати ближче до вузла призначення, щоб фільтрувати небажані пакети лише на кінцевих етапах їхнього маршруту.

Розширені ACL-списки забезпечують значно більшу гнучкість і контроль. Вони дозволяють фільтрувати трафік не лише за вихідною та кінцевою IP-адресами, а й за іншими параметрами, такими як протоколи мережевого (IP, ICMP) і транспортного рівнів (TCP, UDP) та номери портів. Це дозволяє створювати детальні правила доступу, які враховують специфіку трафіку, наприклад, блокування HTTP-запитів до певного сервера, залишаючи дозволеними FTP-запити. Щоб уникнути непотрібного навантаження на мережу, розширені ACL рекомендується розміщувати ближче до джерела трафіку. Це дозволяє блокувати небажаний трафік ще до того, як він покине вихідний маршрутизатор, підвищуючи ефективність використання мережевих ресурсів.

Для прикладу, якщо потрібно заборонити трафік із мережі 192.168.1.0/24 до мережі 192.168.4.0/24, але дозволити доступ до інших мереж, можна створити розширений ACL наступним чином:

1. Створення списку:

```
R1(config)# access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
```

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 any
```

2. Прив'язка до інтерфейсу:

```
R1(config)# interface fa0/0
```

```
R1(config-if)# ip access-group 101 out
```

Сучасні версії Cisco IOS дозволяють використовувати іменовані ACL (NACL), які забезпечують зручнішу ідентифікацію списків завдяки унікальним назвам замість числових діапазонів. Це спрощує адміністрування мереж і підвищує зручність у великих інфраструктурах. Наприклад, іменований розширений ACL створюється за допомогою команди:

```
R1(config)# ip access-list extended example_name
```

```
R1(config-ext-nacl)# permit ip 192.168.1.66 0.0.0.0 any
```

R1(config-ext-nacl)# deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255

Прив'язка до інтерфейсу виконується аналогічно:

R1(config)# interface fa0/0

R1(config-if)# ip access-group example_name out

Вимоги:

Необхідно заборонити трафік з мережі 192.168.1.0 в мережу 192.168.4.0. Дозволити трафіку з мережі 192.168.1.0 досягнення інших мереж.

Неправильне розміщення:

Відповідає деяким вимогам. Забороняє трафіку з мережі 192.168.1.0 досягнення мереж 192.168.2.0 та 192.168.3.0

Правильне розміщення:

Відповідає усім вимогам.

```
ACL
access-list 9 deny 192.168.1.0 0.0.0.255
access-list 9 permit any
```

Рис. 11.6. Приклад реалізації завдання за допомогою стандартного ACL
Джерело: [1-6]

Вимоги:

Необхідно заборонити трафік з мережі 192.168.1.0 в мережу 192.168.4.0. Дозволити трафіку з мережі 192.168.1.0 досягнення інших мереж.

Правильне розміщення:

Розширений ACL-список розміщений найближче до вихідної адреси. Він забороняє трафіку з мережі 192.168.1.0 досягнення мережі 192.168.4.0, але дозволяє йому вхід у інші мережі

```
ACL
access-list 109 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 109 permit ip any any
```

Рис. 11.6. Приклад реалізації завдання за допомогою розширеного ACL
списку

Джерело: [1-6]

Сучасні технології також дозволяють поєднувати ACL із іншими методами забезпечення безпеки, такими як контекстно-залежні ACL (СВАС) або зональні фаєрволи. Це додає додаткові рівні захисту, зокрема моніторинг стану з'єднань і динамічну адаптацію правил доступу. Інтеграція ACL із системами моніторингу трафіку, наприклад, NetFlow, дозволяє виявляти аномалії та аналізувати використання правил безпеки. Такі рішення дозволяють більш гнучко реагувати на зміни в мережевому середовищі та автоматично коригувати політики доступу залежно від реального стану мережі. Застосування таких технологій забезпечує кращу захищеність від атак, що базуються на змінах у поведінці трафіку, таких як DDoS-атаки. Додавання функцій перевірки трафіку в реальному часі допомагає своєчасно виявляти і блокувати потенційно небезпечні з'єднання. Завдяки інтеграції з іншими системами безпеки, можна створити комплексну та багаторівневу систему захисту від загроз.

Таким чином, вибір типу ACL залежить від складності вимог до безпеки. Стандартні ACL підходять для базової фільтрації, тоді як розширені ACL забезпечують високий рівень контролю та деталізації. У сучасних мережах, де безпека є пріоритетом, розширені та іменовані ACL разом із іншими технологіями створюють основу для ефективного захисту інформаційних систем.

11.7. ПЕРЕВІРКА СПИСКІВ КОНТРОЛЮ ДОСТУПУ

Перевірка списків контролю доступу (ACL) є важливою складовою забезпечення безпеки інформаційних систем. Процес перевірки допомагає переконатися, що доступ до ресурсів обмежений відповідно до встановлених політик безпеки, а також дозволяє виявити потенційні уразливості чи неправильні налаштування, які можуть призвести до несанкціонованого доступу або порушення конфіденційності. Перевірка списків контролю доступу включає кілька етапів: аналіз структури ACL, перевірку прав доступу, оцінку ефективності налаштувань, перевірку сумісності з політиками безпеки, а також моніторинг та аудит. Спочатку необхідно перевірити структуру ACL на відповідність заданим політикам доступу. Це включає перевірку правил для різних користувачів або груп, щоб переконатися, що доступ обмежений лише до тих ресурсів, які повинні бути доступні для конкретних користувачів. Важливо перевірити, чи надані користувачам чи групам тільки необхідні права (наприклад, лише право читання або запису), а не зайві, які можуть порушити безпеку системи.

Також слід перевірити, як правильно працюють ACL, зокрема, перевірка того, чи правильно налаштовані пріоритети правил (наприклад, чи коректно працюють правила "accept" та "deny" у списках). Необхідно переконатися, що ACL відповідають вимогам загальної політики безпеки організації, зокрема, щоб не було конфліктів між різними правилами доступу. Після налаштування та перевірки списків необхідно постійно здійснювати моніторинг і аудит для виявлення несанкціонованих спроб доступу або змін у конфігураціях ACL. Це може включати аналіз логів доступу та проведення регулярних перевірок безпеки. Перевірка списків контролю доступу є необхідною для підтримання високого рівня інформаційної безпеки і повинна проводитися регулярно, зокрема після будь-яких змін у системах чи правилах доступу.

Списки контролю доступу (ACL) у маршрутизаторах Cisco є важливим інструментом для фільтрації трафіку, забезпечення безпеки та управління доступом у мережі. Їх правильне налаштування та використання дозволяє оптимізувати роботу мережі та запобігати небажаному трафіку. Для перевірки конфігурації ACL-списків і аналізу їх ефективності використовуються спеціальні команди, які дозволяють оцінити правильність синтаксису, порядок інструкцій та їхнє застосування до інтерфейсів. Завдяки використанню ACL можна створити різноманітні політики доступу, визначаючи, який трафік дозволяється, а який блокується. ACL також можуть бути застосовані для обмеження доступу до конкретних ресурсів, підвищуючи безпеку мережі. Під час налаштування важливо враховувати порядок правил, оскільки маршрутизатор обробляє інструкції послідовно і зупиняється при першому збігу. Важливим аспектом є також регулярний моніторинг і оновлення ACL, щоб враховувати зміни в мережевих вимогах та потенційних загрозах.

Команда `show ip interface` надає інформацію про IP-інтерфейси маршрутизатора, включаючи застосовані до них ACL-списки. Це дозволяє швидко перевірити, чи прив'язаний потрібний список до відповідного інтерфейсу та в якому напрямку (вхідному чи вихідному) він застосовується. Для перегляду вмісту списків доступу використовується команда `show access-lists`, яка виводить всі ACL-списки маршрутизатора разом із детальним описом кожної інструкції та кількістю збігів (hits). Це допомагає оцінити ефективність правил і виявити інструкції, які не використовуються. Якщо потрібно переглянути конкретний список, можна вказати його ім'я або номер у команді. Наприклад, `show access-lists 101` відобразить лише вміст ACL із номером 101.

Команда `show running-config` є одним із ключових інструментів для аналізу поточної конфігурації маршрутизатора. Вона дозволяє побачити всі налаштовані ACL-списки, навіть ті, які на цей момент не застосовані до жодного інтерфейсу. Це зручно для перевірки конфігурації перед її активним використанням.

При роботі з нумерованими ACL-списками важливо пам'ятати, що нові інструкції додаються в кінець списку. Це може спричинити небажані результати, якщо порядок правил не відповідає логіці фільтрації. У таких випадках рекомендується видалити існуючий список за допомогою команди `no access-list [номер списку]` і створити його заново. Наприклад, для видалення ACL із номером 101 використовується команда `no access-list 101`. Крім того, при створенні нового списку важливо ретельно визначити пріоритетність правил, щоб забезпечити правильну обробку трафіку. Для того, щоб уникнути помилок і зайвих витрат часу на коригування, рекомендується спочатку спланувати структуру ACL перед її застосуванням. У випадку необхідності застосування змін до існуючого списку, варто враховувати вплив на загальну безпеку мережі та можливі порушення доступу до ресурсів. Регулярний перегляд і тестування ACL дозволяє зберігати їх ефективність і актуальність у процесі експлуатації мережі.

Щоб спростити редагування та управління ACL-списками, часто рекомендують створювати їх у текстовому редакторі. Це дозволяє легко змінювати порядок інструкцій, зберігати резервні копії та копіювати готові списки у конфігурацію маршрутизатора. Перед вставкою нового списку необхідно видалити поточний, інакше нові інструкції будуть додані в кінець існуючого списку.

Для тимчасових змін у політиках доступу сучасні маршрутизатори підтримують динамічне управління ACL-списками. Наприклад, можна використовувати тимчасові списки доступу, які автоматично видаляються після закінчення заданого періоду часу. Це корисно для створення правил, які діють лише у визначені години, наприклад, робочий час.

Систематичний аналіз ACL-списків за допомогою команд `show access-lists` і `show ip interface` дозволяє виявляти неефективні правила, видаляти зайві інструкції та підтримувати оптимальну продуктивність мережі. Сучасні технології, такі як контекстно-залежні ACL (CBAC) або зональні політики фаєрволів (ZFW), значно розширюють можливості традиційних ACL-списків. Вони забезпечують глибокий аналіз трафіку, динамічне створення правил і інтеграцію із системами моніторингу.

Отже, правильне використання ACL-списків у поєднанні з сучасними інструментами контролю доступу є ключовим елементом ефективного

управління мережею та забезпечення її безпеки. Завдяки цьому можна не лише обмежити доступ до чутливих ресурсів, а й забезпечити моніторинг і аналіз трафіку для виявлення потенційних загроз. Важливо, щоб конфігурація ACL була гнучкою і відповідала потребам організації, дозволяючи швидко адаптуватися до змін у мережевому середовищі. Крім того, інтеграція ACL з іншими системами безпеки, такими як системи виявлення вторгнень (IDS) та фаєрволи, дає змогу забезпечити багаторівневий захист. З часом регулярне оновлення і вдосконалення політик доступу допомагає зберігати ефективність захисту в умовах розвитку нових загроз.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 11

1. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.
2. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.
3. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
4. Shevchenko, S., Zhdanova Y. ., & Spasiteleva, S. (2023). Математичні методи в кібербезпеці: теорія катастроф. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 165–175.
5. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.
6. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.
7. Машталяр, Я., Козачок, В., Бржезьська, З., Богданов, О., Оксанич, І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 156–167.

8. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 68–83.

9. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях . Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 338–347.

10. B. Zhurakovskiy, et al., Secured Remote Update Protocol in IoT Data Exchange System, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 67–76.

11. Костюк Ю.В., Шапран В.О. Технології виявлення аномальних подій та сигнатур в реальному часі. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1069-1084.

12. D. Virovets, et al., Ways of Interaction of Autonomous Economic Agents in Decentralized Autonomous Organizations, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 182–190.

13. Костюк Ю.В., Войткевич А.А. Дослідження технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1017-1032.

14. D. Berestov, et al., Analysis of Features and prospects of Application of Dynamic Iterative Assessment of Information Security Risks, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 329–335.

15. M. Moshenchenko, et. al., Optimization Algorithms of Smart City Wireless Sensor Network Control, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 32–42.

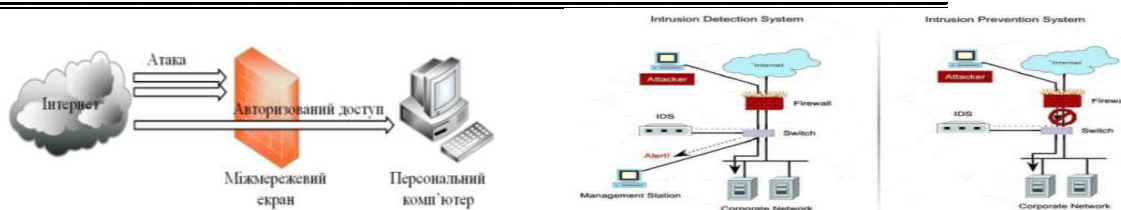
16. V. Buhas, et al., Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188, no. 2 (2021) 273–281.

17. M. TajDini, et al., Brainwave-based Authentication using Features Fusion, Comput. Secur. 129, no. 103198 (2023) 1–11.

18. D. Shevchuk, et al., Designing Secured Services for Authentication, Authori-zation, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.

РОЗДІЛ 12

ТЕХНОЛОГІЯ МІЖМЕРЕЖЕВИХ ЕКРАНІВ ТА СИСТЕМ ВІЯВЛЕННЯ АТАК



- 12.1. Класифікація та архітектура міжмережевих екранів**
- 12.2. Міжмережеві екран прикладного рівня**
 - Проксі сервери**
- 12.3. Проксі-сервер Squid**
- 12.4. Системи виявлення атак (СВА)**
- 12.5. Системи виявлення та запобігання вторгнень**
- 12.6. Системи контролю та управління доступом у мережі (Active Directory, ACL)**

"В умовах сучасної кіберзагрози, коли інформація є основною цінністю, технології міжмережевих екранів та системи виявлення атак стають основними лініями оборони. Вони не лише захищають мережі від вторгнень, а й дозволяють своєчасно реагувати на підозрілі активності, що забезпечує збереження безпеки на всіх рівнях."

Джон Вон Нойман, відомий математик і комп'ютерний вчений

12.1. КЛАСИФІКАЦІЯ ТА АРХІТЕКТУРА МІЖМЕРЕЖЕВИХ ЕКРАНІВ

Міжмережевий екран (англ. firewall, нім. Brandmauer) є комплексом апаратних і програмних засобів, які здійснюють контроль і фільтрацію мережевих пакетів, що проходять через нього, відповідно до заданих правил. Основною функцією міжмережевого екрану є забезпечення захисту мережі або окремих її вузлів від несанкціонованого доступу. Такий

пристрій або програмне забезпечення, також часто зване фільтром, реалізує політику безпеки, блокуючи або пропускаючи пакети залежно від їх відповідності визначеним критеріям.

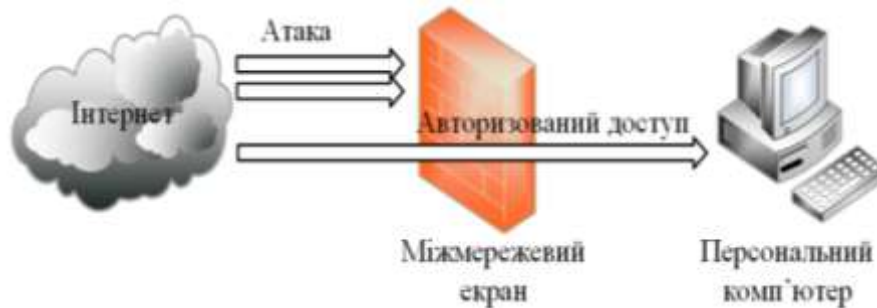


Рис. 12.1. Схема роботи міжмережевого екрану

Джерело: [2-5]

Типові можливості міжмережевих екранів включають:

- ✓ Фільтрацію доступу до відомих незахищених служб.
- ✓ Перешкоджання витоку конфіденційної інформації з захищених підмереж і попередження впровадження помилкових даних за допомогою вразливих служб.
- ✓ Контроль доступу до вузлів мережі.
- ✓ Реєстрацію всіх спроб доступу, як ззовні, так і з внутрішньої мережі, що дозволяє вести облік використання доступу до Інтернету окремими вузлами мережі.
- ✓ Регулювання порядку доступу до мережі.
- ✓ Сповіщення про підозрілу діяльність, спроби зондування або атаки на вузли мережі або сам екран.

Міжмережеві екрани мають кілька ключових особливостей:

- Трафік ззовні всередину і навпаки повинен проходити через брандмауер.
- Трафік дозволяється або блокується відповідно до політики, яка застосовується на брандмауері.
- Міжмережевий екран має бути висококваліфікованим пристроєм з захищеною операційною системою, оскільки він не може бути застрахований від проникнення.
- Політика трафіку визначається на основі діапазону IP-адрес, мережевих протоколів, програм, що діють в мережі, типу вмісту трафіку та його спрямованості (вхідний або вихідний).

Для фільтрації трафіку міжмережеві екрани використовують різні механізми:

- IP-адреси та значення полів протоколів – використовуються пакетними фільтрами та брандмауерами, які перевіряють стан для обмеження доступу до певних послуг.
- Прикладний протокол – використовується шлюзами на рівні додатків для контролю обміну інформацією за конкретними прикладними протоколами.
- Ідентифікатор користувача – застосовується для внутрішніх користувачів, які ідентифікуються за допомогою технологій безпечної аутентифікації.
- Мережева активність – управляє доступом на основі критеріїв, таких як час, швидкість запитів або інші схеми діяльності.

Політики фільтрації трафіку повинні визначатися на основі оцінки ризику організації, її ділової місії та вимог до безпеки.

Для того щоб фільтрувати трафік, міжмережевий екран повинен мати щонайменше два мережевих інтерфейси: один для внутрішньої мережі та інший для зовнішньої (наприклад, Інтернету). Міжмережевий екран захищає внутрішню мережу підприємства від загроз, що надходять із зовнішніх мереж. Він також може бути використаний для захисту однієї внутрішньої мережі підприємства від іншої, якщо, згідно з принципом мінімуму повноважень, користувачам цих мереж не потрібен повний взаємний доступ до їхніх ресурсів.

Для ефективного виконання міжмережевим екраном основної функції — аналізу та фільтрації трафіку — необхідно, щоб через нього проходив увесь трафік, яким обмінюються вузли внутрішньої мережі з вузлами зовнішніх мереж. У випадках, коли підприємство має декілька ліній зв'язку із зовнішніми мережами, кожна з них повинна бути захищена окремим міжмережевим екраном або спільною централізованою системою захисту.

Міжмережевий екран забезпечує захист мережі не лише від зовнішніх атак і несанкціонованого доступу, але й від ненавмисних або помилкових дій користувачів внутрішньої мережі, наприклад передачі конфіденційної інформації до зовнішніх ресурсів.

Основними функціями міжмережевого екрану є:

- ▲ Фільтрація трафіку для запобігання доступу до внутрішніх ресурсів несанкціонованим користувачам.
- ▲ Аудит подій, що включає фіксацію дій, пов'язаних із виявленням і блокуванням підозрілих пакетів.

Окрім базових функцій, сучасні міжмережеві екрани виконують додаткові завдання, які підвищують рівень інформаційної безпеки:

- Антивірусний захист для виявлення та блокування шкідливих файлів.
- Шифрування трафіку, що забезпечує конфіденційність переданої інформації.
- Логічне посередництво (проксі-сервер) між внутрішніми клієнтами та зовнішніми серверами для приховування деталей мережі.
- Фільтрація повідомлень за вмістом, включаючи типи файлів, імена DNS і ключові слова.
- Попередження і виявлення вторгнень для запобігання мережевим атакам.
- Підтримка VPN для створення захищених каналів передачі даних.
- Трансляція мережесих адрес (NAT) для приховування структури внутрішньої мережі.
-

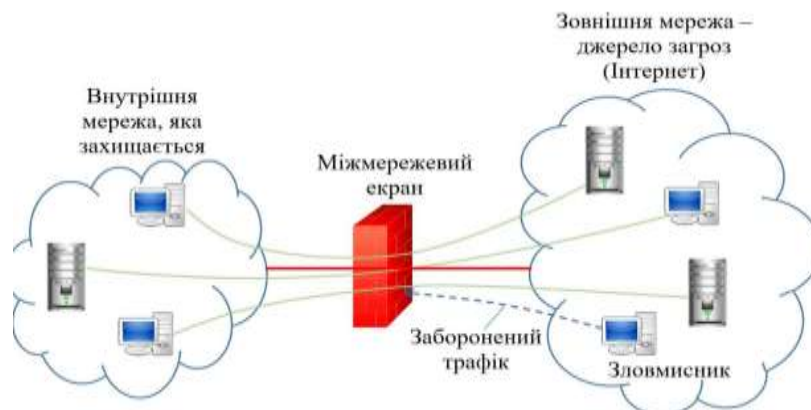


Рис. 12.2. Використання фаєрвола для захисту внутрішньої мережі від зовнішніх загроз

Джерело: [2-5]

Частина цих функцій може реалізовуватися окремими продуктами або інтегруватися у складі комплексних систем захисту. Наприклад, базові функції фільтрації трафіку доступні у більшості сучасних маршрутизаторів. Завдання виявлення вірусів виконуються спеціалізованими антивірусними програмами, а шифрування трафіку є невід’ємною частиною технологій побудови захищених каналів, таких як IPsec або SSL. Проксі-сервери, окрім функцій посередництва, часто забезпечують контент-фільтрацію або NAT.

Сучасні міжмережесі екрани також використовують штучний інтелект і машинне навчання для виявлення складних атак, аналізу аномалій у трафіку та побудови поведінкових моделей. Використання інтелектуальних функцій дозволяє швидко реагувати на нові загрози,

автоматизувати рутинні процеси та забезпечити вищий рівень безпеки для підприємств.

Таким чином, міжмережевий екран є багатофункціональним інструментом, що виконує ключову роль у забезпеченні інформаційної безпеки мережі. Його правильне налаштування та інтеграція з іншими засобами захисту забезпечують стабільність роботи мережі, конфіденційність даних і стійкість до кіберзагроз.

Міжмережеві екрани є одним із ключових елементів забезпечення інформаційної безпеки мереж підприємств. Вони виконують функції фільтрації, моніторингу та захисту мережевого трафіку, запобігаючи несанкціонованому доступу, мережевим атакам і витоку конфіденційної інформації. Для ефективного виконання цих функцій міжмережеві екрани мають низку технічних характеристик, які дозволяють класифікувати їх за способом реалізації, методом фільтрації та рівнями моделі OSI.

Способи реалізації міжмережевих екранів

За способом реалізації міжмережеві екрани поділяються на:

Програмні міжмережеві екрани

Вони реалізуються як програмне забезпечення, яке працює під управлінням універсальних операційних систем, таких як Microsoft Windows, Linux або MacOS. Їх основною перевагою є гнучкість у налаштуванні та інтеграція з іншими системами.

Апаратні міжмережеві екрани

Ці екрани є спеціалізованими пристроями, вбудованими в маршрутизатори або Ethernet-комутатори. Вони забезпечують високу швидкість роботи за рахунок використання апаратного забезпечення для виконання функцій фільтрації.

Програмно-апаратні міжмережеві екрани

Такі рішення поєднують програмне забезпечення з апаратною платформою. Операційна система та апаратне забезпечення оптимізуються для виконання завдань безпеки. Наприклад, спеціалізовані сервери із сертифікованим програмним забезпеченням забезпечують максимальний рівень захисту.

Способи фільтрації

Міжмережеві екрани також класифікують за способом фільтрації трафіку:

✱ Екрани без запам'ятовування стану (stateless)

Вони фільтрують трафік на основі статичних правил, які задаються адміністратором. Ці правила визначають, які пакети можуть проходити

через екран. Недоліком такого підходу є відсутність аналізу поточного стану з'єднання, що знижує ефективність виявлення складних загроз.

✳ Екрани із запам'ятовуванням стану (stateful)

Ці екрани враховують поточний стан сеансів і їхню історію, що дозволяє динамічно приймати рішення про пропуск чи блокування трафіку. Такий підхід значно підвищує рівень захисту та дозволяє виявляти підозрілу активність.

Сучасні функції та тенденції

З розвитком інформаційних технологій міжмережеві екрани стали багатофункціональними системами, які забезпечують не лише базовий захист, але й виконують складні завдання:

- **Виявлення та запобігання вторгненням (IDS/IPS)**

Інтеграція з системами попередження про загрози для блокування атак у реальному часі.

- **Шифрування трафіку**

Забезпечення конфіденційності даних через захищені канали зв'язку.

- **Аналіз загроз за допомогою штучного інтелекту**

Використання машинного навчання для виявлення аномалій у трафіку.

- **Контроль доступу до веб-ресурсів (Secure Web Gateway)**

Блокування небажаних або небезпечних веб-сайтів.

- **Функції VPN**

Захист з'єднань через віртуальні приватні мережі.

Переваги інтегрованих рішень

Інтегровані міжмережеві екрани, які поєднують функції DPI, IDS/IPS, антивірусного захисту та VPN, забезпечують комплексний підхід до захисту мереж підприємств. Вони дозволяють адаптуватися до сучасних загроз, таких як кібератаки на основі соціальної інженерії, розповсюдження шкідливого ПЗ та DDoS-атаки.

Отже, міжмережеві екрани є важливим елементом забезпечення кібербезпеки, а їхній розвиток дозволяє ефективно захищати мережі навіть у складних і динамічних середовищах.

Міжмережеві екрани з запам'ятовуванням стану

Міжмережеві екрани, що підтримують запам'ятовування стану, створюють динамічну таблицю станів для кожного активного сеансу. Ця таблиця оновлюється в реальному часі під час обробки пакетів, що відповідають певним правилам. При отриманні чергового пакету такого сеансу міжмережевий екран аналізує його стан, коригує таблицю та приймає рішення: пропустити чи відхилити пакет.

Робота таких екранів вимагає значних ресурсів, зокрема оперативної пам'яті для зберігання таблиці станів і високопродуктивних процесорів для обробки трафіку. Недостатня продуктивність міжмережевого екрану може спричинити затори на його інтерфейсах, що зробить внутрішні сервери недоступними навіть за відсутності атак.

Міжмережеві екрани класифікуються за рівнями OSI, на яких вони працюють:

- **Канальний рівень**

Забезпечує базову фільтрацію кадрів на основі списків контролю доступу (ACL). Цей тип реалізується, наприклад, у керованих комутаторах.

- **Мережевий рівень**

Фільтрує пакети за IP-адресами, портами TCP/UDP і протоколами. Використовується в маршрутизаторах із підтримкою ACL і персональних програмних міжмережевих екранах.

- **Сеансовий рівень**

Відстежує стани протоколів TCP/UDP, контролюючи встановлення та завершення сеансів. Забезпечує захист від атак на логіку з'єднань, таких як DoS або TCP-SYN flood.

- **Прикладний рівень**

Аналізує вміст повідомлень і підтримує складні політики доступу. Прикладом є проксі-сервери, які забезпечують найвищий рівень захисту, але вимагають значних обчислювальних ресурсів.

Сучасні можливості міжмережевих екранів

1. Контроль трафіку на прикладному рівні:

- ✓ Інтерпретація протоколів (HTTP, SMTP, FTP, SQL).
- ✓ Заборона небезпечних команд (наприклад, PUT, DELETE у HTTP).
- ✓ Перехоплення запитів до внутрішніх серверів із забезпеченням додаткової аутентифікації.

2. Функції контент-фільтрації та антивірусного захисту:

- ✓ Обмеження доступу до небажаних ресурсів.
- ✓ Перевірка файлів та електронних листів у реальному часі.

3. Підтримка VPN та NAT:

- ✓ Захищений обмін даними між підрозділами підприємства.
- ✓ Трансляція IP-адрес для захисту внутрішньої мережі.

4. Цифрове підписання та шифрування даних:

- ✓ Централізоване шифрування листів користувачів.
- ✓ Використання цифрових сертифікатів для аутентифікації.

5. Інтеграція з хмарними технологіями:

- ✓ Використовувати моделі штучного інтелекту для аналізу аномалій у трафіку.
- ✓ Забезпечувати автоматичне оновлення сигнатур загроз.

Тенденції розвитку міжмережевих екранів

У 2025 році особливу увагу приділяють таким аспектам:

- **Zero Trust Architecture (ZTA)** - міжмережеві екрани стають частиною архітектури нульової довіри, забезпечуючи постійний контроль доступу на основі контексту та аутентифікації.
- **Підтримка IoT** - нові типи міжмережевих екранів створені для моніторингу та захисту пристроїв Інтернету речей.
- **Масштабованість** - сучасні міжмережеві екрани працюють у середовищах з високими навантаженнями, підтримуючи швидкості понад 100 Гбіт/с.

Міжмережеві екрани є ключовим елементом комплексного захисту інформаційних систем підприємств, забезпечуючи адаптивний захист від сучасних кіберзагроз.

Класифікація міжмережевих екранів

Міжмережеві екрани (МЕ) виконують важливу роль в забезпеченні безпеки мереж, фільтруючи і контролюючи мережевий трафік на основі заданих правил. Різні типи міжмережевих екранів застосовуються для різних рівнів фільтрації та управління доступом, залежно від складності мережі та вимог до безпеки. Зазначимо основні категорії міжмережевих екранів, їх переваги і недоліки. Типи міжмережевих екранів:

▲ Пакетні фільтри

Пакетні фільтри є одним з основних типів міжмережевих екранів, що використовуються для контролю мережевого трафіку. Вони здійснюють фільтрацію на основі аналізу окремих пакетів, перевіряючи різноманітні характеристики кожного з них, і дозволяють або блокують їх проходження залежно від встановлених правил. Основними характеристиками, за якими здійснюється фільтрація, є IP-адреси джерела та одержувача, транспортний протокол (наприклад, TCP, UDP або ICMP), порти джерела і одержувача, а також напрямок трафіку (вхідний або вихідний). За допомогою цих параметрів пакетний фільтр може контролювати доступ до мережі або її ресурсу на основі конкретних умов. Пакетні фільтри можуть бути реалізовані в різних компонентах мережевої інфраструктури. Зазвичай вони використовуються на прикордонних маршрутизаторах для фільтрації трафіку, що проходить через межі мережі, в операційних системах для захисту окремих хостів, а також в персональних міжмережевих екранах

▲ Пакетні фільтри з аналізом стану

Пакетні фільтри з аналізом стану є більш просунутим типом міжмережевих екранів порівняно з простими пакетними фільтрами. Вони здійснюють фільтрацію трафіку не лише на основі характеристик окремих пакетів, а й враховують стан з'єднання між двома хостами. Це дозволяє здійснювати більш точний контроль над мережевим трафіком, оскільки аналіз стану дозволяє відслідковувати історію кожного з'єднання та блокувати пакети, які не відповідають очікуваному стану. Відмінність від традиційних пакетних фільтрів полягає в тому, що міжмережевий екран з аналізом стану підтримує таблицю станів, яка містить інформацію про кожне з'єднання, таку як IP-адреси джерела та одержувача і поточний стан з'єднання (відкрите, закрите, наприклад).

Пакетні фільтри з аналізом стану дозволяють пропускати тільки ті пакети, які належать до вже встановлених з'єднань. Це значно підвищує рівень безпеки, оскільки тільки трафік, що є частиною активного з'єднання, проходить через міжмережевий екран. Це дозволяє запобігти атакам типу «відмова в обслуговуванні» (DoS), а також зменшує ймовірність несанкціонованого доступу до мережі.

Однією з головних переваг міжмережевих екранів з аналізом стану є їх прозорість для клієнтів і серверів. Вони не розривають TCP-з'єднання, що робить їх ефективними для підтримки стабільних і безпечних з'єднань. Крім того, аналіз стану дозволяє блокувати лише ті пакети, які не відповідають встановленому стану з'єднання, що дозволяє зменшити кількість помилкових спрацьовувань і підвищити ефективність роботи міжмережевого екрану.

Однак, як і у випадку з простими пакетними фільтрами, пакетні фільтри з аналізом стану мають певні обмеження. Вони фактично застосовуються тільки в мережах, що використовують протоколи TCP/IP, і не підтримують інші мережеві протоколи в такій же мірі. Тому їх використання в гетерогенних мережах, де є різні протоколи, може бути обмежене. Крім того, хоча міжмережеві екрани з аналізом стану значно підвищують безпеку в порівнянні з простими фільтрами, вони все ж не здатні здійснювати глибокий аналіз вмісту пакетів і не підтримують аутентифікацію користувачів, що може бути важливим для більш складних загроз.

▲ Міжмережеві екрани прикладного рівня

Міжмережеві екрани прикладного рівня (або фаєрволи прикладного рівня) здійснюють фільтрацію на основі аналізу даних, що передаються через прикладний рівень протоколів мережі. Вони більш детально

вивчають вміст мережевих пакетів, а не лише метадані, такі як IP-адреси чи номери портів, як у випадку з пакетними фільтрами. Міжмережеві екрани прикладного рівня порівнюють поведінку мережевого протоколу з заздалегідь визначеними профілями, що дозволяє виявляти відхилення в поведінці мережевих додатків. Це забезпечує високий рівень контролю і дозволяє зупиняти спроби несанкціонованого доступу або зловмисні дії на прикладному рівні.

Один з ключових аспектів міжмережевих екранів прикладного рівня — це їх здатність блокувати або дозволяти доступ на основі вмісту переданих даних. Це дозволяє ефективно фільтрувати трафік таких протоколів, як HTTP, SMTP, POP3, IMAP, FTP, VoIP та багатьох інших. Крім того, міжмережеві екрани прикладного рівня можуть виконувати аутентифікацію користувачів, що є важливою перевагою в контексті підвищених вимог до безпеки.

Оскільки вони здійснюють аналіз на глибшому рівні, ніж звичайні фільтри, ці екрани значно менш уразливі до атак типу підробки мережевої адреси (spoofing) і можуть створювати детальніші логи, що допомагають виявляти та аналізувати загрози. Це дає адміністраторам систем більше можливостей для контролю над мережевим трафіком і виявлення потенційних зловмисних дій.

Однак міжмережеві екрани прикладного рівня мають і кілька недоліків. Оскільки вони аналізують кожен пакет більш детально, це може суттєво знижувати швидкість обробки трафіку, що створює певні проблеми для мереж з високим навантаженням. Крім того, міжмережеві екрани прикладного рівня часто обробляють лише обмежену кількість мережевих додатків і протоколів, а також не завжди можуть автоматично підтримувати нові протоколи або додатки без додаткового налаштування.

Таким чином, міжмережеві екрани прикладного рівня є потужним інструментом для забезпечення безпеки в мережах, особливо коли йдеться про контроль за специфічними додатками та протоколами, а також коли необхідно здійснювати глибший аналіз трафіку. Вони є важливим компонентом багаторівневої стратегії захисту мережі, де вони працюють разом з іншими типами міжмережевих екранів для забезпечення комплексного захисту від різноманітних загроз.

▲ Проксі-шлюзи прикладного рівня

Проксі-шлюзи прикладного рівня є спеціалізованими компонентами мережевої безпеки, які виконують функції посередника між двома хостами, що взаємодіють через мережу. На відміну від звичайних міжмережевих екранів, проксі-шлюзи не просто фільтрують пакети, а створюють два окремих з'єднання: одне між клієнтом і проксі-агентом, а

інше між проксі-агентом і реальним сервером. Це дозволяє ефективно контролювати та обмежувати доступ до серверів, захищаючи їх від прямих атак і небажаного трафіку.

Основною перевагою проксі-шлюзів є те, що вони дозволяють виконувати глибокий аналіз вмісту кожного пакету на прикладному рівні, що забезпечує високий рівень безпеки. Завдяки цьому проксі-шлюзи можуть виконувати аутентифікацію користувачів, що дозволяє фільтрувати доступ на основі конкретних прав користувачів, а не тільки на основі IP-адрес чи номерів портів. Це також робить проксі-шлюзи менш уразливими до атак типу підробки адреси (spoofing), оскільки всі з'єднання проходять через проксі, а не безпосередньо між клієнтом і сервером.

Іншою перевагою є те, що проксі-шлюзи дозволяють здійснювати більш детальний аналіз мережевого трафіку, ніж традиційні фаєрволи, оскільки вони можуть перевіряти не лише заголовки пакетів, але й самі дані, що передаються. Це створює можливість для більш точного визначення та блокування шкідливого контенту, який може бути переданий через мережу.

Однак є й недоліки. Оскільки проксі-шлюзи здійснюють глибокий аналіз кожного пакету, це може призвести до значного зниження продуктивності мережі, особливо в умовах високого трафіку. Крім того, проксі-шлюзи зазвичай підтримують обмежену кількість протоколів і мережевих додатків, що може вимагати додаткових налаштувань або навіть створення нових специфікацій для підтримки нових протоколів.

Таким чином, проксі-шлюзи прикладного рівня є потужними інструментами для забезпечення безпеки в мережах, зокрема для захисту серверів і додатків, а також для здійснення глибокого аналізу трафіку на прикладному рівні. Вони використовуються в середовищах, де важливо контролювати не тільки фізичні, але й логічні аспекти мережевого трафіку, а також виконувати додаткові функції, такі як аутентифікація користувачів і блокування шкідливого контенту.

▲ Виділені проксі-сервера

Виділені проксі-сервера є спеціалізованими рішеннями для розвантаження міжмережеских екранів, які виконують специфічні функції фільтрації та аналізу трафіку. Основною метою таких серверів є оптимізація навантаження на основні компоненти безпеки та надання можливості для більш детального аналізу мережевого трафіку або для виконання додаткових функцій, яких може не вистачати звичайним міжмережеским екранам.

Виділені проксі-сервера зазвичай встановлюються між внутрішньою мережею та основним міжмережеским екраном, надаючи додатковий рівень

фільтрації та створення логів для мережевого трафіку. Вони можуть бути налаштовані для виконання спеціалізованого фільтрування, такого як сканування вмісту на наявність вірусів, перевірка сумісності протоколів чи аналіз трафіку для виявлення аномалій. Це дозволяє знизити навантаження на основний міжмережвий екран, який займається загальним фільтруванням трафіку, і зосередитися на виконанні основних завдань безпеки.

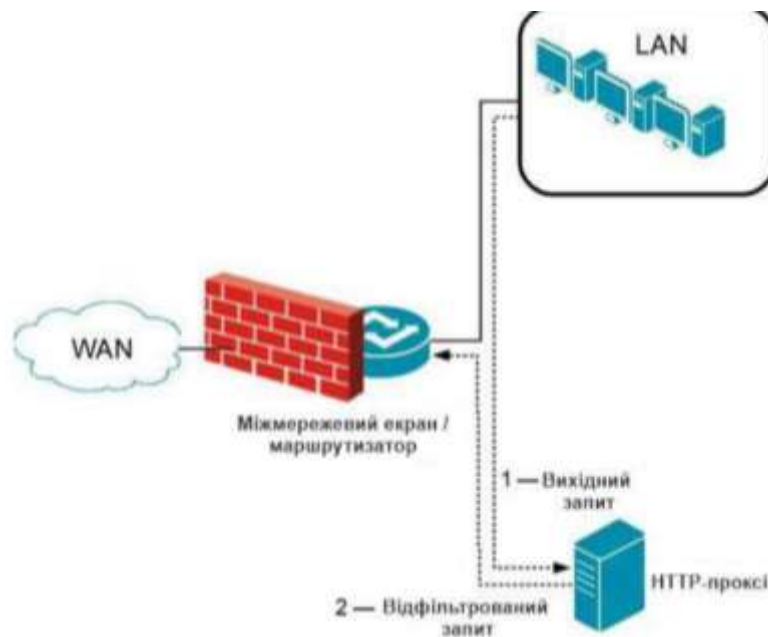


Рис. 12.4. Схема розташування виділеного проксі серверу в комп'ютерній мережі

Джерело: [2-4]

Однією з основних переваг виділених проксі-серверів є можливість забезпечити високий рівень спеціалізації, оскільки такі сервери часто використовуються для конкретних типів трафіку або додатків. Наприклад, виділений проксі-сервер може бути налаштований для обробки лише HTTP/HTTPS-запитів, що дозволяє йому забезпечувати детальний контроль за доступом до веб-ресурсів, а також перевірку вмісту веб-сторінок на наявність шкідливих компонентів або невідповідних ресурсів.

Недоліком є те, що виділені проксі-сервера також можуть стати потенційною точкою відмови у разі неправильного налаштування або перенавантаження, оскільки вони виконують додаткову обробку трафіку. Крім того, вони можуть додавати додаткову складність в мережеву інфраструктуру та вимагають окремого адміністрування та моніторингу.

У загальному контексті виділені проксі-сервера є важливими компонентами в забезпеченні безпеки мережі, особливо в великих організаціях або середовищах, де необхідно здійснювати більш глибокий і детальний аналіз трафіку для запобігання загрозам і забезпечення безпеки.

Інші типи міжмережевих екранів

- Кінцеві точки VPN використовуються для шифрування трафіку між захищеними мережами.
- Гібридні технології поєднують функціональності кількох типів міжмережевих екранів.
- Міжмережеві екрани для веб-додатків, віртуальних інфраструктур, окремих хостів і домашніх мереж - спеціалізовані брандмауери для різних сценаріїв використання.

Політика міжмережевого екрану

Політика міжмережевого екрану (брандмауера) є невід'ємною частиною системи безпеки підприємства чи організації. Вона визначає, як саме міжмережевий екран буде обробляти мережевий трафік, що проходить через нього, з огляду на визначені правила доступу. Політика брандмауера повинна бути ретельно продумана та налаштована, адже саме вона забезпечує баланс між відкритістю мережі для необхідних користувачів і додатків та захистом від потенційних загроз, таких як несанкціонований доступ, атаки або віруси.

Основою розробки політики є оцінка ризиків та вивчення можливих загроз і уразливостей. Це дає змогу визначити типи трафіку, які необхідно дозволити, і ті, що повинні бути заблоковані. Ключовими аспектами розробки є чітке визначення правил доступу до ресурсів і служб, а також налаштування брандмауера для обробки трафіку на основі конкретних характеристик, таких як IP-адреси, протоколи, порти або додатки.

Політика брандмауера може бути різною в залежності від вимог і специфіки роботи мережі. Одним із найбільш простих та поширених варіантів є політика, заснована на IP-адресах та протоколах. Вона регулює доступ на основі IP-адрес та типу мережевого протоколу (TCP, UDP, ICMP), дозволяючи або блокуючи з'єднання з конкретними адресами чи протоколами. Така політика є ефективною для забезпечення базового рівня захисту, але не дає можливості детально контролювати типи додатків чи користувачів, що підключаються до мережі.

Більш складними є політики, засновані на додатках, де враховується конкретне програмне забезпечення або служба, що використовує певний

протокол. Це дозволяє встановлювати детальніші правила для доступу до таких додатків, як веб-сайти (HTTP/HTTPS), поштові сервери (SMTP, POP3, IMAP) або VoIP-сервіси. Така політика дозволяє підвищити рівень безпеки, адже дає можливість точніше визначати, які додатки мають право на доступ до мережі, а які ні.

Особливою категорією є політика, заснована на ідентифікації користувача. Вона передбачає аутентифікацію користувачів перед наданням доступу до мережі. Це дає змогу блокувати доступ для неавторизованих осіб і забезпечує високий рівень контролю, оскільки дозволяє відслідковувати, які користувачі здійснюють доступ до мережі в реальному часі. Використання таких механізмів дозволяє ще більше обмежити доступ до внутрішніх ресурсів, запобігаючи таким чином можливим загрозам з боку небажаних або недобросовісних користувачів.

Не менш важливою є політика, заснована на мережевій активності. Вона аналізує активність у мережі та приймає рішення про доступ залежно від того, чи відповідає трафік певним критеріям безпеки. Такі політики часто використовуються для запобігання атак типу «відмова в обслуговуванні» (DoS), де система може блокувати з'єднання після певної кількості запитів або в разі підозрілої активності.

Розробка і впровадження політики міжмережевого екрану вимагає постійного моніторингу та коригування. Оскільки загрози і технології швидко змінюються, важливо, щоб політика брандмауера була гнучкою і могла бути адаптована до нових умов. Крім того, до політики варто додавати додаткові методи захисту, такі як шифрування трафіку, використання VPN, а також аналіз трафіку на рівні додатків для виявлення більш складних загроз, таких як атаки на рівні додатків або міжмережеві шифровані канали.

Загалом, політика міжмережевого екрану є ключовим елементом безпеки, який не лише забезпечує захист від зовнішніх атак, але й дозволяє ефективно управляти доступом в межах мережі, запобігаючи витокам даних та іншим загрозам безпеці інформаційної системи.

Типи політик міжмережевого екрану:

1. Політики на основі IP-адрес і протоколів.
2. Політики на основі додатків.
3. Політики на основі ідентифікації користувачів.
4. Політики на основі мережевої активності.

Міжмережеві екрани ефективні лише для трафіку, який вони можуть аналізувати. Якщо екран не розуміє певний тип трафіку (наприклад, зашифрований чи тунельований), він не може правильно обробити його за встановленими правилами.

Міжмережеві екрани з можливостями NAT (Network Address Translation)

Технологія трансляції мережевих адрес (NAT) має кілька різновидів, і найпоширенішою є традиційна технологія, яка дозволяє вузлам приватної мережі прозора для користувачів отримувати доступ до зовнішніх вузлів. У цьому варіанті NAT вирішує задачу організації зв'язку, що виходить з приватної мережі, тобто з'єднання ініціюються тільки з внутрішньої мережі, навіть якщо в процесі обміну даними інформація надходить ззовні. Усі ці з'єднання вважаються вихідними, якщо ініціатором є додаток, що працює на вузлі внутрішньої мережі.

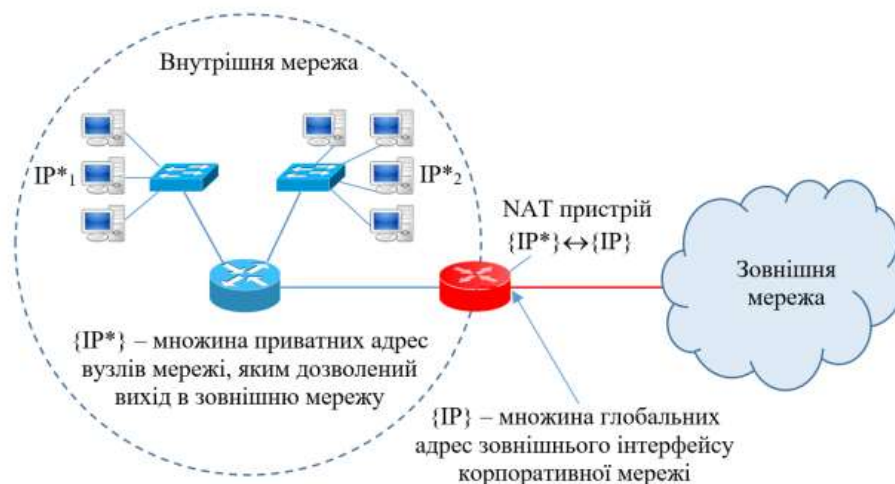


Рис. 12.5. Схема дії традиційної технології NAT

Джерело: [2-4]

Основна ідея технології NAT полягає в динамічному відображенні набору приватних адрес вузлів внутрішньої мережі на набір глобальних адрес, отриманих підприємством від постачальника послуг. Це відображення здійснюється на маршрутизаторі, який з'єднує підприємство з зовнішньою мережею. Маршрутизатор має зовнішній інтерфейс з глобальною IP-адресою, і програмне забезпечення NAT динамічно здійснює трансляцію адрес для того, щоб вузли приватної мережі могли встановлювати з'єднання з ресурсами зовнішнього світу.

Важливою особливістю роботи NAT є правила поширення маршрутних оголошень через кордони приватних мереж. Оголошення про маршрути зовнішніх мереж передаються в приватну мережу, але оголошення про маршрути внутрішніх мереж не пропускаються через прикордонні маршрутизатори, які фільтрують ці дані перед передачею на зовнішні інтерфейси. Завдяки цьому внутрішні маршрутизатори знають

маршрути до всіх зовнішніх мереж, але зовнішні маршрутизатори не мають доступу до структур і маршрутів приватних мереж.

Традиційна технологія NAT поділяється на дві основні категорії: базову трансляцію мережевих адрес (Basic NAT) і трансляцію мережевих адрес і портів (NAPT). У технології Basic NAT для відображення використовуються тільки IP-адреси. Це означає, що кожному внутрішньому IP-адресу присвоюється відповідний глобальний IP-адрес, що дозволяє здійснювати обмін даними з зовнішніми серверами. В технології NAPT, окрім IP-адрес, також відбувається трансляція портів TCP і UDP, що дозволяє використовувати одну глобальну IP-адресу для кількох внутрішніх вузлів через різні порти, що підвищує ефективність використання доступних глобальних IP-адрес.

Міжмережеві екрани з можливостями NAT (Network Address Translation) використовуються для перетворення IP-адрес, що дає змогу здійснювати прозору маршрутизацію між різними мережами з різними областями адрес. NAT є ефективним інструментом для оптимізації використання IP-адрес, дозволяючи кільком пристроям в локальній мережі використовувати одну публічну IP-адресу при виході в Інтернет. Міжмережеві екрани з NAT здатні виконувати трансляцію мережевих адрес на межі між двома областями адрес, забезпечуючи належну маршрутизацію пакетів, що проходять через ці межі.

Міжмережевий екран з NAT може мати з'єднання з кількома областями адрес і здійснювати трансляцію адрес таким чином, щоб пакет коректно маршрутизувався в нову область адрес, зберігаючи правильність заголовків і маршрутизації. Це дає змогу розмежувати внутрішні мережі та зовнішні, забезпечуючи безпеку і захист від несанкціонованого доступу. Міжмережевий екран з NAT дозволяє здійснювати контроль за трафіком між різними мережевими сегментами, зокрема, шляхом переписування IP-адрес у заголовках пакетів, що проходять через нього. Це забезпечує маскування внутрішніх IP-адрес від зовнішнього світу, що ускладнює спроби несанкціонованого доступу до корпоративних мереж. Така система дозволяє також економити адресний простір, використовуючи одну публічну IP-адресу для кількох внутрішніх пристроїв. Крім того, міжмережеві екрани з NAT можуть працювати з різними методами трансляції, такими як статична та динамічна NAT, для забезпечення належного функціонування в різних умовах мережевої інфраструктури.



Рис. 12.6. Схема розташування міжмережевого екрану з можливостями NAT

Джерело: [2-4]

Існують три основні типи трансляції адрес, що використовуються в NAT:

1. **Статичний NAT** забезпечує відображення незареєстрованої IP-адреси на конкретну зареєстровану IP-адресу один до одного. Статичний NAT особливо корисний у випадках, коли пристрій в локальній мережі повинен бути доступним ззовні, наприклад, сервер, який надає публічні сервіси (веб-сайт, поштовий сервер тощо). У цьому випадку кожен пристрій у внутрішній мережі має постійну, заздалегідь визначену публічну адресу для доступу ззовні.

2. **Динамічний NAT** відображає незареєстровану IP-адресу на одну з кількох зареєстрованих IP-адрес із певного пулу зареєстрованих адрес. Відображення може змінюватися в залежності від того, яка зареєстрована адреса є доступною в пулі під час комунікації. Цей тип NAT корисний, коли потрібно використовувати багато зареєстрованих адрес для підтримки з'єднань, але з плином часу адресація може змінюватися залежно від наявності в пулі вільних адрес.

3. **Перевантажений NAT (NAPT, NAT Overload, PAT)** - це спеціальна форма динамічного NAT, що дозволяє транлювати кілька незареєстрованих адрес в одну зареєстровану IP-адресу, використовуючи різні порти для кожного з'єднання. Відомий також як Port Address Translation (PAT), цей метод забезпечує максимальну економію зареєстрованих IP-адрес, дозволяючи декільком комп'ютерам або пристроям в приватній мережі використовувати одну публічну IP-адресу при виході в Інтернет. Кожен пристрій буде мати унікальний номер порту для кожного з'єднання, що дозволяє надавати доступ до Інтернету великій кількості користувачів з обмеженою кількістю публічних IP-адрес.

Міжмережеві екрани з можливостями NAT є важливим компонентом для підтримки безпечного й ефективного зв'язку між внутрішніми

мережами і зовнішнім середовищем. Використання NAT допомагає зберегти внутрішні адреси приватними і непомітними для зовнішнього світу, а також дозволяє оптимізувати використання обмежених IP-адрес, зменшуючи навантаження на систему.

Топологія мережі при використанні міжмережевих екранів

Топологія мережі при використанні міжмережевих екранів зазвичай передбачає кілька рівнів захисту, які забезпечують безпеку внутрішньої мережі від зовнішніх загроз. Однією з найбільш поширених топологій є DMZ (демілітаризована зона), де міжмережевий екран розділяє внутрішню мережу підприємства та зовнішню мережу (Інтернет). В DMZ розміщуються сервери, які повинні бути доступні з Інтернету (наприклад, веб-сервери або поштові сервери), але при цьому вони ізольовані від внутрішньої мережі для зменшення ризику компрометації. Для більшої безпеки трафік з Інтернету до DMZ проходить через один міжмережевий екран, а між внутрішньою мережею та DMZ фільтрується ще одним екраном. Існує також топологія з подвійними міжмережевими екранами, де два екрани контролюють трафік: один фільтрує вхідний трафік з Інтернету, а другий контролює вихідний трафік, що дозволяє додатково обмежити доступ до внутрішньої мережі, навіть якщо один з екранів буде зламаний. Крім того, застосовуються моделі з периметральними міжмережевими екранами, які створюють захисну "перешкоду" між внутрішніми пристроями та зовнішнім світом, що допомагає захистити всі точки доступу до мережі. Для забезпечення більшої гнучкості в захисті використовуються методи сегментації внутрішньої мережі за допомогою міжмережевих екранів, що дозволяє обмежити доступ до окремих частин мережі і захистити критично важливі ресурси. Топології, засновані на використанні міжмережевих екранів, дозволяють знижувати ризики зовнішніх атак і мінімізувати потенційний вплив на внутрішню інфраструктуру організації.

Міжмережеві екрани (брандмауери) грають ключову роль у забезпеченні безпеки мережі, запобігаючи небажаному вхідному (і, в деяких випадках, вихідному) трафіку. Вони повинні бути розташовані в стратегічних точках входу на логічних межах мережі, де відбувається розподіл або збирання мережевого трафіку. Зазвичай, міжмережеві екрани виконують роль вузлів, що відповідають за керування трафіком між різними мережевими областями. Однією з ключових функцій брандмауерів є створення демілітаризованих зон (DMZ), що використовуються для

розміщення публічно доступних серверів, таких як веб-сервери або поштові сервери, які можуть бути доступні ззовні або зсередини мережі.

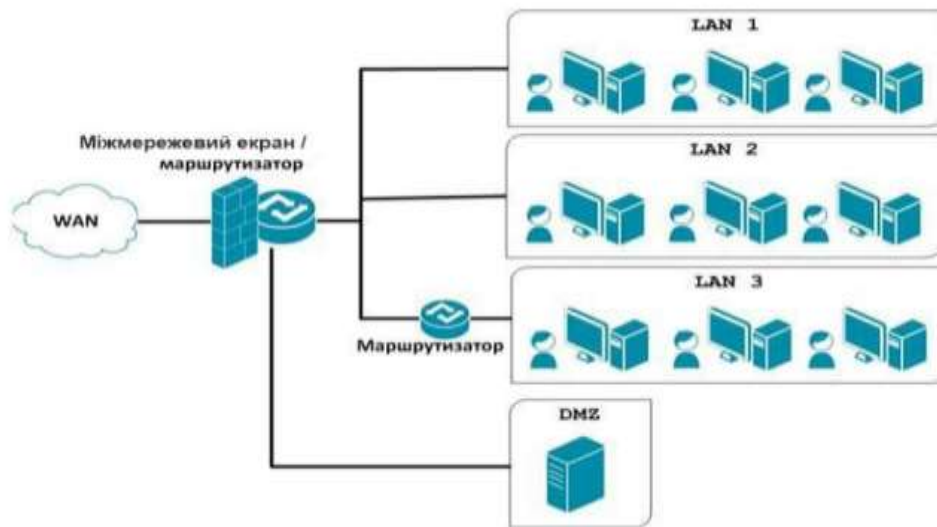


Рис. 12.7. Комп'ютерна мережа з виділеною DMZ

Джерело: [2-4]

DMZ призначена для розміщення систем і ресурсів, до яких необхідно отримати доступ із зовнішньої мережі або зсередини організації, але не повинні вони бути безпосередньо з'єднані з внутрішньою захищеною мережею. Причина цього в тому, що, незважаючи на всі заходи безпеки, ніколи не можна повністю гарантувати захищеність таких систем від атак. Важливо, щоб злом цих систем не призводив до автоматичного компрометації внутрішньої мережі.

Однією з поширених конфігурацій DMZ-мереж є так звана «service leg» конфігурація брандмауера, де міжмережвий екран має три мережевих інтерфейси: один підключений до Інтернету, другий — до внутрішньої мережі, а третій — до DMZ-мережі. Це дозволяє чітко розмежувати доступ до публічних і приватних ресурсів. Така конфігурація дозволяє забезпечити контроль над доступом до сервісів і гарантувати безпеку для внутрішньої мережі, зокрема шляхом застосування правил фільтрації трафіку між DMZ та іншими мережами, що знижує ймовірність несанкціонованого доступу або атаки з боку злоумисників. Крім того, у разі компрометації публічного сервісу в DMZ, внутрішня мережа залишається ізольованою і захищеною від прямого впливу. Мережевий трафік між DMZ і внутрішньою мережею часто перевіряється на наявність шкідливих програм і аномалій, що додає додатковий рівень захисту.



Рис. 12.8. Конфігурація Service Leg DMZ

Джерело: [2-4]

Також важливо, що у конфігурації «service leg» мережеві інтерфейси можуть бути налаштовані так, щоб здійснювати лише необхідні для сервісу з'єднання, мінімізуючи потенційні точки входу для зловмисників.

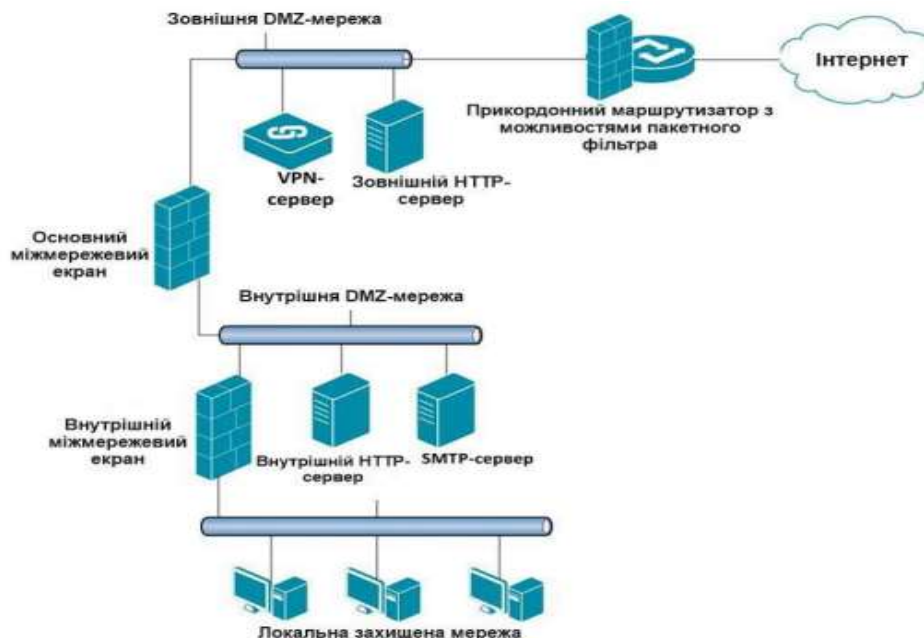


Рис. 27.9. Приклад оточення міжмережевого екрану з двома DMZмережами

Джерело: [2-4]

Оскільки DMZ містить публічні сервіси, такі як вебсайти або поштові сервери, обмеження доступу на рівні брандмауера допомагає зменшити

вплив можливої атаки на ці ресурси. Завдяки такій архітектурі, організації можуть ефективно підтримувати високий рівень безпеки для критичних внутрішніх даних, при цьому не порушуючи доступність публічних сервісів.

У випадку двох DMZ-мереж, міжмережевий екран з'єднується з двома різними DMZ-сегментами, забезпечуючи фільтрацію пакетів і доступ до серверів. Прикордонний маршрутизатор фільтрує пакети, щоб забезпечити захист серверів, а міжмережевий екран відповідає за управління доступом і захист серверів в кожній із DMZ, ізольованих від внутрішніх або зовнішніх атак.

VPN (Virtual Private Network) також є важливою частиною архітектури міжмережевих екранів, що дозволяє створити безпечні з'єднання між віддаленими користувачами і організацією через ненадійні мережі, такі як Інтернет. VPN забезпечує шифрування і аутентифікацію для захисту трафіку між кінцевими точками.

Екстранет є своєрідним бізнес-to-бізнес інтранетом, що дозволяє забезпечити обмежений і керований доступ віддалених користувачів до чутливої інформації організації за допомогою тієї ж форми аутентифікації і шифрування, що й у VPN. Це дозволяє контролювати доступ до даних, зберігаючи їх безпечними і захищеними від несанкціонованого доступу з боку сторонніх осіб.



Рис. 12.10. VPN й екстранет, що з'єднує дві інтранет мережі
Джерело: [2-4]

Принципи ефективної роботи міжмережевого екрану включають кілька важливих аспектів:

1. Визначення вимог з боку зовнішнього оточення: необхідно враховувати вплив зовнішнього середовища на функціонування брандмауера.

2. Створення політики брандмауера: необхідно розробити чітку політику щодо того, як слід обробляти вхідний і вихідний трафік, встановлюючи чіткі правила фільтрації.

3. Розробка правил брандмауера: потрібно визначити набір правил, що реалізують політику безпеки організації, забезпечуючи при цьому максимальну продуктивність системи.

4. Аналіз продуктивності брандмауера: важливо регулярно перевіряти ефективність роботи міжмережевого екрану, щоб вчасно виявляти проблеми з продуктивністю.

5. Управління архітектурою і компонентами МЕ: слід забезпечити безперервне управління і налаштування міжмережевих екранів, їх програмним забезпеченням і політиками протягом усього їх функціонування.

Таким чином, топологія мережі з використанням міжмережевих екранів дозволяє ефективно контролювати потоки трафіку, забезпечуючи захист внутрішніх ресурсів і систем організації.

12.2. МІЖМЕРЕЖЕВІ ЕКРАН ПРИКЛАДНОГО РІВНЯ. ПРОКСІ-СЕРВЕРИ

Міжмережевий екран прикладного рівня (Application Layer Firewall) є спеціалізованим типом міжмережевого екрана, який працює на найвищому рівні моделі OSI, тобто на рівні додатків. Цей тип екрану фільтрує трафік не тільки за IP-адресами та портами, а й на основі конкретних характеристик і поведінки програм, що передають дані через мережу. Міжмережевий екран прикладного рівня має змогу аналізувати зміст пакетів на рівні додатків, таких як HTTP, FTP, SMTP тощо, та блокувати небажану активність або зловмисні запити, які можуть не бути помічені традиційними міжмережевими екранами. Наприклад, він може перевіряти запити на відкриття файлів через HTTP або перевіряти команди в електронних листах через SMTP для виявлення шкідливого вмісту, такого як віруси або спам.

Основна перевага таких екранів полягає в їхній здатності аналізувати пакети на глибшому рівні, дозволяючи забезпечити більш точний контроль за трафіком і блокуванням специфічних атак, таких як SQL-ін'єкції, крос-сайт скриптинг (XSS) або атаки на програмне забезпечення сервера. Міжмережевий екран прикладного рівня може застосовувати фільтрацію контенту, ідентифікацію підозрілих запитів або активність, а також

глибокий аналіз трафіку для виявлення аномальних патернів або спроб несанкціонованого доступу. Таким чином, цей тип міжмережевого екрана забезпечує додатковий рівень захисту від більш складних загроз, що можуть бути пропущені на рівні традиційних екранів.

Прикладні шлюзи, або міжмережеві екрани (МЕ) прикладного рівня, виконують функції посередників, працюючи як проксі-сервери для прикладних протоколів, таких як HTTP, FTP, Telnet тощо. Вони забезпечують високий рівень безпеки, оскільки здійснюють фільтрацію трафіку на прикладному рівні, перевіряючи вміст усіх пакетів, що передаються між клієнтами та серверами.



Рис. 12.11. Робота проксі-сервісу

Джерело: [2-4]

Завдяки цьому, прикладний шлюз може обмежувати доступ до певних ресурсів на основі різних критеріїв, таких як адреси, номери портів, повноваження користувачів, час доби тощо. Крім того, прикладні шлюзи дозволяють виконувати аутентифікацію користувачів, фільтрувати окремі типи файлів або команди, що передаються через мережу, наприклад, забороняти використання команди PUT в FTP або блокувати певні вкладення в електронних листах.

Додатково, прикладні шлюзи можуть виконувати перевірку справжності інформації, захищати мережу від вірусів і спаму, здійснювати шифрування та дешифрування даних, реєструвати події і виконувати аудит. Вони також можуть генерувати звіти про події в мережі та здійснювати кешування даних з зовнішніх мереж, що допомагає знизити навантаження на канал зв'язку і прискорити доступ до часто запитуваних ресурсів. Завдяки таким можливостям, прикладні шлюзи забезпечують високий рівень захисту локальних мереж, хоча і мають деякі недоліки. Одним із таких недоліків є складність налаштування та конфігурації, а також висока вимогливість до ресурсів комп'ютерних платформ, на яких вони реалізовані. Крім того, відмова прикладного шлюзу може призвести

до порушення доступності, хоча безпека локальної мережі не буде порушена.

Проксі-сервери

Проксі-сервери (від англ. "proxy" — представник, агент) є проміжними серверами, які виступають посередниками між кінцевим користувачем і іншими ресурсами в мережі, наприклад, веб-сайтами або внутрішніми серверами підприємства. Вони виконують роль посередників у процесі доступу до ресурсів, приймаючи запити від клієнтів і передаючи їх відповідним серверам. Проксі-сервери можуть використовуватись для різних цілей, таких як забезпечення безпеки, покращення продуктивності, а також анонімізації інтернет-трафіку.

Основна функція проксі-сервера полягає у фільтрації запитів та відповідей, що дозволяє здійснювати контроль за трафіком, наприклад, блокувати доступ до небажаних сайтів або перевіряти вміст даних на наявність шкідливих програм. Також проксі-сервери можуть бути використані для кешування, що дозволяє зменшити час завантаження веб-сторінок та знижує навантаження на зовнішні сервери. Вони дозволяють створювати анонімний доступ до Інтернету, приховуючи реальну IP-адресу користувача та ускладнюючи відстеження його онлайн-діяльності. Проксі-сервери також можуть допомогти в оптимізації використання мережевих ресурсів, здійснюючи балансування навантаження або обмеження пропускної здатності.

Існують різні типи проксі-серверів, зокрема:

1. HTTP-проксі — використовується для обробки запитів HTTP і дозволяє обмежити доступ до веб-сайтів або аналізувати веб-трафік.
2. SOCKS-проксі — може працювати з різними типами трафіку, включаючи HTTP, FTP, SMTP, і дозволяє працювати з будь-яким протоколом, що передає дані через TCP/IP.
3. FTP-проксі — використовується для передачі даних між клієнтами і FTP-серверами, часто з метою захисту від загроз безпеці.
4. Анонімні проксі — використовуються для забезпечення анонімності в Інтернеті, приховуючи реальну IP-адресу користувача.

Проксі-сервери є важливими інструментами для підприємств і організацій, оскільки дозволяють контролювати доступ до корпоративних ресурсів, захищати внутрішню мережу від зовнішніх загроз і забезпечувати моніторинг інтернет-діяльності.

Проксі-сервери є важливим елементом сучасних мережевих інфраструктур, забезпечуючи анонімність, безпеку та ефективність обробки запитів між користувачем та Інтернет-ресурсами. Вони функціонують як посередники, через які проходять усі запити користувача

до веб-сервера. Коли користувач намагається отримати доступ до веб-сайту, замість прямого зв'язку з сервером, запит направляється до проксі-сервера, який передає його далі на сервер, отримує відповідь і повертає її користувачу. Такий підхід дозволяє приховувати реальну IP-адресу користувача, що забезпечує його анонімність в Інтернеті.

Крім того, проксі-сервери виконують функції безпеки, блокуючи доступ до шкідливих сайтів і фільтруючи небажаний контент, а також можуть перевіряти запити на наявність шкідливих програм або вірусів.

Однією з важливих функцій проксі є кешування, яке дозволяє зберігати часто використовуваний контент і значно зменшувати час завантаження веб-сторінок. Це покращує продуктивність мережі, особливо у великих організаціях або при високому навантаженні на сервери. Також проксі-сервери можуть виконувати роль контролю доступу до ресурсів, обмежуючи або фільтруючи користувачів за певними критеріями, наприклад, блокуючи доступ до певних сайтів або застосовуючи політику обмеженого доступу в рамках корпоративних мереж.

Залежно від завдань, проксі-сервери бувають різних типів: форвард-проксі, реверс-проксі, прозорі та анонімні проксі. Форвард-проксі використовуються для анонімізації трафіку користувача, в той час як реверс-проксі обробляють запити, що надходять до серверів, і перенаправляють їх на внутрішні сервери. Прозорі проксі не вимагають додаткових налаштувань на стороні клієнта і лише прозоро обробляють трафік. Анонімні проксі приховують реальну IP-адресу користувача від веб-сервера. Таким чином, проксі-сервери є важливими інструментами для оптимізації мережевої взаємодії, покращення безпеки, зниження навантаження на сервери та забезпечення анонімності користувачів.

Проксі-сервер є важливим елементом системи безпеки розподілених мережових додатків, виконуючи функції посередника між клієнтськими та серверними частинами, що дозволяє контролювати трафік, що проходить між ними. Проксі-сервер виступає в ролі транзитного вузла, що логічно розриває пряме з'єднання між клієнтом і сервером, таким чином дозволяючи здійснювати контроль над процесом обміну повідомленнями та забезпечувати безпеку передавання даних. Як і мережевий екран, проксі-сервер може ефективно виконувати свої функції лише за умови, що весь трафік проходить через нього, а не обходить його шляхом прямого з'єднання між клієнтом і сервером.

Проксі-сервер здатний виконувати низку важливих функцій для забезпечення інформаційної безпеки. Перша з них — контроль доступу, що дозволяє визначати, які клієнти мають право доступу до зовнішніх ресурсів, а які запити слід заблокувати. Також важливою є функція

фільтрації трафіку, яка забезпечує виявлення і блокування шкідливого контенту, такого як віруси, фішингові сайти чи небажана реклама. Проксі-сервер може також здійснювати кешування часто використовуваних ресурсів, що значно знижує навантаження на зовнішні сервери та підвищує швидкість доступу до них. Ще однією важливою функцією є анонімізація, яка приховує реальні IP-адреси клієнтів, що ускладнює їх ідентифікацію на зовнішніх серверах і тим самим додає рівень безпеки. Для моніторингу і аналізу діяльності мережі проксі-сервер може вести журнал активності користувачів, що дозволяє виявляти підозрілі або небажані дії в системі.

Існують кілька варіантів розміщення проксі-сервера, в залежності від цілей та потреб організації.

Основні варіанти:

✿ Проксі-сервер на рівні мережі (*Network-based Proxy Server*)

Цей тип проксі-сервера розміщується на перехресті між внутрішньою мережею підприємства та Інтернетом. Всі вихідні запити користувачів спочатку проходять через цей сервер, що дозволяє здійснювати централізовану фільтрацію та моніторинг трафіку. Це може включати блокування доступу до певних веб-сайтів, аналіз шкідливих програм, а також кешування для підвищення швидкості доступу до популярних ресурсів.

✿ Проксі-сервер на рівні клієнта (*Client-side Proxy*)

Цей варіант передбачає встановлення проксі-сервера на кожному кінцевому пристрої або на робочих станціях користувачів. Це дозволяє контролювати доступ до Інтернету безпосередньо на пристрої користувача, що корисно для індивідуальних налаштувань безпеки або фільтрації трафіку. Наприклад, в домашніх мережах часто використовуються VPN-проксі, які забезпечують анонімність і безпеку при серфінгу.

✿ Проксі-сервер на рівні веб-програми (*Application-level Proxy*)

В цьому випадку проксі-сервер інтегрується безпосередньо в веб-додатки, такі як сервери для електронної пошти, веб-сервери, або інші програми, що потребують специфічного типу обробки запитів. Проксі може здійснювати детальнішу перевірку трафіку і контенту, що дозволяє гнучко налаштовувати доступ до ресурсів в межах конкретних додатків, підвищуючи безпеку і знижуючи навантаження на сервери.

✿ Розподілений проксі-сервер (*Distributed Proxy*)

Розподілений проксі-сервер складається з кількох вузлів, розміщених в різних частинах мережі або навіть на віддалених локаціях. Цей варіант є

корисним для організацій з великою кількістю офісів або віддалених співробітників, оскільки він дозволяє зберігати високу продуктивність і забезпечувати зручний доступ до ресурсів, оптимізуючи використання пропускної здатності між локаціями.

✱ *Проксі-сервер як частина VPN (VPN Proxy)*

У цьому випадку проксі-сервер використовується разом з віртуальною приватною мережею (VPN), забезпечуючи додатковий рівень анонімності та безпеки. VPN-проксі дозволяє користувачам створювати зашифровані з'єднання з інтернет-ресурсами, маскуючи їх реальні IP-адреси та забезпечуючи захист даних від сторонніх спостерігачів.

✱ *Зовнішній проксі-сервер (External Proxy)*

Зовнішні проксі-сервери зазвичай знаходяться поза межами внутрішньої корпоративної мережі і можуть використовуватись для підвищення рівня анонімності або для обходу географічних обмежень. Вони дозволяють користувачам отримати доступ до ресурсів Інтернету, при цьому приховуючи реальну IP-адресу і забезпечуючи певний рівень захисту від кіберзагроз.

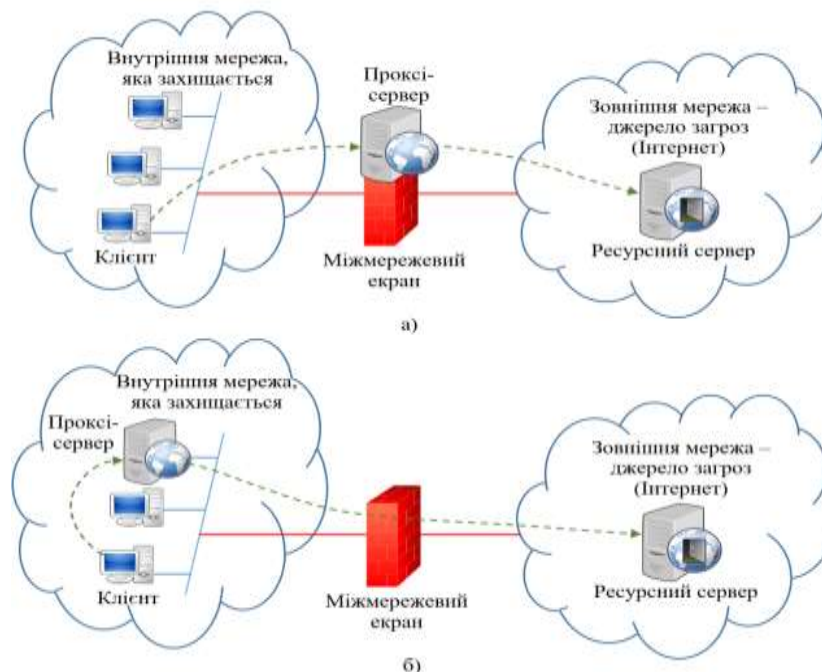


Рис. 12.12. Варіанти розміщення проксі-сервера
Джерело: [2-4]

Принцип роботи проксі-сервера полягає в тому, що всі запити клієнтів надсилаються через сервер, який перевіряє їх на відповідність політикам безпеки та лише після цього передає запити до зовнішніх серверів. Завдяки

цьому, проксі-сервер може контролювати та обмежувати доступ до потенційно небезпечних ресурсів або здійснювати додаткову перевірку запитів. У разі потреби проксі-сервер може також забезпечити шифрування трафіку для підвищення безпеки передавання даних.

Існує кілька варіантів розміщення проксі-сервера. Перший передбачає інтеграцію проксі-сервера безпосередньо на платформу, де працюють інші елементи брандмауера, що дозволяє забезпечити централізовану контрольовану взаємодію між внутрішньою та зовнішньою мережами. Другий варіант передбачає встановлення проксі-сервера на окремому вузлі, що може знаходитися в демілітаризованій зоні або в іншій частині внутрішньої мережі. В такому випадку програмне забезпечення клієнтів має бути налаштоване таким чином, щоб не дозволяти прямі з'єднання з ресурсами безпосередньо, минаючи проксі-сервер. Це гарантує, що всі з'єднання проходять через посередницький сервер, що забезпечує належний рівень безпеки.

Для ефективної роботи проксі-сервера необхідно, щоб усі клієнтські запити обов'язково проходили через цей сервер. У разі наявності можливості для обхідних шляхів, коли клієнти можуть підключатися до серверів безпосередньо, ефективність проксі-сервера значно знижується, оскільки його функції будуть обмежені лише частиною трафіку. Тому важливо налаштувати мережу таким чином, щоб обхідний доступ був заблокований, і весь трафік направлявся через проксі-сервер для перевірки і фільтрації.

У той же час, проксі-сервери виконують важливу роль у мережевій безпеці, забезпечуючи посередницький доступ до зовнішніх ресурсів і приховування даних користувачів. Проксі-сервери дозволяють кешувати дані, що знижує навантаження на канал зв'язку і прискорює доступ до ресурсів, а також виконують стиснення даних для економії трафіку. Вони можуть бути налаштовані для захисту локальних мереж від зовнішніх атак, обмеження доступу до певних ресурсів або анонімізації з'єднань, що дозволяє користувачам здійснювати запити до ресурсів без розкриття їхніх реальних даних. Існують різні типи проксі-серверів, кожен з яких має свої специфічні функції та застосування.

Коли клієнт бажає отримати ресурс, такий як файл, веб-сторінка або поштове повідомлення, він надсилає запит до проксі-сервера. Проксі-сервер, отримавши цей запит, аналізує його згідно з заданими адміністратором правилами і приймає рішення, як його обробити. Це може включати відкидання запиту, передачу його без змін до ресурсного сервера або модифікацію запиту перед передачею. Правила, за якими працює проксі-сервер, можуть бути досить складними. Наприклад, доступ до

певних серверів чи додатків може бути заблокований в робочі години, а доступ до інших ресурсів дозволений лише певним користувачам. В деяких випадках обмеження можуть стосуватися і певних операцій, таких як дозволяти лише завантаження файлів з FTP-серверів, але блокувати їх вивантаження. Також, проксі-сервери можуть фільтрувати поштові повідомлення за типами файлів або їх змістом, наприклад, забороняючи отримання додатків певних форматів (як, наприклад, MP3). Важливим аспектом є можливість застосування різних правил фільтрації до різних користувачів, що часто вимагає аутентифікації користувачів на проксі-сервері.

Якщо після оцінки запиту проксі-сервер вважає його дозволеним, він від імені додатку, але за власною ініціативою, встановлює з'єднання з необхідним сервером для виконання запиту. В деяких випадках проксі-сервер може модифікувати запит, наприклад, змінюючи в пакеті IP-адреси або порти TCP/UDP відправника. Це дозволяє уникнути можливості зломисника сканувати внутрішню мережу для виявлення IP-адрес і структури мережі. В таких випадках єдиною доступною для зломисника адресою буде адреса комп'ютера, на якому працює проксі-сервер, що ускладнює атаки, що базуються на знанні адрес вузлів внутрішньої мережі.

Оскільки проксі-сервер взаємодіє з клієнтом і сервером через певний протокол, він повинен враховувати специфіку цього протоколу. Наприклад, для кожного з таких протоколів, як HTTP, HTTPS, SMTP/POP, FTP чи telnet, існують окремі проксі-сервери, орієнтовані на роботу з відповідними додатками — веб-браузерами, програмами для електронної пошти, FTP-клієнтами або клієнтами telnet. Кожен тип проксі-сервера приймає і обробляє тільки ті пакети, які відповідають певному протоколу. У деяких випадках різні типи проксі-серверів об'єднуються в один програмний продукт для підтримки різних протоколів.

Проксі-сервери поділяються на два типи: *прикладного* та *сеансового* рівнів. Проксі-сервер прикладного рівня інтегрується в процедуру взаємодії між клієнтом і сервером по конкретному прикладному протоколу (наприклад, HTTP або FTP). Такий сервер "розуміє" зміст команд і послідовність повідомлень, якими обмінюються клієнт і сервер, що дозволяє проводити детальний аналіз вмісту повідомлень та виявляти підозрілі дії. З іншого боку, проксі-сервер сеансового рівня працює на транспортному рівні, контролюючи TCP-з'єднання. Оскільки він працює на більш низькому рівні, такий сервер має менше можливостей для аналізу і виявлення атак, але при цьому він універсальніший і може бути використаний будь-якими додатками, що працюють по TCP або іноді UDP-протоколах. Проксі-сервери прикладного рівня, завдяки своїй здатності

"розуміти" специфіку протоколів, використовуються для забезпечення безпеки, фільтрації контенту, а також для оптимізації передачі даних через кешування. Вони здатні перевіряти наявність шкідливого контенту, блокувати небажані запити та виконувати аутентифікацію клієнтів. Проксі-сервери сеансового рівня, в свою чергу, зазвичай використовуються для забезпечення анонімності або для створення VPN-з'єднань, оскільки вони здатні змінювати або приховувати інформацію про джерело з'єднання на рівні IP-адрес. Хоча вони не мають такої гнучкості для перевірки вмісту даних, їх перевага полягає в простоті використання та швидкості роботи, оскільки вони не потребують складних алгоритмів для обробки даних.

Проксі-сервер може працювати в наступних трьох основних режимах: **прозорий режим, аутентифікуючий режим, зворотний проксі-сервер.**

Прозорий режим

Прозорий проксі-сервер працює без необхідності налаштування клієнтів і автоматично перенаправляє HTTP-з'єднання. Він отримав свою назву через те, що користувачі та додатки не потребують спеціальної конфігурації для його використання. Прозорий проксі може бути використаний для таких цілей, як кешування веб-сторінок, блокування доступу до певних ресурсів, моніторинг трафіку або фільтрація контенту. Оскільки він не вимагає змін у налаштуваннях кінцевих пристроїв, прозорі проксі зазвичай застосовуються на рівні мережевої інфраструктури організації, для контролю трафіку без втручання в роботу користувачів. Це зручне рішення для адміністраторів, оскільки дозволяє ефективно управляти доступом до Інтернету та покращувати швидкість роботи мережі без необхідності залучення кінцевих користувачів до налаштувань. Прозорі проксі-сервери також широко використовуються в системах безпеки для моніторингу і фільтрації трафіку, допомагаючи забезпечити додатковий рівень захисту від шкідливих веб-сайтів або небажаного контенту.

Прозорі проксі-сервери також можуть бути використані для оптимізації роботи корпоративних мереж, зменшуючи навантаження на основні сервери шляхом кешування часто відвідуваних веб-ресурсів. Це дозволяє скоротити час завантаження сторінок для користувачів та зменшити споживання пропускну здатності Інтернет-каналів. Однак, однією з основних проблем прозорих проксі є можливість їх обходу через використання зашифрованих з'єднань (наприклад, HTTPS), що ускладнює фільтрацію трафіку та моніторинг. Для вирішення цієї проблеми може застосовуватись SSL-термінація на проксі-сервері, що дозволяє

дешифрувати та аналізувати зашифровані з'єднання перед їхнім передаванням до кінцевих пристроїв.



Рис. 12.13. Прозорий режим роботи проксі серверу
Джерело: [2-4]

Аутентифікуючий режим

Аутентифікуючий проксі-сервер вимагає налаштування клієнтів для роботи з ним і дозволяє виконувати аутентифікацію користувачів через різні протоколи, такі як Kerberos або LDAP. Цей тип проксі-сервера надає додатковий рівень безпеки, оскільки перед дозволом доступу до мережі або ресурсів вимагає перевірки особи користувача. Аутентифікація здійснюється на основі наданих облікових даних, таких як ім'я користувача і пароль, або через більш складні методи, як, наприклад, двофакторна аутентифікація. Використання таких протоколів, як Kerberos або LDAP, дозволяє інтегрувати аутентифікацію проксі-сервера з існуючими корпоративними системами управління користувачами, забезпечуючи централізовану перевірку і контроль доступу.

Аутентифікуючий проксі-сервер дозволяє організаціям гнучко контролювати доступ до мережевих ресурсів, обмежуючи його лише для авторизованих користувачів. Це важливо для забезпечення безпеки, особливо в корпоративних середовищах, де необхідно відслідковувати та фільтрувати доступ до Інтернету. Крім того, такий проксі дозволяє вести детальну статистику про використання ресурсів, що допомагає в аудиті та моніторингу діяльності користувачів.

Цей тип проксі-сервера використовується не тільки для контролю доступу, але і для забезпечення політики безпеки на рівні мережі, наприклад, для блокування небажаних веб-сайтів, обмеження доступу до

певних ресурсів або для реалізації спеціальних умов доступу для різних груп користувачів.

Зворотний проксі-сервер

Зворотний проксі-сервер використовується для кешування запитів від клієнтів до серверів і може застосовуватися для розподілу навантаження та маскуванню серверів. Це дає змогу приховувати реальні адреси серверів від зовнішнього світу, що суттєво підвищує безпеку і конфіденційність. Зворотний проксі не обмежує доступ для кінцевих користувачів, а, навпаки, забезпечує правильне скерування запитів до відповідних серверів чи сервісів, зокрема, для балансування навантаження між кількома серверами.

Основною функцією зворотного проксі є балансування навантаження. Він ефективно розподіляє запити між декількома серверами, що дозволяє зменшити навантаження на окремі ресурси та підвищити продуктивність системи в цілому. Цей підхід дозволяє системам обслуговувати більше користувачів без зниження швидкості роботи або стабільності. Крім того, зворотний проксі може виступати в ролі шлюзу для шифрування трафіку, виконуючи SSL термінацію, що дозволяє зменшити навантаження на сервери та спростити керування сертифікатами.

Зворотні проксі-сервери також часто використовуються для забезпечення безпеки. Вони можуть виконувати контроль доступу, перевіряючи запити на відповідність політикам безпеки, а також використовувати систему аутентифікації для перевірки користувачів перед тим, як пропустити їх до внутрішніх ресурсів. Така система забезпечує додатковий рівень захисту для сервісів, що знаходяться всередині мережі.

Ще однією важливою функцією зворотного проксі є кешування, яке дозволяє зберігати відповіді від серверів і тим самим зменшувати навантаження на сервери та прискорювати завантаження сторінок для кінцевих користувачів. Зворотний проксі може зберігати копії часто запитуваних даних, що дає змогу значно зменшити час відгуку і скоротити використання ресурсів.

Крім того, всі запити, що проходять через зворотний проксі, можуть бути записані в журнали для подальшого аналізу і моніторингу. Це дозволяє виявляти аномалії, зловмисні спроби доступу або інші проблеми, що можуть виникнути в процесі роботи сервісів. Зворотні проксі часто використовуються для масштабованих веб-додатків і хмарних сервісів, де необхідно забезпечити високий рівень доступності, безпеки та ефективного використання ресурсів.

Тим самим, зворотний проксі-сервер відіграє ключову роль у забезпеченні продуктивності, безпеки та стабільності роботи мережевих

сервісів, а також сприяє оптимізації управління трафіком і підвищенню надійності серверної інфраструктури.



Рис. 12.14. Режим роботи зворотного проксі серверу
Джерело: [2-4]

Транзитні проксі-сервери

Транзитні проксі-сервери здійснюють запити між різними зонами безпеки, приховуючи дані про користувачів, а кешуючі проксі-сервери зберігають копії часто запитуваних ресурсів для прискорення доступу і зниження навантаження на зовнішні канали. Транзитні проксі-сервери використовуються для передавання запитів між різними мережевими зонами безпеки, виконуючи роль проміжного етапу між користувачем і кінцевим сервером. Вони приховують реальні IP-адреси користувачів, тим самим забезпечуючи анонімність і додатковий рівень захисту від можливих атак. Це дозволяє зменшити ризики витіку конфіденційної інформації або атак на систему. Кешуючі проксі-сервери, з іншого боку, зберігають копії часто запитуваних ресурсів, що значно прискорює доступ до них, знижуючи навантаження на зовнішні канали і сервіси. Вони є корисним інструментом для оптимізації швидкості роботи мережі, особливо в великих організаціях, де доступ до одних і тих самих ресурсів відбувається регулярно.

Кешуючі проксі-сервери (caching proxies)

Кешуючі проксі-сервери (caching proxies) — це тип серверів, які зберігають копії часто запитуваних ресурсів (наприклад, веб-сторінок, зображень, файлів), щоб повторно використовувати їх при наступних

запитах. Це дозволяє значно прискорити доступ до ресурсів, знижуючи навантаження на основні сервери і зовнішні канали зв'язку. Важливо правильно налаштувати кешуючий проксі, щоб він зберігав тільки необхідні дані, оптимізуючи його роботу і не зберігаючи зайвий, неактуальний контент. Динамічний або часто оновлюваний контент, як-от новини або інформація, що змінюється в реальному часі, зазвичай не є найкращим вибором для кешування, оскільки може швидко втратити актуальність. Важливим аспектом є також правильне налаштування часу зберігання кешованих ресурсів, щоб уникнути ситуацій, коли застарілі дані використовуються замість оновлених.

Проксі-сервери, які сконфігуровані на повторне використання запитів та ресурсів, шляхом їх зберігання на сервері. Важливо правильно налаштувати даний тип сервера, щоб він кешував лише те що справді потрібно. Динамічний, регулярно оновлюваний контент не кращий вибір для кешування.

Загалом, міжмережеві екрани прикладного рівня та проксі-сервери є важливими елементами в мережевій безпеці, забезпечуючи ефективний захист локальних мереж від небажаних зовнішніх атак, фільтруючи трафік і контролюючи доступ до ресурсів. Однак, їх ефективність залежить від правильного налаштування та конфігурації, а також наявності достатніх ресурсів для їх роботи.

Серед типів проксі-серверів існує кілька видів, кожен з яких має свою специфікацію та підтримує роботу лише з певними протоколами. До найпоширеніших на сьогодні належать **HTTP-, SOCKS- і NAT-проксі**, які входять до стандартних компонентів сучасних операційних систем, таких як Linux і Windows. Програмні NAT-проксі-сервери майже не відрізняються від апаратних (маршрутизаторів) за своїми характеристиками, але поступаються вузькоспеціалізованим проксі-серверам у плані адміністрування.

HTTP-проксі-сервер — один з найпоширеніших типів. Він призначений для роботи з HTTP-протоколом і здебільшого використовується браузерами та подібними додатками. Коли користувач запитує веб-сторінку, проксі-сервер перевіряє, чи є ця сторінка в кеші. Якщо сторінка відсутня або її кешування заборонено, проксі-сервер запитує її від іншого проксі чи безпосередньо з веб-сайту. Однією з основних можливостей HTTP-проксі-серверів є кешування часто використовуваних даних, що дозволяє зменшити трафік і прискорити завантаження сторінок. Однак, через динамічність Інтернету багато серверів забороняють кешування або накладають обмеження на деякі

сторінки. Крім того, HTTP-проксі-сервери можуть обмежувати доступ до певних розділів сайтів, встановлювати додаткову аутентифікацію для доступу до ресурсів, а також блокувати рекламу. Це дозволяє адмініструвати мережу ефективніше та зменшити обсяг зайвого трафіку.

HTTPS-проксі-сервер є аналогом HTTP-проксі, але з можливістю шифрування даних між клієнтом, проксі та кінцевим сервером. Він дозволяє організувати захищений канал передачі даних і підвищує безпеку, оскільки не дозволяє аналізувати передану інформацію. Однак його можливості значно обмежені порівняно з HTTP-проксі. HTTPS-проксі-сервери зазвичай поєднують з HTTP-проксі, що робить їх більш універсальними та гнучкими в налаштуванні клієнтів.

FTP-проксі-сервер працює з FTP-протоколом. Він передає запити до FTP-серверів від імені клієнтів. Є два варіанти використання FTP-проксі: перший передає запити через HTTP-проксі, але не підтримує всі функції FTP-протоколу. Другий варіант — це використання спеціалізованого FTP-проксі-сервера, який підтримує всі опції протоколу. FTP-проксі застосовуються рідше, оскільки більшість користувачів використовують FTP-сервери через HTTP-проксі без потреби в додаткових функціях.

SOCKS-проксі-сервер є універсальним і дозволяє здійснювати аутентифікацію користувачів на серверній стороні. Він працює з практично будь-яким протоколом і дозволяє з'єднувати клієнтів з внутрішніми серверами за межами міжмережевих екранів. SOCKS-проксі використовується для організації доступу клієнтів до внутрішньомережевих ресурсів, а також з зовнішніх серверів, що робить цей тип проксі надзвичайно гнучким і потужним.

Незважаючи на різноманітність типів проксі-серверів, існують також вузькоспеціалізовані сервери, які оптимізовані для роботи з конкретними додатками. Проксі-сервери, доступні для всіх користувачів Інтернету, називаються відкритими. Вони часто використовуються для анонімізації трафіку, проте можуть бути прослухані через відсутність шифрування даних.

Серед найпоширеніших прикладів проксі-серверів можна відзначити такі: 3proxy, CoolProxy, HandyCache, Kerio Control, Microsoft Forefront Threat Management Gateway, Nginx, Squid, Traffic Inspector, UserGate, Internet Control Server, TOR. Всі ці сервери мають різні платформи та функціональні можливості, що дозволяє обирати найкраще рішення в залежності від потреб і специфіки мережі.

12.3. ПРОКСІ-СЕРВЕР SQUID

Squid — це популярний проксі-сервер з відкритим вихідним кодом, який широко використовується для кешування веб-контенту, а також для контролю доступу та фільтрації трафіку в мережах. Основні функції Squid включають кешування, що дозволяє зберігати копії веб-сторінок на локальному сервері, що значно прискорює доступ до них при повторних запитах, знижує навантаження на пропускну здатність каналу і зменшує час завантаження сторінок. Проксі-сервер також дозволяє налаштувати доступ до Інтернету для користувачів, обмежуючи доступ до певних веб-ресурсів або повністю блокуючи його для конкретних IP-адрес або користувачів. Крім того, Squid може працювати як проксі-сервер для анонімізації трафіку, приховуючи реальні IP-адреси користувачів і підвищуючи рівень конфіденційності. Він також забезпечує фільтрацію контенту, наприклад, для блокування небажаних сайтів або реклами, а також веде детальні журнали запитів, що допомагає в моніторингу трафіку та виявленні аномальних або небажаних дій у мережі. Squid підтримує різноманітні протоколи, включаючи HTTP, HTTPS, FTP, і може працювати як як прямий проксі, так і в конфігураціях для обмеження доступу через прозорий проксі-сервер. Він використовується як в малих організаціях, так і на великих підприємствах для оптимізації трафіку та забезпечення безпеки мереж.

Squid є кешуючим проксі-сервером для протоколів HTTP, FTP, HTTPS (при відповідних налаштуваннях). Програмне забезпечення поширюється під ліцензією GNU GPL. Однією з основних особливостей Squid є його здатність працювати в режимі зворотного проксі (reverse proxy), що дозволяє йому служити як прискорювач для запитів, що надходять до вебсайтів. У такому режимі запити декількох користувачів до кількох сайтів кешуються, що дозволяє знизити навантаження на сервери. Зворотний проксі перевіряє запити на їх динамічність і актуальність, забезпечуючи кешування тільки актуальних даних і надаючи їх користувачам без необхідності повторного оброблення запитів на сервері.

Squid також підтримує прозорий режим проксі, в якому не проксуються лише запити FTP та HTTPS. Уся конфігурація сервера здійснюється через файл `/etc/squid/squid.conf`, в якому знаходяться основні параметри налаштувань, такі як `http_port`, `http_access` і `acl` (списки контролю доступу). Параметр `http_port` визначає порти, на яких працює проксі-сервер, а `http_access` дозволяє налаштувати доступ до ресурсів на основі різних критеріїв, зокрема за допомогою `acl`.

Система управління доступом в Squid є дуже гнучкою і дозволяє створювати складні правила для доступу до ресурсів. За допомогою `acl`

можна задати критерії доступу до ресурсів на основі різних параметрів, таких як адреси, порти, методи запиту, браузері тощо. Наприклад, acl може обмежувати доступ до ресурсів на основі IP-адреси або домену.

Що стосується аутентифікації, Squid підтримує кілька методів аутентифікації, подібних до тих, що використовуються в Apache. Серед основних методів є Basic, NTLM, Digest і Negotiate (SPNEGO). Squid взаємодіє з різними хелперами для здійснення аутентифікації, які перевіряють правильність введених користувачем облікових даних. Для роботи аутентифікації в Squid необхідно налаштувати відповідні параметри в конфігурації, зокрема `auth_param`, а також визначити `acl`, які використовуватимуть методи аутентифікації.

У випадку з Basic автентифікацією користувачі повинні надати свої облікові дані у вигляді імені користувача та пароля, закодованих в base64. Цей метод є простим, але має низький рівень безпеки, оскільки пароль передається у відкритому вигляді. Більш безпечні методи, такі як Digest, використовують хешування паролів за допомогою MD5.

NTLM і Negotiate використовуються для інтеграції з системами, що підтримують єдину аутентифікацію (SSO). NTLM є старим методом, який поступово втрачає популярність через проблеми з безпекою, тоді як Negotiate працює на базі Kerberos і є більш безпечним.

Squid також дозволяє налаштувати перенаправлення запитів за допомогою редіректорів. Ці редіректори можуть бути налаштовані для специфічних користувачів, що дозволяє адміністратору гнучко управляти доступом до інтернет-ресурсів. Одним з таких інструментів є SAMS (Squid Account Management System), яка дозволяє здійснювати управління доступом до проксі-сервера на основі баз даних.

В результаті, Squid є потужним інструментом для управління доступом до інтернет-ресурсів, забезпечення кешування і аутентифікації, а також для налаштування прозорого або зворотного проксі в залежності від потреб підприємства або організації.

12.4. СИСТЕМИ ВИЯВЛЕННЯ АТАК

Системи виявлення атак (СВА) є важливими компонентами інфраструктури безпеки сучасних інформаційно-комунікаційних систем. Вони автоматизують процес аналізу подій з точки зору безпеки, що дозволяє оперативно виявляти атаки, як ті, що вже відбуваються, так і потенційно можливі. СВА здатні не лише виявляти атаки, але й реагувати на них, здійснюючи різноманітні дії від простих звітів до активного

втручання у випадку визначення проникнень та інших аномалій. Вони працюють шляхом збору та аналізу даних про трафік, журнали подій та інші параметри, що дає змогу виявляти порушення безпеки в реальному часі. Системи виявлення атак можуть бути налаштовані для виявлення різноманітних типів атак, таких як DDoS, SQL-ін'єкції, фішинг або спроби несанкціонованого доступу. Окрім цього, багато СВА підтримують інтеграцію з іншими компонентами системи безпеки, наприклад, з фаєрволами, проксі-серверами та антивірусними програмами, що дозволяє створити єдину захисну платформу. Важливою функцією є також можливість адаптації до нових загроз через оновлення бази даних про сигнатури атак або використання машинного навчання для виявлення невідомих загроз. Крім того, СВА можуть допомагати у проведенні розслідувань інцидентів, зберігаючи історію подій для подальшого аналізу. Вони є незамінними інструментами для забезпечення безпеки інформаційно-комунікаційних систем у складному і швидко змінюваному середовищі кіберзагроз.

Системи виявлення атак (СВА) є важливим компонентом інфраструктури безпеки сучасних інформаційно-комунікаційних систем, і їх можна класифікувати за різними ознаками. Однією з основних класифікацій є метод виявлення атак, де виділяються сигнатурні СВА, які використовують визначені сигнатури або шаблони для виявлення відомих атак, а також аномальні СВА, які базуються на визначенні нормальної поведінки системи та виявленні відхилень від цієї норми. Гібридні СВА поєднують ці два підходи, що дозволяє поєднати переваги обох методів і забезпечити більш точне виявлення атак, зокрема невідомих загроз. Інша класифікація залежить від типу реалізації системи, де можна виділити системи виявлення атак на рівні мережі (NIDS), що моніторять трафік, що проходить через мережеві інтерфейси, та системи на рівні хостів (HIDS), які аналізують події безпеки на окремих комп'ютерах або серверах. За методами реагування на інциденти системи поділяються на пасивні, які лише виявляють атаки і сповіщають про них адміністратора, та активні, які можуть не лише виявляти, але й реагувати на загрози, наприклад, блокуючи трафік або ініціюючи інші заходи для припинення атаки в реальному часі. Класифікація також передбачає розрізнення СВА за призначенням: системи для моніторингу трафіку (IDS), які аналізують мережеві пакети на наявність аномалій або сигнатур атак, та системи для моніторингу подій (SIEM), які займаються збором та аналізом журналів подій з різних джерел для створення цілісної картини безпеки. Крім того, СВА можна класифікувати за рівнем інтеграції, де автономні системи працюють самостійно, а інтегровані СВА тісно співпрацюють з іншими

компонентами системи безпеки, такими як фаєрволи, антивірусні програми та системи управління подіями безпеки (SIEM), що дозволяє забезпечити комплексний підхід до захисту. Така класифікація дозволяє гнучко підходити до вибору та налаштування СВА в залежності від конкретних вимог безпеки організації та специфіки її інфраструктури.

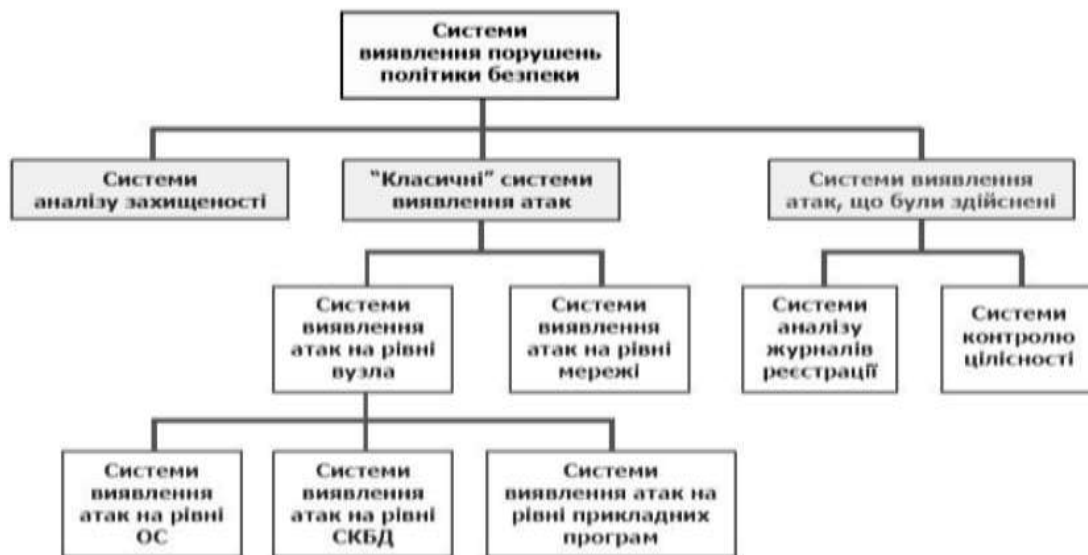


Рис. 12.15. Узагальнена класифікація СВА
Джерело: [2-4]

СВА рівня мережі

Системи виявлення атак (СВА) рівня мережі забезпечують моніторинг і аналіз мережевого трафіку для виявлення загроз у реальному часі. Їх мета — ідентифікувати атаки, такі як DDoS, сканування портів чи експлуатація уразливостей, і запобігти їх реалізації. Системи виявлення атак (СВА) рівня мережі забезпечують моніторинг і аналіз мережевого трафіку для виявлення загроз у реальному часі. Їх мета — ідентифікувати атаки, такі як DDoS, сканування портів чи експлуатація уразливостей, і запобігти їх реалізації. Ці системи здатні виявляти аномалії в мережевому трафіку, порівнюючи їх з відомими шаблонами атак або використовуючи методи машинного навчання для виявлення нових, ще не задокументованих загроз. Завдяки здатності аналізувати трафік на всіх рівнях протоколів, СВА можуть фіксувати навіть тонкі сигнали атак, які залишаються непоміченими для інших систем безпеки. Вони також здатні автоматично реагувати на виявлені загрози, блокуючи зловмисні дії або попереджаючи адміністраторів про потенційні інциденти. Однак для досягнення максимальної ефективності системи виявлення атак потребують

постійного оновлення баз даних сигнатур і адаптації до нових методів атак, що постійно розвиваються.

СВА використовують сигнатурний аналіз для виявлення відомих атак та аналіз аномалій для ідентифікації невідомих загроз. Гібридні підходи підвищують ефективність, але можуть створювати хибнопозитивні спрацьовування.

Архітектура таких систем включає сенсори, аналізатори, центр управління та сховище даних. Вони здатні охоплювати весь мережевий трафік, але мають обмеження, зокрема труднощі з аналізом зашифрованих даних і високі вимоги до ресурсів.

Популярні приклади СВА — Snort, Suricata, Zeek. У поєднанні з іншими засобами захисту, СВА створюють багаторівневу архітектуру безпеки для ефективного реагування на сучасні загрози.

СВА рівня вузла

Системи виявлення атак (СВА) рівня вузла забезпечують захист окремих пристроїв, серверів або кінцевих точок в інформаційній системі. Основне завдання таких систем — моніторинг активності на конкретному вузлі для виявлення потенційно шкідливих дій, що можуть загрожувати безпеці.

СВА рівня вузла аналізують журнали операційної системи, поведінку процесів, доступ до файлів, дії користувачів та інші локальні події. Вони можуть використовувати методи сигнатурного аналізу для виявлення відомих шкідливих дій, а також методи поведінкового аналізу для ідентифікації аномалій, характерних для невідомих загроз.

Основними компонентами таких систем є агенти, які встановлюються на вузли, модулі аналізу, які обробляють зібрані дані, та механізми сповіщення або блокування. Важливою функцією є інтеграція з іншими системами безпеки, такими як антивіруси або платформи EDR (Endpoint Detection and Response).

Приклади СВА рівня вузла: OSSEC, Wazuh, CrowdStrike Falcon. Вони ефективні для захисту від атак на локальних пристроях, проте потребують ресурсів для постійного моніторингу та оновлення баз даних. У поєднанні з мережевими СВА забезпечують комплексний рівень кіберзахисту.

СВА рівня прикладних програм

Системи виявлення атак (СВА) рівня прикладних програм спрямовані на забезпечення безпеки специфічних програмних рішень, таких як веб-додатки, бази даних та інші сервіси, що взаємодіють із користувачами або

системами. Основна їхня мета — аналізувати вхідні та вихідні дані прикладних програм для виявлення шкідливих дій, аномалій чи спроб атак. Це надзвичайно важливо, оскільки уразливості на рівні прикладних програм є одними з найбільш поширених каналів кібератак.

СВА цього рівня використовують аналіз специфічних протоколів і форматів даних, таких як HTTP, SQL чи XML, щоб виявляти загрози, пов'язані з веб-додатками, включно із SQL-ін'єкціями, міжсайтовими скриптинг-атаками (XSS) та піддробкою міжсайтових запитів (CSRF). Завдяки цьому такі системи здатні розпізнавати не лише відомі атаки за допомогою сигнатурного аналізу, але й нові загрози через поведінковий аналіз і машинне навчання. Це дозволяє їм адаптуватися до динамічного ландшафту кіберзагроз.

Інтеграція з іншими інструментами, такими як веб-фаєрволи (WAF), системи управління журналами (SIEM) чи платформи моніторингу додатків (APM), дозволяє СВА рівня прикладних програм працювати як частина комплексної системи захисту. Наприклад, використання рішень на кшталт OWASP ZAP допомагає тестувати веб-додатки на наявність уразливостей, тоді як системи типу Imperva захищають веб-додатки і API від реальних атак у реальному часі.

Таким чином, СВА рівня прикладних програм є важливим інструментом забезпечення безпеки бізнес-процесів, які функціонують через веб-інтерфейси або серверні програми. Їхня ефективність залежить від здатності виявляти сучасні загрози, захищати від експлуатації уразливостей і інтегруватися в загальну систему безпеки підприємства.

Технологія виявлення атак у СВА базується на трьох основних складових: ознаках, що описують порушення політики безпеки, джерелах, у яких ці ознаки шукаються, і методах аналізу інформації, отриманої з різних джерел. Архітектура СВА складається з кількох підсистем, що працюють разом для досягнення мети. Сенсорна підсистема займається збором подій, пов'язаних з безпекою системи, що захищається. Підсистема аналізу виявляє атаки та підозрілі дії, а сховище забезпечує накопичення як первинних подій, так і результатів аналізу. Консоль управління дозволяє здійснювати конфігурацію системи, спостерігати за її станом та переглядати інциденти, що виявлені підсистемою аналізу.

Для ефективного функціонування СВА необхідно налаштувати кілька каналів зв'язку. Це включає канали для моніторингу хостів і мереж, канали між сенсорами та керуючим сервером для передачі даних про події, а також канали для виконання відповідних дій у разі виявлення атак. Управління СВА може бути централізованим, частково розподіленим або

повністю розподіленим, залежно від рівня контролю та організації прийняття рішень.

Системи виявлення атак можуть здійснювати різні можливості, серед яких блокування джерела атаки, що є важливим при виявленні відомих уразливостей, а також реакція на атаку після її фіксації. СВА також можуть виявляти преамбули атак, такі як зондування мережі, і блокувати доступ злоумисників до системи. Вони здатні здійснювати документування існуючих загроз, що може бути корисним при складанні звітів та оцінці заходів безпеки.

Існують різні класифікації СВА, зокрема за етапом фіксації атаки (реальний час, аналіз журналів чи попередження про потенційні атаки), джерелами інформації (мережеві СВА або СВА рівня вузлів та програм), методом аналізу (виявлення зловживань чи аномалій) та швидкістю реакції. Системи реального часу обробляють інформацію на ходу, що дозволяє здійснювати автоматичне реагування на атаки, тоді як системи пакетного режиму обробляють інформацію в інтервалах.

Пасивні та активні СВА

Системи виявлення атак (СВА) є важливим елементом забезпечення кібербезпеки підприємства, забезпечуючи ідентифікацію та аналіз потенційних загроз у мережевих і інформаційних системах. Залежно від способу взаємодії з мережею та рівня втручання, СВА поділяються на пасивні та активні.

Пасивні СВА виконують моніторинг трафіку та журналів подій без втручання у сам процес обміну даними. Їх основне завдання полягає у виявленні підозрілої активності та інформуванні адміністраторів про потенційні загрози. Вони працюють у режимі реального часу, аналізуючи сигнатури відомих атак або поведінкові аномалії. Пасивні системи не впливають на мережевий трафік, що робить їх легко впроваджуваними та не навантажує інфраструктуру. Проте їхній основний недолік — неможливість самостійного реагування на атаки, що робить ефективність таких систем залежною від швидкості реакції персоналу або інтеграції з іншими засобами захисту.

Активні СВА, на відміну від пасивних, здатні не лише виявляти атаки, але й активно втручатися для їх запобігання. Вони аналізують трафік у реальному часі, блокуючи шкідливі пакети або перериваючи з'єднання у разі виявлення загроз. Ці системи забезпечують захист у режимі реального часу та зменшують ризик успішного проведення атак завдяки швидкому автоматизованому реагуванню. Однак активні СВА потребують значних обчислювальних ресурсів, можуть впливати на продуктивність мережі та мають ризик хибнопозитивних спрацьовувань, що іноді призводить до

блокування легітимного трафіку. Крім того, вони можуть вимагати налаштування та постійного оновлення для адаптації до нових типів загроз, що також може збільшити витрати на їх експлуатацію. Враховуючи ці фактори, комбіноване використання пасивних та активних СВА є найбільш ефективною стратегією для забезпечення комплексного захисту мережі.

Обидва типи систем мають свої переваги й недоліки, тому оптимальним підходом є їх комбіноване використання. Пасивні СВА забезпечують глибокий аналіз і створення звітів про підозрілі події, тоді як активні системи доповнюють їх швидким реагуванням на виявлені загрози. У комплексі ці системи підвищують загальний рівень безпеки інформаційної інфраструктури, дозволяючи ефективно протидіяти як відомим, так і новим типам атак. Пасивні СВА здатні зібрати і зберігати великий обсяг даних для подальшого аналізу, що дозволяє виявляти довгострокові тенденції та можливі загрози. Однак вони не завжди можуть реагувати на загрози в реальному часі, що робить їх уразливими до швидко змінюваних атак. Тому активні СВА, з їх здатністю реагувати негайно, додають додатковий рівень захисту, що дозволяє заблокувати або зменшити вплив загрози на початкових етапах її реалізації.

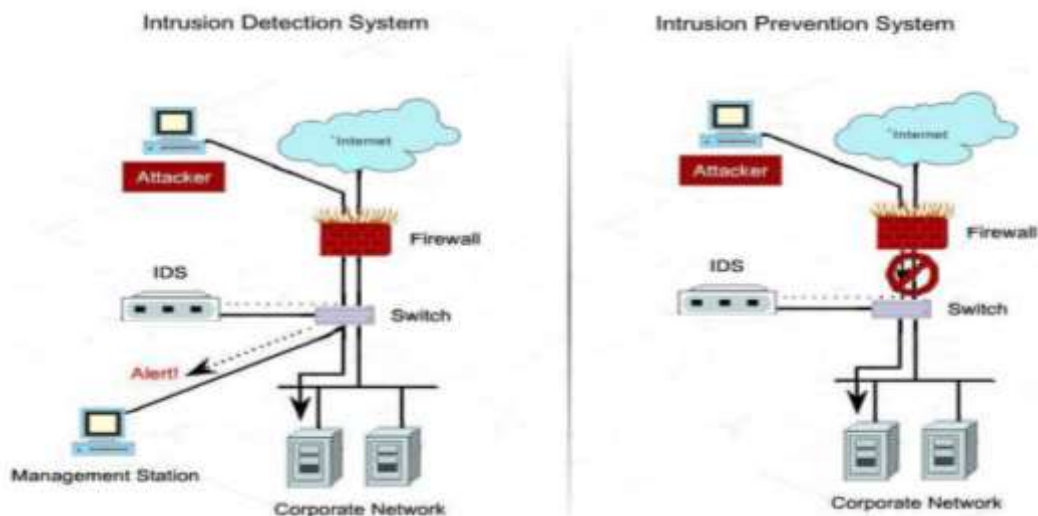


Рис. 12.16. Дія пасивної (IDS) та активної (IPS) СВА
Джерело: [2-4]

СВА можуть мати активні або пасивні методи реагування. Активні системи здійснюють автоматичне втручання, наприклад, блокуючи мережеві маршрути, тоді як пасивні лише генерують звіти, що потім аналізуються людьми для прийняття рішень.

Залежно від рівня аналізу, існують мережеві СВА, які аналізують мережеві пакети, та СВА рівня вузлів, що працюють з інформацією,

зібраною на окремих комп'ютерах. Мережеві СВА мають переваги в тому, що можуть стежити за великими мережами без значного впливу на їхню продуктивність, проте мають обмеження в можливостях аналізувати зашифровані дані та визначати, чи була атака успішною. СВА рівня вузлів, навпаки, можуть аналізувати системну інформацію та реагувати на більш детальні рівні атак, однак можуть бути вразливими до певних атак і потребують більших обчислювальних ресурсів.

СВА і Брандмауер

Системи виявлення атак (СВА) та брандмауери є важливими елементами забезпечення інформаційної безпеки, які взаємодоповнюють один одного, формуючи багаторівневий захист мережі. Кожен із цих інструментів має унікальні функції та завдання, які разом забезпечують більш ефективне протистояння кіберзагрозам.

Брандмауер (або міжмережевий екран) виступає першою лінією оборони, забезпечуючи контроль мережевого трафіку на основі встановлених правил. Його основна функція — запобігати несанкціонованому доступу до ресурсів мережі, блокуючи підозрілий або небажаний трафік. Це досягається шляхом фільтрації даних за такими критеріями, як IP-адреси, порти чи протоколи. Брандмауери можуть бути апаратними, програмними або комбінованими, працюючи на межі між внутрішньою мережею та зовнішнім середовищем.

СВА, своєю чергою, орієнтовані на виявлення шкідливої активності як у зовнішньому трафіку, так і всередині мережі. Вони аналізують поведінку користувачів, сигнатури відомих атак та аномалії в роботі системи. СВА бувають пасивними, які лише сповіщають адміністраторів про потенційні загрози, та активними, здатними автоматично реагувати на інциденти, наприклад, блокувати атаку або ізолювати уражений сегмент.

Основна різниця між брандмауером і СВА полягає в їхніх підходах до захисту. Брандмауери діють превентивно, блокуючи небажаний трафік до того, як він потрапить у мережу. Натомість СВА працюють реактивно, виявляючи атаки, які змогли обійти периметр захисту, або загрози, що виникли всередині системи. СВА також здатні аналізувати складніші патерни загроз, включно з поведінковими аномаліями, які не можуть бути виявлені лише на основі правил.

Інтеграція цих технологій забезпечує комплексний підхід до кіберзахисту. Брандмауер виступає бар'єром для більшості загроз, зупиняючи відомі атаки та блокуючи небажаний доступ. СВА, своєю чергою, надають додатковий рівень захисту, ідентифікуючи складні або нові загрози, які можуть обійти традиційні методи фільтрації. Таке

поєднання дозволяє знизити ризики та забезпечити безперервний моніторинг безпеки, ефективно реагуючи на сучасні кіберзагрози.

Таким чином, СВА відіграють важливу роль у забезпеченні безпеки інформаційно-комунікаційних систем, забезпечуючи виявлення та реагування на загрози, але їх ефективність залежить від правильної конфігурації та комбінування різних типів систем, що дозволяють забезпечити надійний захист.

12.5. СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ

Системи виявлення та запобігання вторгнень (IDS/IPS) є важливими компонентами інформаційної безпеки, що забезпечують захист мереж від несанкціонованого доступу та атак. IDS зосереджуються на моніторингу та аналізі мережевого трафіку для виявлення підозрілих дій та атак, в той час як IPS, на відміну від IDS, активно реагують на виявлені загрози, блокуючи шкідливий трафік або перериваючи з'єднання в реальному часі. Вони можуть працювати як на рівні мережі, так і на прикладному рівні, забезпечуючи комплексний захист від різноманітних атак, включаючи DDoS, сканування портів та спроби експлуатації уразливостей. Враховуючи важливість таких систем, їх інтеграція в інфраструктуру безпеки підприємства є необхідною для підтримки належного рівня захисту інформаційних ресурсів та забезпечення безперебійної роботи мережі.

Система виявлення вторгнень (IDS) виконує моніторинг мережі або комп'ютерної системи, виявляючи підозрілі дії або порушення політик безпеки. Вона аналізує трафік, шукаючи сигнатури або аномалії, які можуть свідчити про зловмисні дії. Система виявлення вторгнень (IDS) фокусується на аналізі мережевого трафіку та активності на комп'ютерних системах для виявлення потенційних загроз або підозрілих дій. Вона працює шляхом порівняння поточної активності з відомими сигнатурами атак або створенням профілю нормальної поведінки, на основі якого визначаються аномалії.

IDS може працювати як на рівні мережі, аналізуючи трафік, що проходить через маршрутизатори і фаєрволи, так і на рівні хостів, де здійснюється моніторинг подій на окремих пристроях. Виявлені підозрілі дії можуть бути зафіксовані в журналах для подальшого аналізу або використані для генерації попереджень для адміністратора системи безпеки. В залежності від типу IDS, вона може використовувати сигнатурний метод виявлення, що дозволяє знаходити відомі загрози, або

аномальний метод, який допомагає виявляти нові або невідомі атаки. Важливою характеристикою IDS є її здатність виявляти не лише атаки, але й аномалії в поведінці користувачів або пристроїв, що можуть свідчити про спроби злому або помилки в системі. Однак система IDS сама по собі не може здійснювати активну реакцію на загрози — для цього існують системи виявлення та запобігання вторгненням (IPS). Тим не менш, інтеграція IDS з іншими елементами системи безпеки дозволяє швидше реагувати на загрози та знижувати ризики. Використання IDS допомагає організаціям забезпечити більш високий рівень безпеки шляхом раннього виявлення загроз і запобігання потенційним атакам.

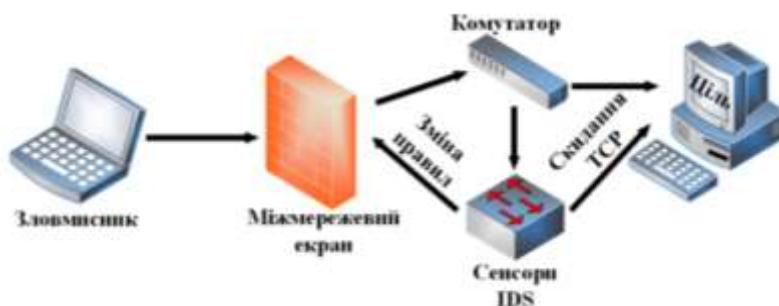


Рис. 12.17. Система виявлення вторгнень (IDS)

Джерело: [2-4]

У разі виявлення загрози IDS генерує попередження для адміністратора безпеки, що дозволяє йому вчасно реагувати на ситуацію. IDS може бути сигнатурним, коли вона перевіряє трафік на наявність відомих патернів атак, або аномальним, коли система виявляє відхилення від нормальної поведінки системи чи мережі. Проте IDS не здійснює активного реагування на загрози, її роль обмежується лише виявленням і попередженням про можливі інциденти.

Для активного реагування на загрози використовуються системи виявлення та запобігання вторгненням (IPS), які, на відміну від IDS, можуть блокувати підозрілі дії або трафік. IDS є важливим інструментом для збору і аналізу інформації про безпеку, оскільки дозволяє виявити потенційні загрози на ранніх етапах. Зазвичай, системи IDS вимагають постійного оновлення сигнатур для ефективної роботи, що дозволяє підтримувати їхню актуальність у боротьбі з новими типами атак. Однак, аномальні системи IDS мають перевагу в тому, що вони можуть виявляти нові або раніше невідомі загрози, не потребуючи попереднього знання про конкретні атаки. Оскільки IDS часто генерує велику кількість попереджень, важливим аспектом є налаштування системи для зменшення

кількості хибних спрацьовувань, що може значно підвищити ефективність реагування. Інтеграція IDS з іншими елементами системи безпеки, такими як SIEM, може допомогти покращити збирання та аналіз даних з різних джерел. В цілому, IDS забезпечує критичне спостереження за мережею і системами, сприяючи підвищенню загального рівня безпеки організації.

Система запобігання вторгнень (IPS) має більш активний підхід, не лише виявляючи, але й автоматично реагуючи на загрози. Вона може блокувати підозрілі з'єднання, знижувати ризик атак і запобігати потенційним збоям в роботі мережі. Існує два основних типи IPS: мережеві, що працюють на рівні мережевого трафіку, і хостові, що забезпечують захист на рівні конкретного пристрою або сервера. Натомість система запобігання вторгненням (IPS) виконує активні дії для запобігання атакам у реальному часі. Вона не тільки виявляє загрози, але й може автоматично блокувати підозрілі з'єднання, пакети або зупиняти шкідливі процеси, тим самим зменшуючи можливі збитки від атаки. IPS інтегрується з мережевим середовищем і моніторить трафік або хостові системи, де може виявляти атаки на основі сигнатур або аномалій. Якщо загроза виявляється, IPS автоматично вживає відповідних заходів для її блокування, що забезпечує негайний захист від атак.



Рис. 12.18. Система запобігання вторгнень (IPS)

Джерело: [2-4]

IPS може використовувати різноманітні технології виявлення атак, такі як сигнатурний аналіз, аналіз на основі аномалій та поведінковий аналіз, що дозволяє оперативно виявляти навіть невідомі або нові загрози. Це робить систему більш гнучкою та ефективною у боротьбі з новітніми видами атак, що можуть обходити традиційні методи захисту. Оскільки IPS працює в реальному часі, вона може здійснювати захист від DDoS-атак, шкідливих спроб проникнення або несанкціонованого доступу до чутливих даних, запобігаючи значним збиткам. Однак, необхідно враховувати, що IPS може впливати на продуктивність системи або мережі, тому її налаштування має бути оптимізоване для забезпечення належного рівня безпеки без зниження ефективності роботи. Оскільки

атаки стають усе більш складними, IPS необхідно постійно оновлювати для врахування нових тактик, технік і процедур, що використовують зловмисники. Це включає в себе регулярне оновлення баз даних сигнатур і вдосконалення алгоритмів для детекції аномалій. Враховуючи всі ці фактори, IPS є важливим компонентом багаторівневого захисту, що забезпечує комплексний підхід до безпеки мереж і систем.

Системи IPS можуть бути мережевими (NIPS), коли моніторинг здійснюється на рівні мережі, або хостовими (HIPS), де система працює безпосередньо на хостах, контролюючи активність на них. Їх головна перевага — це можливість миттєвого реагування на загрози, що дозволяє зменшити час впливу атаки і захистити системи та дані від серйозних ушкоджень. Мережеві IPS ефективно блокують загрози на рівні інфраструктури, аналізуючи весь вхідний і вихідний трафік, в той час як хостові системи зосереджуються на конкретних пристроях, забезпечуючи захист від атак, які можуть оминати мережеву безпеку. Зазвичай для досягнення максимальної ефективності використовують гібридний підхід, поєднуючи обидва типи систем, що забезпечує більш глибоке покриття. Важливою характеристикою IPS є здатність автоматично блокувати атаки, зменшуючи потребу в людському втручанні. Однак, оскільки ці системи можуть впливати на продуктивність мережі та систем, їх налаштування та оптимізація є важливими аспектами для забезпечення ефективного захисту.

IPS можуть використовувати різні методи виявлення загроз, зокрема сигнатурні, аномальні та гібридні, що дає можливість детектувати як відомі, так і нові атаки. Вони активно взаємодіють з іншими компонентами системи безпеки, такими як фаєрволи та системи моніторингу, для узгодженого реагування на загрози. Крім того, IPS можуть інтегруватися з системами управління подіями безпеки (SIEM), що дозволяє проводити глибший аналіз подій і виявляти більш складні атаки. Однак, через високу швидкість реагування, необхідно враховувати можливість хибних спрацьовувань, що можуть спричинити помилкове блокування легітимного трафіку або дій. Підвищена складність налаштування та обслуговування систем IPS вимагає висококваліфікованих фахівців для оптимального впровадження та підтримки цих систем. IPS також необхідно регулярно оновлювати для забезпечення захисту від нових типів атак, що постійно з'являються. У результаті, системи IPS забезпечують критичний захист для інфраструктури організацій, ефективно запобігаючи значним збиткам від кібератак.

IDS і IPS часто використовуються разом, створюючи багаторівневу систему захисту. IDS відповідає за виявлення і попередження загроз, тоді

як IPS бере на себе функцію автоматичного реагування та блокування. Така комбінація дозволяє більш ефективно захищати інформаційні системи: IDS допомагає виявити нові або невідомі загрози, а IPS негайно їх нейтралізує. У зв'язку з цим разом ці системи забезпечують не тільки високу якість виявлення атак, а й швидке і ефективно запобігання їм, що є ключовим для підтримки кібербезпеки. Однак важливо враховувати, що використання цих систем потребує правильного налаштування для мінімізації кількості помилкових спрацьовувань, оскільки як IDS, так і IPS можуть генерувати хибні тривоги. Ідеально налаштована система забезпечує надійний захист, знижуючи ризик шкоди від кіберзагроз та забезпечуючи своєчасне реагування на потенційні інциденти.

Інтеграція IDS і IPS також дозволяє створити систему, яка не тільки виявляє і реагує на загрози, але й проводить глибший аналіз мережевого трафіку та системних подій для виявлення потенційних вразливостей. Важливою перевагою такої комбінації є можливість виявлення нових форм атак, які можуть не мати явних сигнатур, за допомогою аномалійного аналізу IDS, в той час як IPS швидко нейтралізує загрозу. Це дозволяє знижувати ризик успішних атак на організацію, запобігаючи серйозним збиткам. Крім того, система, яка поєднує IDS та IPS, може оптимізувати використання ресурсів безпеки, зменшуючи необхідність ручного моніторингу і втручання в реальному часі. Проте, для максимальної ефективності, ці системи повинні регулярно оновлюватися з урахуванням нових типів атак і уразливостей, що з'являються в мережі. Також важливо, щоб ці системи були інтегровані з іншими засобами безпеки, такими як фаєрволи та системи моніторингу, для досягнення комплексного захисту. У результаті, IDS і IPS, працюючи разом, створюють багатоетапну оборону, яка дозволяє значно підвищити рівень кіберзахисту організацій.

12.6. СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ У МЕРЕЖІ (ACTIVE DIRECTORY, ACL)

Списки контролю доступу (ACL) є важливим компонентом сучасних систем безпеки, оскільки вони забезпечують механізм, за допомогою якого можна контролювати доступ до об'єктів на основі прав, наданих окремим користувачам або групам користувачів. ACL визначає, які операції дозволено виконувати певному суб'єкту (користувачу або групі) над об'єктом, таким як файл чи мережевий ресурс. Кожен запис у ACL зазвичай містить інформацію про суб'єкта і відповідне право, наприклад, дозволити або заборонити видалення файлу.

Системи, що використовують ACL, зазвичай зберігають списки доступу окремо для кожного об'єкта, що дозволяє індивідуально налаштовувати права для різних користувачів. Однак, зростання кількості користувачів може зробити ці списки громіздкими. Для полегшення управління правами доступу часто використовуються групи користувачів або концепція ролей, де права на доступ до об'єктів об'єднуються в ролі, що призначаються користувачам.

Існує два основних типи ACL: файлові та мережеві. Файлові ACL фільтрують доступ до файлів або каталогів на комп'ютерах, визначаючи, які користувачі можуть виконувати певні операції над файлами, такі як читання, запис або виконання. Мережеві ACL працюють на рівні мережі і визначають, який трафік дозволено або заборонено на маршрутизаторах чи комутаторах. Мережеві ACL контролюють доступ до ресурсів мережі, базуючись на IP-адресах джерела та призначення, а також портах.

Файлові ACL

Файлові системи з підтримкою ACL зазвичай використовують ідентифікатор користувача (UID), щоб пов'язати об'єкт з відповідним списком контролю доступу. У операційних системах, таких як Linux та Mac OS X, розширені атрибути файлової системи можуть виконувати роль ACL, де для кожного об'єкта зберігається список прав доступу. У Microsoft Windows для цього використовуються записи керування доступом (ACE), що є частинами ACL. Ці записи визначають права доступу до об'єкта для конкретних користувачів або груп. Файлові системи з підтримкою ACL дозволяють гнучко керувати доступом до ресурсів, забезпечуючи різні рівні прав для кожного користувача чи групи, що значно підвищує безпеку. У системах Linux, наприклад, права доступу можуть бути додатково налаштовані за допомогою команд, що дозволяють додавати або видаляти користувачів і групи зі списку доступу. Вони використовують ACL для точного контролю доступу до файлів, що може включати права на читання, запис, виконання або інші специфічні операції. В операційних системах, таких як Mac OS X, ACL можуть бути застосовані не тільки до файлів, але й до каталогів, забезпечуючи налаштування доступу на рівні структур даних. В Windows ACL здійснюється через інтерфейс безпеки, де адміністратор може вручну змінювати доступ до файлів і папок за допомогою графічного інтерфейсу або командного рядка. Права доступу можуть бути конкретизовані для кожної окремої групи користувачів, визначаючи, чи мають вони право на зміну файлів, перегляд вмісту або їх виконання. Таким чином, підтримка ACL дозволяє знизити ризики несанкціонованого доступу до важливих даних, забезпечуючи високий рівень захисту інформації в організаціях.

Мережеві ACL

Мережеві ACL (Access Control Lists) є важливим інструментом для фільтрації трафіку в мережах та маршрутизаторах, дозволяючи контролювати доступ до ресурсів на основі визначених правил. Вони функціонують на рівні мережеских інтерфейсів, перевіряючи пакети перед тим, як дозволити їм пройти через маршрутизатор чи інший пристрій мережі. Мережеві ACL поділяються на два основні типи: стандартні та розширені.

Стандартні ACL дозволяють фільтрувати трафік лише на основі вихідних IP-адрес, що значно обмежує їх застосування, оскільки не можна врахувати додаткові параметри, такі як порти чи протоколи. Це робить їх ідеальними для простих випадків, коли необхідно лише обмежити доступ з певних IP-адрес. Розширені ACL надають набагато більшу гнучкість, дозволяючи фільтрувати трафік за множиною критеріїв, таких як не тільки IP-адреси, але й порти, протоколи (TCP, UDP), а також інтерфейси маршрутизатора.

Розширені ACL дозволяють більш точно контролювати, який трафік може проходити через мережу, і можуть бути використані для реалізації складних політик безпеки, таких як обмеження доступу до певних сервісів чи ресурсів на основі портів (наприклад, доступ до HTTP або FTP). Це дозволяє адміністраторам мереж значно підвищити рівень захисту мережі та знижувати ризик атак, таких як несанкціонований доступ або DoS-атаки. Мережеві ACL можуть бути застосовані не лише для контролю трафіку між мережами, а й для фільтрації трафіку між внутрішніми сегментами мережі, що дозволяє додатково посилити політики безпеки в організації.

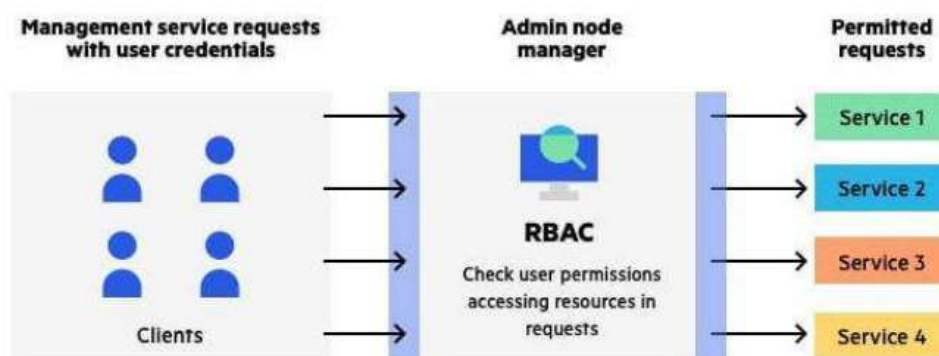


Рис. 12.19. Приклад системи керування доступом
Джерело: [2-4]

Правильне налаштування мережевих ACL є критично важливим для забезпечення ефективної безпеки мережі, оскільки неправильні або надмірно обмежувальні правила можуть призвести до блокування важливого трафіку чи порушення роботи мережі.

Що стосується мережевих ACL, то вони використовуються для фільтрації пакетів в мережах і маршрутизаторах, визначаючи, який трафік може пройти через мережеві інтерфейси. Мережеві ACL поділяються на стандартні та розширені. Стандартні ACL обмежуються лише вихідною IP-адресою, тоді як розширені ACL дозволяють детальніше налаштовувати правила доступу, враховуючи як IP-адреси, так і порти.

Різниця між ACL, ACE, DACL та SACL полягає в їхніх функціях та призначеннях. DACL (дискреційний список контролю доступу) визначає користувачів і групи, яким дозволено або заборонено доступ до об'єкта. SACL (список контролю доступу до системи) використовується для моніторингу доступу та аудиту, реєструючи успішні або невдалі спроби доступу до об'єкта.

Застосування ACL передбачає дотримання кількох важливих найкращих практик, таких як налаштування ACL на всіх інтерфейсах, створення правил від загального до конкретного для кращої продуктивності, а також ретельне документування правил для уникнення непорозумінь. ACL також можуть бути порівняні з іншими методами контролю доступу, такими як RBAC (контроль доступу на основі ролей), який дозволяє централізовано керувати правами доступу через призначення ролей замість конкретних прав для кожного користувача.

Таким чином, списки контролю доступу є потужним інструментом для забезпечення безпеки в інформаційних системах, які дозволяють точно налаштовувати доступ до ресурсів на основі ролей або індивідуальних прав, зберігаючи ефективність і гнучкість.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 12

1. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.
2. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.

3. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

4. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

5. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 99–120.

6. Костюк Ю.В., Владислав Марценюк. «Аналіз ефективності та розгляд сучасних тенденцій в застосуванні принципів двофакторної аутентифікації для забезпечення безпеки в веб-застосунках у сфері комерційних закладів охорони здоров'я»(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 6(34) 2024.

7. Довженко, Н., Мазур, Н., Костюк, Ю., & Рзаєва, С. (2024). Інтеграція іот та штучного інтелекту в інтелектуальні транспортні системи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 430–444

8. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.

9. Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25.

10. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

11. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 390–400.

12. Костюк Ю.В., Єгор Константінов. «Вдосконалені методи безпеки в 4G мережах з метою забезпечення ефективного захисту від атак на передачу даних»(Серія «Педагогіка», Серія «Право», Серія

«Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 6(34) 2024.

13. Костюк Ю.В., Гейдар Гейдаров. Роль токенів та сесійного керування в системах інформаційної безпеки для протидії міжсайтовим атакам. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1216-1231.

14. S. Yevseiev, Models of Socio-Cyber-Physical Systems Security: monograph, PC TECHNOLOGY CENTER (2023).

15. Z. Brzhevska, et al., Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 257–264.

16. Костюк Ю.В., Войткевич А.А. Дослідження технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1017-1032.

17. M. TajDini, V. Sokolov, V. Buriachok, Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio, in: 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 287–296.

18. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.

19. A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

20. O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.

21. Костюк Ю.В., Шапран В.О. Технології виявлення аномальних подій та сигнатур в реальному часі. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1069-1084.

РОЗДІЛ 13

МОНІТОРИНГ ПРОЦЕСІВ ФУНКЦІОНУВАННЯ ІКС



13.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторингу

13.2. Система візуалізації та управління подіями (SIEM)

13.3. Аналіз подій SIEM

13.1. ДЖЕРЕЛА ІНФОРМАЦІЇ ПРО ПОДІЇ ТА ТИПИ ПОДІЙ, ЩО АНАЛІЗУЮТЬСЯ В СИСТЕМАХ МОНІТОРИНГУ

Системи моніторингу інформаційної безпеки використовують різноманітні джерела інформації для виявлення та аналізу подій, що можуть свідчити про загрози або порушення безпеки в інформаційних системах. Одним з основних джерел є журнали подій серверів та робочих станцій, які забезпечують контроль доступу, дотримання політик безпеки та безперервність операцій. Ці журнали записуються як тонкими, так і товстими клієнтами, що дає змогу отримувати важливу інформацію про дії користувачів і систем. Важливу роль у моніторингу також відіграють антивірусні програми, які генерують події, пов'язані з працездатністю програмного забезпечення, оновленнями баз даних, змінами в конфігураціях і політиках безпеки, а також з виявленням шкідливого програмного забезпечення. Вони допомагають швидко ідентифікувати нові типи загроз, зокрема невідомі, завдяки використанню технологій машинного навчання.

Ще одним важливим елементом є засоби антиексплоїт захисту, які виявляють та блокують використання уразливостей у програмному

забезпеченні, що можуть бути експлуатовані атакувальниками. Сучасні системи антиексплойт можуть поєднувати функції з виявленням аномальних дій, що дозволяє знижувати ризики на етапах уразливих або недостатньо оновлених систем. Окрім цього, інструменти, такі як пісочниці (sandboxing), дозволяють ізолювати підозрілі файли та програми у віртуальному середовищі для вивчення їх поведінки, що запобігає потенційному зараженню основної операційної системи. Такі технології дозволяють глибше аналізувати підозрілі файли і виявляти шкідливу активність на ранніх етапах.

З іншого боку, системи запобігання витоку даних (DLP) використовують різноманітні механізми для аналізу і блокування передачі конфіденційної інформації за межі організації. Ці системи можуть автоматично виявляти спроби витоку даних через різні канали, включаючи електронну пошту, соціальні мережі та хмарні сервіси. Вони є важливим інструментом для запобігання інсайдерським витокам або помилкам користувачів, що можуть призвести до порушення безпеки. Крім того, для забезпечення безпеки доступу до інформаційних систем використовуються системи контролю доступу (Access Control, Authentication), які забезпечують правильне використання привілеїв і моніторинг доступу в реальному часі, особливо з впровадженням багатофакторної аутентифікації.

Важливою складовою є системи виявлення і запобігання вторгнень (IDS/IPS), які дозволяють відстежувати мережеву активність і виявляти атаки або порушення безпеки. Ідентифікація аномальних дій в реальному часі дає змогу вчасно реагувати на загрози. Системи IPS здатні не лише виявляти, але й блокувати атаки, що забезпечує високий рівень автоматизації у відповіді на вторгнення. У доповнення до цього, міжмережеві екрани є важливим інструментом захисту на рівні периметра організації, контролюючи трафік та виявляючи несанкціоновані спроби доступу або атаки.

Мережеве активне обладнання застосовується для моніторингу мережевого трафіку і обліку доступу до ресурсів. Вони працюють в реальному часі, дозволяючи оперативно виявляти порушення політик безпеки або несанкціоновані спроби доступу. Системи веб-фільтрації використовують бази даних для визначення шкідливих або підозрілих веб-сайтів, забезпечуючи доступ лише до безпечних ресурсів, що важливо в умовах зростаючого числа фішингових атак та інших загроз через інтернет. Окрім того, сканери уразливостей проводять інвентаризацію активів та програмного забезпечення, виявляючи потенційні уразливості, що можуть бути використані зловмисниками для проникнення в систему.

Системи інвентаризації та управління активами (asset-management) надають організаціям інструменти для моніторингу своїх активів і виявлення нових або невідомих пристроїв і програм, що можуть бути частиною інфраструктури. Вони важливі для забезпечення цілісності й безпеки інфраструктури, оскільки дозволяють виявляти несанкціоновані зміни або додавання нових елементів до системи. В рамках протидії зловмисникам використовуються системи-приманки (honeypots), які є заздалегідь створеними «муляжами» інформаційних систем. Зловмисники, потрапивши в таку пастку, намагаються застосувати свій інструментарій для атаки, а в цей момент їхні дії ретельно реєструються для подальшого аналізу.

Завершує цей список засоби управління портативними пристроями (MDM), які забезпечують безпечне використання мобільних пристроїв співробітниками організації. Вони дозволяють встановлювати правила доступу до корпоративних ресурсів, шифрувати дані та керувати додатками на портативних пристроях, що є важливим для безпеки в умовах широкого використання мобільних пристроїв і віддаленої роботи.

Усі ці інструменти взаємодіють і доповнюють один одного, створюючи багаторівневу систему захисту, що дозволяє забезпечити надійний моніторинг і захист від різноманітних загроз у реальному часі.

13.2. СИСТЕМА ВІЗУАЛІЗАЦІЇ ТА УПРАВЛІННЯ ПОДІЯМИ (SIEM)

Система візуалізації та управління подіями безпеки (SIEM) є важливим інструментом для забезпечення безпеки в організаціях. Вона поєднує в собі функції збору, аналізу та управління подіями безпеки з різних джерел інформації, що дозволяє виявляти, корелювати та реагувати на загрози в реальному часі. SIEM є комплексним рішенням, яке поєднує два основні компоненти: управління інформацією про безпеку (SIM) та управління подіями безпеки (SEM), що забезпечує інтеграцію даних з різних джерел, їх аналіз та швидке виявлення потенційних інцидентів.

Основною метою SIEM-системи є забезпечення можливості моніторингу та аналізу всіх подій, які відбуваються в інформаційній інфраструктурі організації. Це досягається через збір даних з різних джерел, таких як мережеві пристрої, сервери, бази даних та додатки. Зібрані дані потім фільтруються, нормалізуються і зберігаються в єдиній базі, що дозволяє здійснювати їх подальшу кореляцію та аналіз. Один із основних процесів в SIEM-системі — кореляція подій, коли система шукає взаємозв'язки між різними подіями для виявлення складних загроз, які можуть бути невидимими при окремому аналізі.

Важливою функцією є також автоматичне генерування сповіщень про потенційні загрози або інциденти безпеки, що дозволяє спеціалістам оперативного реагувати на них. В SIEM-системах передбачена можливість візуалізації подій у вигляді звітів, графіків і діаграм, що спрощує процес прийняття рішень та подальший аналіз. Крім того, такі системи надають можливість зберігати журнали подій для проведення аудитів і забезпечення відповідності нормативним вимогам, таким як GDPR, HIPAA, PCI DSS.

SIEM-системи мають розподілену архітектуру, що дозволяє масштабувати їх використання в великих організаціях або на кількох об'єктах. Збір даних відбувається за допомогою агентів або безагентних методів, а збереження інформації відбувається в централізованому сховищі, що полегшує доступ до необхідних даних для подальшого аналізу. У поєднанні з аналітичними інструментами, такими як машинне навчання і штучний інтелект, SIEM-системи можуть автоматично виявляти аномалії і прогнозувати загрози, що значно підвищує рівень безпеки.

Незважаючи на численні переваги, SIEM-системи мають і деякі недоліки, серед яких висока вартість впровадження і обслуговування, а також складність інтеграції з існуючою інфраструктурою. Висока кількість подій, які з'являються у великих організаціях, може призводити до навантаження на систему, що вимагає потужних обчислювальних ресурсів. Однак завдяки постійному розвитку технологій, таких як аналіз великих даних, автоматизація процесів та інтеграція з іншими системами безпеки, SIEM-системи стають все більш ефективними у виявленні та реагуванні на інциденти безпеки.

Сучасні тренди у розвитку SIEM включають використання машинного навчання та штучного інтелекту для більш точного виявлення загроз, а також інтеграцію з іншими технологіями безпеки для створення більш комплексних рішень. Ці інновації дозволяють значно зменшити час реагування на інциденти та підвищити рівень захисту організацій від кіберзагроз. Загалом, SIEM є незамінним інструментом для забезпечення безпеки та контролю за інформаційними системами, особливо в умовах постійно зростаючих кіберзагроз.

SIEM (Security Information and Event Management) — це потужна технологія, що об'єднує два ключових компоненти: SIM (Security Information Management) — управління інформацією про безпеку та SEM (Security Event Management) — управління подіями безпеки. SIEM-системи виконують критичну роль у забезпеченні безпеки інформаційних систем завдяки своєчасному аналізу подій безпеки та управлінню ними в реальному часі. Вони дозволяють виявляти та реагувати на загрози до того,

як вони призведуть до серйозних збитків. Зі збільшенням обсягів переданої та обробленої інформації в сучасних підприємствах зростає потреба у таких рішеннях, здатних швидко реагувати на загрози.

Системи SIEM покликані ефективно управляти інформацією про події безпеки в режимі реального часу. Вони забезпечують централізований збір даних з різних джерел, таких як мережеві пристрої, додатки, засоби ідентифікації користувачів, системи керування доступом та інші компоненти безпеки. Ці дані агрегуються, нормалізуються та корелюються для виявлення потенційних загроз і інцидентів безпеки. Результати обробки надаються в зручному для аналізу форматі через єдиний інтерфейс, що дозволяє аналітикам швидко виявляти аномалії та реагувати на інциденти.

Функціональні можливості SIEM-систем охоплюють широкий спектр завдань, спрямованих на забезпечення інформаційної безпеки підприємства. Функціональні можливості SIEM-систем:

▲ Збір та обробка даних

Події безпеки збираються з різних джерел, таких як файлові сервери, міжмережеві екрани, антивірусні програми та інші системи безпеки.

▲ Моніторинг у реальному часі

Системи SIEM надають інструменти для оперативного моніторингу та аналізу подій, що відбуваються в інформаційній інфраструктурі, дозволяючи виявляти загрози безпеки миттєво.

▲ Інцидент-менеджмент

SIEM дозволяють ідентифікувати, класифікувати та пріоритизувати інциденти безпеки, а також зберігати всі дані для подальшого аналізу.

▲ Автоматизація реагування

Системи забезпечують автоматичне виконання дій у відповідь на виявлені загрози, таких як блокування IP-адрес, ізоляція пристроїв чи сповіщення адміністратора.

▲ Забезпечення відповідності регуляторним вимогам

SIEM-системи генерують звіти для аудиту, забезпечуючи відповідність підприємства вимогам стандартів, таких як GDPR, PCI DSS, ISO 27001 тощо.

▲ Нормалізація та класифікація

Події з різних джерел мають різні формати, тому SIEM-система приводить їх до єдиного формату для подальшої обробки.

▲ Кореляція та агрегація

Це процес поєднання подій, що можуть бути схожими за змістом, а також виявлення зв'язків між різними подіями для більш точного аналізу.

▲ Пріоритезація подій

Система визначає, які події є найбільш критичними для безпеки та потребують негайної уваги, застосовуючи заздалегідь визначені правила пріоритетності.

▲ Оповіщення та сповіщення

Коли система виявляє підозрілі події або порушення політик безпеки, вона генерує попередження (тривоги), які можуть бути надіслані через різні канали, зокрема на електронну пошту чи GSM-шлюз.

▲ Візуалізація

Результати аналізу подій можуть бути представлені в графічному вигляді для зручності виявлення аномалій або патернів, що відрізняються від звичної поведінки.

▲ Інтеграція з іншими засобами безпеки

SIEM може інтегруватися з IDS/IPS, антивірусами, системами управління уразливостями та іншими інструментами для створення єдиної екосистеми захисту.

▲ Аналіз поведінки користувачів та об'єктів

Деякі SIEM-системи мають функції UEBA (User and Entity Behavior Analytics), що дозволяє виявляти аномалії в поведінці користувачів або систем.

Аналіз та оцінка загроз в реальному часі є важливим аспектом функціонування SIEM. Завдяки кореляції та нормалізації даних, SIEM-системи здатні виявити потенційні атаки чи порушення безпеки на ранніх етапах, що дозволяє значно знизити ймовірність серйозних інцидентів. Крім того, за допомогою аналізу подій можна прогнозувати майбутні загрози та налаштовувати параметри моніторингу в реальному часі для підвищення ефективності захисту.

Еволюція SIEM-систем

Від першого покоління до сучасних рішень, SIEM-системи значно вдосконалюються. Системи першого покоління здебільшого зосереджувались на нормалізації, фільтрації, кореляції та агрегації подій, у той час як новіші версії включають додаткові можливості для аналізу наслідків інцидентів, прогнозування атак, автоматизованого прийняття рішень та візуалізації результатів. Це дозволяє значно підвищити ефективність виявлення загроз та реагування на них.

Роль автоматизації

В сучасних SIEM-системах автоматизація відіграє важливу роль. Вони можуть самостійно аналізувати великі обсяги даних, генерувати звіти та оповіщення, а також проводити автоматичне коригування параметрів безпеки в залежності від поточного стану системи. Це дозволяє значно

скоротити час на реагування на інциденти та підвищити ефективність захисту.

Інтеграція з іншими системами

Важливою особливістю сучасних SIEM-систем є їх здатність до інтеграції з іншими інструментами безпеки та моніторингу, такими як системи виявлення вторгнень (IDS), засоби виявлення аномалій, системи управління уразливостями, а також з платформами для виконання комп'ютерно-технічних експертиз. Це забезпечує більш комплексний підхід до захисту інформаційних систем.

Застосування SIEM-систем допомагає організаціям підтримувати високий рівень інформаційної безпеки, зменшувати ризики та швидко реагувати на загрози, що виникають. Система має важливе значення для забезпечення відповідності нормативним вимогам та стандартам безпеки, що важливо в умовах сучасного цифрового середовища.

13.3. Аналіз подій SIEM

Аналіз подій у системі візуалізації та управління подіями безпеки (SIEM) є ключовою функцією, яка дозволяє виявляти, корелювати та реагувати на загрози безпеки в реальному часі. Події — це зафіксовані інциденти або дії, що відбуваються в інформаційній інфраструктурі підприємства, і можуть стосуватися різних компонентів системи: мережевих пристроїв, серверів, додатків, баз даних та інших елементів інфраструктури. SIEM-системи забезпечують централізований збір, аналіз і зберігання журналів подій з різних джерел, що дає змогу отримати комплексне уявлення про стан безпеки. Вони використовують механізми кореляції, які дозволяють зіставляти події з різних джерел для виявлення складних атак або підозрілої активності. Однією з ключових переваг SIEM є можливість автоматизації процесів реагування на інциденти за допомогою попередньо визначених сценаріїв або правил. Завдяки цьому можна мінімізувати час реагування на загрози і зменшити потенційний вплив атак. SIEM також дозволяє здійснювати моніторинг в режимі реального часу, що особливо важливо для виявлення та запобігання атакам, які розвиваються швидко. Окрім цього, система надає засоби для проведення ретроспективного аналізу подій, що допомагає в розслідуванні інцидентів безпеки та вдосконаленні політик захисту. Інтеграція з іншими засобами кіберзахисту, такими як IDS/IPS або системи управління уразливостями, робить SIEM важливим елементом загальної архітектури безпеки підприємства.

Процес аналізу подій у SIEM включає кілька етапів, на кожному з яких відбувається обробка даних для виявлення потенційних загроз і аномалій:

Збір і нормалізація даних

Першим етапом є збір даних з різних джерел — журналів подій, системних повідомлень, мережевого трафіку, застосунків тощо. Ці дані можуть бути зібрані за допомогою агентів або безагентних методів. Після цього вони нормалізуються, тобто приводяться до єдиного формату для подальшої обробки. Нормалізація дозволяє стандартизувати різні формати даних, що надходять із різних джерел.

Кореляція подій

На основі нормалізованих даних SIEM-система здійснює кореляцію подій. Це процес пошуку зв'язків між різними подіями для виявлення складних загроз, які можуть бути непомітними при окремому розгляді кожної події. Наприклад, кілька незначних інцидентів, таких як несанкціоновані спроби входу або нехарактерна активність на сервері, можуть вказувати на спробу кібератаки.

Аналіз аномалій

Аномалії в поведінці користувачів або систем можуть свідчити про порушення безпеки. SIEM-система використовує алгоритми аналізу аномалій для виявлення відхилень від звичайної поведінки. Це може включати незвичайні спроби доступу до конфіденційних даних, спроби доступу з незвичних локацій чи аномальні зміни в системах безпеки.

Інтелектуальний аналіз

Сучасні SIEM-системи інтегрують алгоритми машинного навчання та штучного інтелекту, що дозволяє автоматично виявляти складні загрози, прогнози та відхилення. Це дозволяє значно підвищити точність аналізу та зменшити кількість хибних сповіщень.

Візуалізація подій

Для зручності операційного аналізу SIEM-системи надають можливість візуалізації подій у вигляді графіків, таблиць і діаграм. Це дозволяє операційним аналітикам швидко оцінити ситуацію, визначити критичні загрози та прийняти необхідні заходи. Візуалізація також допомагає виявляти тренди та патерни в загрозах, що дозволяє прогнозувати можливі інциденти в майбутньому.

Сповіщення та реагування

Коли система виявляє загрозу або аномалію, вона генерує сповіщення, що дає змогу спеціалістам з безпеки оперативно реагувати на інциденти. Це може включати автоматичну блокування шкідливої активності, запуск

відповідних сценаріїв реагування або направлення повідомлень до адміністратора для прийняття рішення.

Зберігання і аудит

Зберігання журналів подій є важливою складовою частиною аналізу в SIEM. Це не тільки дозволяє забезпечити належний аудит діяльності, але й забезпечує можливість подальшого дослідження інцидентів. Журнали подій можуть бути збережені на визначений період для подальшого аналізу, перевірки відповідності стандартам безпеки та забезпечення необхідної документації для зовнішніх перевірок.

Аналіз причин

Після того, як інцидент буде виявлено, SIEM-система дозволяє проводити глибокий аналіз причин події. Це дає змогу зрозуміти, чи була загроза результатом помилки користувача, уразливості в системі, чи це була спроба кібератаки. Оцінка таких причин дозволяє коригувати політики безпеки та посилювати заходи захисту.

Аналіз подій в SIEM має вирішальне значення для забезпечення безпеки організації, оскільки дозволяє швидко виявляти загрози, знижувати ризики та підвищувати ефективність реагування на інциденти. Завдяки інноваційним технологіям, таким як машинне навчання та штучний інтелект, SIEM-системи стають все більш точними та здатними до самонавчання, що дозволяє адаптуватися до нових типів загроз.

Перспективи розвитку SIEM-систем

Перспективи розвитку SIEM-систем (системи управління інформаційними подіями та їх обробкою) охоплюють кілька важливих напрямків, що сприяють покращенню їх здатності виявляти та реагувати на кіберзагрози. Одним із ключових напрямків є автоматизація реагування на інциденти. Враховуючи, що більшість фахівців з інформаційної безпеки витрачають значний час на роботу з помилковими спрацьовуваннями та налаштування правил кореляції, автоматизація цих процесів здатна значно зменшити час реагування та підвищити ефективність системи безпеки. Це дозволить швидше виявляти загрози і приймати необхідні заходи для їх нейтралізації.

Другим важливим напрямком є інтеграція SIEM-систем з іншими технологіями, зокрема аналізом трафіку (NTA), кінцевих точок (EDR) та моніторингом користувачів і сутностей (UEBA). Розширення можливостей SIEM за рахунок таких технологій дозволяє значно розширити спектр виявлення загроз. У найближчі роки аналіз мережевого трафіку та подій на кінцевих точках стане необхідним для забезпечення повного функціоналу

SIEM-систем, що забезпечить більш точне та детальне виявлення аномалій і можливих атак.

UEBA (User and Entity Behavior Analytics) — ще одна інноваційна технологія, яка допомагає побудувати поведінкові моделі користувачів та сутностей. Це дозволяє виявляти аномальну поведінку, що є критично важливим для ідентифікації складних атак, таких як внутрішні загрози чи використання зловмисних користувачів для компрометації системи. Технології, які здатні автоматично виявляти такі аномалії, суттєво підвищують ефективність моніторингу і запобігання інцидентам.

Окрему увагу заслуговує інтеграція SIEM з хмарними платформами, такими як AWS, Google Cloud Platform і Microsoft Azure. Враховуючи тренд на перехід підприємств до використання хмарних технологій, можливість збору даних з хмарних джерел і надання SIEM як послуги (SIEM as a Service) стає дедалі важливішою. Це дозволяє організаціям гнучко масштабувати систему безпеки, спрощуючи її розгортання і обслуговування.

Завершальним напрямком є інтеграція з платформами SOAR (Security Orchestration, Automation, and Response), які автоматизують реагування на інциденти. Інтеграція SOAR з SIEM-системами дозволяє швидше виявляти і реагувати на загрози, забезпечуючи більш ефективне управління інцидентами та спрощуючи операції реагування в реальному часі. Це сприяє зниженню кількості помилок, пов'язаних із людським фактором, і підвищує оперативність у виявленні та нейтралізації атак.

Всі ці напрямки розвитку сприяють тому, що SIEM-системи стають потужнішими інструментами для виявлення кіберзагроз і більш ефективного реагування на них, що підвищує загальний рівень безпеки підприємств.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 13

1. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

2. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.

3. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.

4. Лахно В. А., Гусєв Б. С., Блозва А. І. Касаткін Д. Ю., Осипова Т. Ю. (2020) Кластеризація ознак мережових атак в задачах аналізу захищеності інформації. *Кібербезпека: освіта, наука, техніка*. № 1(9). С. 45–58.

5. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. *Information Technology*, 4(6), 14-33.

6. Технологія VPN може загрожувати кібербезпеці. URL: <https://detector.media/infospace/article/126505/2017-05-31-tekhnologiya-vpnmozhe-zagrozhuvati-kiberbezpetsi-inau>

7. Спасітелева, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(21), 193–210.

8. Костюк Ю.В., Єгор Константинов. «Вдосконалені методи безпеки в 4G мережах з метою забезпечення ефективного захисту від атак на передачу даних»(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 6(34) 2024.

9. V. Sokolov, P. Skladannyi, A. Platonenko, Video Channel Suppression Method of Unmanned Aerial Vehicles, in: *IEEE 41st International Conference on Electronics and Nanotechnology* (2022) 473–477.

10. Kryvoruchko O., Kostiuk Y., Desiatko A. Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods// *Ukrainian Scientific Journal of Information Security*, 2024, vol. 30, issue 1, pp. 140-149.

11. Костюк Ю.В., Владислав Марценюк. «Аналіз ефективності та розгляд сучасних тенденцій в застосуванні принципів двофакторної аутентифікації для забезпечення безпеки в веб-застосунках у сфері комерційних закладів охорони здоров'я»(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 6(34) 2024.

12. Марценюк, М., Козачок, В., Богданов, О., Іосіфов, Є., & Брже夫ська, З. (2023). АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ Дезінформації в соціальних мережах за допомогою машинного навчання. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2(22), 148–155.

13. Костюк Ю.В., Андрій Голинський. Стратегії інтегрованого захисту бездротових сенсорних мереж. *«Наука і техніка сьогодні»* (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-

математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1232-1247.

14. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 338–347.

15. Костюк Ю.В., Гейдар Гейдаров. Роль токенів та сесійного керування в системах інформаційної безпеки для протидії міжсайтовим атакам. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1216-1231.

16. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(24), 185–195.

17. Костюк Ю.В., Войткевич А.А. Дослідження технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1017-1032.

18. Крючкова, Л., & Ємельяненко, М. (2024). Захист web-ресурсу intranet від зовнішніх і внутрішніх загроз. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 318–327.

19. V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526.

20. A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

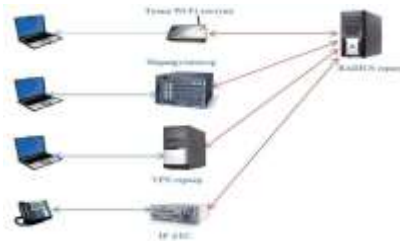
21. Z. Brzhevska, et al., Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 257–264.

22. R. Marusenko, V. Sokolov, V. Buriachok, Experimental Evaluation of Phishing Attack on High School Students, Advances in Computer Science for Engineering and Education III, vol. 1247 (2020) 668–680.

23. V. Buhas, et al., Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188, no. 2 (2021) 273–281.

РОЗДІЛ 14

МЕХАНІЗМИ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ



- 14.1. Віртуальні приватні мережі (VPN)**
- 14.2. Протоколи аутентифікації RADIUS**
- 14.3. Протоколи SSL/TLS**
- 14.4. Захищений протокол віддаленого доступу SSH**
- 14.5. PGP (Pretty Good Privacy)**

14.1. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ (VPN)

Віртуальні приватні мережі (VPN) забезпечують безпечне передавання даних через відкриті або небезпечні мережі, такі як Інтернет, створюючи зашифрований тунель між пристроями користувачів і мережею або сервером. Такий підхід гарантує конфіденційність, цілісність і доступність інформації. Основна перевага VPN полягає в забезпеченні конфіденційності завдяки шифруванню даних, яке захищає інформацію від перехоплення або несанкціонованого доступу з боку сторонніх осіб.

Ключовою складовою роботи VPN є автентифікація, яка перевіряє достовірність користувачів і пристроїв перед підключенням до мережі, тим самим запобігаючи несанкціонованому доступу. Віртуальний тунель, що створюється VPN, забезпечує безпечне з'єднання через Інтернет або іншу небезпечну мережу, функціонуючи як приватний канал для обміну даними. Для захисту переданої інформації VPN використовує сучасні протоколи, такі як IPSec, SSL/TLS, або OpenVPN, які гарантують, що дані залишатимуться недоступними для злоумисників навіть у разі перехоплення трафіку. VPN є невід'ємною частиною сучасної

кібербезпеки, забезпечуючи захист даних і конфіденційність користувачів під час роботи в мережі.

Таким чином, VPN забезпечує комплексний захист інформації, дозволяючи користувачам безпечно працювати в мережі та отримувати доступ до ресурсів, навіть якщо вони знаходяться у вразливих або небезпечних мережах.

Віртуальна приватна мережа (VPN) — це технологія, яка дозволяє створювати захищені з'єднання через інші, зазвичай ненадійні, мережі, наприклад Інтернет. VPN використовує криптографічні методи, такі як шифрування, аутентифікацію та інфраструктуру відкритих ключів, для забезпечення довіри до мережі, незалежно від рівня довіри до базових мереж. Це забезпечує захищену передачу даних навіть у публічних чи незахищених мережах. В залежності від застосовуваних протоколів VPN можна класифікувати за трьома основними типами з'єднань: вузол-вузол, вузол-мережа та мережа-мережа.

VPN зазвичай реалізується на мережевому рівні, оскільки використання криптографії дозволяє зберегти транспортування даних без змін для таких протоколів, як TCP та UDP. Найпоширенішими варіантами VPN є PPTP, інкапсульований протокол PPP поверх IP або Ethernet, який використовує, наприклад, протокол PPPoE. VPN часто застосовується для створення приватних мереж, а також для надання доступу до Інтернету через провайдерів останньої милі.

VPN складається з двох основних компонентів: внутрішньої (підконтрольної) мережі та зовнішньої мережі, зазвичай Інтернету, через який проходить зашифроване з'єднання. Підключення віддаленого користувача до VPN зазвичай здійснюється через сервер доступу, який знаходиться як в межах внутрішньої, так і зовнішньої мережі. Після аутентифікації користувач отримує доступ до ресурсів мережі через процес авторизації. Це дозволяє створити захищену мережу навіть через публічні канали зв'язку.

VPN можна класифікувати за кількома параметрами. По-перше, за рівнем захищеності використовуваного середовища. Захищені VPN, такі як IPSec, застосовуються для створення надійних захищених мереж поверх менш надійних, наприклад, Інтернету. Зростаюча популярність VPN-технологій сприяла розвитку VPN-з'єднань на маршрутизаторах, що забезпечують шифрування всього трафіку пристроїв у мережі. Другим типом є довірчі VPN, коли середовище, яке передає трафік, вважається надійним, і забезпечення безпеки зводиться до створення віртуальних підмереж.

VPN забезпечує конфіденційність, цілісність та автентичність даних, що передаються, шляхом їх шифрування та використання механізмів аутентифікації, дозволяючи безпечно обмінюватися даними між віддаленими користувачами або мережами. VPN дозволяє створювати зашифровані канали зв'язку, що важливо для захисту від перехоплення даних або інших типів атак, які можуть виникати при роботі в публічних або ненадійних мережах.

Основні функції VPN включають:

Шифрування даних — усі дані, що передаються через VPN, шифруються, що забезпечує їх конфіденційність та запобігає їх перегляду або змінам під час передачі.

Анонімність та захист від відстеження — VPN приховує реальну IP-адресу користувача, замінюючи її адресою VPN-сервера, що дозволяє обходити географічні обмеження або обмеження доступу.

Захист від перехоплення — завдяки шифруванню переданих даних, VPN захищає від можливості їх перехоплення злоумисниками під час передачі через публічні мережі.

Аутентифікація — VPN використовує різноманітні методи аутентифікації для підтвердження ідентичності користувачів або пристроїв, що забезпечує додатковий рівень безпеки.

Типи VPN:

- ▲ **Віддалений доступ (Remote Access) VPN** — цей тип VPN дозволяє віддаленим користувачам підключатися до корпоративної мережі через Інтернет. Зазвичай використовується для віддаленої роботи, де співробітники можуть безпечно підключатися до внутрішніх ресурсів компанії.
- ▲ **Міжмережовий VPN (Site-to-Site VPN)** — використовується для з'єднання двох або більше мереж через Інтернет. Цей тип VPN підходить для з'єднання філій компанії або віддалених офісів з центральною мережею, забезпечуючи безпечну передачу даних між ними.
- ▲ **Intranet VPN** — це VPN, що з'єднує різні підсистеми або компоненти однієї організації для створення єдиного віртуального простору, де забезпечується конфіденційність та безпека.
- ▲ **Extranet VPN** — створюється для забезпечення доступу зовнішніх користувачів або партнерів до частини ресурсів компанії, зокрема, до певних внутрішніх систем або даних.
- ▲ **VPN для мобільних пристроїв** - пропонує безпечне підключення для смартфонів і планшетів.

Протоколи VPN:

1. **PPTP (Point-to-Point Tunneling Protocol)** — один із найстаріших і найпростих протоколів, що використовується для VPN-з'єднань. Хоча він забезпечує базовий рівень шифрування, його безпека застаріла і не рекомендується для використання в сучасних умовах.

2. **L2TP (Layer 2 Tunneling Protocol)** — зазвичай використовують разом із IPsec для забезпечення шифрування і безпеки з'єднання. Забезпечує більш високу безпеку в порівнянні з PPTP.

3. **OpenVPN** — один з найбільш безпечних і популярних протоколів з відкритим кодом. Він використовує SSL/TLS для шифрування і підтримує велику кількість методів аутентифікації.

4. **IPsec (Internet Protocol Security)** — часто використовується для забезпечення безпеки з'єднань через Інтернет. Використовує методи шифрування та аутентифікації для захисту трафіку на рівні мережі.

5. **IKEv2 (Internet Key Exchange version 2)** — сучасний протокол для встановлення та підтримки VPN-з'єднань, відомий своєю стабільністю, швидкістю та здатністю автоматично відновлювати з'єднання після розриву.

Уразливості VPN-мереж включають такі загрози, як витік IP-адрес через WebRTC, що дозволяє зловмисникам дізнатися реальну IP-адресу користувача навіть при використанні VPN. Ще однією загрозою є атака дактилоскопії трафіку, коли зловмисник може визначити, який сайт відвідується користувачем, спостерігаючи за зашифрованим трафіком.

До найбільш відомих реалізацій VPN відносяться такі протоколи, як IPsec, PPTP, PPPoE, L2TP, OpenVPN та інші. OpenVPN, зокрема, є безкоштовною реалізацією VPN з відкритим вихідним кодом, що дозволяє створювати зашифровані канали зв'язку між клієнтами і серверами. OpenVPN використовує SSL/TLS для забезпечення безпеки і підтримує кілька методів аутентифікації, таких як сертифікати або паролі.

VPN також класифікують за призначенням: Intranet VPN для об'єднання філій компанії, Remote-access VPN для підключення віддалених користувачів, Extranet VPN для доступу зовнішніх користувачів до певних ресурсів, а також Internet VPN, який дозволяє постачальникам інтернет-послуг забезпечувати доступ до Інтернету через спільні фізичні канали. Кожен з цих типів VPN має свої особливості в забезпеченні безпеки і налаштування з'єднань.

Переваги VPN:

- **Безпека** — забезпечує захист даних, що передаються, за допомогою шифрування.

- **Конфіденційність** — дозволяє приховувати реальну IP-адресу користувача.
- **Доступ до обмежених ресурсів** — дозволяє обходити географічні обмеження та цензуру в Інтернеті.
- **Захист в публічних мережах** — VPN дозволяє безпечно працювати з Інтернетом у публічних мережах, таких як Wi-Fi в кафе або аеропортах.

Недоліки VPN:

- **Зниження швидкості** — шифрування та маршрутизація трафіку через сервер VPN можуть дещо знизити швидкість з'єднання.
- **Складність налаштування** — для налаштування деяких типів VPN може знадобитися технічний досвід.
- **Залежність від постачальника VPN** — надійність і безпека VPN залежить від постачальника послуг.

Віртуальні приватні мережі є важливим інструментом для забезпечення безпеки при роботі в Інтернеті, особливо в умовах віддаленої роботи або підключення до публічних мереж. Вони надають користувачам можливість захищати свої дані, приховувати особисту інформацію та забезпечувати безпечний доступ до корпоративних ресурсів.

14.2. ПРОТОКОЛИ АУТЕНТИФІКАЦІЇ RADIUS

RADIUS (Remote Authentication Dial-In User Service) — це протокол аутентифікації, авторизації та обліку (AAA), що використовується для централізованого управління доступом до мережевих ресурсів. Цей протокол є критично важливим для організацій, оскільки дозволяє ефективно управляти доступом користувачів до таких ресурсів, як VPN, Wi-Fi та інших мережевих сервісів.

Протокол працює таким чином, що кожен запит на доступ до мережі передається від клієнта, наприклад, точки доступу чи маршрутизатора, до серверу RADIUS для перевірки аутентифікації.

Сервер RADIUS проводить аутентифікацію користувача, визначає його права доступу та реєструє інформацію про використання ресурсів.

Основними функціями RADIUS є аутентифікація, авторизація та облік. Після отримання запиту на аутентифікацію сервер перевіряє, чи є користувач уповноваженим, і у разі позитивного результату, надає йому доступ до відповідних мережевих ресурсів. Після авторизації сервер також може вести облік використаних ресурсів, що дозволяє проводити моніторинг та контроль за використанням мережі. RADIUS підтримує централізоване управління доступом, що значно спрощує адміністрування

великих мереж. Він також забезпечує високий рівень безпеки завдяки використанню шифрування для захисту даних автентифікації. Крім того, система дозволяє інтеграцію з іншими протоколами та сервісами, що робить її універсальним рішенням для управління доступом у сучасних інформаційних системах.



Рис. 14.1. Аутентифікація та авторизація через RADIUS-сервер
Джерело: [2-4]

Протокол RADIUS підтримує різні методи аутентифікації, серед яких є PAP (Password Authentication Protocol), який є простим, але незахищеним, оскільки передає дані в незашифрованому вигляді, і CHAP (Challenge Handshake Authentication Protocol), що є більш безпечним завдяки використанню хешування паролів.

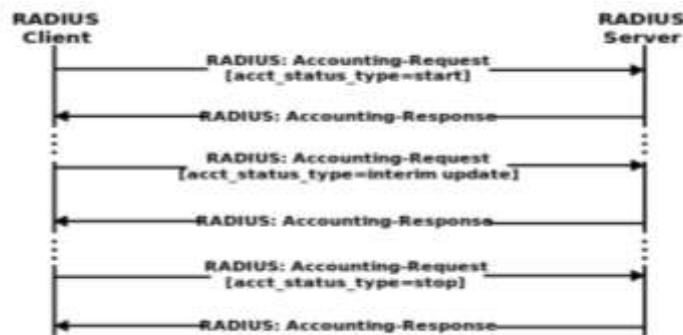


Рис. 14.2. Онлайн облік через RADIUS-сервер
Джерело: [2-4]

Крім того, протокол підтримує розширення, такі як EAP (Extensible Authentication Protocol), що дозволяє застосовувати більш складні методи аутентифікації, включаючи сертифікати та смарт-карти.

Протоколи та механізми аутентифікації в RADIUS:

RADIUS підтримує різні методи аутентифікації для забезпечення більш високого рівня безпеки:

1. **PAP (Password Authentication Protocol)** — це найпростіший метод аутентифікації, при якому ім'я користувача і пароль передаються в текстовому вигляді. Однак PAP є незахищеним, оскільки пароль передається без шифрування.

2. **CHAP (Challenge Handshake Authentication Protocol)** — цей протокол є більш безпечним, оскільки передача пароля здійснюється у вигляді захищеного хешу, що значно ускладнює перехоплення даних.

3. **MS-CHAP (Microsoft CHAP)** — розширення CHAP, використовуване в системах, що базуються на Microsoft, забезпечує підвищену безпеку порівняно з простим PAP.

4. **EAP (Extensible Authentication Protocol)** — це набір методів аутентифікації, який дозволяє використовувати різні протоколи для аутентифікації, такі як EAP-TLS (яке використовує сертифікати для аутентифікації), EAP-TTLS (який підтримує шифрування на всіх етапах аутентифікації) та інші.

Протокол RADIUS (Remote Authentication Dial-In User Service) широко використовується для забезпечення аутентифікації, авторизації та обліку (AAA) в системах управління доступом, зокрема в телекомунікаційних та ІТ-мережах. Цей протокол є основним елементом для підтримки систем тарифікації в мережах, де користувачі або абоненти мають доступ до різних ресурсів, таких як інтернет, VPN, Wi-Fi, чи IP-телефонія. RADIUS дозволяє не лише автентифікувати користувачів, але й забезпечує авторизацію їх доступу до ресурсів, а також веде облік використаних послуг та ресурсів, таких як трафік.

Основні функції протоколу RADIUS включають:

- Authentication (Аутентифікація) - перевірка ідентифікаційних даних користувача, таких як ім'я користувача та пароль. Цей процес дозволяє перевірити справжність запиту доступу.
- Authorization (Авторизація) - визначення прав доступу користувача до різних мережевих ресурсів після успішної аутентифікації.
- Accounting (Облік) - моніторинг використаних ресурсів користувачем, таких як обсяг переданого або прийнятого трафіку, час сесії тощо.

Протокол був розроблений в 1990-х роках компанією Livingston Enterprises для використання в їх серверах доступу до мережі інтернет (Network Access Servers, NAS). З того часу він став основним стандартом для багатьох типів доступу до мереж, включаючи VPN, Wi-Fi, DSL і Ethernet. Протокол RADIUS дозволяє інтегрувати різні системи для управління доступом та обліку, що робить його універсальним інструментом для адміністрування великих та складних мереж.

Незважаючи на свою популярність, протокол RADIUS має обмеження, зокрема щодо безпеки (наприклад, використання простих методів шифрування паролів) і не підтримує деякі сучасні вимоги до обробки великих обсягів даних. Для подолання цих обмежень було розроблено новий протокол DIAMETER, який має більшу гнучкість та більш складні механізми безпеки. Проте, RADIUS залишається широко використовуваним через свою відкритість, простоту налаштування та підтримку старих систем.

Сучасне використання RADIUS передбачає інтеграцію з системами управління доступом, білінговими системами, а також системами моніторингу та звітності. Протокол RADIUS використовує UDP (User Datagram Protocol) для обміну пакетами, що забезпечує високу швидкість обробки запитів, але також може бути вразливим до атак, таких як перехоплення трафіку або атаки на сервери.

Механізми аутентифікації в RADIUS

RADIUS забезпечує надійні механізми аутентифікації, які дозволяють підтверджувати особу користувачів, що намагаються отримати доступ до мережесих ресурсів. Одним із базових методів є використання паролів, зокрема протоколів PAP (Password Authentication Protocol) і CHAP (Challenge-Handshake Authentication Protocol). PAP передає паролі у відкритому вигляді, що робить його менш безпечним, тоді як CHAP використовує хешування, забезпечуючи захист даних під час передачі. Більш сучасним підходом є автентифікація на основі цифрових сертифікатів, яка гарантує високий рівень безпеки, особливо у корпоративних мережах.

Для підвищення рівня захисту використовуються одноразові паролі (OTP), які генеруються спеціальними пристроями або додатками. Це дозволяє мінімізувати ризик доступу зловмисників навіть у разі компрометації основного паролю. Розширена автентифікація (EAP) є ще одним важливим механізмом, що підтримує різні методи, такі як TLS (Transport Layer Security) та PEAP (Protected EAP), які дозволяють використовувати як паролі, так і сертифікати.

Додатково застосовується двофакторна автентифікація (2FA), яка поєднує два різні фактори перевірки, наприклад, пароль та одноразовий код. Ще одним рівнем захисту є MAC-автентифікація, коли доступ до мережі обмежується тільки для пристроїв із відомими MAC-адресами. Усі ці механізми в сукупності забезпечують гнучкість і високий рівень безпеки, дозволяючи підприємствам адаптувати систему RADIUS до своїх потреб і захищати критичні дані від несанкціонованого доступу.

До основних переваг протоколу RADIUS можна віднести:

- Відкритість і підтримка нових функцій без порушення сумісності з застарілими системами.
- Висока швидкість обробки запитів завдяки використанню UDP.
- Можливість функціонувати в кластерних архітектурах для забезпечення високої доступності та відмовостійкості.

Популярність протоколу також підтримується великою кількістю вільно розповсюджуваних серверів RADIUS, які підтримують різні бази даних для зберігання облікових записів користувачів, а також інтерфейси для інтеграції з іншими системами моніторингу та адміністрування, такими як SNMP.

Протокол RADIUS також підтримує різні механізми аутентифікації, такі як PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MD5 та EAP (Extensible Authentication Protocol), що дозволяють налаштовувати різні рівні безпеки в залежності від потреб організації. Протокол EAP, зокрема, дозволяє інтегрувати різні методи аутентифікації, включаючи підтримку карток доступу та одноразових паролів.

В результаті, RADIUS залишається ефективним і надійним інструментом для забезпечення безпеки та управління доступом до мережевих ресурсів, а його постійне вдосконалення та інтеграція з іншими технологіями робить його важливим елементом сучасних інформаційних систем.

14.3. Протоколи SSL/TLS

Протоколи SSL (Secure Sockets Layer) та TLS (Transport Layer Security) забезпечують захищений обмін даними між клієнтами та серверами через Інтернет. Вони є фундаментальними стандартами для забезпечення конфіденційності, цілісності та автентичності під час передавання інформації, наприклад, у веб-браузерах, електронній пошті чи інших мережевих додатках. SSL був першим широко поширеним протоколом, але з часом його замінив більш безпечний і сучасний TLS.

Основний принцип роботи SSL/TLS полягає у використанні криптографії з симетричними та асиметричними ключами. Спочатку під час встановлення з'єднання відбувається так званий «рукошестискання» (handshake), у ході якого клієнт і сервер обмінюються сертифікатами та узгоджують алгоритми шифрування. Після завершення рукошестискання

встановлюється зашифроване з'єднання, у якому використовується симетричне шифрування для швидкості передавання даних.

SSL/TLS також забезпечують цілісність даних за допомогою механізмів хешування, таких як SHA (Secure Hash Algorithm). Це гарантує, що дані не були змінені під час передавання. Для автентифікації використовується інфраструктура відкритих ключів (PKI), яка включає цифрові сертифікати, що підтверджують достовірність серверів або клієнтів.

Протокол TLS має кілька версій: TLS 1.0, TLS 1.1, TLS 1.2 і TLS 1.3, з яких остання є найсучаснішою і найбезпечнішою. Вона усуває деякі застарілі алгоритми, прискорює встановлення з'єднання та підвищує загальну ефективність. SSL, зокрема його версії SSL 2.0 і SSL 3.0, визнано застарілими через вразливості, такі як POODLE.

Протоколи SSL/TLS широко застосовуються в HTTPS (HyperText Transfer Protocol Secure), що є стандартом для захищених веб-з'єднань. Їх використання є ключовим для захисту персональних даних, фінансової інформації та інших конфіденційних даних від перехоплення чи атак, таких як атаки «людина посередині» (MITM). Таким чином, SSL/TLS залишаються основними елементами сучасної кібербезпеки.

Історія та версії SSL і TLS

1. SSL 1.0 — ця версія не була публічно випущена.
2. SSL 2.0 — була випущена в 1995 році, але мала численні уразливості, що призвели до розробки SSL 3.0.
3. SSL 3.0 — випущена в 1996 році, стала основою для подальших версій протоколу TLS.
4. TLS 1.0 — визначений у RFC 2246 в 1999 році, став наступником SSL 3.0.
5. TLS 1.1 — випущений в 2006 році, включав захист від атак на блокові шифри.
6. TLS 1.2 — визначений у RFC 5246 у 2008 році, став стабільною версією протоколу.
7. TLS 1.3 — офіційно прийнятий у 2018 році за стандартом RFC 8446, був розроблений для покращення швидкості та безпеки.

Основні властивості TLS/SSL:

❖ Безпека - використовує симетричне шифрування для захисту даних від несанкціонованого доступу.

❖ Аутентифікація - дозволяє перевірити особистість учасників з'єднання за допомогою асиметричного шифрування.

❖ Цілісність - кожне повідомлення містить код аутентифікації (MAC), що дозволяє перевірити, чи не було змінено або втрачено дані під час передачі.

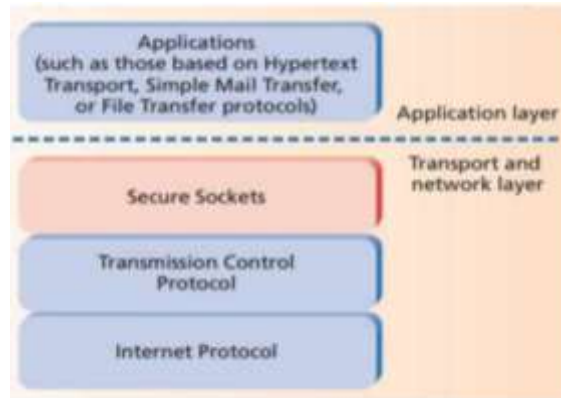


Рис. 14.3. Опис протоколу SSL

Джерело: [2-4]

Протоколи SSL:

SSL реалізується через два основних шари:

- Шар підтвердження підключення (Handshake Protocol) — визначає параметри з'єднання та здійснює аутентифікацію.
- Шар протоколу запису (Record Layer) — забезпечує шифрування даних і контроль цілісності через MAC.

Як працює SSL:

1. Фаза рукоштовання - клієнт і сервер обмінюються повідомленнями для вибору алгоритмів шифрування та встановлення спільного секретного ключа.
2. Передача даних - після підтвердження ключа дані шифруються і передаються з використанням симетричного шифрування. При цьому також перевіряється цілісність і автентичність даних.

Цифрові сертифікати

Цифрові сертифікати — це електронні документи, які використовуються для підтвердження автентичності особи або організації в цифровому середовищі. Вони надають інформацію про власника сертифіката, включаючи його публічний ключ, а також дані про організацію, що видала сертифікат, і період його дії. Сертифікати видаються центрами сертифікації (CA), які є довіреними організаціями, що забезпечують правдивість інформації про власника сертифіката. Завдяки цифровим сертифікатам можна здійснювати безпечну комунікацію,

оскільки вони дозволяють підтвердити особу відправника і забезпечити захист переданої інформації через шифрування.

Цифровий сертифікат часто використовуються в протоколах SSL/TLS для забезпечення захищених з'єднань в Інтернеті, таких як HTTPS, де сервери та клієнти використовують сертифікати для взаємної аутентифікації та шифрування трафіку. Важливими компонентами сертифікатів є їх публічний та приватний ключі, які дозволяють здійснювати криптографічні операції, такі як підписання повідомлень і перевірка їх цілісності.

Для аутентифікації з'єднання SSL використовує цифрові сертифікати, які підтверджуються центром сертифікації (CA). Сертифікат містить публічний ключ сервера, і клієнт використовує його для перевірки автентичності сервера. Цифрові сертифікати також включають інформацію про власника сертифіката, термін дії та ідентифікаційний номер сертифікації, що допомагає запобігти фальсифікації. При отриманні сертифіката клієнт перевіряє його справжність через центр сертифікації, що забезпечує верифікацію і гарантує, що з'єднання не було перехоплене. Якщо сертифікат є дійсним, встановлюється зашифроване з'єднання між сервером і клієнтом, що забезпечує конфіденційність переданих даних. В разі використання SSL/TLS для аутентифікації клієнтів, сервер може вимагати надання клієнтського сертифіката для двосторонньої аутентифікації.

Способи отримання сертифікатів:

- Від центру сертифікації (CA).
- Самопідписаний сертифікат, коли сертифікат видається самим користувачем.
- "Порожній" сертифікат, який не містить перевірених даних.

SSL та TLS дозволяють забезпечити захист даних на різних етапах передачі, тому вони є основними протоколами для забезпечення безпеки в Інтернеті. Ці протоколи забезпечують шифрування даних, аутентифікацію серверів і клієнтів, а також цілісність переданої інформації, що робить їх важливими для захисту онлайн-транзакцій та комунікацій. TLS є оновленою та більш безпечною версією SSL, і його використання рекомендується для забезпечення найвищого рівня захисту. Вони застосовуються не лише для захисту веб-трафіку (HTTPS), але й для інших протоколів, таких як FTP, SMTP та IMAP, що забезпечує комплексний захист на рівні всіх мережевих комунікацій. Протоколи SSL/TLS використовують асиметричне та симетричне шифрування для забезпечення конфіденційності передачі даних між клієнтом і сервером. Під час встановлення з'єднання відбувається процес рукоостискання (handshake),

під час якого узгоджуються параметри шифрування та аутентифікація сторін. Цей процес гарантує, що передані дані не можуть бути перехоплені або змінені злоумисниками. Крім того, SSL/TLS підтримує використання сертифікатів безпеки, які підтверджують автентичність серверів і запобігають фішинговим атакам.

Хешування

Хеш-значення є ідентифікатором повідомлення, його розмір менший за розмір оригінального повідомлення. Найвідомішими хеш-алгоритмами є MD5 (Message Digest 5), який створює 128-бітове хеш-значення, SHA-1 (Standard Hash Algorithm), що створює 160-бітове хеш-значення, SHA-2 та SHA-3. Результат роботи алгоритму хешування – значення, яке використовується для перевірки цілісності передачі даних. Хеш-значення є унікальним для кожного набору даних і навіть невелика зміна в оригінальному повідомленні призводить до значних змін у хеш-значенні. Це робить хешування ефективним інструментом для виявлення несанкціонованих змін в даних або під час передачі. Для посилення безпеки в криптографічних протоколах використовуються сучасні алгоритми хешування, такі як SHA-256 або SHA-512, що забезпечують вищий рівень захисту завдяки більшим розмірам хеш-значень. Вони застосовуються в таких сферах, як цифрові підписи, сертифікати безпеки та блокчейн-технології, де необхідно гарантувати цілісність і автентичність даних. Крім того, хешування використовується в системах автентифікації для зберігання паролів у захищеному вигляді, що унеможливує їх пряме відновлення. Наприклад, хешовані паролі порівнюються під час автентифікації користувача, що значно знижує ризик компрометації. Також хеш-функції відіграють важливу роль у механізмах генерації цифрових підписів, забезпечуючи перевірку автентичності документів чи повідомлень. Використання стійких хеш-алгоритмів є необхідною умовою для сучасних систем безпеки, адже слабкі алгоритми, такі як MD5 або SHA-1, можуть бути скомпрометовані через атаки, як-от підбір колізій.

Шифрування

Існує два основні способи шифрування даних:

– **Симетричний ключ (загальний секретний ключ)** передбачає використання одного і того ж ключа для шифрування та дешифрування даних. Обидві сторони, які обмінюються зашифрованою інформацією, повинні мати цей ключ, що ставить вимогу надійного його зберігання та

передачі. Це робить симетричне шифрування швидким і ефективним для великих обсягів даних, але також створює ризик компрометації безпеки, якщо ключ потрапить до зловмисників.

– **Асиметричний ключ (відкритий ключ)** використовує пару ключів: один відкритий (для шифрування) і один закритий (для дешифрування). Відкритий ключ можна вільно розповсюджувати, тоді як закритий ключ зберігається в таємниці. Цей метод забезпечує високий рівень безпеки, оскільки навіть якщо відкритий ключ відомий, без закритого неможливо дешифрувати повідомлення. Асиметричне шифрування зазвичай застосовується в цифрових підписах, протоколах SSL/TLS та при обміні даними через Інтернет.

Відкритий ключ

Суть асиметричного шифрування у тому, що використовується пара ключів. Один з них використовується як відкритий (як правило, він публікується в самому сертифікаті власника), другий ключ називається секретним – він тримається в таємниці і ніколи нікому не відкривається. Обидва ключі працюють у парі: один використовується для запуску протилежних функцій іншого ключа. Якщо відкритий ключ використовується для того, щоб зашифрувати дані, розшифрувати їх можна тільки секретним ключем і навпаки. Такий взаємозв'язок дозволяє робити дві важливі речі. Будь-який користувач може отримати відкритий ключ за призначенням і використовувати його для шифрування даних, які може розшифрувати тільки користувач, який володіє секретним ключем. (RSA) Якщо заголовок шифрує дані, використовуючи секретний ключ, кожен може розшифрувати дані, використовуючи відповідний відкритий ключ. Саме це є основою цифрових підписів. (DSA) RSA – найпоширеніший алгоритм шифрування з використанням асиметричних ключів.



Рис. 14.4. Шифрування з використанням асиметричних (несиметричних, з відкритим ключем) алгоритмів

Джерело: [2-4]

Секретний ключ

При шифруванні секретним ключем використовується той самий ключ для шифрованих даних. Якщо сторони хочуть обмінятися зашифрованими повідомленнями в безпечному режимі, то обидві сторони повинні мати однакові симетричні ключі. Такий тип шифрування використовується великого обсягу даних. Зазвичай використовуються алгоритми DES, 3-DES, RC2, RC4 та AES.

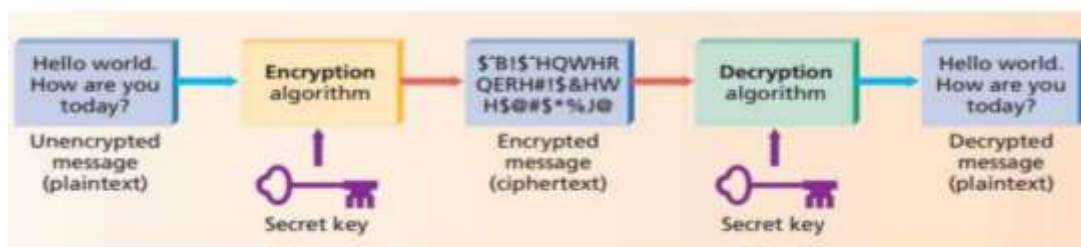


Рис. 14.5. Шифрування з використанням симетричних алгоритмів
Джерело: [2-4]

Комбінований підхід у використанні алгоритмів симетричного та асиметричного шифрування, а також основні моменти щодо протоколу SSL, його реалізації та застосування. Ключові аспекти, що висвітлюються:

1. Комбінований підхід

У протоколах безпеки часто використовують поєднання симетричного та асиметричного шифрування. Асиметричне шифрування, яке використовує публічні та приватні ключі, застосовується для безпечної передачі секретного ключа. Після передачі ключа симетричне шифрування використовує цей секретний ключ для шифрування даних, що дозволяє зменшити обчислювальні витрати. Комбінований підхід забезпечує баланс між високим рівнем безпеки та ефективністю. Асиметричне шифрування гарантує безпечний обмін ключами, а симетричне — швидку обробку великих обсягів даних, що робить цей метод ідеальним для використання в сучасних системах захисту інформації.

2. Протокол SSL

SSL (Secure Sockets Layer) є протоколом, який забезпечує безпечну передачу даних в Інтернеті, зокрема через HTTPS. Протокол SSL використовує як асиметричне, так і симетричне шифрування для забезпечення конфіденційності і цілісності даних. SSL забезпечує захист від атак, таких як прослуховування і модифікація даних під час їх передачі. Протокол створює зашифроване з'єднання між сервером та клієнтом, гарантує автентифікацію обох сторін та підтверджує цілісність переданих даних.

3. Фаза встановлення з'єднання в SSL:

- ✓ Перша фаза включає обмін повідомленнями "hello" між клієнтом та сервером, де вони узгоджують базовий шифр, а також, якщо необхідно, генерують новий секретний ключ.
- ✓ Друга фаза передбачає аутентифікацію клієнта та сервера. Після цього відправляються повідомлення finished для завершення встановлення безпечного з'єднання.

4. Реалізація SSL

SSL широко застосовується в таких технологіях, як HTTPS (для забезпечення безпеки веб-з'єднань), VPN та електронна пошта. Найпоширенішою реалізацією є бібліотека OpenSSL, яка забезпечує підтримку різних криптографічних алгоритмів і сертифікатів для налаштування безпечних з'єднань.

5. Структура записів SSL

Всі дані в SSL передаються у вигляді записів (рекордів), які мають заголовки і дані. В залежності від довжини заголовка, він може містити 2 або 3 байти. Заголовки також включають інформацію про розмір рекорду, що дозволяє отримувачу правильно обробити дані після їх дешифрування.

Цей підхід дозволяє досягти як високого рівня безпеки, так і ефективності в роботі протоколу.

Аутентифікація та обмін ключами

Процес аутентифікації та обміну ключами в SSL (Secure Sockets Layer) є важливою частиною забезпечення безпеки в комунікаціях між клієнтом і сервером. Він включає кілька етапів, основними з яких є встановлення секрету між сторонами, аутентифікація учасників з використанням сертифікатів, а також обмін ключами для забезпечення захищеного каналу зв'язку. Під час процесу аутентифікації сервер надає свій цифровий сертифікат клієнту, що дозволяє перевірити його автентичність та підтвердити, що зв'язок встановлюється з правомірною стороною. Обмін ключами зазвичай здійснюється за допомогою алгоритму, такого як RSA або Diffie-Hellman, що дозволяє зашифрувати та передати секретний ключ, який потім використовується для симетричного шифрування даних. Це забезпечує конфіденційність і захист від можливих атак на етапі обміну даними між клієнтом і сервером.

Основні типи аутентифікації в SSL:

1. Аутентифікація обох сторін (клієнт-сервер) – кожна зі сторін перевіряє ідентичність іншої за допомогою сертифікатів.
2. Аутентифікація сервера з неавтентифікованим клієнтом – клієнт не автентифікується, але сервер надає сертифікат, щоб підтвердити свою ідентичність.

3. Повна анонімність – жодна зі сторін не автентифікується, і немає необхідності в сертифікатах, що може бути вразливим до атак.

Алгоритми для аутентифікації:

Для аутентифікації використовуються алгоритми:

- ❖ RSA (Rivest-Shamir-Adleman)
- ❖ DSA (Digital Signature Algorithm)
- ❖ ECDSA (Elliptic Curve Digital Signature Algorithm)

Процес аутентифікації:

- Аутентифікація сервера - сервер надає клієнту сертифікат, який містить публічний ключ. Клієнт перевіряє сертифікат через сертифікаційний ланцюг, що веде до надійного центру сертифікації.
- Аутентифікація клієнта (якщо передбачено) - за допомогою підпису повідомлення клієнт може підтвердити свою особу.

Обмін ключами:

Метою обміну ключами є створення секрету, відомого лише клієнту та серверу, який використовується для шифрування даних і забезпечення цілісності переданих повідомлень. Цей спільний секрет забезпечує конфіденційність та автентичність інформації під час її передачі між сторонами. Обмін ключами гарантує, що тільки учасники з правильними приватними ключами можуть розшифрувати повідомлення. Таким чином, навіть якщо злоумисник перехопить комунікацію, він не зможе відновити секрет без доступу до приватних ключів учасників. Ось як це працює:

1. **Створення *pre_master_secret*** - це первинний секрет, який використовується для обчислення спільного секрету між сторонами.
2. **Генерація *master_secret*** - на основі *pre_master_secret* сторони генерують загальний секрет (*master_secret*), який використовується для шифрування та створення кодів аутентифікації повідомлень (MAC).

Анонімний обмін ключами:

Анонімні сесії можливі за допомогою алгоритмів RSA або Діффі-Хеллмана. Анонімні сесії дозволяють користувачам здійснювати шифрування даних без необхідності вказувати свою особисту інформацію чи використовувати цифрові сертифікати. Алгоритм RSA забезпечує аутентифікацію і шифрування за допомогою публічних та приватних ключів, де публічний ключ використовується для шифрування даних, а приватний — для їх розшифрування. У свою чергу, алгоритм Діффі-Хеллмана використовується для безпечного обміну ключами між сторонами без необхідності їх попередньої автентифікації. Обидва ці алгоритми можуть забезпечити конфіденційність комунікації, навіть якщо з'єднання не підкріплене цифровими сертифікатами. Вони є важливими

для анонімних сесій, де сторони не хочуть чи не можуть використовувати традиційні методи верифікації, такі як цифрові підписи. Замість цього, анонімні сесії застосовують механізми для генерування тимчасових ключів для шифрування і дешифрування повідомлень. В результаті, алгоритми RSA і Діффі-Хеллмана забезпечують високу ступінь конфіденційності, не розкриваючи особисту інформацію про користувачів.

• **RSA** - клієнт шифрує `pre_master_secret` публічним ключем сервера, і сервер використовує свій приватний ключ для розшифровки. Це забезпечує конфіденційність секрету. Після того, як сервер розшифрує `pre_master_secret`, обидві сторони (клієнт і сервер) використовують його для генерування спільного симетричного ключа, який буде використовуватися для шифрування подальших даних. Цей симетричний ключ забезпечує ефективне шифрування даних під час сеансу зв'язку. Таким чином, RSA використовується для безпечної передачі `pre_master_secret`, що дозволяє клієнту та серверу синхронізувати свої шифрувальні ключі без ризику їх перехоплення сторонніми особами.

• **Діффі-Хеллман** обмінюються відкритими параметрами, але перехоплювач не може відновити секрет без знання приватних значень. Цей метод забезпечує обмін секретними ключами без необхідності їх безпосередньої передачі через мережу. Кожен учасник генерує свій приватний ключ та обчислює відповідний відкритий параметр, після чого обмінюється ними. Зрештою, обидва учасники можуть використовувати відкриті параметри для обчислення спільного секрету, не передаючи його в явному вигляді, що забезпечує високу безпеку обміну.

Аутентифікація та обмін ключами з RSA:

Аутентифікація та обмін ключами за допомогою алгоритму RSA базуються на використанні пари публічних і приватних ключів. Кожен учасник обміну має пару ключів: публічний ключ, який можна вільно розповсюджувати, і приватний ключ, який зберігається в таємниці. Процес аутентифікації з RSA зазвичай полягає в тому, що відправник підписує повідомлення своїм приватним ключем, а отримувач може перевірити автентичність цього підпису, використовуючи публічний ключ відправника. Під час обміну ключами, наприклад, в протоколах, як SSL/TLS, одна зі сторін генерує випадковий симетричний ключ для шифрування даних. Цей симетричний ключ шифрується публічним ключем одержувача і передається через незахищене з'єднання. Одержувач використовує свій приватний ключ для розшифрування симетричного ключа. Таким чином, навіть якщо злоумисник перехопить зашифроване повідомлення, він не зможе розшифрувати його без приватного ключа

одержувача. RSA забезпечує безпечний обмін інформацією завдяки складності обчислення приватного ключа з публічного, що гарантує захист від несанкціонованого доступу.

- Сервер надає публічний ключ (або тимчасовий ключ) для шифрування `pre_master_secret`.
- Клієнт шифрує секрет і відправляє його серверу.
- Сервер розшифровує секрет і підтверджує автентичність, відправивши повідомлення "finished".
- Якщо використовується RSA для аутентифікації клієнта, клієнт підписує повідомлення для підтвердження своєї автентичності.

Цей процес гарантує, що дані, які передаються між клієнтом і сервером, захищені від несанкціонованого доступу та маніпуляцій.

Аутентифікація та обмін ключами під час використання протоколу Діффі-Хеллмана

У цьому випадку сервер може також підтримувати алгоритм Діффі-Хеллмана, що містить конкретні параметри, або може використовувати повідомлення обміну ключами від сервера для посилення набору тимчасових параметрів, підписаних сертифікатами DSS або RSA. Тимчасові параметри гешуються з повідомленням `hello.random` перед підписанням, щоб зловмисник не зміг зробити повторення старих параметрів. У будь-якому випадку, клієнт може перевірити сертифікат або сигнатуру для впевненості, що параметри належать серверу. Якщо клієнт має сертифікат, що містить параметри алгоритму DiffieHellman, то сертифікат також містить інформацію, потрібну для того, щоб завершити обмін ключами. У цьому випадку клієнт і сервер повинні будуть згенерувати однакові Diffie-Hellman результати (`pre_master_secret`) щоразу, коли вони встановлюють з'єднання. Для того, щоб запобігти збереженню секрету (`pre_master_secret`) в пам'яті комп'ютера на час довше, ніж необхідно, секрет повинен бути переведений в загальний секрет (`master_secret`) настільки швидко, наскільки це можливо. Параметри клієнта повинні бути сумісні з тими, що підтримує сервер для того, щоб працював обмін ключами.

Відновлення сесії

Творці SSL знали, що алгоритми шифрування відкритим ключем обчислювально складні, і клієнт, що створює кілька нових з'єднань до одного і того ж сервера протягом короткого проміжку часу може навантажити сервер, що призведе до помітних тимчасових затримок

відповіді. Однак, якщо клієнт і сервер вже встановили з'єднання, йому відповідатиме унікальний ідентифікатор сесії, що дозволяє посилатися на нього і використовувати такий же секретний ключ при наступних з'єднаннях в рамках деякого часового відрізка. Безумовно, такий підхід привносить певний ризик у безпеку з'єднання. Тому, якщо необхідно, клієнт може створити новий ідентифікатор і секретний ключ для даної сесії. Microsoft Internet Explorer, наприклад, роблять цю операцію кожні 2 хвилини.

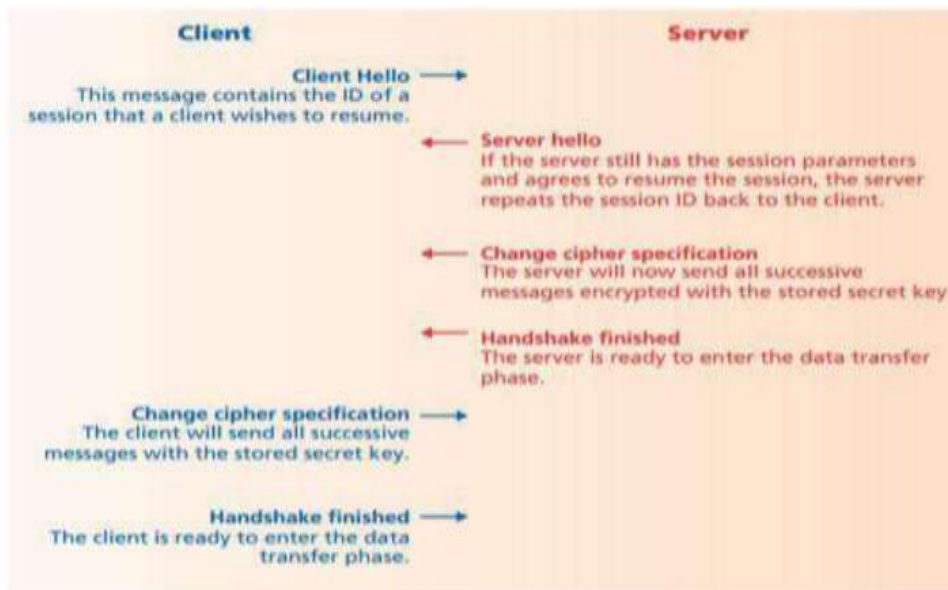


Рис. 14.6. Відновлення сесії

Джерело: [2-7]

Протокол Transport Layer Security (TLS)

Протокол Transport Layer Security (TLS) є стандартом для забезпечення безпеки даних, що передаються через мережу. Він використовується для захисту інформації між клієнтом та сервером, забезпечуючи конфіденційність, аутентифікацію та цілісність даних.

Протокол TLS складається з двох основних етапів: TLS Record та TLS Handshake.

1. Адміністрація сертифікатів та ключів

- Клієнтська аутентифікація

Якщо сервер вимагає аутентифікацію клієнта, то клієнт повинен мати сертифікат та пов'язаний з ним приватний ключ. Цей сертифікат використовується для підтвердження ідентичності клієнта.

- Серверна аутентифікація

Сервер також повинен мати сертифікат і приватний ключ для аутентифікації. Сертифікат підтверджує ідентичність сервера та дозволяє клієнту впевнитись, що він підключається до правильного сервера.

- Зберігання сертифікатів

Сертифікати та відповідні приватні ключі зберігаються у спеціальних сховищах. Для серверів і клієнтів це можуть бути файли на сервері або сховища, такі як KeyStore для Java або PKCS#12.

- Сховище ідентифікаторів сесій

Клієнт і сервер зберігають ідентифікатори сесій та пов'язані з ними секретні ключі для відновлення з'єднання в майбутньому без повторного виконання всього процесу рукоостискання.

2. Принцип роботи TLS

TLS поділяється на два основні шари:

- TLS Record: забезпечує захист даних під час передачі.
- TLS Handshake: використовується для встановлення захищеного з'єднання між клієнтом і сервером.

3. Підтвердження зв'язку (TLS Handshake)

Під час підтвердження зв'язку (handshake) виконується кілька етапів:

1. ClientHello - клієнт надсилає повідомлення, в якому вказує версію протоколу TLS або SSL, підтримувані методи шифрування (CipherSuite), а також випадкове число для подальших обчислень.

2. ServerHello - сервер відповідає повідомленням, в якому вибирає метод шифрування із запропонованих клієнтом, надає ідентифікатор сесії та випадкове число. Також сервер надсилає свій сертифікат, а якщо потрібно, запитує сертифікат клієнта.

3. Перевірка сертифіката сервера - клієнт перевіряє наданий сервером сертифікат.

4. Шифрування випадкового числа - клієнт надсилає випадкове число, яке шифрується публічним ключем сервера для забезпечення безпеки.

5. Клієнтська аутентифікація - якщо сервер вимагає сертифікат клієнта, клієнт надсилає зашифроване повідомлення разом з його цифровим сертифікатом.

6. Перевірка сертифіката клієнта - сервер перевіряє сертифікат клієнта.

7. ChangeCipherSpec - клієнт та сервер відправляють повідомлення, що оголошують про перехід до захищеного каналу.

8. Завершення рукостискання - клієнт відправляє повідомлення "Finished", зашифроване його секретним ключем, тим самим завершуючи процес підтвердження зв'язку зі своєї сторони.

9. Завершення рукостискання з боку сервера - сервер також надсилає повідомлення "Finished" після перевірки та встановлення захищеного каналу.

10. Обмін зашифрованими повідомленнями - після цього клієнт і сервер можуть обмінюватися даними, які шифруються за допомогою спільного секрету, що був створений під час процесу рукостискання.

Цей процес забезпечує належний рівень захисту даних від перехоплення, підробки та атак.

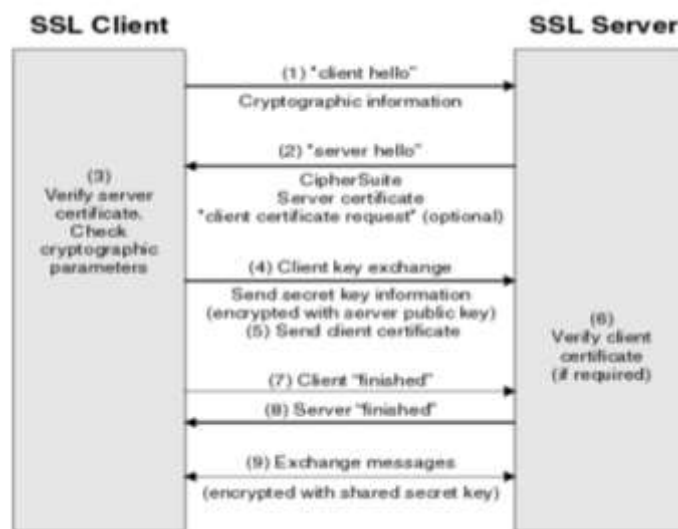


Рис. 14.7. Підтвердження зв'язку (handshake)

Джерело: [2-4]

Протокол TLS (Transport Layer Security) є ключовим елементом для забезпечення безпечної комунікації в мережах, зокрема для захисту даних під час передачі по Інтернету. Основним завданням цього протоколу є забезпечення конфіденційності та цілісності даних, а також аутентифікації обох сторін зв'язку. TLS складається з двох основних шарів: TLS Record та TLS Handshake.

Шар TLS Record відповідає за захист даних, перевірку їх цілісності, а також за правильну передачу через мережу. Цей протокол розбиває вихідні повідомлення на блоки відповідного розміру і формує вхідні повідомлення, застосовуючи методи стиснення, шифрування та аутентифікації. Після обробки за допомогою TLS Record, зашифровані дані передаються через протокол TCP. Важливими складовими цього запису є

тип контенту, версія протоколу, довжина повідомлення, а також MAC (Message Authentication Code) для перевірки цілісності даних.

Протокол TLS Handshake відповідає за встановлення та підтвердження захищеного з'єднання між клієнтом і сервером. Клієнт починає процес зв'язку, надсилаючи повідомлення ClientHello, в якому вказує версію протоколу та методи шифрування, що підтримуються. Сервер у відповідь надсилає повідомлення ServerHello, в якому вибирає відповідний метод шифрування та надсилає свій цифровий сертифікат для підтвердження автентичності. Клієнт перевіряє цей сертифікат, а далі процес переходить до генерації спільних ключів для шифрування подальших повідомлень. Після цього відбувається обмін повідомленнями ChangeCipherSpec, що позначає перехід до захищеного режиму передачі даних. Завершується підтвердження зв'язку за допомогою повідомлення Finished.

У разі, якщо з'єднання потрібно відновити, протокол TLS передбачає механізм відновлення сесії. Клієнт надсилає повідомлення ClientHello з ідентифікатором сесії, яку потрібно відновити. Сервер перевіряє наявність цього ідентифікатора у своєму кеші та, якщо це можливо, відновлює сесію без необхідності повторного виконання повної процедури handshake. Якщо ж відновити сесію не вдається, сервер генерує новий ідентифікатор і починає нову сесію.

Цифрові сертифікати (стандарт X.509)

Ключову роль в аутентифікації сторін і захисті даних у TLS відіграють цифрові сертифікати, які базуються на стандарті X.509. Ці сертифікати є засобом підтвердження, що певна особа або сервер володіє конкретним публічним ключем, і видаються сертифікаційними центрами (CA). Процес отримання сертифікату включає генерацію пари ключів, надсилання запиту до CA, отримання сертифікату після перевірки даних користувача та підписання сертифікатом CA. Кожен сертифікат містить інформацію про власника, публічний ключ, а також підпис CA, який підтверджує автентичність сертифікату. Сертифікати можуть бути відкликані, і в цьому випадку підтримується список відкликаних сертифікатів (CRL), який регулярно оновлюється. Усі ці процеси гарантують, що обмін даними між клієнтом та сервером у мережі буде захищений від несанкціонованого доступу та змін, забезпечуючи високий рівень безпеки в онлайн-операціях.

Цифрові сертифікати використовуються не лише для аутентифікації серверів, але й для верифікації клієнтів у деяких випадках, наприклад, при використанні двосторонньої аутентифікації. Під час встановлення з'єднання за допомогою TLS клієнт перевіряє підпис сертифіката сервера за допомогою публічного ключа сертифікаційного центру, що підтверджує

його довіру до з'єднання. Завдяки використанню таких сертифікатів забезпечується захист від атак, таких як "man-in-the-middle", оскільки навіть якщо злоумисник спробує перехопити трафік, він не зможе підробити сертифікат, оскільки його підпис неможливо відтворити без приватного ключа. Сертифікати X.509 також підтримують різні рівні довіри в залежності від сертифікаційного центру, що додає гнучкості в управлінні безпекою різних систем і платформ.

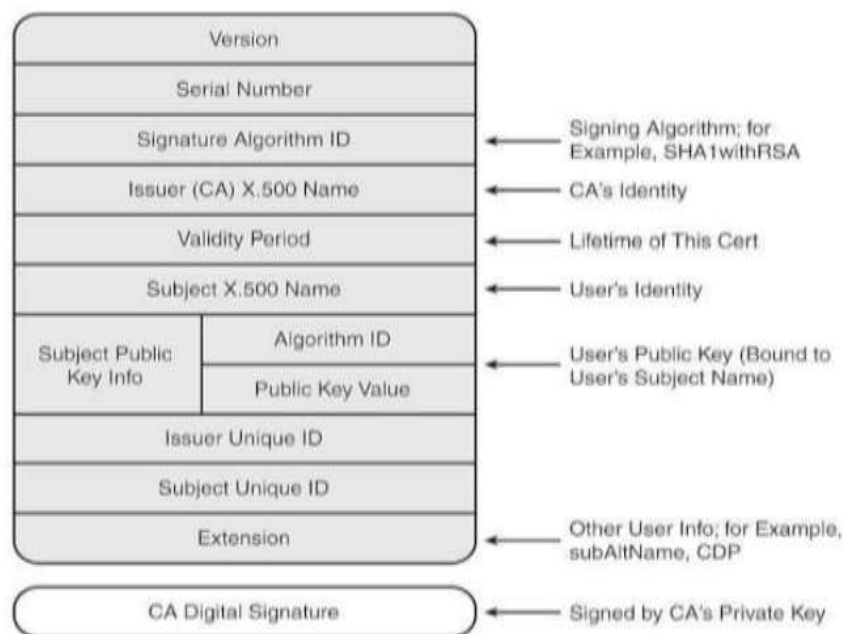


Рис. 14.8. Структура сертифікату X.509

Джерело: [2-4]

Протокол TLS (Transport Layer Security) є важливим засобом забезпечення безпеки передачі даних через мережу, зокрема шляхом шифрування інформації та аутентифікації обох сторін. Один з основних аспектів забезпечення безпеки в TLS — це захист від downgrade-атак, які можуть знижувати версію протоколу до менш захищених варіантів або використовувати менш надійні методи шифрування. Для цього протокол передбачає перевірку версії і забезпечує підтримку тільки актуальних, надійних шифрів і алгоритмів. Іншим важливим заходом є використання нумерації послідовних записів і порядкового номера в коді аутентифікації повідомлення (MAC), що дозволяє захистити дані від атак на повторення та зміну повідомлень, оскільки лише власник ключа може створювати правильний код аутентифікації для повідомлень.

Процес підтвердження зв'язку між клієнтом і сервером завершується повідомленням "Finished", яке містить хеш усіх попередніх повідомлень,

що дає змогу обом сторонам перевірити автентичність вибраних параметрів з'єднання та підтвердити надійність встановленого з'єднання. Важливу роль у безпеці відіграє і псевдовипадкова функція, яка ділить вхідні дані на дві частини, застосовує різні хеш-алгоритми (MD5 і SHA-1) до кожної з частин, а потім поєднує результати через операцію XOR для отримання MAC. Це дозволяє підвищити безпеку в разі виявлення уразливості в одному з алгоритмів хешування.

Ключові відмінності між SSL та TLS полягають у кількох важливих аспектах. По-перше, в аутентифікації повідомлень TLS використовує HMAC (Hash-based Message Authentication Code), який працює з будь-якою хеш-функцією, на відміну від SSL, що обмежується лише MD5 або SHA. По-друге, процес генерації ключів в TLS базується на використанні псевдовипадкової функції стандарту HMAC, тоді як SSL використовував RSA, Diffie-Hellman або Fortezza/DMS. Третя відмінність полягає у перевірці сертифікатів: у TLS перевірка сертифікатів значно спрощена, оскільки вся необхідна інформація передається у повідомленнях під час handshake, в той час як у SSL для перевірки передавалася складна послідовність повідомлень. Також важливою відмінністю є підтримка методів шифрування: TLS відмовився від старих методів шифрування, таких як Fortezza/DMS, і забезпечує можливість додавання нових методів шифрування в майбутніх версіях протоколу.

Незважаючи на високий рівень безпеки, TLS не є повністю захищеним від атак. Серед можливих типів атак можна відзначити атаку за словником, яка спрямована на перебір слабких паролів або секретних ключів, атаку відображенням, що передбачає маніпуляції з відповідями сервера, та атаку протоколу рукостискання, коли зловмисник намагається вплинути на процес handshake і змінити параметри з'єднання. Іншою серйозною загрозою є зламування SSL-з'єднань всередині ЦОД, де відбувається обробка з'єднань, а також атака BEAST, яка націлена на криптографічні уразливості TLS 1.0. Серед інших атак можна згадати розкриття шифрів, що має на меті витягнення секретної інформації, атаку «зловмисник посередині» (Man-in-the-Middle), що дозволяє перехоплювати та змінювати повідомлення між клієнтом і сервером, THC-SSL-DOS, яка націлена на створення відмови в обслуговуванні через надмірну кількість запитів, а також SSLstrip, атака, що перетворює захищене з'єднання HTTPS в незахищене HTTP, дозволяючи зловмисникам зчитувати передані дані.

Для захисту від цих атак важливо правильно налаштувати протоколи, використовувати новітні методи шифрування та постійно моніторити безпеку з'єднань.

14.4. ЗАХИЩЕНИЙ ПРОТОКОЛ ВІДДАЛЕНОГО ДОСТУПУ SSH

Захищений протокол віддаленого доступу SSH (Secure Shell) є криптографічним протоколом, який забезпечує безпечний віддалений доступ до комп'ютерів і мережевих пристроїв. Протокол використовує шифрування та аутентифікацію для захисту даних, що передаються через незахищені мережі, наприклад, Інтернет. SSH дозволяє здійснювати безпечне адміністрування серверів, виконувати віддалені команди та отримувати доступ до файлів.

Принцип роботи SSH базується на клієнт-серверній архітектурі, де клієнт ініціює підключення до сервера, а сервер проводить аутентифікацію та встановлює зашифрований канал зв'язку. Весь трафік між клієнтом і сервером шифрується з використанням асиметричних або симетричних алгоритмів шифрування, що забезпечує високий рівень конфіденційності. Аутентифікація користувача може здійснюватися через паролі, пари ключів або двофакторну аутентифікацію. Протокол також захищає сервер від атак типу "man-in-the-middle", оскільки кожен сервер має свій публічний ключ для перевірки автентичності. SSH використовує хешування для забезпечення цілісності даних, що передаються, захищаючи їх від змінювання під час передачі.

Основними перевагами SSH є високий рівень безпеки, можливість віддаленого доступу, гнучкість у налаштуванні аутентифікації, підтримка тунелювання та масштабованість.

SSH використовується для адміністрування серверів, дистанційного доступу до мережевих пристроїв, переміщення файлів через протоколи SCP або SFTP, а також для виконання віддалених команд на серверах. Це один з основних інструментів для забезпечення безпеки віддаленого доступу до інформаційних систем, оскільки він запобігає прослуховуванню, несанкціонованому доступу та підробці даних, що передаються.

SSH (Secure Shell) — це мережевий протокол прикладного рівня, який забезпечує віддалене управління операційними системами та тунелювання TCP-з'єднань. Протокол шифрує весь трафік, включаючи паролі, і підтримує вибір різних алгоритмів шифрування. SSH-клієнти та сервери доступні для більшості операційних систем, що робить його універсальним інструментом для забезпечення безпеки віддалених підключень.

SSH підтримує аутентифікацію за RSA-ключами, що забезпечує високий рівень безпеки для каналу передачі даних, а також можливість двофакторної аутентифікації користувачів. Протокол дозволяє безпечно передавати будь-який мережевий трафік, включаючи звукові та відео

потоки, що передаються через незахищені мережі. SSH також підтримує стиснення переданих даних, що забезпечує ефективне шифрування, наприклад, для віддаленого запуску клієнтів X Window System.

Перша версія SSH (SSH-1) була розроблена в 1995 році Тату Улененом, але згодом була замінена на більш безпечну версію SSH-2, що стала стандартом з 2006 року. SSH-2 стійкий до атак "людина посередині" та забезпечує захист від атак шляхом приєднання до сесії, таких як session hijacking.

Сьогодні є дві основні реалізації SSH: безкоштовна OpenSSH, що є найбільш популярною реалізацією, і пропріетарна реалізація, розроблена компанією SSH Inc. Протокол застосовується для безпечного адміністрування серверів, віддаленого доступу до мереж і передачі файлів через SCP або SFTP.

Основні функції SSH включають:

1. Безпечне виконання віддалених команд (SSH, slogin, scp).
2. Підтримка X11 Forwarding для віддаленого запуску клієнтів X Window.
3. Перенаправлення портів для шифрування трафіку між портами на різних машинах.

Безпека SSH досягається за допомогою шифрування з'єднання, аутентифікації серверів і клієнтів, перевірки цілісності пакетів та тимчасових параметрів аутентифікації. Ці механізми забезпечують захист від атак, таких як підміна IP-адрес або DNS-записів, перехоплення паролів або зміни в трафіку.

SSH є важливим інструментом для захисту віддалених з'єднань, забезпечуючи надійний захист даних в мережах з відкритим доступом.

Архітектура протоколу SSH (Secure Shell) і компоненти SSH-системи складаються з низки елементів, що забезпечують безпечне з'єднання між клієнтом і сервером. Це дозволяє виконувати різні операції через незахищену мережу, забезпечуючи конфіденційність, цілісність та аутентифікацію. Протокол SSH складається з кількох ключових компонентів, кожен з яких виконує свою роль у забезпеченні безпеки з'єднання.

Архітектура протоколу SSH

Архітектура протоколу SSH (Secure Shell) є багаторівневою і складається з кількох ключових компонентів, що забезпечують безпечне з'єднання між клієнтом і сервером через незахищену мережу. Вона включає три основні рівні протоколу, кожен з яких виконує свою функцію для забезпечення конфіденційності, цілісності даних та аутентифікації

користувачів і серверів. Архітектура протоколу SSH спрямована на забезпечення високого рівня безпеки для віддалених підключень до серверів і комп'ютерних систем, захищаючи інформацію від несанкціонованого доступу і атак.



Рис. 14.9. Архітектура протоколу SSH

Джерело: [2]

SSH має трирівневу архітектуру, яка складається з трьох основних протоколів:

1. **Протокол транспортного рівня (Transport Layer Protocol)** відповідає за створення зашифрованого каналу між клієнтом і сервером. Протокол транспортного рівня забезпечує:

- ✓ Конфіденційність даних шляхом використання симетричного шифрування.
- ✓ Цілісність даних за допомогою криптографічних хеш-функцій.
- ✓ Аутентифікацію сервера для того, щоб клієнт міг підтвердити, що він підключається до правильного сервера. Цей процес зазвичай включає перевірку публічного ключа сервера.

2. **Протокол аутентифікації користувача (User Authentication Protocol)** займається перевіркою особистості користувача, що намагається підключитися до сервера. Користувач може пройти аутентифікацію за допомогою кількох методів:

- ✓ Використання пароля.

- ✓ Аутентифікація за публічним ключем, коли клієнт надає серверу свій публічний ключ, і сервер перевіряє відповідність збереженому запису.
- ✓ Керберос-аутентифікація для інтеграції з іншими системами аутентифікації.

3. **Протокол з'єднання (Connection Protocol)** відповідає за обробку запитів після аутентифікації користувача, таких як:

- ✓ Створення логічних каналів для різних видів трафіку, включаючи командний інтерфейс або передачу файлів.
- ✓ Мультиплексування одного фізичного з'єднання для кількох логічних каналів, що дозволяє передавати кілька потоків даних одночасно.

Компоненти SSH-системи:

SSH-система — це сукупність програмних та апаратних компонентів, що реалізують протокол SSH (Secure Shell) для забезпечення безпечних віддалених з'єднань між комп'ютерними системами через незахищену мережу, зокрема Інтернет.

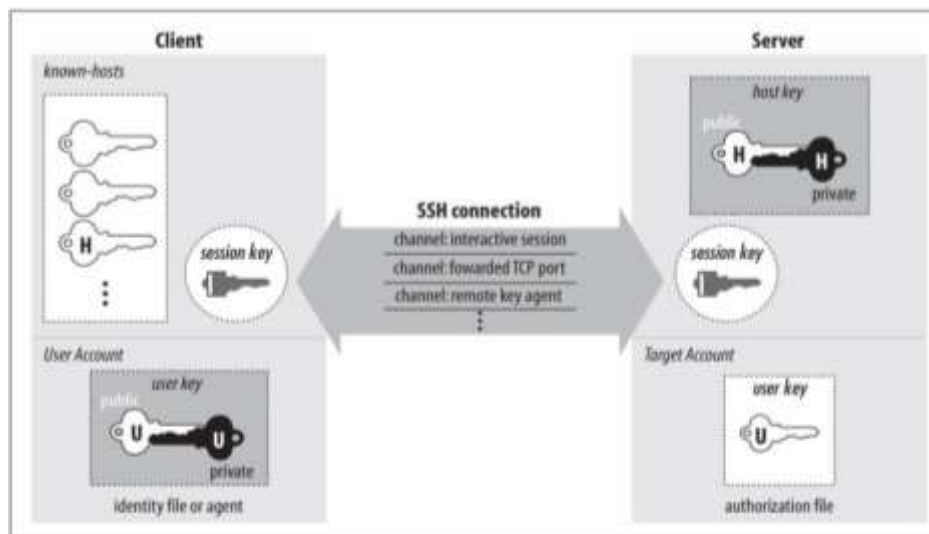


Рис. 14.10. Архітектура системи SSH

Джерело: [2]

SSH-система забезпечує конфіденційність, цілісність даних та аутентифікацію користувачів і серверів. SSH (Secure Shell) використовує криптографічні методи для забезпечення захищеного каналу зв'язку, що дозволяє віддалену роботу з серверами та іншими пристроями в мережі. Завдяки аутентифікації за допомогою публічних та приватних ключів, SSH

забезпечує високу надійність при підключенні до віддалених систем, запобігаючи несанкціонованому доступу.

SSH-система складається з кількох основних компонентів, які взаємодіють між собою для забезпечення функціональності та безпеки:

1. SSH-сервер (sshd)

Це програма, що працює на сервері та приймає вхідні з'єднання від клієнтів. Сервер виконує основні функції аутентифікації, шифрування і налаштування захищеного каналу. Він також відповідає за надання доступу користувачам після їхньої аутентифікації та виконує додаткові функції, такі як перенаправлення портів.

2. SSH-клієнт (ssh, scp, sftp)

Це програми, що використовуються для підключення до SSH-сервера. Клієнт ініціює з'єднання, передає свої автентифікаційні дані (наприклад, за допомогою публічного ключа) і після аутентифікації виконує команди на сервері або передає файли. Відомими SSH-клієнтами є програми ssh для віддалених сесій, scp для копіювання файлів і sftp для безпечної передачі файлів.

3. Ключі SSH (OpenSSH Keys)

Ключі є основним методом аутентифікації в SSH-системах. Вони бувають двох типів:

- ✓ Публічний ключ — передається серверу для аутентифікації користувача.
- ✓ Приватний ключ — зберігається на клієнті і використовується для доведення ідентичності користувача. Приватний ключ завжди захищений паролем або іншим механізмом безпеки.
- ✓ Ключі хоста — використовуються для аутентифікації сервера. Вони дозволяють клієнту перевірити, що він підключається саме до того сервера, до якого має намір підключитися.

4. Файли конфігурації:

- ✓ sshd_config — конфігураційний файл на сервері, в якому вказуються параметри доступу для клієнтів (наприклад, які методи аутентифікації дозволено, які порти використовуються тощо).
- ✓ known_hosts — файл на клієнтській стороні, в якому зберігаються публічні ключі відомих серверів. Цей файл використовується для перевірки автентичності сервера при кожному підключенні.

5. **Агенти SSH (SSH Agent)** використовуються для зберігання приватних ключів в пам'яті протягом сеансу. Це дозволяє користувачам уникати необхідності вводити парольну фразу для кожного підключення.

Агент SSH підключається до сервера і передає йому відповідні ключі для аутентифікації.

6. **Шифрування та алгоритми** використовує різні криптографічні алгоритми для забезпечення безпеки з'єднання. Основні алгоритми включають:

- ✓ Алгоритми симетричного шифрування (AES, 3DES, Blowfish) для шифрування даних.
- ✓ Алгоритми хешування (SHA-2, MD5) для перевірки цілісності переданих даних.
- ✓ Алгоритми асиметричного шифрування (RSA, DSA, ECDSA) для обміну ключами та аутентифікації.

Процес встановлення з'єднання SSH виглядає наступним чином:

1. Клієнт ініціює з'єднання з сервером через TCP (порт 22).
2. Сервер надсилає свій публічний ключ і інші параметри шифрування.
3. Клієнт і сервер домовляються про методи шифрування та аутентифікації.
4. Клієнт автентифікується за допомогою пароля або публічного ключа.
5. Після успішної аутентифікації створюється захищений канал для передачі даних.



Рис. 14.11. Алгоритм встановлення з'єднання по протоколу SSH
Джерело: [2]

Всі ці компоненти разом утворюють систему, що забезпечує високий рівень безпеки для віддаленого доступу до комп'ютерних систем, захищаючи дані від несанкціонованого доступу та атак в мережі.

14.5. Протоколи IPSec

Протоколи IPSec (Internet Protocol Security) є набір стандартів, який забезпечує захист даних, що передаються через мережу Інтернет або інші IP-мережі. Вони використовують шифрування, автентифікацію та цілісність для забезпечення конфіденційності та безпеки з'єднань між пристроями в мережі.

Основні компоненти IPSec включають два основні протоколи:

1. АН (Authentication Header) — забезпечує автентифікацію і цілісність даних, але не шифрує їх. Це дозволяє перевіряти, чи не були змінені дані під час передачі.
2. ESP (Encapsulating Security Payload) — забезпечує як шифрування, так і автентифікацію даних, що дозволяє забезпечити конфіденційність і цілісність переданої інформації.

Існують два основних режими роботи IPSec:

- *Транспортний режим* — шифрується лише корисне навантаження пакету, що дозволяє захищати дані, передані між кінцевими точками (наприклад, між двома комп'ютерами).
- *Тунельний режим* — шифрується весь IP-пакет, що забезпечує безпеку між мережею та її користувачами (наприклад, між двома мережами через VPN).

IPSec також використовує механізми для створення захищених з'єднань між двома пристроями (наприклад, через методи обміну ключами, такі як IKE — Internet Key Exchange).

Розподіл функцій між протоколами IPSec

Протокол IPSec у стандартах Інтернету є системою захисту даних, яка забезпечує конфіденційність, цілісність та автентичність інформації, що передається через мережу. Він являє собою узгоджений набір відкритих стандартів із чітко визначеним ядром, яке може бути легко розширене новими функціями та протоколами. Це робить IPSec універсальним і масштабованим рішенням для забезпечення мережевої безпеки в умовах сучасних викликів кіберзагроз.

Ядро IPSec складається з трьох основних протоколів. Перший із них — АН (Authentication Header), який забезпечує автентичність і цілісність даних шляхом додавання спеціального заголовка до кожного пакета. Це дозволяє перевіряти, що дані не були змінені під час передачі, і гарантує, що вони надійшли від довіреного джерела. Другий протокол, ESP (Encapsulating Security Payload), забезпечує шифрування даних для гарантування їх конфіденційності, а також може підтримувати

аутентифікацію та цілісність. На відміну від АН, ESP має ширший функціонал, оскільки дозволяє одночасно захищати дані від несанкціонованого доступу та забезпечувати їх автентичність. Третій компонент, IKE (Internet Key Exchange), відповідає за автоматизацію процесу обміну секретними ключами між кінцевими точками. Це забезпечує безперебійну роботу шифрування та аутентифікації, дозволяючи системі залишатися стійкою до атак.

Функціонал АН і ESP частково перекривається: ESP може виконувати ті ж функції аутентифікації та перевірки цілісності, що й АН, але також додає шифрування. Це дозволяє використовувати ESP у різних комбінаціях — лише для шифрування, лише для аутентифікації або для обох функцій одночасно. Такий підхід забезпечує гнучкість і адаптивність системи до різних умов використання. Поділ функцій між цими протоколами обумовлений обмеженнями в окремих країнах щодо експорту та імпорту засобів шифрування. У таких випадках IPSec може використовувати лише АН для захисту даних від змін та підтвердження їх автентичності, хоча цього недостатньо для забезпечення конфіденційності, оскільки дані залишаються незашифрованими.

IPSec є ключовим стандартом для захисту корпоративних та державних мереж завдяки своїй універсальності та масштабованості. Сучасні впровадження цього протоколу підтримують новітні криптографічні алгоритми, такі як AES-GCM, які забезпечують високу швидкість обробки даних і стійкість до атак. Це дозволяє IPSec успішно використовуватися для захисту інформації в мережах, що функціонують на базі протоколів IPv4 і IPv6, забезпечуючи високий рівень безпеки в умовах зростання кіберзагроз.

БЕЗПЕЧНА АСОЦІАЦІЯ

Протоколи АН і ESP у складі IPSec забезпечують захист даних, що передаються, завдяки створенню спеціальних логічних з'єднань, які називаються безпечними асоціаціями (Security Association, SA). Ці асоціації формуються протоколом IKE (Internet Key Exchange), який виступає як механізм для встановлення, обміну та керування ключами. Безпечні асоціації можуть використовуватись як для всієї взаємодії через захищений канал, так і для кожного TCP-з'єднання окремо, залежно від вимог до деталізації та рівня захисту. Це дозволяє налаштовувати IPSec відповідно до потреб користувача чи мережі, забезпечуючи гнучкість і масштабованість. Безпечні асоціації (SA) визначають параметри шифрування та автентифікації, такі як тип шифрування, довжина ключа та методи перевірки цілісності. Кожна SA включає в себе набір специфікацій, що забезпечують захист даних на різних етапах передачі, від початкового

запиту до остаточного отримання. Для ефективного керування кількома SA в мережі використовуються таблиці безпечних асоціацій, що дозволяють оптимізувати обробку і забезпечити стабільну і безпечну комунікацію між пристроями.



Рис. 14.12. Безпечна асоціація

Джерело: [2-4]

Кожна безпечна асоціація в IPSec є односпрямованою (симплексною). Це означає, що для забезпечення двостороннього обміну даними необхідно встановити дві окремі асоціації: одну для передачі даних в одному напрямку, а іншу – в протилежному. При цьому параметри цих асоціацій можуть відрізнятися. Наприклад, для запитів до бази даних може бути достатньо аутентифікації та перевірки цілісності, тоді як для відповідей із чутливою інформацією потрібне додаткове шифрування для забезпечення конфіденційності.

Процес створення безпечної асоціації починається зі взаємної аутентифікації сторін, що є критично важливим для захисту від атак, спрямованих на підробку джерела даних. Параметри SA визначають, який із протоколів (AH або ESP) буде використовуватися, які функції він виконуватиме (аутентифікація, перевірка цілісності, шифрування), а також які секретні ключі застосовуватимуться. Ці ключі є основним елементом забезпечення безпеки, і їх компрометація може призвести до порушення захищеності даних.

Встановлення SA може виконуватись вручну або автоматично. При ручному способі адміністратор вручну налаштовує параметри асоціації, включаючи ключі, на обох кінцевих вузлах. Автоматичний спосіб задіює протокол IKE, який в процесі переговорів між вузлами автоматично визначає параметри SA. Цей підхід дозволяє уникнути помилок, властивих ручному конфігуруванню, і забезпечує більш динамічну та надійну роботу. Протокол IKE не лише автоматизує обмін параметрами SA, але й забезпечує захищений канал для передачі цих даних, що підвищує рівень безпеки. Під час процесу переговорів IKE використовує різні методи аутентифікації, такі як використання цифрових сертифікатів або попередньо поділених ключів, щоб перевірити ідентичність вузлів. Автоматичне налаштування SA через IKE також дозволяє адаптувати

захист до змін у мережевих умовах, що підвищує ефективність системи в умовах динамічних змін у мережах.



Рис. 14.13. Узгодження параметрів в протоколі ESP

Джерело: [2-4]

IPSec є гнучким протоколом, що підтримує широкий спектр алгоритмів аутентифікації та шифрування. У стандартній версії IPSec обов'язковим є використання алгоритмів MD5 або SHA-1 для аутентифікації даних і алгоритму DES для шифрування. Однак сучасні реалізації IPSec значно розширили цей набір. Наприклад, широко використовуються алгоритми Triple DES, AES, Blowfish, Cast, RC5 та інші. Алгоритм AES-GCM, зокрема, забезпечує одночасне шифрування та перевірку цілісності даних, що підвищує ефективність і рівень захисту.

На сьогодні IPSec активно використовується для побудови віртуальних приватних мереж (VPN), захисту корпоративних даних та безпечного з'єднання між різними мережами. Завдяки підтримці IPv4 та IPv6, протокол залишається актуальним навіть у сучасних високошвидкісних мережах, де важливі не лише захист інформації, але й швидкість її обробки. Сучасні криптографічні алгоритми, що підтримуються IPSec, забезпечують його відповідність новітнім стандартам безпеки, роблячи його надійним інструментом для протидії кіберзагрозам.

ТРАНСПОРТНИЙ І ТУНЕЛЬНИЙ РЕЖИМИ

Протоколи AH (Authentication Header) і ESP (Encapsulating Security Payload) у складі IPSec забезпечують захист даних у двох режимах: транспортному та тунельному. Вибір режиму залежить від вимог до захисту інформації та ролі вузла в мережі. У транспортному режимі передача даних здійснюється за допомогою оригінального IP-заголовка пакета, при цьому шифрується лише корисне навантаження, що робить цей режим оптимальним для прямого обміну між кінцевими вузлами. У тунельному режимі вихідний пакет інкапсулюється в новий IP-пакет із

додатковим заголовком, що дозволяє захистити весь пакет, включаючи початковий заголовок, забезпечуючи високий рівень безпеки при передачі через загальнодоступні мережі.

Залежно від ролі вузлів і вимог до захисту даних, IPSec реалізується за трьома основними схемами: хост-хост, шлюз-шлюз і хост-шлюз. У схемі хост-хост захищений канал встановлюється між двома кінцевими вузлами. Це дозволяє забезпечити безпеку передачі даних між хостами безпосередньо, найчастіше використовуючи транспортний режим. Схема шлюз-шлюз застосовується для захисту трафіку між двома мережами, з'єднаними через загальнодоступну мережу. У цьому випадку шлюзи безпеки (Security Gateway) відповідають за шифрування і дешифрування трафіку. Вузли всередині мережі можуть передавати дані у відкритому вигляді, оскільки довіряють внутрішньому середовищу, тоді як тунельний режим IPSec забезпечує захист даних під час їх передачі через незахищені середовища. Наприклад, користувач із адресою IP1 надсилає дані на IP2. Шлюз SG1 шифрує весь пакет і додає новий IP-заголовок із адресами SG1 (відправника) та SG2 (одержувача). Після проходження публічною мережею SG2 розшифровує пакет, повертаючи його до початкового стану.

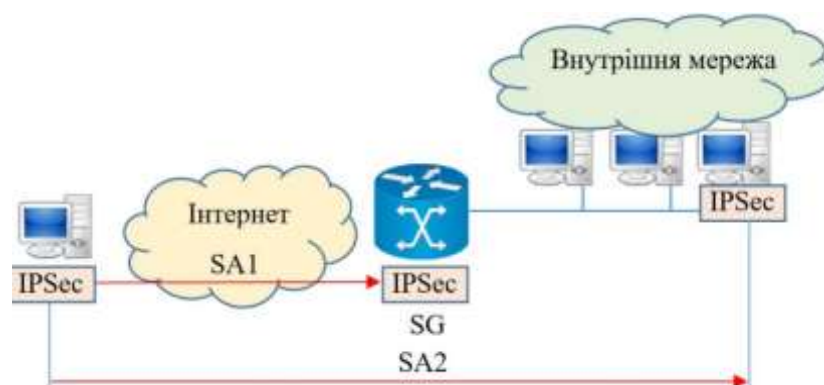


Рис. 14.14. Схема захищеного каналу хост-шлюз

Джерело: [2-4]

Схема хост-шлюз часто використовується для організації безпечного віддаленого доступу. У цій моделі захищений канал створюється між віддаленим хостом і шлюзом безпеки, який відповідає за захист трафіку для всієї внутрішньої мережі підприємства. За необхідності можна додатково встановити окремий канал між віддаленим хостом і певним внутрішнім хостом, що забезпечує подвійний рівень захисту. Це особливо актуально для корпоративних систем, де важливо гарантувати безпеку як у зовнішньому, так і у внутрішньому середовищі.

Завдяки своїй гнучкості IPSec залишається провідним протоколом у сфері захисту даних. Сучасні реалізації IPSec підтримують передові алгоритми шифрування, такі як AES-256, і хешування, наприклад SHA-256 і SHA-3, що забезпечує високий рівень криптографічного захисту. Протокол широко застосовується для побудови віртуальних приватних мереж (VPN), захисту IoT-пристроїв, а також у хмарних рішеннях. Інтеграція новітніх методів аутентифікації та шифрування дозволяє IPSec відповідати сучасним викликам у сфері кібербезпеки й залишатися актуальним для захисту даних в умовах зростаючих загроз.

Протокол АН

Протокол АН (Authentication Header) є важливою частиною IPSec і забезпечує перевірку автентичності та цілісності переданих даних, а також захист від повторного відтворення пакетів. Його основне завдання — гарантувати, що пакет дійсно був відправлений стороною, з якою встановлена безпечна асоціація, і що його вміст не було змінено під час передачі. Додатково АН може захищати від зловмисного повторного використання пакетів, перевіряючи їх порядкові номери.

Основні функції протоколу реалізуються через спеціальний заголовок АН, що включає кілька ключових полів. Поле Next Header вказує протокол більш високого рівня (наприклад, TCP, UDP або ICMP), чий трафік розміщено в IP-пакеті. Поле Payload Length визначає розмір заголовка АН. Поле Security Parameters Index (SPI) використовується для зв'язку пакета з відповідною безпечною асоціацією, а Sequence Number (SN) допомагає захиститися від повторного відтворення пакетів, використовуючи механізм ковзаючого вікна для зменшення навантаження на буферну пам'ять.



Рис. 14.15. Структура заголовку протоколу АН
Джерело: [2-4]

Одним із ключових компонентів заголовка є поле Authentication Data, яке містить значення перевірки цілісності пакета (Integrity Check Value, ICV). Це значення обчислюється за допомогою криптографічних хеш-функцій, наприклад, HMAC-SHA256 або HMAC-SHA3, які замінили

застарілі MD5 і SHA1. Для обчислення ICV використовується симетричний ключ, встановлений заздалегідь або автоматично через протокол управління ключами IKEv2.

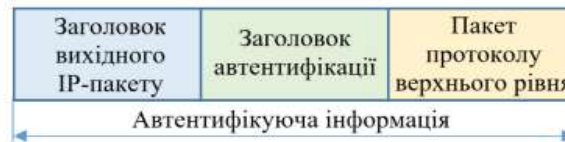


Рис. 14.16. Структура IP-паketу, обробленого протоколом АН в транспортному режимі

Джерело: [2-4]

АН підтримує два режими роботи: транспортний і тунельний. У транспортному режимі захищаються лише дані паketу, тоді як IP-заголовок залишається відкритим, що дозволяє маршрутизаторам виконувати свою роботу. У тунельному режимі весь оригінальний паket інкапсулюється у новий IP-заголовок, забезпечуючи повний захист, що є корисним для передачі даних через незахищені мережі.



Рис. 14.17. Структура IP-паketу, обробленого протоколом АН в тунельному режимі

Джерело: [2-4]



Рис. 14.18. Структура IP-паketу, обробленого протоколом ESP в транспортному режимі

Джерело: [2-4]

Протокол ESP (Encapsulating Security Payload), який також є частиною IPSec, забезпечує ширші можливості, ніж АН. Окрім аутентифікації та перевірки цілісності, ESP підтримує шифрування переданих даних, що захищає їх від несанкціонованого доступу. Заголовок

ESP містить поля SPI і SN, які передаються у відкритому вигляді, щоб можна було ідентифікувати асоціацію пакета і уникнути його повторного відтворення. У кінцевіку ESP розташовані поля для забезпечення цілісності та шифрування, а також заповнювач, який використовується для сумісності з алгоритмами шифрування, вирівнювання розміру пакета або приховування його реальної довжини.

ESP також підтримує транспортний і тунельний режими. У транспортному режимі дані пакета шифруються, але IP-заголовок залишається відкритим для маршрутизації. У тунельному режимі весь оригінальний IP-пакет шифрується і захищається, а новий IP-заголовок використовується для передачі даних.

Застосування протоколів АН і ESP є ключовим для побудови захищених VPN, мобільних мереж і хмарних середовищ. АН часто використовується там, де потрібна аутентифікація без шифрування, тоді як ESP забезпечує як аутентифікацію, так і конфіденційність. Завдяки сучасним криптографічним алгоритмам, таким як AES-GCM, IPSec залишається надійним рішенням для захисту мережевого трафіку в умовах постійно зростаючих кіберзагроз.

БАЗИ ДАНИХ SAD І SPD

Технологія IPSec пропонує широкий спектр методів захисту мережевого трафіку. IPSec може працювати як на хості, так і на шлюзі, визначаючи необхідний рівень захисту трафіку на основі двох ключових баз даних: бази безпечних асоціацій (SAD) та бази політики безпеки (SPD). Кожен вузол IPSec підтримує ці бази, щоб забезпечити ефективну обробку і захист даних.



Рис. 14.19. Структура IP-пакету, обробленого протоколом ESP в тунельному режимі

Джерело: [2-6]

База безпечних асоціацій (SAD) містить параметри для кожної активної асоціації, що встановлюються між вузлами. До таких параметрів належать тип і режим роботи протоколу (АН або ESP), методи шифрування, секретні ключі, поточні номери пакетів та інші

характеристики. SAD забезпечує збереження двох окремих наборів асоціацій — для вхідного і вихідного трафіку, що дозволяє незалежно обробляти трафік у двох напрямках.

База політики безпеки (SPD) відповідає за визначення правил обробки для IP-пакетів, що проходять через IPSec. SPD містить записи, які включають селектори пакета (IP-адреси, порти, тип транспортного протоколу, імена систем або користувачів) і політики безпеки для відповідних селекторів. На основі SPD IPSec приймає рішення про передачу пакета без змін, його відкидання або застосування захисних заходів.

При передачі пакета IPSec порівнює його параметри із селекторами в SPD. Якщо пакет відповідає заданим критеріям, застосовується політика безпеки, що може передбачати обробку засобами IPSec. У разі обробки пакет пов'язується з відповідним записом у SAD, який містить усі необхідні параметри безпечної асоціації.

Для захисту вихідного пакета IPSec використовує протоколи AH або ESP залежно від обраної політики. У полі SPI (Security Parameters Index) протокол вказує на запис у базі SAD, що зберігає параметри безпечної асоціації. Коли пакет досягає кінцевого вузла, значення SPI використовується для ідентифікації потрібної асоціації, після чого виконується дешифрування або перевірка цілісності. Цей механізм дозволяє ефективно ідентифікувати відповідні параметри для обробки пакета, забезпечуючи високий рівень захисту на кожному етапі передачі даних. Завдяки використанню SPI, система IPSec здатна забезпечити швидко і точно управління безпекою на основі поточної конфігурації та політик, що зберігаються в SAD.

У випадках, коли для пакета потрібна безпечна асоціація, але вона ще не існує, IPSec створює нову асоціацію за допомогою протоколу IKE (Internet Key Exchange), додаючи відповідні записи до баз SPD і SAD. Це забезпечує гнучке і динамічне управління безпекою для різних потоків трафіку. Протокол IKE здійснює обмін ключами між сторонами, що дозволяє створити безпечний канал для подальшої передачі даних. Після успішного завершення обміну ключами, SPD та SAD оновлюються для забезпечення відповідної політики безпеки та налаштувань аутентифікації для поточних і майбутніх з'єднань. Цей процес гарантує, що всі передані пакети відповідатимуть заданим вимогам безпеки, таким як шифрування, цілісність та автентичність даних. Таким чином, IPSec забезпечує надійний захист даних, враховуючи різноманітні потреби в безпеці при передаванні інформації через неспокійні або публічні мережі.

Використання баз даних SAD (Security Attributes Database) і SPD (Security Policy Database) є важливими аспектами в контексті забезпечення інформаційної безпеки в комп'ютерних мережах, особливо при реалізації систем, що підтримують політики безпеки на різних рівнях. SAD містить інформацію про безпекові атрибути, такі як рівні доступу, правила для користувачів і пристроїв, а також інші характеристики, що визначають, яким чином ресурси системи можуть бути доступні або змінені. Ці атрибути використовуються для авторизації доступу до даних і ресурсів, що дозволяє здійснювати контроль за доступом і запобігати несанкціонованому доступу.

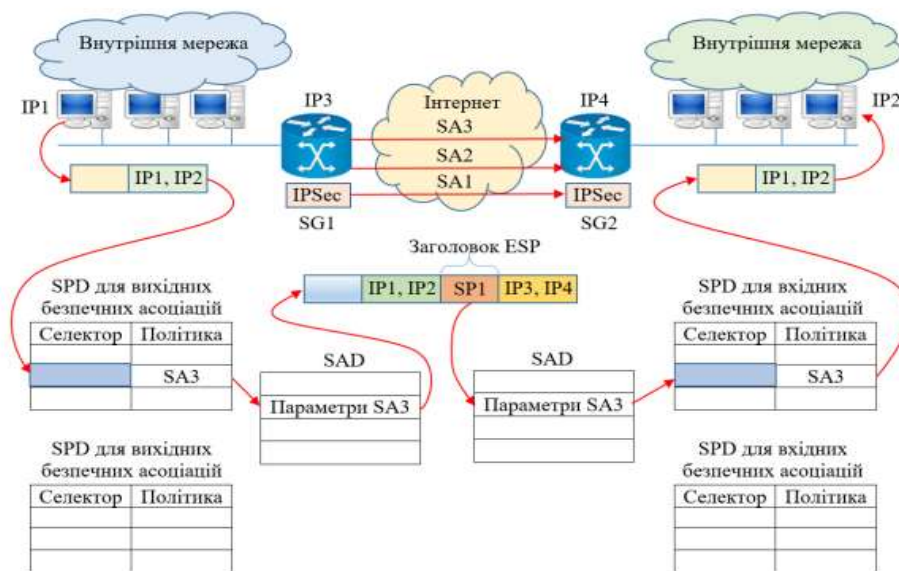


Рис. 14.20. Використання баз даних SAD і SPD

Джерело: [2-6]

SPD, з іншого боку, визначає політики безпеки, що описують, як саме дані повинні передаватися, захищатися і оброблятися в рамках мережі. Політика в SPD включає правила шифрування, аутентифікації, а також обробки трафіку, що проходить через мережу. Разом ці бази даних забезпечують необхідну інфраструктуру для підтримки політики безпеки і виконання її через всі етапи обробки даних, що є критично важливим для захисту інформації в сучасних мережах і системах.

Бази даних політики безпеки можуть створюватися вручну користувачем, системним адміністратором або автоматично за допомогою додатків. Для кожного нового пакета, що надходить до вузла, IPsec здійснює перевірку його параметрів на відповідність політиці безпеки, гарантуючи захист і цілісність даних відповідно до заданих правил.

Таким чином, поєднання баз SPD і SAD дозволяє гнучко і ефективно застосовувати механізм безпечних асоціацій у середовищі з датаграмним характером IP-трафіку. Це забезпечує високий рівень захисту, зберігаючи сумісність із традиційними мережевими протоколами та дозволяючи налаштовувати політики безпеки відповідно до потреб користувача чи адміністратора.

14.6. PGP (PRETTY GOOD PRIVACY)

PGP (Pretty Good Privacy) — це потужна комп'ютерна програма, яка реалізує криптографічні операції для забезпечення конфіденційності та цілісності даних, включаючи шифрування та цифрові підписи для повідомлень, файлів та іншої електронної інформації. Програма була розроблена Філіпом Цимерманом у 1991 році та з того часу стала однією з найвідоміших криптосистем для захисту інформації. Вона поєднує дві основні техніки криптографії: симетричне і асиметричне шифрування.

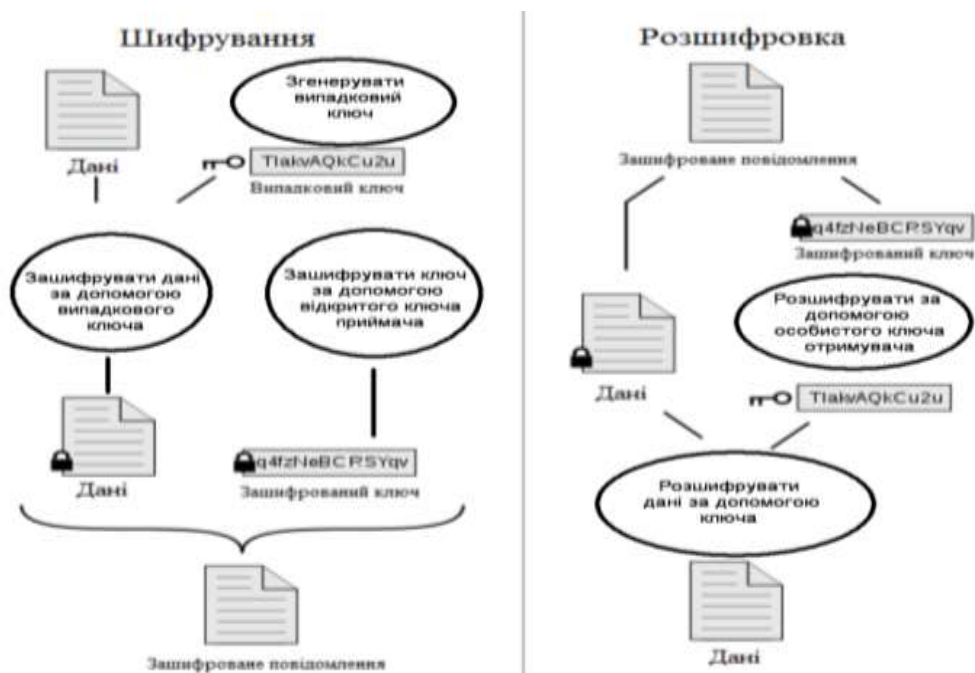


Рис. 14.21. Шифрування PGP

Джерело: [2-4]

Симетричне шифрування використовується для швидкого шифрування даних, де той самий ключ застосовується для шифрування та дешифрування, в той час як асиметричне шифрування застосовує пару ключів — відкритий і закритий, де відкритий ключ використовується для

шифрування, а закритий — для дешифрування. Цей підхід забезпечує безпечний обмін симетричними ключами через відкриті канали зв'язку.

Після того як дані стискаються, для їх шифрування генерується сеансовий симетричний ключ, який шифрується за допомогою відкритого ключа одержувача, і вже зашифроване повідомлення передається. Одержувач дешифрує сеансовий ключ за допомогою свого закритого ключа, а потім використовується цей ключ для дешифрування самого повідомлення.

PGP забезпечує високу безпеку завдяки використанню сучасних криптографічних алгоритмів, таких як RSA для шифрування та DSA для підписів. Це робить систему дуже надійною і стійкою до атак. Одним із важливих аспектів PGP є система довіри до відкритих ключів, яка дозволяє користувачам перевіряти автентичність ключів та підтверджувати їх справжність через підписи довірених осіб. В результаті, користувачі можуть безпечно обмінюватися повідомленнями без ризику того, що їхня інформація буде перехоплена або змінена під час передачі. Це дуже важливо для застосувань у галузях, де конфіденційність має вирішальне значення, таких як бізнес, урядові структури чи інші сектори з високими вимогами до безпеки.

Сьогодні PGP є відкритим стандартом, на основі якого створені реалізації, сумісні з іншими програмами, наприклад, GnuPG, FileCrypt тощо, завдяки стандарту OpenPGP (RFC 4880).

PGP використовує гібридну криптосистему, поєднуючи симетричне шифрування і криптографію з відкритим ключем для досягнення високого рівня безпеки та ефективності. Ключовою особливістю PGP є те, що він використовує стиснення даних перед їх шифруванням, що не тільки економить місце на диску, але й підвищує криптографічну стійкість, оскільки зменшується кількість ознак, що можуть бути використані в криптоаналізі.

Процес шифрування PGP починається з того, що дані стискаються, після чого створюється одноразовий сеансовий ключ для симетричного шифрування. Цей сеансовий ключ зашифровується за допомогою відкритого ключа одержувача і передається разом з зашифрованими даними. Одержувач використовує свій закритий ключ для дешифрування сеансового ключа, а потім використовує його для розшифрування самих даних. Завдяки цьому комбінуванню симетричного і асиметричного шифрування PGP досягає високої швидкості обробки даних без втрати безпеки.

Криптографічна стійкість PGP базується на припущенні, що використовувані алгоритми стійкі до криптоаналізу за допомогою

сучасних обчислювальних потужностей. Наприклад, в ранніх версіях PGP використовувався алгоритм RSA для шифрування сеансових ключів, а також додавалися інші алгоритми, такі як IDEA.

Однією з важливих особливостей PGP є система довіри до ключів. Для кожного користувача існує набір довіри до інших ключів, що дозволяє визначати, чи можна вважати певний відкритий ключ справжнім або довіреним. Існують три рівні довіри: повна, часткова та відсутність довіри. Для кожного ключа також встановлюється рівень дійсності, що дозволяє оцінювати його надійність.

PGP підтримує різноманітні криптографічні алгоритми і має високу сумісність із сучасними стандартами. Однак для забезпечення максимальної безпеки рекомендується використовувати новітні версії PGP, оскільки старіші реалізації можуть мати уразливості.

PGP також надає потужні засоби для управління відкритими ключами, що дозволяє користувачам перевіряти їх справжність через фізичне отримання ключів або перевірку через довірених посередників. Ідентифікація відкритих ключів здійснюється через унікальні ідентифікатори, що допомагають уникнути помилок при використанні неправильних ключів для шифрування та розшифрування повідомлень.

На практиці PGP найчастіше використовується для шифрування електронної пошти та захисту файлів. Воно дозволяє захищати від несанкціонованого доступу повідомлення, що містять конфіденційну інформацію, а також забезпечувати цілісність файлів, запобігаючи їх підробці. Для зручності PGP інтегрується в багато поштових програм та систем для автоматизації процесу шифрування, що робить використання технології доступним навіть для людей без глибоких технічних знань. Крім того, PGP активно використовується для створення цифрових підписів, що дозволяють підтвердити авторство документів і забезпечити їх цілісність.

PGP стало основою для створення відкритого стандарту OpenPGP, який визначає формат ключів і повідомлень, що дозволяє різним реалізаціям PGP бути сумісними між собою. Один із найбільш популярних варіантів реалізації цього стандарту — це GnuPG (GNU Privacy Guard), який є безкоштовною альтернативою комерційним продуктам, таким як PGP. Використання OpenPGP дозволяє створювати інтегровані системи безпеки для захисту повідомлень, файлів і навіть цілого диска.

Сучасні реалізації PGP використовуються не лише для шифрування даних, але й для забезпечення безпеки в Інтернеті та захисту конфіденційної інформації в умовах зростаючих кіберзагроз. Це робить PGP важливим інструментом в арсеналі будь-якої організації чи особи, яка прагне забезпечити високу ступінь безпеки своїх електронних комунікацій.

Таким чином, PGP є потужним інструментом для забезпечення конфіденційності і цілісності електронної інформації, який активно використовується в сучасних системах безпеки для захисту даних від несанкціонованого доступу.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 14

1. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
2. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.
3. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.
4. Лахно В. А., Гусев Б. С., Блозва А. І. Касаткін Д. Ю., Осипова Т. Ю. (2020) Кластеризація ознак мережевих атак в задачах аналізу захищеності інформації. Кібербезпека: освіта, наука, техніка. № 1(9). С. 45–58.
5. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроектні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242.
6. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 68–83.
7. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 338–347.
8. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

9. A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.
10. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.
11. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.
12. O. Deineka, et al., Designing Data Classification and Secure Store Policy According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 398409.
13. I. Bogachuk, V. Sokolov, V. Buriachok, Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers, in: 5th International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (2018) 581–585.
14. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.
15. A. Carlsson, et al., Sustainability Research of the Secure Wireless Communication System with Channel Reservation, in: 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020).
16. F. Kipchuk, et al., Investigation of Availability of Wireless Access Points based on Embedded Systems, in: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (2019).
17. P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 169–176.
18. H. Shevchenko, et al., Information Security Risk Analysis SWOT, Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021) 309-317.
19. A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

20. Burov, et al., Cybersecurity in Educational Networks, *Advances in Intelligent Systems and Computing*, 359–364, 2020.

21. M. TajDini, V. Sokolov, P. Skladannyi, Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, in: *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics* (2021) 7–11.

22. M. TajDini, V. Sokolov, V. Buriachok, Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio, in: *8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science*, vol. 2386 (2019) 287–296

КОНТРОЛЬНІ ПИТАННЯ

1. Які основні сервіси безпеки реалізовані за допомогою програмних засобів?
2. Поясніть різницю між ідентифікацією, автентифікацією і авторизацією.
3. Які прийоми використовують для аутентифікації?
4. Які основні типи апаратних пристроїв аутентифікації використовуються для забезпечення безпеки інформаційних систем?
5. У чому полягає відмінність між апаратними і програмними засобами аутентифікації?
6. Як працюють смарт-картки і чим вони відрізняються від звичайних карток пам'яті?
7. Які основні переваги використання біометричних даних для аутентифікації користувачів?
8. Які основні види біометричних характеристик використовуються для аутентифікації, і як вони працюють?
9. Як відбувається процес верифікації користувача за допомогою біометричних параметрів?
10. Що таке цифровий сертифікат, і як він використовується для аутентифікації в інформаційних системах?
11. Які кроки включає процедура аутентифікації на основі цифрових сертифікатів?
12. Як система Kerberos забезпечує безпечну аутентифікацію через цифрові сертифікати?

13. Які переваги та обмеження існують у використанні цифрових сертифікатів у порівнянні з іншими методами аутентифікації, такими як паролі або біометрія?
14. Які особливості аутентифікації в системах електронного бізнесу B2C?
15. Які обов'язкові параметри використання парольної аутентифікації передбачені в політиці безпеки організації?
16. Як можна підвищити безпеку парольної системи аутентифікації?
17. Наведіть приклади пасивних і активних апаратних автентифікаторів.
18. У чому відмінність USB-токенів від OTP-токенів?
19. Що таке біометрія і які фізіологічні характеристики можуть використовуватися для аутентифікації?
20. Що відносять до поведінкових біометричних характеристик і в чому їх недоліки і переваги?
21. Як працює біометрична система аутентифікації?
22. У чому полягає різниця між біометричною ідентифікацією і біометричною автентифікацією?
23. Як система довіри в PGP забезпечує перевірку автентичності відкритих ключів і яку роль відіграє підпис довірених осіб у цьому процесі?
24. У чому полягають основні відмінності між симетричним та асиметричним шифруванням у контексті використання PGP для забезпечення конфіденційності повідомлень?
25. Дайте характеристику помилок, що виникають при роботі систем біометричної аутентифікації.
26. Як вирішити проблему аутентифікації для систем, де кількість користувачів вимірюється сотнями тисяч?
27. Як працюють системи централізованої аутентифікації?
28. У чому полягає концепція єдиного логічного входу SSO?
29. Як працює система аутентифікації Kerberos?

ТЕМА 5. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

РОЗДІЛ 15 ОСНОВНІ ПОНЯТТЯ І ЗАДАЧІ КРИПТОЛОГІЇ



15.1. Симетричні та асиметричні криптосистеми

15.2. Основи криптоаналізу

15.3. Методи стеганографії

15.4. Модель стеганосистеми

15.5. Поняття ЦВЗ та їх класифікація

15.6. Метод модифікації найменшого значущого біта

" Криптографія — це наука про перехід від незрозуміння до розуміння, що є фундаментальним для забезпечення конфіденційності та безпеки в будь-якій інформаційній системі."

Клод Шеннон

Криптографічний захист інформації є основою сучасної безпеки в цифровому світі, забезпечуючи конфіденційність, цілісність, автентичність та незаперечність даних. Він полягає в застосуванні математичних методів та алгоритмів для захисту інформації від несанкціонованого доступу, зміни або фальсифікації. Однією з головних цілей криптографії є забезпечення конфіденційності, тобто гарантоване збереження таємниці даних, які можуть бути доступні тільки авторизованим особам. Для цього застосовуються різні методи шифрування, які перетворюють відкритий текст у зашифровану форму, яку неможливо прочитати без наявності спеціального ключа.

Цілісність інформації також є важливою складовою криптографічного захисту, адже вона гарантує, що передані або збережені дані не були змінені або пошкоджені. Це досягається через використання механізмів хешування, які створюють унікальні цифрові підписи для кожного набору даних, що дозволяє виявити навіть найменші зміни в інформації.

Автентичність є наступним аспектом, який підтверджує достовірність джерела інформації та дозволяє переконатися, що повідомлення дійсно надійшло від того, хто заявлений. Для цього використовуються цифрові підписи, що підтверджують право особи на відправлення певних даних.

Незаперечність гарантує, що особа не зможе відмовитися від своїх дій, наприклад, від підписання документу або відправлення повідомлення, що важливо для юридичних та комерційних транзакцій. Це також забезпечується за допомогою цифрових підписів, що є невід'ємною частиною криптографічних систем.

У криптографії використовуються різні підходи, зокрема симетричне та асиметричне шифрування. В симетричному шифруванні один ключ застосовується як для шифрування, так і для дешифрування інформації, що є швидким, але вимагає безпечного обміну ключами між сторонами. Асиметричне шифрування використовує пару ключів — відкритий для шифрування і закритий для дешифрування, що дає додатковий рівень безпеки.

Завдяки криптографії, інформаційні системи можуть забезпечити високий рівень захисту даних, особливо в умовах, коли інформація передається через відкриті канали зв'язку, такі як інтернет. Це критично важливо для захисту особистої, фінансової та комерційної інформації, яка є основою сучасних цифрових технологій.

15.1. СИМЕТРИЧНІ ТА АСИМЕТРИЧНІ КРИПТОСИСТЕМИ

Історія криптографії тісно пов'язана з розвитком писемності, починаючи з античних часів. Спочатку її застосовували дипломати і військові для захисту повідомлень, а з розвитком технологій шифрування стали використовуватися механічні та електронні пристрої, такі як шифрмашини «Енігма». З 70-х років XX століття впроваджуються нові криптографічні методи на основі комп'ютерних технологій, зокрема стандарти DES та RSA. Сучасна криптографія застосовує математичні методи для перетворення інформації з використанням секретних параметрів. Основними напрямками криптології є криптографія та криптоаналіз. Криптографія займається розробкою алгоритмів для захисту

інформації, а криптоаналіз вивчає методи відновлення зашифрованої інформації без знання секретних параметрів.

Основні задачі криптографії включають забезпечення конфіденційності, контролю цілісності та автентичності даних, а також аутентифікацію та підтвердження авторства. Сучасні криптографічні системи включають симетричні системи, системи з відкритим ключем, а також протоколи для електронного підпису та розповсюдження ключів.

Криптологія — це наука, яка займається захистом інформації через її перетворення, використовуючи математичні методи. Вона включає два основних напрямки: криптографію та криптоаналіз, які мають протилежні цілі. Криптографія спрямована на розробку та застосування математичних методів для шифрування інформації, щоб захистити її від несанкціонованого доступу. Криптоаналіз, в свою чергу, займається дослідженням методів розшифровування зашифрованих даних, зокрема шляхом пошуку вразливих місць у криптографічних системах.

Сучасна криптографія активно розвивається у кількох напрямках, враховуючи нові виклики, зокрема зростаючу потребу в безпеці інформації через швидке розширення цифрових технологій. Вона охоплює як симетричні, так і несиметричні криптосистеми, кожна з яких має свої особливості та переваги. Криптографічні методи захисту є основою для забезпечення конфіденційності, цілісності, автентичності та доступності інформації. Вони використовують різні математичні та алгоритмічні методи для перетворення даних таким чином, щоб зробити їх непридатними для розшифровування або модифікації без відповідних ключів чи дозволу.

Криптосистеми — це сукупність алгоритмів, протоколів і процедур, які забезпечують захист інформації за допомогою криптографії. Вони використовуються для шифрування, автентифікації, хешування та інших операцій, що дозволяють захистити дані від несанкціонованого доступу, забезпечити їх цілісність і автентичність. Криптосистеми можуть бути класифіковані за різними ознаками, такими як тип шифрування (симетричне чи асиметричне), мета використання, складність обміну ключами та інші.

Однією з основних категорій є **симетричні криптосистеми**, де для шифрування та дешифрування використовується один і той самий ключ. Прикладом такої системи є DES (Data Encryption Standard) або AES (Advanced Encryption Standard). Ці криптосистеми швидкі й ефективні, але вимагають безпечного обміну ключами між сторонами, що є їх основним недоліком.

Асиметричні криптосистеми використовують пару ключів: публічний, який може бути відомим усім, і приватний, який зберігається у таємниці. Вони застосовуються для електронного підпису, захисту даних під час передачі, а також для протоколів обміну ключами, таких як RSA або ECC (Elliptic Curve Cryptography). Асиметричні системи дозволяють вирішити проблему обміну ключами, але часто мають більшу обчислювальну складність.

До додаткових елементів криптосистем належать протоколи обміну ключами, цифрові підписи, а також механізми для перевірки цілісності даних через хешування. Розвиток квантових обчислень ставить перед криптографією нові виклики, тому активно ведеться дослідження криптосистем, стійких до атак, здійснених за допомогою квантових технологій.

Основні криптографічні методи захисту

1. Шифрування — перетворення відкритого тексту в зашифрований, за допомогою певного алгоритму і ключа. Цей процес забезпечує конфіденційність переданої інформації, ускладнюючи доступ до неї стороннім особам. Шифрування може бути симетричним, коли один і той самий ключ використовується для шифрування і розшифрування, або асиметричним, коли для цих операцій використовуються різні ключі (публічний і приватний). У сучасних криптосистемах застосовуються складні алгоритми шифрування, які враховують різноманітні загрози і вразливості, щоб забезпечити високий рівень безпеки. Шифрування є важливим елементом інформаційної безпеки, використовуваним у багатьох сферах, від захисту особистих даних до забезпечення безпеки фінансових транзакцій.

✱ **Симетричне шифрування** (симетричні алгоритми) використовують один і той самий ключ для шифрування та розшифрування інформації. Це дає високий рівень продуктивності, але потребує безпечного каналу для передачі ключа. Приклади:

- ✓ **AES (Advanced Encryption Standard)** — один з найбільш використовуваних алгоритмів симетричного шифрування, який є стандартизованим і застосовується в багатьох системах захисту даних.
- ✓ **DES (Data Encryption Standard)** — застарілий, але історично важливий алгоритм.
- ✓ **Blowfish** — гнучкий алгоритм з варіативною довжиною ключа.
- ✓ **RC4** — поточний шифр потоку.

• **Несиметричне шифрування** (асиметричні алгоритми) використовує пару ключів — відкритий і закритий. Відкритий ключ використовується для шифрування даних, а закритий — для їх розшифрування. Це забезпечує безпечний обмін даними без необхідності передачі секретних ключів.

- ✓ RSA (Rivest-Shamir-Adleman) — класичний алгоритм, який ґрунтується на складності факторизації великих чисел.
- ✓ ECC (Elliptic Curve Cryptography) — ефективніший за RSA, оскільки забезпечує таку ж безпеку при менших розмірах ключа.

2. Хешування — перетворення даних (повідомлення) у фіксовану довжину "хеш-значення". Хешування застосовується для перевірки цілісності даних і використовується в цифрових підписах і зберіганні паролів. Цей процес є одностороннім, тобто з хеш-значення неможливо відновити оригінальні дані. Хеш-функції повинні бути стійкими до колізій, що означає, що два різних набори даних не повинні давати однакове хеш-значення. Хешування використовується для перевірки того, чи не були змінені дані при їх передачі або зберіганні. Також хеш-функції є важливим елементом у процесах криптографічної аутентифікації та забезпечення конфіденційності, оскільки вони дозволяють безпечно зберігати паролі та інші чутливі дані.

• **SHA (Secure Hash Algorithm)** — один з найпоширеніших алгоритмів для хешування. SHA-256, наприклад, використовується в системах криптовалют і блокчейн-технологіях.

• **MD5 (Message Digest Algorithm 5)** — старий, але швидкий алгоритм, хоча і вважається вразливим до атак на колізії.

3. Цифрові підписи — механізм, що дозволяє підтвердити автентичність та цілісність електронного документа або повідомлення. Цифровий підпис використовує асиметричне шифрування для створення підпису, який можна перевірити за допомогою публічного ключа. Цифровий підпис гарантує, що документ не було змінено після його підписання, оскільки будь-які зміни призведуть до порушення цілісності підпису. Підписувач створює цифровий підпис за допомогою свого приватного ключа, а отримувач може перевірити підпис, використовуючи публічний ключ підписувача. Цей механізм забезпечує не тільки автентичність документа, але й надає юридичну силу в багатьох країнах, що визнають цифрові підписи. Цифрові підписи широко використовуються в електронних договорах, фінансових операціях та при поданні офіційних запитів в електронному вигляді.

- ✱ Використовуються в протоколах електронної пошти (наприклад, PGP), у фінансових транзакціях, в юридичних та контрактних документах.

4. Аутентифікація за допомогою криптографії —

використання криптографічних методів для підтвердження особи користувача або системи. Цей процес дозволяє забезпечити безпеку доступу до інформаційних систем, запобігаючи несанкціонованому використанню. Аутентифікація може бути заснована на чотирьох основних факторах: знання (пароль, PIN), володіння (смарт-картка, токен), властивості (біометричні дані, відбитки пальців) або місце (геолокація). У криптографічних системах часто використовуються цифрові сертифікати або двофакторна аутентифікація, що забезпечує додатковий рівень захисту. Крім того, сучасні методи аутентифікації, такі як використання одноразових паролів (OTP) або технології блокчейн, дозволяють значно підвищити рівень безпеки у взаємодії користувачів з онлайн-сервісами. Для цього використовуються різні методи, такі як:

- ✱ **Цифрові сертифікати** — підтверджують ідентичність користувача або сервера в мережах, таких як HTTPS.
- ✱ **Біометричні методи** (відбитки пальців, сканування райдужної оболонки ока) у поєднанні з криптографічними технологіями для двофакторної аутентифікації.

5. Протоколи обміну ключами — методи безпечного обміну ключами між сторонами, які забезпечують конфіденційність під час передачі даних. Ці протоколи дозволяють двом сторонам домовитися про спільний секретний ключ, який буде використано для шифрування та розшифрування повідомлень. Один із найбільш відомих протоколів — це протокол Диффі-Хеллмана, який дозволяє двом сторонам створити спільний ключ, навіть не передаючи його безпосередньо по каналу зв'язку. Протоколи обміну ключами використовують складні математичні алгоритми, що забезпечують захист від атак, таких як атаки "посередника". Сучасні криптографічні системи, включаючи TLS/SSL для безпеки в Інтернеті, також використовують ці протоколи для безпечного встановлення з'єднань і забезпечення конфіденційності під час передачі даних.

- ✱ **Протокол Диффі-Хеллмана** — один з найстаріших методів для безпечного обміну ключами через незахищену мережу.
- ✱ **Протокол Еліптичних кривих Диффі-Хеллмана (ECDH)** — більш ефективний аналог традиційного протоколу Диффі-Хеллмана, який використовує еліптичні криві для забезпечення безпеки.

6. Захист каналів зв'язку (TLS/SSL) — криптографічний протокол для забезпечення безпеки комунікацій через Інтернет. Він використовує поєднання симетричного шифрування для передачі даних і асиметричного шифрування для обміну ключами. Протокол TLS/SSL забезпечує конфіденційність, автентичність та цілісність даних, що передаються між клієнтом і сервером. Під час встановлення з'єднання використовуються сертифікати, що підтверджують ідентичність сторін і дозволяють уникнути атак "посередника". Симетричне шифрування застосовується для швидкої передачі даних, тоді як асиметричне шифрування використовується лише для безпечного обміну ключами, що робить процес більш ефективним. Завдяки цьому протоколу користувачі можуть впевнено здійснювати онлайн-платежі, вводити особисті дані та використовувати інші сервіси, що вимагають високого рівня захисту інформації.

- **TLS (Transport Layer Security)** — сучасний стандарт для захисту передавання даних через Інтернет (веб-сайти HTTPS).
- **SSL (Secure Sockets Layer)** — застарілий протокол, що використовувався раніше, але зараз його замінено на TLS.

7. Блокування та захист даних на рівні диска — застосування криптографічних методів для захисту даних на фізичних носіях. Цей метод включає в себе шифрування всього диска або окремих файлів, що дозволяє забезпечити захист даних навіть у випадку фізичної крадіжки або втрати пристрою. Операційні системи, такі як Windows (BitLocker) і macOS (FileVault), використовують ці технології для автоматичного шифрування даних при завантаженні системи. Важливим аспектом є використання сильних паролів або апаратних засобів, таких як TPM (Trusted Platform Module), для забезпечення доступу до зашифрованих даних. Це дозволяє запобігти несанкціонованому доступу до конфіденційної інформації, навіть якщо злоумисник отримає фізичний доступ до пристрою.

- **BitLocker** (для Windows) та **FileVault** (для macOS) використовують повне шифрування дисків, забезпечуючи захист інформації від несанкціонованого доступу.

8. Мультфакторна аутентифікація (MFA) — технологія, яка поєднує кілька методів для підтвердження особи користувача. MFA зазвичай включає в себе комбінацію щонайменше двох із трьох основних факторів: щось, що знає користувач (пароль), щось, що має користувач (смартфон або токен), та щось, що є у користувача (біометричні дані, як-от відбиток пальця або розпізнавання обличчя). Такий підхід значно підвищує

безпеку, оскільки навіть якщо один із факторів зламано, доступ до системи все одно залишається захищеним. Мультфакторна аутентифікація використовується в багатьох критичних для безпеки сферах, таких як онлайн-банкінг, медичні записи та корпоративні мережі. Це дозволяє знизити ризики від фішинг-атак, викрадення паролів або інших форм несанкціонованого доступу. Це може бути поєднання:

- **Щось, що ви знаєте** (пароль, PIN),
- **Щось, що ви маєте** (смарт-карта, телефон),
- **Щось, що ви є** (біометричні дані).

Проблеми сучасної криптографії та їх вирішення

▲ Квантові обчислення

Вони здатні зламати традиційні криптографічні методи, такі як RSA і ECC, використовуючи алгоритм Шора для факторизації великих чисел та алгоритм Гровера для пошуку в ненаправлених базах даних. Тому активно розробляються нові методи, здатні витримати квантові атаки — це **квантова криптографія та квантово-стійкі алгоритми**.

▲ Загрози на етапі зберігання ключів

Один із найбільших ризиків криптографічних систем полягає в тому, що самі ключі можуть бути викрадені або втрачено через збої в безпеці. Тому використовуються **апаратні модулі безпеки (HSM)** для зберігання ключів у фізично захищених пристроях. Ці модулі забезпечують захист ключів від фізичних атак, таких як спроби витягнути їх з пристрою, а також захищають від несанкціонованого доступу. HSM використовуються не лише для зберігання ключів, але й для виконання криптографічних операцій, таких як підписання та шифрування, без необхідності виведення ключа на зовнішні пристрої. Це значно знижує ризик компрометації системи через злоумисників. Крім того, для забезпечення більшої безпеки часто використовують технології двофакторної аутентифікації або розподілені системи зберігання ключів. Водночас важливим аспектом є регулярне оновлення криптографічних ключів для запобігання їх витоку протягом тривалого використання. Багато сучасних криптосистем також включають механізми для автоматизованого моніторингу та управління безпекою ключів. Ці заходи дозволяють значно посилити стійкість криптографічних систем до можливих атак та злоумисних дій.

У разі симетричного шифрування створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал

зв'язку. Адресат, запустивши ту ж шифрувальну програму з отриманим ключем, зможе прочитати повідомлення. Симетричне шифрування не таке надійне, як несиметричне, оскільки ключ може бути перехоплений, але через високу швидкість обміну інформацією воно широко використовується, наприклад, в операціях електронної торгівлі.



Рис. 15.1. Симетричне шифрування

Джерело: [2-6]

Симетричні алгоритми шифрування поділяють на:

- **потоківі алгоритми**, які працюють побітно, де кожен біт відкритого тексту зашифровується відповідним бітовим потоком, згенерованим ключем. Потоківі шифри є швидкими і ефективними для шифрування даних в реальному часі (наприклад, при передачі голосу або відео). Вони є менш стійкими до атак, якщо ключ не змінюється регулярно. **RC4** — один з найбільш відомих поточкових алгоритмів, який раніше широко використовувався в протоколах SSL/TLS, але зараз вважається небезпечним через виявлені уразливості;

- **блокові алгоритми** розбивають відкритий текст на блоки фіксованої довжини (звичайно 64 біти), кожен з яких обробляється окремо. Це забезпечує більш високий рівень захисту і дозволяє реалізувати різноманітні режими роботи (наприклад, ECB, CBC).

- ✓ **DES (Data Encryption Standard)** — один із найстаріших і класичних алгоритмів для блокового шифрування, хоча зараз вважається застарілим через короткість ключа (56 біт).
- ✓ **Blowfish** — гнучкий алгоритм, який забезпечує захист за допомогою довжини ключа до 448 біт. Завдяки своїй простоті він часто використовується в програмах для захисту інформації.
- ✓ **IDEA (International Data Encryption Algorithm)** — алгоритм з довжиною ключа 128 біт, який часто застосовується в системах для захисту даних.
- ✓ **AES (Advanced Encryption Standard)** — найпоширеніший сучасний стандарт для симетричного шифрування, який використовує блоки

довжиною 128 біт і ключі 128, 192 або 256 біт. AES має високу швидкість та рівень захисту, тому широко використовується в криптографічних системах.

Алгоритми, у яких відкритий текст обробляється побітно, називаються потоковими алгоритмами або потоковими шифрами. В інших алгоритмах відкритий текст розбивається на блоки, що складаються з декількох біт. Такі алгоритми називаються блоковими або блоковими шифрами. У сучасних комп'ютерних алгоритмах блокового шифрування довжина блока звичайно складає 64 біти. Симетричні алгоритми у разі виявлення в них будь-яких слабкостей можуть бути дороблені шляхом внесення невеликих змін, а для несиметричних – така можливість відсутня. Симетричні алгоритми працюють значно швидше, ніж алгоритми з відкритим ключем. На практиці несиметричні алгоритми шифрування часто застосовуються в сукупності з симетричними алгоритмами: відкритий текст зашифровується симетричним алгоритмом, а секретний ключ цього симетричного алгоритму зашифровується на відкритому ключі несиметричного алгоритму. Такий механізм називають цифровим конвертом (digital envelope).

У симетричних криптоалгоритмах (DES, ДСТ, Blowfish, RC5, IDEA) для шифрування і розшифрування інформації використовується той же секретний ключ.

Перевагами таких алгоритмів є:

- простота програмної та апаратної реалізації;
- висока швидкість роботи в прямому і зворотному напрямках;
- забезпечення необхідного рівня захисту інформації під час використання коротких ключів.

Симетричні криптосистеми

Симетричне шифрування використовує один секретний ключ для шифрування та розшифрування інформації. Це один з найбільш швидких способів шифрування, але він має обмеження, адже передача ключа може стати уразливою, якщо канал зв'язку не є достатньо захищеним. Для підвищення безпеки ключі обираються з великого простору значень, щоб ускладнити їх розшифрування при перехопленні. Такі алгоритми, як DES (Data Encryption Standard), Blowfish, IDEA (International Data Encryption Algorithm), і AES (Advanced Encryption Standard), широко використовуються в різноманітних галузях, зокрема в банківській справі, електронній комерції та захисті корпоративних даних. Однак, навіть при високій складності ключів, проблема передачі ключа залишається важливою, оскільки він має бути захищений від перехоплення. Зазвичай для цього використовуються додаткові криптографічні протоколи, які

забезпечують безпечний обмін ключами, наприклад, через асиметричне шифрування або протоколи обміну ключами, такі як Diffie-Hellman. Іншою проблемою є необхідність зберігання ключа у безпечному місці, що додає складність в управлінні криптографічними системами. Однак при належному управлінні та використанні сильних ключів, симетричне шифрування залишається ефективним і швидким способом захисту даних.

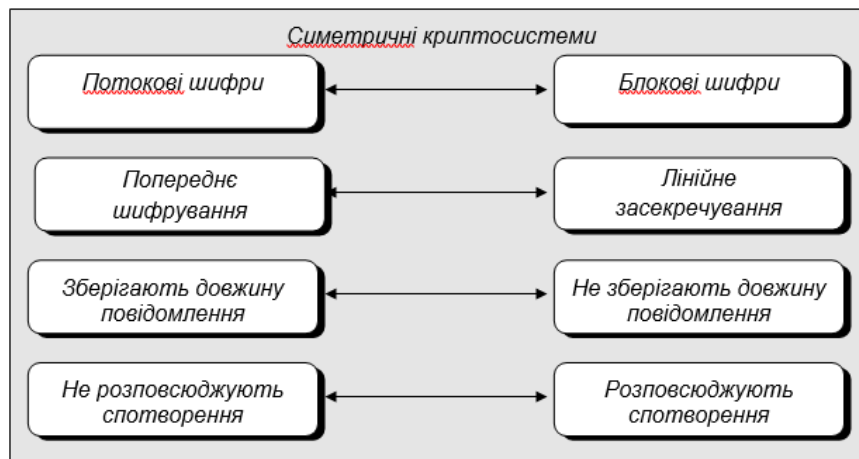


Рис. 15.2. Класифікація симетричних криптосистем

Джерело: [7-9]

Проте в умовах швидкого розвитку обчислювальних потужностей виникає необхідність удосконалення криптографічних алгоритмів, щоб вони залишалися стійкими до атак. Оновлення алгоритмів і їх довжини ключів є важливим етапом у забезпеченні безпеки, особливо в умовах глобальних загроз кібербезпеки.

Несиметричні криптосистеми

У несиметричних криптосистемах використовуються два ключі: відкритий і закритий. Відкритий ключ може бути доступний всім, хто бажає надіслати зашифроване повідомлення, а закритий — тільки власнику ключа, який може розшифрувати отримане повідомлення. Це дозволяє забезпечити високий рівень безпеки без необхідності передачі секретних ключів через відкриті канали зв'язку. Класичними прикладами несиметричного шифрування є алгоритм **RSA** (Rivest-Shamir-Adleman), **ECC** (Elliptic Curve Cryptography) і **PGP** (Pretty Good Privacy), які забезпечують стійкість до сучасних атак.

Розвиток квантових обчислень може стати серйозним викликом для традиційних несиметричних криптосистем, оскільки квантові комп'ютери здатні розв'язувати математичні задачі значно швидше, ніж класичні

комп'ютери. Це може зробити актуальним питання переходу до нових криптографічних методів, зокрема квантової криптографії.

Несиметричне шифрування складніше, але і надійніше. Для його реалізації потрібні два взаємозалежних ключі: відкритий і закритий. Одержувач повідомляє всім, хто бажає, свій відкритий ключ, що дозволяє шифрувати для нього повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення. Коли комусь потрібно послати зашифроване повідомлення, він виконує шифрування, використовуючи відкритий ключ одержувача. Одержавши повідомлення, останній розшифровує його за допомогою свого закритого ключа. Підвищена надійність несиметричного шифрування потребує складнішого обчислення, тому процедура розшифровки займає більше часу.

Коли надійність криптографічного алгоритму забезпечується за рахунок збереження в таємниці суті самого алгоритму, такий алгоритм шифрування називається обмеженим. Обмежені алгоритми становлять значний інтерес з погляду історії криптографії, однак зовсім непридатні у сучасних вимогах, які висуваються до шифрування. Адже, в цьому разі, кожна група користувачів, які бажають обмінюватися секретними повідомленнями, повинна мати свої оригінальні алгоритми шифрування.



Рис. 15.3. Несиметричне шифрування

Джерело: [2-6]

У сучасній криптографії зазначені вище проблеми вирішуються за допомогою використання ключа, який потрібно вибирати серед значень, що належать безлічі (ключовий простір). Функції шифрування і розшифрування залежать від цього ключа. Деякі алгоритми шифрування використовують різні ключі для шифрування і розшифровування. Це означає, що ключ шифрування відрізняється від ключа розшифровування.

Надійність алгоритму шифрування з використанням ключів досягається за рахунок їх належного вибору і наступного збереження в секреті. Це означає, що такий алгоритм не потрібно тримати в таємниці. Можна організувати масове виробництво криптографічних засобів, в

основу функціонування яких покладений цей алгоритм. Навіть знаючи криптографічний алгоритм, зловмисник не зможе прочитати зашифровані повідомлення, оскільки він не знає секретний ключ, використаний для його зашифровування

Аутентифікація та цілісність інформації

Аутентифікація та цілісність інформації є важливими аспектами забезпечення безпеки в інформаційних системах. Аутентифікація — це процес підтвердження особи або системи, який гарантує, що користувач або сервіс є тим, за кого себе видає. Вона може бути здійснена за допомогою різних методів, таких як паролі, біометричні дані, токени, або криптографічні ключі. Цілісність інформації забезпечується шляхом перевірки, що дані не були змінені під час передачі або зберігання. Для досягнення цілісності використовуються механізми хешування, цифрових підписів або контрольних сум, які дозволяють виявити несанкціоновані зміни в даних. Важливим аспектом є використання криптографії для забезпечення як аутентифікації, так і цілісності, адже зловмисники можуть намагатися підробити або змінити інформацію в процесі її передачі. Таким чином, аутентифікація та цілісність є основними компонентами криптографічного захисту, що гарантують безпеку комунікацій та збереження даних у цифровому середовищі.

Одним з ключових аспектів сучасної криптографії є забезпечення аутентифікації та цілісності повідомлень. Аутентифікація гарантує, що повідомлення дійсно надійшло від заявленого відправника. Для цього використовуються різноманітні методи, включаючи смарт-карти, біометрію, криптографічні протоколи та цифрові підписи. Технології, такі як мультфакторна аутентифікація (MFA), активно використовуються для підвищення рівня безпеки доступу до систем.

Ці методи забезпечують надійну перевірку особи та захист від несанкціонованого доступу. Крім того, криптографія грає важливу роль у забезпеченні цілісності даних, що передаються через незахищені канали зв'язку. Для цього застосовуються хеш-функції та коди автентифікації повідомлень (MAC), що дозволяють перевірити, чи не були дані змінені під час передачі. Механізми хешування забезпечують унікальне представлення даних і використовуються для перевірки їх цілісності без необхідності зберігати самі дані. Впровадження криптографічних протоколів, таких як TLS/SSL, дозволяє забезпечити захищене з'єднання в Інтернеті та захистити передану інформацію від атак типу "man-in-the-middle". Сучасні криптографічні системи також підтримують можливість відновлення доступу до даних у випадку втрати ключів через використання резервних ключів або механізмів відновлення паролів.

Таким чином, криптографія є основним інструментом для захисту особистої, комерційної та державної інформації в цифрову епоху.

Цілісність повідомлень забезпечується через застосування контрольних сум (наприклад, MAC — Message Authentication Code) або електронно-цифрових підписів (ЕЦП). Ці технології дозволяють перевірити, чи не було змінено дані в процесі їх передачі, що особливо важливо в умовах передавання важливих або конфіденційних даних через відкриті канали зв'язку.

Контрольні суми, зокрема MAC, обчислюються за допомогою криптографічних алгоритмів, які дозволяють створити унікальну перевірку для кожного повідомлення на основі його вмісту. Це дозволяє приймаючій стороні перевірити, чи не було змінено повідомлення під час передачі. Електронно-цифрові підписи забезпечують ще більш високий рівень захисту, оскільки вони не тільки гарантують цілісність, а й підтверджують авторство повідомлення. Підписане повідомлення можна перевірити за допомогою публічного ключа відправника, що додає додаткову гарантію надійності. Ці технології використовуються у різноманітних сферах, від фінансових транзакцій до юридичних документів, забезпечуючи захист від підробок. Вони також застосовуються в системах електронної пошти, онлайн-банкінгу та інших критичних для безпеки сферах. Використання таких механізмів дозволяє створювати надійні захищені канали для передавання даних, що особливо актуально в умовах постійного розвитку кіберзагроз.

Біометричні системи ідентифікації використовують унікальні фізичні або поведінкові характеристики людини для підтвердження її особи. Це один з найбільш надійних методів аутентифікації, оскільки біометричні ознаки важко підробити або передати іншій особі. До основних біометричних характеристик, що використовуються в таких системах, належать відбитки пальців, розпізнавання обличчя, райдужка ока, геометрія руки, голос, а також поведінкові ознаки, такі як стиль набору тексту чи хода. Перевагою біометричних систем є те, що для підтвердження особи не потрібно запам'ятовувати паролі або носити додаткові пристрої, як, наприклад, смарт-карти чи токени. Однак, хоча такі системи забезпечують високий рівень безпеки, вони не є абсолютно захищеними, оскільки можливі випадки фальсифікації або крадіжки біометричних даних. Тому для покращення безпеки часто застосовують комбіновані підходи, такі як мультфакторна аутентифікація, де біометрія поєднується з іншими методами підтвердження особи (наприклад, паролями чи токенами).

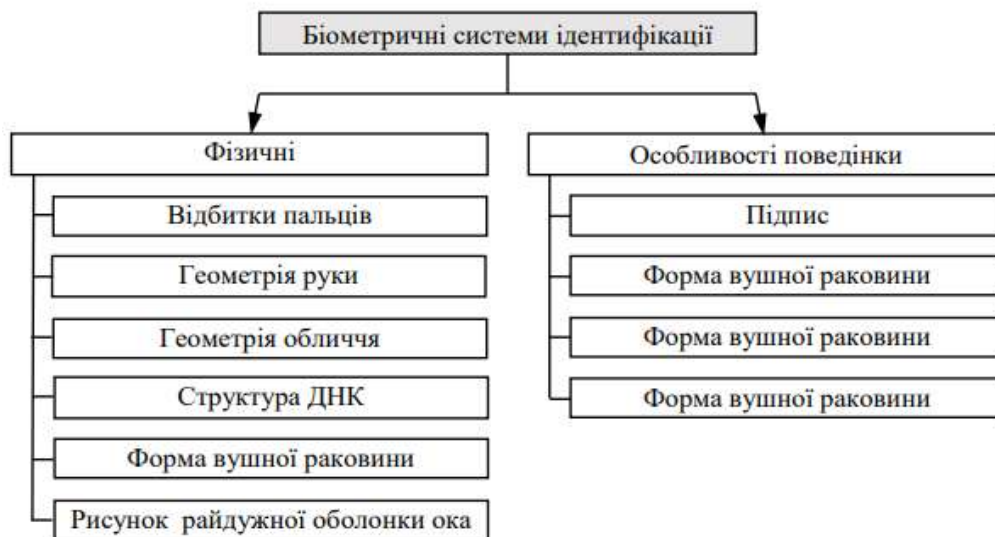


Рис. 15.4. Біометричні системи ідентифікації

Джерело: [6-9]

Біометричні системи широко використовуються у різних сферах, включаючи фінансові послуги, доступ до будівель, мобільні пристрої та навіть у правоохоронних органах для ідентифікації осіб. Однак важливими питаннями для їх впровадження є захист персональних даних і конфіденційність, адже біометрична інформація є дуже чутливою і її використання може викликати етичні та юридичні питання.

Сучасні криптографічні методи

Сучасні криптографічні методи ґрунтуються на використанні складних математичних алгоритмів для забезпечення безпеки передавання та зберігання інформації. До основних методів криптографії належать:

1. **Шифрування з симетричним ключем** — у цьому методі для шифрування та дешифрування використовується один і той самий ключ. Прикладами є алгоритми AES (Advanced Encryption Standard) і DES (Data Encryption Standard), які забезпечують високу швидкість обробки даних та використовуються для захисту конфіденційної інформації. Шифрування з симетричним ключем зазвичай має високу ефективність, оскільки використовується один ключ для обох операцій, що робить процес швидким і економічним. Однак його головним недоліком є необхідність безпечного обміну ключем між сторонами до початку передачі даних, оскільки той самий ключ повинен бути збережений у таємниці. Для підвищення безпеки у великих системах використовуються методи генерації ключів, такі як алгоритми обміну ключами (наприклад, Diffie-Hellman). Важливою характеристикою сучасних алгоритмів є їх стійкість

до атак, що дозволяє забезпечувати конфіденційність даних навіть при використанні потужних обчислювальних ресурсів для криптоаналізу.

2. Шифрування з асиметричним ключем — цей метод використовує пару ключів: публічний (для шифрування) і приватний (для дешифрування). Протоколи, такі як RSA, використовують цю модель для забезпечення безпеки в Інтернеті, зокрема для електронного підпису та захисту електронної пошти. Асиметричне шифрування дозволяє уникнути проблем з безпечним обміном ключами, оскільки публічний ключ можна передавати відкрито, тоді як приватний залишається в секреті. Однак цей метод є більш повільним порівняно з симетричним шифруванням, тому часто використовується у поєднанні з симетричними алгоритмами для шифрування даних. У таких випадках асиметричне шифрування застосовується для захисту ключа симетричного алгоритму, який потім використовується для шифрування великого обсягу даних. Крім RSA, існують і інші алгоритми асиметричного шифрування, такі як ECC (Elliptic Curve Cryptography), які забезпечують більшу безпеку при меншій довжині ключів.

3. Хешування — процес перетворення вхідних даних у фіксовану довжину хеш-коду, який є унікальним для кожного набору вхідних даних. Це дозволяє ефективно перевіряти цілісність даних без потреби зберігати їх у незмінному вигляді. Алгоритми, як SHA (Secure Hash Algorithm), використовуються для перевірки цілісності даних. Хешування є незворотним процесом, тобто неможливо відновити оригінальні дані з хеш-коду, що додає рівень безпеки при зберіганні чутливих даних, таких як паролі. Хеш-коди використовуються також у цифрових підписах, де вони гарантують, що підписаний документ не був змінений після підписання. Залежно від потреб безпеки та швидкості, використовуються різні варіанти хеш-алгоритмів, наприклад, SHA-256 або SHA-3, які забезпечують високий рівень стійкості до колізій. Крім того, хешування є основою для створення механізмів перевірки цілісності файлів, що широко застосовується в криптовалютах та блокчейн-технологіях.

4. Цифрові підписи — забезпечують аутентифікацію та цілісність даних за допомогою криптографічного підпису, який можна перевірити за допомогою публічного ключа. Цей метод активно використовується для підтвердження авторства електронних документів. Цифрові підписи забезпечують юридичну силу та довіру до електронних транзакцій, дозволяючи сторонам перевіряти справжність підписаних документів. Вони використовуються в різних сферах, таких як електронний уряд, фінансові операції та правові контракти. Цифровий підпис забезпечує також захист від підробки, оскільки будь-яка зміна в документі призведе

до порушення підпису. Для створення цифрового підпису використовуються приватні ключі, а для його перевірки — публічні ключі, що дозволяє підтвердити достовірність та цілісність документів.

5. Криптографічні протоколи — використовуються для безпечного обміну даними через незахищені канали, такі як Інтернет. Протоколи TLS (Transport Layer Security) та SSL (Secure Sockets Layer) забезпечують захищене з'єднання для передачі чутливих даних, наприклад, при здійсненні фінансових операцій через Інтернет. Ці протоколи забезпечують конфіденційність, цілісність та автентичність даних під час їх передачі, захищаючи від атак типу "man-in-the-middle" та інших загроз. Вони використовують поєднання симетричного та асиметричного шифрування для забезпечення безпеки з'єднання. Протокол TLS є оновленою та більш безпечною версією SSL, з більш сильними алгоритмами шифрування і механізмами перевірки. Сучасні криптографічні протоколи активно застосовуються не лише для захисту веб-сайтів, а й для забезпечення безпеки електронної пошти, VPN-з'єднань та інших критичних комунікацій.

6. Мультифакторна аутентифікація (MFA) — поєднує кілька методів перевірки особи, таких як пароль, смарт-карти або біометричні дані, для підвищення рівня безпеки доступу до систем. Цей підхід значно знижує ймовірність несанкціонованого доступу, оскільки зломисник повинен отримати кілька факторів одночасно. Мультифакторна аутентифікація активно використовується в фінансових установах, корпоративних мережах та в інших чутливих сферах, де безпека є пріоритетом. Одним з поширених варіантів MFA є поєднання пароля з кодом, що генерується на мобільному пристрої або за допомогою додаткового апаратного пристрою. MFA також зменшує ризик атак, таких як фішинг або крадіжка паролів, оскільки зломиснику не достатньо лише одного методу доступу для проникнення в систему.

Ці методи активно використовуються в електронних платіжних системах, банківських додатках, системах електронного підпису та інших сферах, що потребують високого рівня захисту даних.

Сучасні криптографічні системи мають ряд важливих вимог:

1. Конфіденційність

Зашифроване повідомлення має бути доступне тільки для тих, кому воно призначене.

2. Цілісність

Забезпечується точність та достовірність інформації, що передається, а також захист від будь-яких спроб модифікації.

3. Доступність

Інформація повинна бути доступна для користувачів, коли вона необхідна.

У сучасному цифровому світі основними проблемами криптографії є забезпечення криптостійкості шифрів навіть перед потужними комп'ютерами, а також захист від нових видів атак, зокрема **квантових атак**. Зараз активно розвиваються нові алгоритми, здатні протистояти цим загрозам, серед яких **квантова криптографія** та **квантові ключі обміну**.

Програмні та апаратні засоби захисту

Криптографія може реалізовуватися як програмно, так і апаратно. Програмне шифрування є більш гнучким та дешевим варіантом, але має свої обмеження щодо швидкості та захищеності. Апаратне шифрування використовує спеціалізовані пристрої (наприклад, HSM — Hardware Security Module) для захисту ключів і забезпечення високої продуктивності, однак його вартість є значною.

Сьогодні також активно розвиваються програмні рішення для захисту хмарних сервісів, що використовують шифрування всіх даних, зберігання ключів в безпечних контейнерах та використання мультфакторної аутентифікації для додаткового захисту.

Криптологія залишається важливою складовою сучасних систем інформаційної безпеки. З огляду на нові виклики та технології, важливість криптографії не зменшується, а, навпаки, зростає. Завдяки розвитку нових методів шифрування та аутентифікації, сучасні криптографічні системи здатні забезпечити високу стійкість перед різноманітними атаками, включаючи ті, що здійснюються за допомогою квантових комп'ютерів.

Принципи застосування комбінацій симетричних та несиметричних алгоритмів

Для досягнення оптимальної безпеки, на практиці використовують комбінацію **симетричного** та **несиметричного шифрування**. Це часто називають **цифровим конвертом** (digital envelope):

1. Відкритий текст шифрується **симетричним алгоритмом** (наприклад, AES).
2. **Секретний ключ** для симетричного шифрування зашифровується за допомогою **несиметричного алгоритму** (наприклад, RSA).
3. Отримана зашифрована інформація передається до отримувача, який розшифровує секретний ключ за допомогою свого приватного ключа і використовує його для розшифрування основного повідомлення.

Переваги та недоліки симетричних алгоритмів

- **Переваги:**
 - ✓ **Швидкість роботи** — алгоритми симетричного шифрування, як правило, значно швидші за несиметричні.

- ✓ **Простота реалізації** — їх можна реалізувати як програмно, так і апаратно.
- ✓ **Низькі вимоги до обчислювальних ресурсів** — це робить їх ідеальними для використання в умовах, де важлива висока продуктивність і низьке споживання ресурсів.
- **Недоліки:**
 - ✓ **Проблеми безпеки ключів** — основна проблема симетричного шифрування полягає в безпеці зберігання і передачі секретного ключа.

Використання цифрових підписів і захисту каналу зв'язку

Використання цифрових підписів і захисту каналу зв'язку є важливими аспектами забезпечення безпеки в сучасних інформаційних системах. Цифрові підписи забезпечують аутентифікацію та цілісність даних, гарантуючи, що інформація не була змінена після підписання і дійсно надходить від вказаного відправника. Вони використовують криптографічні алгоритми, такі як RSA або ECDSA (Elliptic Curve Digital Signature Algorithm), для створення унікального підпису, який можна перевірити за допомогою публічного ключа. Завдяки цифровим підписам можна ефективно захищати електронні документи, контракти та інші чутливі дані від несанкціонованих змін.

Захист каналу зв'язку забезпечується через використання криптографічних протоколів, таких як SSL/TLS, які створюють зашифроване з'єднання між клієнтом і сервером. Це забезпечує конфіденційність та захист від перехоплення даних під час їх передачі через незахищені канали, наприклад, Інтернет. При використанні SSL/TLS з'єднання між користувачем і сервером шифрується, а також проводиться верифікація серверу через цифрові сертифікати, що знижує ризики підробки та атак типу "людина посередині". В результаті, комбінація цифрових підписів і захищених каналів зв'язку дає потужний механізм для забезпечення безпеки при здійсненні електронних транзакцій та обміні конфіденційною інформацією.

Для додаткового захисту, особливо в Інтернеті, використовують протоколи для забезпечення цілісності та автентичності переданої інформації:

- ➔ **PGP (Pretty Good Privacy)** — застосовує комбінацію симетричних та несиметричних алгоритмів для шифрування електронної пошти та файлів. Це дозволяє користувачам обмінюватися зашифрованими повідомленнями, гарантуючи їх конфіденційність та автентичність.

- ➔ SSL/TLS — для захисту даних у мережі Інтернет використовуються ці протоколи, які застосовують комбінацію симетричного і несиметричного шифрування для забезпечення безпеки з'єднання між клієнтом і сервером (наприклад, при використанні HTTPS для веб-сайтів).

Сучасні криптографічні методи продовжують еволюціонувати, адаптуючись до нових загроз і технологічних змін. Симетричні алгоритми забезпечують швидке і ефективне шифрування, але вони потребують безпеки ключів. Тому сучасні системи часто поєднують симетричне шифрування для швидкої обробки даних і несиметричне для забезпечення безпечного обміну ключами.

Принцип Керкхгоффа

Принцип Керкхгоффа, сформульований у 1883 році Агустом Керкхгоффсом, є основоположним для сучасної криптографії. Він стверджує, що єдиним секретом у криптографічній системі має бути ключ, а сам алгоритм шифрування не повинен бути прихованим або секретним. Це важлива ідея, яка не втратила своєї актуальності і в сучасному криптографічному середовищі. Керкхгоффс підкреслив, що навіть якщо алгоритм відомий публічно, система буде безпечною, якщо ключ залишатиметься конфіденційним. Сучасні криптографи підтримують цей принцип, оскільки він дозволяє забезпечити стійкість системи до атак, навіть якщо алгоритм шифрування стає доступним для потенційних злоумисників.

Принцип Керкхгоффа також запобігає небезпеці, яка може виникнути, якщо система намагається заховати не тільки ключ, але й алгоритм шифрування, що призводить до так званої "безпеки через неясність". Такий підхід вважається застарілим і ненадійним, оскільки навіть якщо алгоритм працює правильно, загроза виникає через компрометацію секретів або можливість їх отримання через уразливості системи. Система, яка покладається на секретність алгоритму, може мати більше точок для атаки, що робить її менш стабільною і надійною.

Згідно з принципом Керкхгоффа, чим менше секретів містить система, тим вона безпечніша. Кількість таємниць, що використовуються для підтримки безпеки, створює додаткові уразливості, і кожен таємний елемент збільшує потенційний ризик компрометації. Сучасні криптографічні системи зосереджені на використанні перевірених публічних алгоритмів і надійних механізмів захисту ключів. Такий підхід дозволяє зменшити кількість точок атаки та забезпечити більшу стійкість

систем до зовнішніх загроз. В результаті, цей принцип сприяє розвитку більш відкритих, прозорих і надійних криптографічних систем, що знижують потенційні ризики, пов'язані з утриманням секретів.

15.2. ОСНОВИ КРИПТОАНАЛІЗУ

Криптоаналіз (від грецького *κρυπτός* — прихований і *ανάλυσις* — аналіз) — це наука, що вивчає методи розшифровки зашифрованої інформації без наявності ключа, призначеного для цієї розшифровки. Термін був введений американським криптографом Уільямом Ф. Фрідманом в 1920 році. Криптоаналіз також часто неформально називають «зломом шифру». Основна мета криптоаналізу — з'ясувати ключ або виявити уразливості криптографічних алгоритмів чи протоколів, що використовуються для захисту інформації.

На початкових етапах криптоаналіз був заснований на лінгвістичних закономірностях природного тексту, і для цього використовувалися прості інструменти, такі як олівець і папір. Однак з розвитком комп'ютерних технологій, криптоаналіз став набагато більш складним і математичним, з використанням спеціалізованих комп'ютерних систем для розшифровки та виявлення уразливостей в алгоритмах шифрування.

Криптографічні атаки, що виникають внаслідок криптоаналізу, мають на меті розкрити шифр або знайти уразливості в алгоритмах, які забезпечують захист даних.

Криптоаналіз — це процес вивчення криптографічних систем з метою виявлення слабкостей або методів, які дозволяють розкодувати зашифровану інформацію без доступу до секретного ключа. Основною метою криптоаналізу є розробка методів, які дозволяють відновити оригінальний текст (plain text) або ключ з зашифрованого повідомлення. Він є важливою складовою частиною криптографії, оскільки допомагає виявити вразливості у використаних алгоритмах шифрування, що дозволяє покращувати їх безпеку.

Існує кілька типів криптоаналізу:

1. **Криптоаналіз за допомогою перебору (brute-force attack)** — це метод, коли криптоаналітик перевіряє всі можливі варіанти ключів, щоб знайти правильний. Оскільки метод вимагає великих обчислювальних ресурсів, він є неефективним для довгих та складних ключів. Криптоаналіз за допомогою перебору є одним із найстаріших методів атаки на криптографічні системи, проте його ефективність знижена при використанні достатньо довгих і складних ключів. З розвитком

комп'ютерних технологій і зокрема паралельних обчислень, метод перебору став менш практичним для сучасних алгоритмів, таких як AES, де для правильного розшифрування ключів необхідно витратити невідповідно велику кількість часу. Зважаючи на це, більшість сучасних криптографічних систем проектується так, щоб бути стійкими до перебору, використовуючи довгі ключі та ускладнюючи перебір можливих варіантів. Однак, навіть за таких умов, атака через перебір все ще залишається можливим методом для деяких застарілих або неправильно реалізованих шифрів.

2. **Криптоаналіз на основі статистики (statistical analysis)** — цей метод ґрунтується на аналізі частотного розподілу символів у шифрованому повідомленні. Використовується для криптосистем, які не використовують додаткових методів шифрування або відхилення стандартних шаблонів. Криптоаналіз на основі статистики є ефективним для атак на деякі прості методи шифрування, такі як шифр Цезаря або інші типи шифрів з заміною, де букви замінюються на інші відповідно до певного шаблону. Аналіз частотного розподілу символів у шифрованому тексті дозволяє криптоаналітику виявити закономірності, що існують у мові, і за допомогою цих закономірностей зламати шифр. Особливо ефективний цей метод, коли зашифроване повідомлення велике і має багато повторюваних елементів, що дозволяє виявити співвідношення між шифрованими та звичайними літерами. Для підвищення безпеки в сучасних криптографічних системах використовуються складніші методи шифрування, такі як заміна на основі ключа або поліалфавітні шифри, що робить цей метод менш ефективним.

3. **Криптоаналіз за допомогою диференційного аналізу (differential cryptanalysis)** — це метод виявлення слабких місць у шифрувальних алгоритмах шляхом порівняння різниць між вхідними та вихідними значеннями для зашифрованих блоків. Цей метод базується на вивченні зміни вихідного тексту при зміні певних вхідних значень, що дозволяє виявити закономірності, які можуть бути використані для розшифрування повідомлень. Диференційний аналіз активно застосовується до симетричних шифрів, таких як DES та AES, де вивчаються зміни в результаті застосування конкретних операцій заміни та перестановки. Зазначений метод дозволяє криптоаналітикам розкрити ключі або знайти інші вразливості, що знижують ефективність шифрування. Для захисту від диференційного аналізу розробники сучасних шифрів застосовують складні операції, включаючи використання більш складних алгоритмів, зокрема з використанням кількох раундів шифрування та змішаних перетворень.

4. **Криптоаналіз за допомогою лінійного аналізу (linear cryptanalysis)** — аналогічний до диференційного аналізу, але з використанням лінійних апроксимацій між вихідними значеннями. Цей метод полягає у виявленні лінійних зв'язків між вихідними і вхідними даними шифрованого тексту, що дозволяє зменшити складність розкриття ключа. Лінійний аналіз, як і диференційний, активно застосовується до класичних симетричних шифрів, таких як DES, де шукаються спрощення у складних нелінійних функціях, що використовуються при шифруванні. Основна ідея полягає в побудові лінійних апроксимацій, які описують як вхідні бітові комбінації корелюють з вихідними. Для протидії такому аналізу криптографи вводять додаткові елементи хаотичності та складності в алгоритми шифрування, що ускладнює встановлення лінійних залежностей.

5. **Атака через уразливості в програмному забезпеченні (side-channel attacks)** — цей тип атаки орієнтований на вивчення фізичних властивостей криптографічних пристроїв або програм, таких як час виконання операцій, споживана потужність або радіоактивні випромінювання. Такі атаки дозволяють здобувати інформацію про секретні ключі або інші конфіденційні дані без необхідності порушення математичних принципів шифрування. Один із поширених прикладів — це аналіз часу виконання операцій, де навіть мілісекунди, витрачені на обчислення, можуть розкрити частину інформації про ключ. Інші види таких атак включають вимірювання споживаної потужності або аналіз електромагнітних випромінювань, що виходять від пристрою під час виконання криптографічних операцій. Для протидії цьому типу атак використовують техніки шифрування, що мінімізують варіації часу виконання або споживаної потужності, а також додаткові засоби захисту, такі як екранування або маскування сигналів.

Криптоаналітики використовують ці методи для тестування та вдосконалення криптографічних алгоритмів, оскільки їх ефективність прямо залежить від того, наскільки стійким є алгоритм до аналізу і намагань зламати захист. Сучасний криптоаналіз, завдяки розвитку обчислювальних потужностей, займається пошуком нових підходів до захисту від атак, враховуючи можливості новітніх технологій, таких як квантові обчислення.

Серед основних методів криптоаналізу, що описав Брюс Шнайер, можна виділити такі види атак:

1. *Атака на основі шифротексту*

Атака на основі шифротексту часто базується на порівнянні кількох зашифрованих повідомлень, які були створені за допомогою одного й того самого ключа. Криптоаналітик намагається виявити закономірності або слабкі місця в шифрі, використовуючи аналіз статистичних характеристик шифротекстів. Це дозволяє йому зробити припущення про відповідні відкриті тексти або виявити інформацію, яка може допомогти в розкритті секретного ключа. Один з основних методів криптоаналізу в такій атаці — це дослідження можливих кореляцій між шифротекстами і їх відкритими текстами. Важливим аспектом є те, що атака може бути реалізована навіть при обмежених знаннях про структуру шифру, однак ефективність таких атак часто залежить від якості шифру і його стійкості до статистичних методів аналізу. В сучасних системах шифрування, які використовують складні алгоритми, атаки на основі шифротексту часто не дають змоги швидко знайти правильний ключ, однак вони залишаються корисними при роботі з менш надійними методами. Щоб захиститися від таких атак, криптографи використовують методи додаткової обробки даних, такі як застосування сольових значень, випадкових ініціалізаційних векторів і інші техніки для підвищення стійкості систем. Загалом, цей метод полягає у використанні кількох шифротекстів, зашифрованих одним і тим же алгоритмом. Криптоаналітик намагається знайти відповідні відкриті тексти або визначити секретний ключ, що був використаний для шифрування. Така атака може бути реалізована, якщо шифровані повідомлення доступні для перехоплення, і зазвичай це один з найпростіших методів криптоаналізу, хоча і менш ефективний.

2. Атака на основі відкритих текстів та відповідних шифротекстів

Атака на основі відкритих текстів та відповідних шифротекстів є більш потужною формою криптоаналізу, оскільки криптоаналітик має як зашифровані повідомлення, так і їх оригінали. Знаючи відповідний відкритий текст для кожного шифротексту, він може використовувати різноманітні методи для аналізу і знаходження зв'язку між шифротекстом і відкритим текстом. Зокрема, криптоаналітик може спробувати визначити структуру алгоритму шифрування, виявити ключ або дослідити статистичні характеристики шифротекстів, які дозволяють робити висновки про метод шифрування. Відомі відкриті тексти дають можливість побудувати моделі, які можуть бути використані для розкриття інших шифрованих повідомлень, створених тим самим ключем. Цей метод є ефективним, якщо криптоаналітик має доступ до великої кількості зашифрованих повідомлень і відповідних їм відкритих текстів, що дозволяє йому систематично тестувати можливі ключі і алгоритми. Більш

того, атака на основі відкритих текстів допомагає виявити слабкі місця у шифрі, які можна використати для розкриття більш складних або прихованих повідомлень. Для захисту від таких атак криптографи часто використовують технології, які забезпечують додаткову стійкість, такі як зміна ключів, додавання шуму до шифротекстів або застосування комбінованих алгоритмів шифрування. Існують два основних варіанти:

- ✓ Визначити секретний ключ, використаний для перетворення відкритого тексту в шифротекст.
- ✓ Створити алгоритм, здатний дешифрувати будь-яке повідомлення, закодоване за допомогою цього ключа.

Щоб реалізувати таку атаку, криптоаналітик може використовувати знання про типові фрази у відкритому тексті (наприклад, привітання, підпис або звичайні вирази), що дозволяє йому ефективно підбирати можливі варіанти.

3. Атака на основі підбраного відкритого тексту

Цей метод передбачає, що криптоаналітик має як відкриті тексти, так і відповідні шифротексти, і має можливість вибирати певні фрагменти відкритого тексту для подальшого шифрування. Цей метод дозволяє отримувати додаткову інформацію про ключ шифрування та створювати алгоритм для його дешифрування. Атака на основі підбраного відкритого тексту є більш потужною, ніж атака на основі просто відкритих текстів, оскільки криптоаналітик має змогу самостійно вибирати конкретні частини відкритого тексту для шифрування. Такий підхід дозволяє йому отримати більше інформації про властивості алгоритму шифрування, оскільки він може впливати на те, як саме буде зашифрований вибраний фрагмент. Криптоаналітик може систематично підбирати різні варіанти відкритих текстів і аналізувати їх шифротексти, що дозволяє йому визначити закономірності, властиві певному алгоритму. Цей метод є ефективним проти слабких алгоритмів шифрування, де навіть обмежена кількість шифрованих текстів може привести до знаходження ключа або виявлення слабкості у шифруванні. Для підвищення стійкості до таких атак шифри зазвичай використовують додаткові методи маскування або зміни ключа для кожного повідомлення, щоб ускладнити криптоаналітику здобуття корисної інформації. Наприклад, використовують динамічні ключі, хешування або інші додаткові криптографічні заходи. Як правило, цей тип атаки потребує великої кількості часу та ресурсів для її реалізації, але він може бути дуже ефективним, якщо криптоаналітик має достатньо вибіркового даних для аналізу.

4. Атаки на основі адаптаційно підбраного відкритого тексту

Це вдосконалена форма атаки на основі підбраного відкритого тексту, де криптоаналітик може адаптувати свої вибори відкритих текстів залежно від результатів попередніх операцій шифрування. Ключовою перевагою цієї атаки є те, що криптоаналітик може на основі вже отриманих результатів приймати рішення щодо вибору наступних блоків відкритого тексту для шифрування, що дозволяє більш ефективно атакувати шифр. Атака на основі адаптаційно підбраного відкритого тексту дозволяє криптоаналітику адаптувати свою стратегію в реальному часі, підбираючи нові відкриті тексти в залежності від того, які результати були отримані при попередніх спробах шифрування. Це дає можливість більш цілеспрямовано і швидко знаходити слабкі місця в алгоритмі шифрування. Така атака може бути особливо ефективною проти систем, де ключові параметри або особливості шифрування змінюються в залежності від вхідних даних. Вона дозволяє значно зменшити кількість необхідних операцій для дешифрування або відновлення ключа, оскільки кожен новий вибір відкритого тексту враховує попередні результати атаки. Крім того, за допомогою цієї стратегії криптоаналітик може поступово обмежувати простір можливих ключів, що також прискорює процес атаки. Важливо, що така атака потребує доступу до системи з можливістю зміни вхідних даних, тобто вона стає проблемою для систем з великими обмеженнями на модифікацію даних. Однак, завдяки своїй адаптивності, цей метод вважається однією з найбільш потужних атак на асиметричні криптографічні системи.

Сучасні тренди в криптоаналізі демонструють значний прогрес у розвитку методів розшифровки та виявлення уразливостей у криптографічних системах. З розвитком комп'ютерних технологій і криптографії, криптоаналіз став складнішим і технічно більш витонченим. Сучасні криптоаналітики використовують різноманітні підходи, зокрема атаки за допомогою гіпотез та статистичних методів, які застосовуються для виявлення закономірностей у шифрованих повідомленнях на основі глибокого аналізу статистики.

Іншим важливим напрямком є атаки на основі методів машинного навчання, де алгоритми машинного навчання здатні автоматично виявляти патерни та кореляції, що дозволяє ефективно розшифровувати дані та виявляти слабкі місця в криптографічних системах.

Окрім цього, квантовий криптоаналіз стає все більш актуальним, оскільки квантові комп'ютери мають потенціал значно швидше зламувати деякі сучасні криптографічні методи, такі як RSA, за допомогою квантового алгоритму Шора. Це змушує криптографів розробляти нові, стійкі до квантових атак алгоритми.

Таким чином, криптоаналіз залишається важливою частиною криптографії, оскільки він постійно удосконалює методи захисту інформації і забезпечує актуальність криптографічних систем у умовах розвитку нових технологій.

15.3. МЕТОДИ СТЕГАНОГРАФІЇ

Стеганографія — це метод прихованого написання інформації, який дозволяє зберігати та передавати повідомлення таким чином, що їх наявність або зміст не можна помітити без спеціальних знань. Відмінність стеганографії від криптографії полягає в тому, що криптографія маскує зміст повідомлення, тоді як стеганографія приховує саме існування повідомлення, роблячи його непомітним для сторонніх осіб. Людина, яка не володіє ключем до розшифровки або не знає про існування повідомлення, не зможе його виявити.

Історія стеганографії налічує століття. Перші згадки про застосування цієї техніки датуються 440 роком до н. е., коли Геродот у своїй "Історії" описав два методи приховування інформації. Один із них полягав у записуванні важливої інформації на дерев'яну підкладку воскової таблички, а інший — у використанні поголеної голови раба для запису повідомлення, яке ставало видимим лише після того, як волосся відростало. Подібні методи використовувалися в різних культурах, зокрема в Китаї, де листи зберігалися на смужках шовку, які ковтали посилені для їхнього доставки.

У XV столітті чернець Трітеміус став відомим завдяки своїм роботам з криптографії та стеганографії, створивши кілька методів прихованої передачі повідомлень, які пізніше були опубліковані у книзі "Steganographia". Відомий також метод мікроточок, вперше застосований під час Франко-пруської війни 1870 року, і лише з часом здобув широке застосування в різних сферах, зокрема в розвідці та наукових дослідженнях.

Сучасний розвиток стеганографії зокрема відзначається появою нових методів, таких як застосування стеганографії для зберігання повідомлень в молекулярних структурах, зокрема в ДНК. Так, у 2000 році американська школярка Вівіана Риска продемонструвала алгоритм для приховування інформації в генній послідовності, що стало важливим кроком для майбутнього розвитку стеганографії у галузі біотехнологій.

Сучасні методи комп'ютерної стеганографії дозволяють зберігати повідомлення в різних типах файлів, таких як аудіо- і відеофайли,

зображення та навіть текстові документи. Наприклад, можна змінити колір пікселів в цифрових зображеннях або замінити незначні частки даних у звукових та відеофайлах, що робить інформацію непомітною для людини, але доступною для спеціалізованого програмного забезпечення. Такий метод широко застосовується для створення цифрових водяних знаків, які можуть використовуватися для перевірки автентичності або недоторканності документів.

Крім того, розроблені програмні засоби, які дозволяють приховувати інформацію в невикористовуваних частинах файлових систем або в зарезервованих полях файлів. Методи стеганографії можуть бути застосовані в різних форматах, таких як текстові документи, зображення, аудіо і відеофайли, що дає можливість використовувати їх для забезпечення конфіденційності, захисту інтелектуальної власності, а також для протидії фальсифікаціям.

Сьогодні існує кілька напрямків стеганографії, серед яких класична стеганографія, комп'ютерна стеганографія, цифрова стеганографія та мережева стеганографія. Класична стеганографія включає методи, такі як використання невидимих чорнил або методи приховування повідомлень у вигляді тексту, що проявляється лише за певних умов, наприклад, при нагріванні або під ультрафіолетовим світлом. У комп'ютерній стеганографії використовуються технології, що базуються на характеристиках цифрових файлів та файлових систем.

Важливо зазначити, що сучасні методи стеганографії мають значну роль в інформаційній безпеці, оскільки вони дозволяють захищати передавання чутливих даних та забезпечувати їх конфіденційність. Наприклад, при використанні стеганографії у системах захисту інформації з'являється можливість приховувати важливі відомості у вигляді, що є абсолютно непомітним для сторонніх осіб, що значно підвищує рівень безпеки в умовах сучасного інформаційного середовища.

Цифрова стеганографія: сучасні тенденції та підходи

З розвитком цифрових технологій з'явилися нові можливості для застосування стеганографії, яка передбачає приховування секретних повідомлень у цифрових об'єктах, таких як зображення, відео, аудіо або текст. Цифрова стеганографія є потужним інструментом для забезпечення конфіденційності даних, де важливу роль відіграють методи, які дозволяють вбудовувати інформацію в мультимедійні об'єкти без помітних змін, що можуть бути виявлені людським оком або слухом.

Основні принципи цифрової стеганографії полягають у використанні цифрових сигналів як контейнерів для прихованої інформації.

Найбільш популярні методи включають:

1. **Метод заміни найменш значущих бітів (LSB, Least Significant Bit)** — один з найпростіших і найбільш застосовуваних методів. Суть полягає в заміні найменших значущих бітів пікселів зображення або аудіо на біти секретного повідомлення. Різниця між оригінальним і модифікованим об'єктом не помітна для людини. Цей метод є ефективним для великих цифрових зображень з високою роздільною здатністю, але менш ефективний для малих зображень або при перегляді на низькоякісних пристроях. Метод LSB широко використовується в стеганографії для приховування даних в зображеннях, аудіо або відео файлах. Однією з переваг цього методу є його простота реалізації та мінімальний вплив на якість носія інформації. Однак цей метод має певні обмеження, зокрема, він вразливий до різних видів атак, таких як аналіз статистичних властивостей або маніпуляції з файлом. Для підвищення рівня захисту можуть бути використані варіанти методу, які замінюють більше ніж один біт або застосовують шифрування перед вставкою повідомлення. Окрім того, метод LSB зазвичай не забезпечує аутентифікацію або цілісність даних, тому часто використовується в поєднанні з іншими техніками для підвищення безпеки. Важливим аспектом є вибір типу носія даних, оскільки деякі формати файлів можуть бути менш підходящими для приховування інформації через їхню структуру або алгоритми стиснення. Попри це, метод LSB залишається популярним через свою простоту та ефективність у певних випадках.

2. **Цифрові водяні знаки (ЦВЗ)** — технологія, що використовується для захисту авторських прав і перевірки цілісності документів. ЦВЗ можуть бути невидимими або видимими, і застосовуються для ідентифікації власника контенту або підтвердження автентичності. ЦВЗ записуються як псевдовипадкові послідовності, згенеровані за допомогою секретних ключів, і можуть бути стійкими до змін або атак, що робить їх важливими для забезпечення захисту інтелектуальної власності. Цифрові водяні знаки можуть бути вбудовані в зображення, відео, аудіофайли чи текстові документи без значної зміни їх візуальних або аудіо характеристик. Вони дозволяють ідентифікувати джерело файлу або вказати на його автентичність, що є важливим для боротьби з підробками та несанкціонованим використанням контенту. Однією з основних переваг ЦВЗ є їхня здатність залишатися непомітними для кінцевого користувача, що ускладнює спроби їх видалення або змін. Для підвищення надійності, цифрові водяні знаки можуть комбінуватися з іншими методами захисту,

такими як шифрування або аутентифікація. Важливою характеристикою є також можливість їх виявлення навіть після стиснення або змін формату файлу. Використання ЦВЗ дозволяє не лише захищати авторські права, але й забезпечити механізм для відновлення оригінального контенту у разі його втрати або зміни. З розвитком технологій ЦВЗ стали важливою частиною стратегії цифрової безпеки, особливо в умовах широкого поширення контенту в Інтернеті. Цифрові водяні знаки є потужним інструментом для виявлення нелегальних копій контенту та попередження їх незаконного використання. Вони можуть бути як пасивними, так і активними, де пасивні водяні знаки не впливають на користувацьке сприйняття контенту, а активні водяні знаки вимагають спеціального програмного забезпечення для їх виявлення та перевірки. Завдяки своїй стійкості до пошкоджень, цифрові водяні знаки забезпечують високий рівень захисту, навіть якщо файл піддається стисненню, редагуванню або змінам формату. Цей метод має широке застосування в медіаіндустрії, де забезпечення авторських прав є критично важливим для підтримки законності і захисту творців контенту. Водночас, існує ризик того, що технології для видалення або модифікації водяних знаків можуть з'явитися, що вимагає постійного вдосконалення методів їх створення та інтеграції. ЦВЗ також використовуються в правових процесах як доказ автентичності або походження документів, що підвищує їхню юридичну цінність. В цілому, цифрові водяні знаки є важливим елементом сучасної стратегії захисту інтелектуальної власності в цифровому світі.

3. Мережева стеганографія — застосування стеганографічних методів для прихованої передачі інформації через комп'ютерні мережі. Вона включає модифікацію мережевих протоколів, наприклад, через затримку пакетів або зміни в метаданих протоколів передачі даних. Це дозволяє передавати секретні повідомлення через стандартні канали комунікації, не викликаючи підозр. Наприклад, методи, які використовуються для приховування даних в протоколах VoIP (Voice over IP) або в бездротових мережах WLAN (Wireless Local Area Networks). Мережева стеганографія може включати зміни в заголовках пакетів або використання нестандартних параметрів у протоколах, щоб приховати наявність даних. Це дозволяє уникнути виявлення трафіку як шифрованого або підозрілого, оскільки передача даних виглядає як звичайна комунікація. Однією з основних переваг є те, що вона може використовувати вже існуючі мережеві інфраструктури без необхідності додаткового встановлення спеціального обладнання або програмного забезпечення. Такий підхід є корисним для захисту інформації в умовах обмежених ресурсів або високого ризику виявлення. Мережева

стеганографія також може застосовуватися для прихованого обміну файлами або конфіденційною інформацією в мережах з обмеженим доступом. Проте, її використання несе в собі певні ризики, оскільки будь-яка модифікація мережевого трафіку може бути виявлена за допомогою спеціалізованих методів аналізу трафіку. Тому важливою складовою є постійний розвиток методів захисту та анонімізації для зменшення ризиків виявлення.

4. Технології для стеганографії в аудіо- та відеофайлах — стеганографічні алгоритми, які вбудовують секретну інформацію у відео або аудіо. Ці технології дозволяють приховувати повідомлення, не змінюючи значно якість медіафайлів. Наприклад, в аудіофайли можуть вбудовуватися біти в найменші значущі біти, або ж використовуються методи, що зміщують фази в аудіо сигналів таким чином, що зміни не впливають на сприйняття. Для відеофайлів стеганографічні методи можуть використовувати зміни в пікселях окремих кадрів або модифікацію елементів кольорової гами, що не помітно для ока. Один із таких підходів — це вбудовування інформації в розділи між сусідніми кадрами, що дозволяє зберегти високу якість зображення. Важливою особливістю таких технологій є здатність забезпечити високу надійність прихованих даних, що робить їх важко виявленими під час аналізу файлів. Крім того, стеганографія в медіафайлах може застосовуватись для аутентифікації контенту, захисту авторських прав або виявлення несанкціонованого доступу до конфіденційної інформації. Методи стеганографії, що використовують аудіо- та відеофайли, особливо ефективні при передачі даних через мережі з високим рівнем трафіку, де виявлення прихованих повідомлень є складним завданням. Однак, ці методи мають свої обмеження, зокрема в залежності від формату файлів та складності обробки великих обсягів даних. Для забезпечення стійкості таких технологій необхідно постійно вдосконалювати алгоритми та шукати нові способи захисту від можливих атак.

5. Методи стеганографії на основі форматів файлів — ці методи використовують специфічні особливості форматів файлів для приховування інформації в таких місцях, як метадані або не використовувані частини файлів. Наприклад, записи в метаданих файлів зображень або відео можуть служити контейнерами для прихованих повідомлень. Такі методи дозволяють передавати дані без суттєвих змін у самому контенті файлу, що ускладнює їх виявлення. Метадані можуть включати інформацію про автора, час створення, місце збереження та інші властивості файлу, що не є критичними для його відтворення, але можуть бути використані для приховування тексту або інших даних. Крім того,

деякі формати файлів, наприклад, PDF або ZIP, можуть включати порожні або невикористовувані секції, в яких також можна безпечно вбудовувати секретні повідомлення. Використання таких методів є ефективним для приховування інформації в цифрових документах, що передаються через Інтернет або зберігаються на пристроях. Інший варіант — вбудовування даних у залишкові частини файлових структур, що зазвичай ігноруються при нормальному використанні, наприклад, останні байти файлів. Однак, ці методи можуть бути виявлені за допомогою спеціальних інструментів, які аналізують файли на наявність аномалій у структурах метаданих або порожніх секціях. Тому для досягнення максимальної безпеки важливо використовувати додаткові техніки шифрування або комбінувати методи стеганографії для підвищення стійкості до атак.

Усе це підкреслює, що стеганографія є не тільки потужним інструментом для захисту даних і комунікацій, але й важливим елементом в контексті кібербезпеки. Сучасні алгоритми і технології дозволяють вбудовувати приховані повідомлення в різноманітні формати та передачі даних, забезпечуючи не лише захист від несанкціонованого доступу, а й збереження конфіденційності в умовах інтенсивного обміну інформацією через глобальні мережі.

Сучасні дослідження та застосування цифрової стеганографії зосереджені на розробці нових алгоритмів, які можуть забезпечити ще більшу стійкість до атак і збереження прихованої інформації навіть в умовах впливу потужних методів виявлення та аналізу.

Цифрова стеганографія є важливою складовою сучасних методів приховування інформації, які використовуються в цифровому середовищі. З розвитком цифрових технологій, зокрема обчислювальної техніки, вона отримала нове застосування в широкому спектрі напрямів, таких як захист конфіденційних даних, боротьба з кіберзагрозами, аутентифікація та контроль цілісності інформації.

Розвиток цифрової стеганографії

Розвиток цифрової обчислювальної техніки дійсно став стимулом для еволюції комп'ютерної стеганографії. Зараз цифрова стеганографія охоплює більше різноманітних форматів файлів, ніж у традиційній аналоговій стеганографії. Вона активно використовує можливості для приховування інформації в мультимедійних даних, таких як зображення, відео та аудіо. Однак сучасні стеганографічні алгоритми також включають приховування даних у текстових файлах, скомпресованих архівах та в метаданих.

Цифрова стеганографія — це технологія приховування інформації в цифрових об'єктах (зображеннях, аудіо-, відеофайлах тощо) таким чином,

щоб не було помітно змін у самому об'єкті. Основна мета цифрової стеганографії — передача секретних повідомлень через відкриті канали комунікації без виявлення сторонніми особами. Для цього використовуються спеціальні алгоритми, які дозволяють вбудовувати секретну інформацію у файли, не змінюючи їх помітним чином для користувача. Один із найпоширеніших методів — це заміна найменш значущих бітів (LSB) у пікселях зображень або аудіофайлах.

Цифрова стеганографія має низку переваг, зокрема можливість приховування великих обсягів інформації в звичайних цифрових об'єктах, таких як фотографії, музика чи відео. Вона широко використовується для захисту авторських прав, перевірки цілісності даних, а також для безпечного обміну даними. Однак для її ефективного застосування важливо, щоб методи стеганографії були поєднані з методами шифрування, щоб забезпечити додатковий рівень безпеки. Сучасні стеганографічні методи можуть включати використання складних математичних моделей і форматів файлів для запобігання виявленню прихованих повідомлень. Основним викликом є розробка методів для виявлення та аналізу стеганографії, тому постійно вдосконалюються технології для захисту від таких атак.

Цифрова стеганографія використовує додаткові рівні складності, включаючи вибір найбільш непомітних частин цифрових об'єктів для вставки прихованої інформації, таких як найменші значущі біти (LSB) або навіть імплантація даних у метадані зображень та відео. Крім того, ці об'єкти часто мають вбудовані цифрові водяні знаки, що додають ще один рівень захисту, що може допомогти виявити маніпуляції з оригіналом.

Мережева стеганографія

З поширенням інтернету і розвитку комп'ютерних мереж з'явилася нова форма стеганографії — мережева стеганографія, яка використовує специфічні властивості мережевих протоколів для приховування інформації. Це може включати приховування в заголовках пакетів, затримку або пошкодження пакетів або приховування даних у полях, які не використовуються зазвичай.

Особливістю сучасних мережевих методів є використання протоколів на низькому рівні, таких як IP, TCP, UDP та навіть VoIP, для передачі прихованих повідомлень через інтернет або внутрішні мережі підприємств. Така стеганографія включає методи, як:

- **WLAN стеганографія** — використовується для передачі секретних повідомлень через бездротові локальні мережі. Це може включати використання нестандартних характеристик в передачі

безпроводових даних, як, наприклад, HICCUPS — система для захованої комунікації в пошкоджених мережах.

- **LACK стеганографія** — включає використання затримок пакетів у VoIP-телефонії для приховування інформації в затриманих або втрачених пакетах аудіо.
- **VoIP стеганографія** — здійснюється через технології передачі голосових даних в реальному часі (RTP протокол). Вона модифікує аудіо пакети для того, щоб приховати в них дані, що можуть бути отримані тільки тим, хто володіє певним ключем.

Стеганографія в медіа контенті та захисті інтелектуальної власності

Модерні стеганографічні методи також активно використовуються для захисту інтелектуальної власності через цифрові водяні знаки (ЦВЗ). Ці знаки можуть бути невидимими або видимими, та служать для підтвердження автентичності мультимедійного контенту, що важливо для захисту авторських прав та боротьби з піратством.

ЦВЗ можуть бути стійкими до атак, таких як спроби їх видалення або спотворення, оскільки вони можуть містити унікальну інформацію про час продажу або покупця продукту. З розвитком технологій на основі блокчейн та шифрування, водяні знаки стають ще більш складними для маніпуляцій. Зокрема, їх використання в юридичних документах, фінансових транзакціях і контенті, що стосується прав власності, стало популярним.

Актуальні стеганографічні алгоритми

Окрім класичних методів, таких як **LSB (Least Significant Bit)** для вставки даних у цифрові об'єкти, сьогодні існують більш складні підходи, які враховують можливість впливу різноманітних атак на приховану інформацію. Сучасні стеганографічні алгоритми використовують розвинені методи для забезпечення високої стійкості до виявлення, такі як статистичний аналіз, перетворення Фур'є або використання хаотичних систем. Одним із таких підходів є методи на основі перетворень зображень у частотній області, де дані вбудовуються в компоненти зображення, що менш помітні для людського ока. Інші сучасні методи застосовують використання стеганографії в мультимедійних форматах, таких як аудіо та відео, де дані приховуються в нетривіальних частинах файлу, що ускладнює їх виявлення. Окрім того, для підвищення безпеки застосовуються комбінації стеганографії та криптографії, що дають змогу шифрувати приховані повідомлення для додаткового захисту. Ці алгоритми застосовуються в широкому спектрі застосувань, включаючи

захист авторських прав, безпечну передачу інформації та захист від цензури.

Наприклад:

- **Метод фільтрації перед записом даних**

Визначення найбільш підходящих місць для вставки даних, на яких зміни будуть непомітними для людського ока.

- **Шумові сигнали для стеганографії в зображеннях**

Поширені методи, що включають застосування псевдовипадкових шумів для приховування повідомлень у зображеннях.

- **Генерація та виявлення водяних знаків** з використанням криптографічних підходів для забезпечення більш високого рівня захисту від спроби їх зміни або видалення.

Сучасні алгоритми, наприклад Adaptive Steganography або Perceptual Masking, використовують більш динамічний підхід, що адаптується до зміни властивостей файлів і потребує меншого людського втручання.

Узагалі, цифрова стеганографія продовжує розвиватися і знаходить нові області застосування в сучасних технологіях, таких як Інтернет речей (IoT), машинне навчання і блокчейн. Це дозволяє створювати ще більш ефективні, адаптивні та стійкі системи для приховування даних.

15.4. МОДЕЛЬ СТЕГАНОСИСТЕМИ

Модель стеганосистеми є комплексною структурою, що включає кілька основних елементів, які взаємодіють для забезпечення прихованої передачі та захисту інформації. Вхідними даними для стеганографії можуть бути різноманітні цифрові об'єкти, такі як зображення, аудіо чи відеофайли, у які вбудовується секретне повідомлення. Алгоритм стеганографії визначає, як саме вбудовуються ці секретні дані в контейнер, змінюючи, наприклад, найменші значущі біти пікселів зображення або звукових хвиль у аудіофайлах.

Для підвищення безпеки часто застосовується додатковий етап шифрування повідомлення, що ускладнює його розкриття навіть у разі виявлення стеганографії. Результатом роботи стеганографічного алгоритму є контейнер, який містить як оригінальні дані, так і вбудовану секретну інформацію, що залишається непомітною для стороннього спостерігача. Після цього, щоб відновити секретне повідомлення, необхідно використати відповідний стеганографічний алгоритм декодування, що дозволяє витягти приховані дані з контейнера. Однак важливим етапом є також виявлення стеганографії, що може включати спеціальні методи аналізу цифрових

об'єктів для виявлення аномалій, які можуть свідчити про приховану інформацію. Для протидії таким атакам використовуються різноманітні методи маскування, шифрування та інші стратегії, що ускладнюють виявлення стеганографії і забезпечують її ефективність у сучасних умовах безпеки інформації.

Основні вимоги до стеганосистеми, яка забезпечує приховану передачу або зберігання інформації, повинні включати наступні аспекти:

1. **Невидимість** — одна з головних вимог до стеганографічних систем полягає в тому, щоб приховане повідомлення було абсолютно невидимим для користувача. Це означає, що зміни в носії даних (наприклад, зображенні, аудіофайлі або відео) повинні бути мінімальними або такими, що не помітні для людини.

2. **Незмінність якості** — після вбудовування секретної інформації, якість вихідного носія (зображення, аудіо, відео) повинна залишатися майже незмінною, тобто не повинно бути спостережувано явних змін у його властивостях, таких як роздільна здатність, якість звуку чи зображення.

3. **Стійкість до атак** — стеганосистема повинна бути стійкою до різних видів атак, зокрема до статистичних і формальних методів виявлення, таких як аналіз зміщення бітів, гістограми зображень чи аудіофайлів. Система має бути спроектована так, щоб ускладнити виявлення прихованої інформації.

4. **Місткість** — стеганосистема повинна підтримувати достатню місткість для вбудовування секретних даних, при цьому не порушуючи якість носія. Місткість визначає максимальний обсяг інформації, яку можна приховати, не викликаючи помітних змін у носії.

5. **Динамічність і масштабованість** — система повинна мати можливість працювати з різними форматами файлів і легко адаптуватися до нових стандартів або змін у вимогах. Масштабованість передбачає здатність працювати з великими обсягами даних.

6. **Безпека** — хоча стеганографія не повинна залежати від секретності алгоритму, проте система повинна бути захищена від потенційних атак, зокрема від спроб виявлення або модифікації прихованої інформації, що може знизити її безпеку.

7. **Простота використання** — система повинна бути зручною та легкою у використанні, навіть для осіб без технічних знань. Це включає прості інтерфейси для користувача та ефективне управління процесом вбудовування і вилучення прихованих даних.

Ці вимоги забезпечують ефективність і надійність стеганографічних систем, дозволяючи їх застосовувати для захисту інформації в різних сферах, таких як передача конфіденційних даних, захист авторських прав або виявлення фальсифікацій.

Атаки на стеганосистеми спрямовані на виявлення або витягнення прихованої інформації, що знаходиться в цифрових об'єктах. Залежно від типу атаки та методу стеганографії, атаки можуть варіюватися за складністю та методами виявлення. Основні типи атак на стеганосистеми включають:

- ✱ **Атаки на виявлення стеганографії** — це атаки, які орієнтовані на виявлення присутності прихованої інформації в цифровому файлі. Для цього використовуються різноманітні статистичні методи, що дозволяють виявити аномалії в звичайному вигляді файлів, наприклад, зміни в розподілі бітів або інші аномалії, що можуть свідчити про використання стеганографії.
- ✱ **Атаки на витягнення інформації** — ці атаки спрямовані на витягнення або дешифрування прихованого повідомлення. Такі атаки можуть бути здійснені шляхом використання зворотного аналізу або застосування алгоритмів дешифрування до виявленої стеганографічної інформації. Витягнення може стати можливим, якщо відомі певні параметри стеганографічної системи або якщо хтось має доступ до ключів шифрування.
- ✱ **Атаки на руйнування стеганографії** — ці атаки спрямовані на знищення або пошкодження вбудованих даних. Один із прикладів такої атаки — це атака, яка полягає в модифікації або корупції контейнера таким чином, щоб приховане повідомлення стало нечитабельним або частково пошкодженим. Такі атаки можуть включати зміну метаданих, спотворення даних або компресування файлів.
- ✱ **Атаки через аналіз на основі контексту** — ці атаки націлені на аналіз специфічних характеристик файлів, що можуть вказувати на наявність прихованих даних. Наприклад, в аналізі зображень можуть бути виявлені аномалії в статистиці кольорів або текстур, що може свідчити про використання стеганографії для передачі повідомлень.
- ✱ **Атаки через спеціальні фільтри та змішування** — такі атаки спрямовані на використання фільтрації або компресії для змішування або розчинення даних, що зберігаються в файлі. Ці методи можуть видаляти або приховувати стеганографічну інформацію, не залишаючи слідів її наявності в кінцевому файлі.

Загалом, для захисту стеганосистеми від цих атак використовуються різноманітні методи, включаючи складніші алгоритми, більш ефективні методи шифрування, маскування, а також вбудовування даних у менш очевидні області файлів.

Відкриті, закриті, напівзакриті стеганосистеми

У стеганографії розрізняють **відкриті**, **закриті** та **напівзакриті** стеганосистеми, залежно від рівня доступу до методу і ключів для приховування та вилучення інформації:

1. Відкриті стеганосистеми

Відкриті стеганосистеми характеризуються тим, що їх алгоритми і методи вбудовування та вилучення інформації є публічно доступними для всіх бажаючих. Це означає, що будь-хто може використовувати сам алгоритм або методику для приховування даних, що робить таку систему відкритою і доступною для загального використання.

Особливості відкритих стеганосистем:

- **Публічний доступ до алгоритму**

Сам алгоритм стеганографії є відкритим і доступним для всіх. Це дозволяє будь-якому користувачеві використати його для приховування інформації, однак безпека такої системи залежить від секретності ключа чи параметрів, що використовуються для вбудовування та вилучення даних.

- **Безпека через секретність ключа**

Хоча алгоритм є публічним, ефективність та безпека такої системи залежить від секретності ключа, який застосовується для вбудовування або вилучення секретної інформації. Система має бути побудована таким чином, щоб навіть при доступі до алгоритму нападник не міг одразу здогадатися про вміст прихованої інформації без ключа.

- **Приклад застосування**

Відкриті стеганосистеми можуть використовуватись у випадках, коли важливіше забезпечити загальний доступ до технології, а не приховати сам алгоритм, наприклад, у публічних інтернет-ресурсах для шифрування повідомлень або приховування міток на зображеннях.

2. Закриті стеганосистеми

Закриті стеганосистеми відрізняються від відкритих тим, що алгоритм стеганографії та всі механізми вбудовування і вилучення інформації є приватними та недоступними для широкого загалу. Ключі, параметри або самі методи обробки даних є засекреченими, що значно підвищує рівень безпеки.

Особливості закритих стеганосистем:

- **Приватний доступ до алгоритму**

Алгоритм та методи для вбудовування й вилучення секретної інформації доступні лише обмеженому колу користувачів або організацій. Це забезпечує високу ступінь захисту, оскільки нападники не мають доступу до методу, що ускладнює спроби пошуку прихованої інформації.

- **Високий рівень захисту**

Безпека такої системи залежить не лише від секретності ключа, але й від того, що сам алгоритм є недоступним для сторонніх осіб. Для доступу до даних або їх виявлення необхідно знати ключ або мати інший доступ до секретної частини системи.

- **Приклад застосування**

Закриті стеганосистеми використовуються у сфері урядових або корпоративних комунікацій, де важливий не лише захист самих даних, а й обмеження доступу до методів їх приховування. Такі системи використовуються для забезпечення захищених каналів зв'язку та зберігання конфіденційної інформації.

3. Напівзакриті стеганосистеми

Напівзакриті стеганосистеми знаходяться на межі між відкритими та закритими системами. Вони характеризуються тим, що алгоритм стеганографії є відкритим, але для вбудовування або вилучення прихованих даних необхідно мати секретний ключ або інші параметри, доступні лише певним користувачам.

Особливості напівзакритих стеганосистем:

- **Публічний алгоритм з секретними параметрами**

Алгоритм стеганографії доступний для всіх, але для вбудовування або вилучення прихованої інформації необхідно мати секретні ключі або паролі. Система надає доступ до методу приховування даних, але обмежує доступ до самого процесу вилучення інформації через використання секретних даних.

- **Збалансована безпека**

Така система забезпечує певний рівень прозорості, оскільки алгоритм відомий публічно, але при цьому зберігається захист від несанкціонованого доступу завдяки використанню секретних ключів або методів.

- **Приклад застосування**

Напівзакриті стеганосистеми можуть використовуватись для передачі інформації, де важливо забезпечити відкритість процесу приховування даних для широкої аудиторії, але доступ до вилучених даних залишається обмеженим. Наприклад, такі системи можуть використовуватись для організації безпечних каналів комунікацій у публічних мережах, де

алгоритм відомий, але доступ до результатів шифрування є тільки для обраних осіб.

Загалом, кожен тип стеганосистеми має свої переваги та недоліки, і вибір між ними залежить від конкретних потреб і рівня безпеки, який потрібен у різних ситуаціях. Відкриті системи є більш доступними, але менш захищеними, закриті системи надають високий рівень безпеки, але за рахунок обмеженого доступу, а напівзакриті системи дозволяють поєднувати доступність та захист в одному рішенні.

15.5. Поняття ЦВЗ та їх класифікація

Цифрові водяні знаки (ЦВЗ) використовуються для захисту авторських прав, перевірки цілісності цифрових файлів та ідентифікації контенту. Класифікація цифрових водяних знаків дозволяє зрозуміти їх різноманітні типи, методи вбудовування і призначення, що в свою чергу допомагає вибрати найефективнішу стратегію захисту в залежності від цілей. Існує кілька основних класифікацій цифрових водяних знаків, які ґрунтуються на таких критеріях, як видимість, спосіб вбудовування, цілі використання та стійкість до атак.

Першим критерієм є видимість водяних знаків. Водяні знаки можуть бути видимими або невидимими. Видимі водяні знаки включають текст, логотипи або графічні елементи, які чітко відображаються на зображеннях чи відео, і мають на меті зазвичай демонстрацію авторських прав або інформації про власника. Це найпоширеніший тип водяних знаків, оскільки вони одразу привертають увагу до контенту і є простими для впровадження. Невидимі водяні знаки, на відміну від видимих, не видні для ока, але можуть бути виявлені за допомогою спеціальних алгоритмів або програм. Вони використовуються для прихованого захисту інформації, перевірки цілісності чи стеження за поширенням контенту, не створюючи видимих змін в медіафайлі. Такий підхід дозволяє забезпечити захист контенту без порушення його візуальної або акустичної якості.

Другим важливим критерієм є спосіб вбудовування водяного знака. Залежно від цього можна виділити просторові та частотні методи вбудовування. Просторовий метод включає безпосередню зміну пікселів зображення або інших елементів медіафайлів, таких як аудіофайли, у таких частинах, які не будуть помітні для користувача, наприклад, зміна значень найменш значущих бітів (LSB). Частотний метод передбачає перетворення медіафайлу в частотну область (за допомогою перетворення на Фур'є або хвильових трансформацій), де водяний знак вбудовується в параметри, які

визначають частотний склад сигналу. Частотні методи забезпечують кращу стійкість водяного знака до стискання чи інших типів обробки.

За цілями використання цифрові водяні знаки можна класифікувати на захисні та ідентифікаційні. Захисні водяні знаки використовуються для захисту авторських прав, вони дозволяють виявити копії медіафайлів або перевірити їх на предмет підробок. Водяний знак може містити інформацію про власника або право володіння контентом, що забезпечує юридичну підтримку у випадку спроби порушення прав. Ідентифікаційні водяні знаки застосовуються для ідентифікації і відслідковування походження файлів, допомагаючи виявити, хто є автором файлу або в якій обстановці він був створений. Вони можуть містити додаткову інформацію про файл, таку як метадані, або бути частиною більш складної системи відстеження.

Ще *одним важливим критерієм є стійкість* до атак. Водяні знаки можна класифікувати як стійкі та нестійкі. Стійкі водяні знаки зберігають свою цілісність навіть після обробки файлу, такої як стискання, зміну формату або інші маніпуляції. Вони широко застосовуються для захисту файлів від підробок і несанкціонованого використання, оскільки навіть при спробах знищити або змінити водяний знак він може бути відновлений або виявлений. Нестійкі водяні знаки, в свою чергу, можуть бути легко видалені або пошкоджені в процесі обробки файлів, але вони можуть бути корисні для забезпечення додаткової ідентифікації чи збереження певної інформації, яка не є критично важливою для захисту.

Класифікація за методами виявлення водяних знаків також є важливою. Водяні знаки можуть бути виявлені за допомогою спеціальних алгоритмів або методів аналітики, таких як статистичні методи для виявлення змін у даних, або за допомогою більш складних алгоритмів, що використовують знання про конкретні властивості водяних знаків.

Таким чином, цифрові водяні знаки класифікуються за різними критеріями, зокрема за видимістю, способом вбудовування, цілями використання, стійкістю до атак і методами виявлення. Кожен із цих критеріїв допомагає вибрати найбільш підходящий метод для конкретної ситуації, забезпечуючи максимальний рівень захисту цифрового контенту.

15.6. МЕТОД МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА

Метод модифікації найменшого значущого біта (LSB, Least Significant Bit) є одним із найпростіших та найпоширеніших методів стеганографії для прихованого вбудовування даних у цифрові зображення, аудіо або відеофайли. Суть методу полягає в заміні найменших значущих бітів

пікселів або сигналів на біти секретної інформації, таким чином, що зміни не помітні для людського сприйняття, оскільки ці зміни незначні і не впливають на якість зображення або звуку.

У зображеннях цей метод зазвичай реалізується шляхом заміни найменш значущих бітів кожного пікселя. Кожен піксель може бути представленим певною кількістю бітів, зазвичай 24 біти для кольорових зображень (8 біт на кожен із трьох кольорових каналів: червоний, зелений і синій). Замінивши найменший біт кожного каналу на біт секретного повідомлення, можна приховати значну кількість бітів без значних змін у зовнішньому вигляді зображення. Наприклад, при зміні одного біта в кожному з трьох каналів на біт секретної інформації для кожного пікселя можна вбудувати 3 біти за один піксель.

В аудіо і відеофайлах метод LSB працює аналогічним чином, змінюючи найменші біти звукових або відео-сигналів. У аудіофайлах заміщення найменших бітів не призводить до значних змін у якості звуку, оскільки найменші біти мають малий вплив на загальне сприйняття. У відеофайлах зміни найменших бітів можуть стосуватися пікселів кадру, і метод може бути використаний для приховування великих обсягів даних у послідовності кадрів.

Перевагою методу LSB є його простота та ефективність, оскільки він не потребує складних алгоритмів і може бути легко реалізований на практиці. Однак цей метод має й недоліки, зокрема він може бути вразливим до атак на основі аналізу шуму або статистичних змін, які виникають при вбудовуванні даних, а також до маніпуляцій із зображеннями або файлами, таких як стискання або обробка, що може знищити або змінити приховану інформацію. Для підвищення стійкості методу LSB до атак зазвичай застосовуються додаткові методи, такі як перетворення даних або використання більш складних стеганографічних алгоритмів.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 15

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім.

Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.

4. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

5. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

6. A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

7. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.

8. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

9. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.

10. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.

11. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.

12. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37. Спасітелева, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних

контейнерних застосунків з мікросервісною архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.

13. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.

14. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.

15. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.

16. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

17. A. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.

18. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.

РОЗДІЛ 16

МОДЕЛІ ЗАГРОЗ БЕЗПЕКИ КРИПТОСИСТЕМ



16.1. Формальна модель загроз криптосистем

16.2. Атаки на симетричні і асиметричні шифрсистеми

16.3. Властивості елементарних шифрів

16.4. Теоретична та практична стійкість, абсолютно стійкий шифр

"Безпека криптографічних систем не повинна залежати від секретності алгоритмів, а лише від секретності ключів."

Клод Шеннон, відомий математик і криптограф

16.1. ФОРМАЛЬНА МОДЕЛЬ ЗАГРОЗ КРИПТОСИСТЕМ

Формальна модель загроз криптосистем — це математичний або абстрактний опис можливих загроз та ризиків для криптографічних систем, який використовується для оцінки їх стійкості та визначення заходів безпеки. Модель передбачає класифікацію різних типів загроз, а також оцінку можливостей зломисників, що можуть впливати на цілісність, конфіденційність і доступність даних у системі.

В основі формальної моделі загроз лежать припущення про здатності атакуючих сторін (зломисників), рівень їх доступу до ресурсів і технічних можливостей, а також конкретні методи або сценарії атак, які вони можуть використовувати. Системи захисту повинні бути спроектовані таким

чином, щоб витримувати найбільш ймовірні та найбільш потужні загрози, при цьому враховуючи можливість комбінацій різних атак.

Ця модель дозволяє створювати криптосистеми, які мають певний рівень стійкості до різних загроз, однак повністю стійкою можна вважати систему лише в межах конкретної моделі загроз. Наприклад, криптосистема може бути стійкою до певних типів атак (наприклад, пасивного підслуховування), але не здатною витримати інші, активніші загрози, як-от атаки через побічні канали або підробку даних.

Для ефективного забезпечення безпеки криптосистем важливо не тільки впроваджувати конкретні захисні механізми, але й формалізувати модель загроз, яка визначає можливості зломисників і способи їх атаки. Доведення стійкості криптосистеми є складним завданням, яке передбачає формулювання припущень про потенційні можливості зломисників і уточнення завдань, що вони прагнуть вирішити. Загрози безпеки криптосистеми виникають через різні види атак, які можуть бути реалізовані в умовах конкретної криптосистеми.

Зломисник у цьому контексті визначається як особа, яка має певні технічні знання в криптографії, доступ до спеціалізованих інструментів та програмного забезпечення, з метою пошуку слабких місць криптосистеми. Зломисник може бути різного рівня складності та оснащення, в залежності від наявних ресурсів. Для криптосистем можна виділити чотири рівні можливостей атакуючої сторони:

1. **Нульовий рівень** — зломисник без спеціальних знань і технічних засобів, використовує лише загальнодоступні ресурси.
2. **Перший рівень** — зломисник, який має досвід у криптографії та використовує спеціалізоване програмне забезпечення і обчислювальну техніку.
3. **Другий рівень** — корпоративний зломисник, який має фінансову підтримку великої бізнес-структури, що дає змогу йому використовувати більш потужні ресурси.
4. **Третій рівень** — зломисник, що має ресурси спеціальних служб держави, включаючи фінансову, технічну і наукову підтримку.

Стійкість криптосистеми визначається залежно від конкретних загроз та атак, які можуть бути націлені на порушення конфіденційності, цілісності та автентичності даних. Загрози можуть бути класифіковані залежно від типу атак і методів їх здійснення. Одним з ключових аспектів криптографії є створення систем, які стійкі до широкого спектра загроз, навіть до таких, які мають малу ймовірність виникнення, але можуть бути дуже руйнівними при реалізації.

Наприклад, шифр Вернама є стійким до пасивного підслуховування, однак він виявляється вразливим до активних атак, коли зломисник має знання частини відкритого тексту. Інші криптосистеми, як система простої заміни, можуть бути стійкими в певних умовах, але неспроможні витримати більш складні атаки, такі як використання фрагментів відкритого тексту для дешифрування.



Рис. 16.1. Криптосистема і загрози її безпеки

Джерело: побудовано на основі [9]

У реальних умовах криптосистеми функціонують в складі обчислювальних мереж або спеціальних систем зв'язку, де аналіз умов безпеки дозволяє виявити основні загрози і розробити стратегії захисту. Система захисту включає в себе шифратори, центри генерації і управління ключами, мережі або канали зв'язку, що дозволяє забезпечити цілісність і конфіденційність передаваних даних.

Криптосистема і загрози її безпеки

Криптосистема — це набір математичних алгоритмів і протоколів, що забезпечують захист даних шляхом шифрування, аутентифікації, підпису та інших засобів захисту інформації. Вона базується на використанні криптографічних методів для досягнення трьох основних цілей: забезпечення конфіденційності, цілісності та аутентифікації даних.

Однак, як і будь-яка технологія, криптосистеми можуть бути піддані загрозам безпеки. Загрози криптосистем — це потенційні події чи дії, які можуть порушити безпеку інформації, яку вони захищають, або знизити ефективність криптографічних методів. Основні загрози безпеці криптосистеми включають: Перехоплення зашифрованих повідомлень та

проведення криптоаналізу з метою відновлення їх змісту або розкриття ключів. Це може включати як використання стандартних атак на криптографічні алгоритми, так і більш складні методи, такі як атаки через канали зв'язку або через слабкі місця в реалізації криптосистеми. Основні загрози безпеці криптосистеми включають:

1. Перехоплення зашифрованих повідомлень

Зловмисники можуть перехоплювати зашифровані дані, сподіваючись провести криптоаналіз і відновити вміст або навіть зламати ключі шифрування. Це загроза для конфіденційності переданих даних.

2. Атаки через побічні канали

Наприклад, електромагнітне випромінювання, акустичні викиди або енергія, що витікає з криптографічних пристроїв, можуть використовуватися для отримання інформації про стан шифратора або ключі. Такі атаки є прикладом використання побічних каналів для компрометації системи.

3. Крадіжка ключів та критичної інформації

Якщо зловмисник здобуде доступ до ключів шифрування або іншої важливої інформації, це може призвести до серйозних порушень безпеки, оскільки ключі є основою захисту.

4. Підслуховування та маніпуляція з даними в каналі зв'язку

Зловмисник може не лише перехоплювати повідомлення, а й змінювати їх в процесі передачі. Це може призвести до підробки даних або атаки "man-in-the-middle", що порушує цілісність і достовірність інформації.

5. Вплив на доступність і цілісність через технічні фактори

Це включає атаки на фізичні або програмні засоби криптосистеми, наприклад, електромагнітний тероризм або відмову в обслуговуванні через технічні несправності або зовнішні атаки.

Для забезпечення надійності криптосистеми важливо враховувати всі потенційні загрози та адаптувати систему відповідно до моделі загроз. Жодна криптосистема не може бути абсолютно стійкою до всіх можливих атак, тому на практиці розробляються моделі загроз, що передбачають найімовірніші та найнебезпечніші сценарії атак. Тільки в межах цих моделей можна оцінити ефективність системи і приймати відповідні заходи для її захисту.

Зазначено, що важливим аспектом є комбіноване використання декількох типів загроз, що може значно посилити їх негативний вплив на безпеку системи. Наприклад, одночасне використання атак на криптографічні алгоритми разом із фізичними атаками, такими як витік побічних даних або крадіжка ключів, здатне привести до значно серйозніших наслідків. Тому необхідно застосовувати комплексний підхід

до захисту, включаючи не лише криптографічні методи, а й заходи фізичної та операційної безпеки.

16.2. АТАКИ НА СИМЕТРИЧНІ І АСИМЕТРИЧНІ ШИФРСИСТЕМИ

Атаки на симетричні та асиметричні шифрсистеми є важливою темою в контексті інформаційної безпеки. Вони визначають способи, якими зловмисники можуть компрометувати шифрування та електронні підписи (ЕЦП). Для розуміння природи атак на криптосистеми необхідно розглянути різні типи атак на симетричні шифрсистеми, де зловмисник намагається отримати доступ до секретної інформації, зокрема до ключа шифрування.

Атака на основі відомих шифртекстів (ciphertext-only attack) є одним із слабших типів атак, оскільки зловмисник має лише доступ до перехоплених зашифрованих повідомлень, але не знає відкритих текстів або секретного ключа. Сучасні криптосистеми успішно протистоять цим атакам завдяки високому рівню криптографічної складності.

Атака на основі відомих відкритих текстів (known-plaintext attack) є більш потужною, оскільки зловмисник має в своєму розпорядженні як зашифровані повідомлення, так і відповідні їм відкриті тексти. Це дозволяє здобути додаткову інформацію для розшифрування, однак деякі шифри, зокрема потокові шифри з лінійними зворотними зв'язками, можуть бути вразливими до таких атак.

Проста атака з вибором відкритих текстів (chosen-plaintext attack) є ще більш небезпечною, оскільки зловмисник може вибрати будь-які відкриті тексти для шифрування і на основі отриманих шифртекстів провести криптоаналіз. Адаптивна атака з вибором відкритого тексту дозволяє зловмиснику на кожному кроці вибирати нові відкриті тексти, спираючись на інформацію, отриману з попередніх операцій.

Ще більш небезпечними є атаки на основі вибору шифртекстів (chosen-ciphertext attack), при яких зловмисник може вибирати криптограми і отримувати відповідні відкриті тексти. Цей тип атаки може бути адаптивним, коли зловмисник має змогу вибирати шифртексти, спираючись на вже отриману інформацію.

Атака з вибором тексту (chosen-text attack) є найсильнішою з усіх перерахованих. Зловмисник може вибирати як зашифровані, так і відкриті тексти, що дає йому значно більшу свободу в атаці на систему шифрування.

Важливо зазначити, що в асиметричних криптосистемах (з відкритим ключем) ситуація дещо інша. Тут зловмисник завжди знає відкритий ключ,

і атака з вибором відкритого тексту є однією з найбільш слабких, оскільки зловмисник може завжди здійснити таку атаку. З іншого боку, якщо число можливих відкритих текстів обмежене, зловмисник може підготувати заздалегідь криптограми для перевірки їх на відповідність перехопленим повідомленням. Це дозволяє йому отримати відкриті тексти з високою ймовірністю. Така атака називається атакою з перевіркою тексту (verifiable-text attack).

Типи загроз, що стоять за атаками, можуть варіюватися від часткового розкриття до повного розкриття. Часткове розкриття означає, що зловмисник отримує лише частину інформації про секретний ключ або відкритий текст. Повне розкриття передбачає, що зловмисник може відновити секретний ключ або знайти еквівалентний алгоритм для дешифрування без необхідності знати секретний ключ. Ці загрози є серйозними, оскільки вони можуть призвести до повного компрометування криптосистеми.

У разі атак на електронний підпис (ЕЦП) класифікація також передбачає кілька типів. Зловмисник може знати лише відкритий ключ, мати доступ до набору підписаних повідомлень або навіть вибирати повідомлення для отримання підпису. Зростання сили атаки зазвичай корелює з доступом до більшої кількості інформації, що дозволяє зловмиснику значно легше знайти слабкі місця у підписній схемі.

Загрози для схеми електронного підпису варіюються від екзистенціальної підробки (коли зловмисник підробляє підпис для випадкових повідомлень) до універсальної підробки (коли зловмисник може знайти алгоритм для обчислення підпису без знання секретного ключа). Стійкість до цих атак забезпечується складністю математичних задач, таких як факторизація чи знаходження дискретного логарифма, але ймовірність атаки зростає з полегшенням доступу до необхідних обчислювальних ресурсів.

Загалом, атаки на шифрсистеми та ЕЦП визначають важливі аспекти безпеки криптографічних протоколів. Розуміння різних типів атак та загроз дозволяє розробляти більш стійкі шифрсистеми і системи електронного підпису, що забезпечують надійний захист від потенційних загроз.

Атаки на симетричні шифрсистеми

✱ **Атака на основі відомих шифртекстів (ciphertext-only attack)**

Зловмисник має доступ лише до криптограм, але не до відкритого тексту або секретного ключа. Це одна з найслабших атак, і багато сучасних криптосистем успішно протистоять їй. Однак деякі старі чи прості шифри, такі як шифр Цезаря, можуть бути вразливими до таких атак. Для успішної

реалізації атаки зловмиснику потрібно застосувати методи статистичного аналізу або атак на основі частотного аналізу. Вони дозволяють виявити закономірності у криптограмах, що можуть дати підказки для розшифрування. У випадку сучасних криптосистем, таких як AES, ймовірність успіху атак на основі шифртекстів мінімальна завдяки високій криптографічній складності.

✿ **Атака на основі відомих відкритих текстів (known-plaintext attack)**

У цьому випадку зловмисник знає пару криптограм та відповідних їм відкритих текстів. Цей тип атаки може бути ефективним проти певних поточкових шифрів, зокрема тих, що використовують лінійні зворотні зв'язки у регістрах зсуву. Зловмисник може використовувати ці відомі пари для створення математичних моделей, що дозволяють вивести секретний ключ або зламати шифр. Деякі криптосистеми, зокрема блокові шифри, можуть бути стійкими до таких атак за умови використання додаткових заходів захисту, таких як заміни чи додавання "псевдовипадкових" елементів. Однак якщо шифр не має достатнього рівня складності, атака на основі відомих відкритих текстів може призвести до компрометації системи. Важливою мірою захисту від цієї атаки є уникнення повторення однакових відкритих текстів, що дозволяє значно ускладнити процес криптоаналізу.

✿ **Атака з вибором відкритих текстів (chosen-plaintext attack)**

Зловмисник може вибрати відкриті тексти для шифрування і отримати відповідні їм шифртексти. Ця атака може стати можливою, наприклад, через фізичні вразливості (погано захищені КЗІ, коли оператор залишив їх активними на деякий час). У такому випадку зловмисник може підготувати набори відкритих текстів, які мають стратегічне значення для подальшого криптоаналізу. Зокрема, якщо система не реалізує достатнього рівня захисту, зловмисник може експлуатувати навіть мінімальні проміжки часу, коли криптосистема не є надійно заблокованою. Це дозволяє йому зібрати достатньо інформації для побудови математичних моделей і відновлення секретного ключа. Протидіяти такій атаці можна, використовуючи методи захисту, які унеможливлюють доступ до системи під час її роботи або забезпечують додаткові механізми захисту даних.

✿ **Адаптивна атака з вибором відкритих текстів (adaptive chosen-plaintext attack)**

У цьому випадку зловмисник може вибирати нові відкриті тексти на основі вже отриманих криптограм. Цей тип атаки дозволяє зловмисникові адаптувати стратегію в реальному часі, що значно підвищує її ефективність. Оскільки зловмисник має доступ до результатів попередніх

операцій шифрування, він може вибрати нові відкриті тексти таким чином, щоб максимізувати кількість корисної інформації. Завдяки адаптивності атаки він може поступово наближатися до розкриття алгоритму шифрування або секретного ключа. Для протидії таким атакам часто застосовуються методи, що включають періодичну зміну ключів або додаткові рівні захисту, які ускладнюють адаптацію атакуючого.

✿ Атака з вибором шифртекстів (chosen-ciphertext attack)

Зловмисник має доступ до криптограм та може отримати відповідні відкриті тексти. Це одна з сильніших атак, оскільки зловмисник може використовувати конкретні криптограми для зворотного шифрування. Атака з вибором шифртекстів дозволяє зловмисникові отримувати доступ до додаткової інформації про систему шифрування, що значно підвищує її ефективність. Зловмисник може вибрати певні шифртексти для дешифрування і таким чином відновити відкриті тексти, що дозволяє аналізувати властивості криптографічного алгоритму. Вибір шифртекстів може бути здійснений через уразливості в системі, наприклад, через доступ до деяких елементів криптографічної інфраструктури або через атакуючі запити до деяких серверів. Для захисту від таких атак використовуються механізми, що ускладнюють доступ до відповідних відкритих текстів, наприклад, техніки аутентифікації шифрованих повідомлень.

✿ Адаптивна атака з вибором шифртекстів (adaptive chosen-ciphertext attack)

Зловмисник вибирає нові криптограми, знаючи вже отримані відкриті тексти. Це ще сильніша атака, оскільки зловмисник може постійно коригувати свої дії на основі попередніх результатів. Адаптивна атака з вибором шифртекстів дозволяє зловмисникові поступово отримувати все більше інформації, що значно підвищує її ефективність. Зловмисник може модифікувати свої запити для досягнення конкретних результатів, що дозволяє йому знизити рівень непередбачуваності в дешифруванні. Завдяки такій атаці зловмисник може з часом дізнатися більше про структуру криптографічної системи та алгоритм, що використовується для шифрування. Для захисту від таких атак часто застосовують техніки, які включають в себе перевірку достовірності даних або використання схем, стійких до адаптивних атак, таких як шифри з підписом або гібридні системи.

✿ Атака з вибором тексту (chosen-text attack)

У цьому випадку зловмисник може вибрати як шифртексти для дешифрування, так і відкриті тексти для шифрування. Це одна з найсильніших атак. Атака з вибором тексту дозволяє зловмисникові

отримати значний контроль над процесом шифрування і дешифрування, оскільки він може вибирати як зашифровані, так і незашифровані дані. Це значно підвищує ймовірність знаходження вразливостей у криптографічній системі, оскільки зловмисник може експериментувати з різними варіантами текстів для з'ясування властивостей шифру. Така атака зазвичай вимагає значних обчислювальних ресурсів та часу для досягнення бажаних результатів. Враховуючи її потужність, проти атаки з вибором тексту застосовуються сучасні схеми шифрування, які включають додаткові механізми захисту, як-от двоетапне шифрування або динамічне генерування ключів.

Атаки на асиметричні шифросистеми

Для асиметричних систем, де використовується публічний та приватний ключ, атаки також можна класифікувати за типом обраного тексту або криптограми:

1. Адаптивна атака з вибором відкритого тексту (chosen-plaintext attack)

Хоча зловмисник завжди має публічний ключ, атака з вибором відкритого тексту є найслабшою в контексті асиметричних криптосистем. Цей тип атаки вимагає, щоб зловмисник мав можливість вибирати відкриті тексти для шифрування, після чого він отримує відповідні шифртексти. У асиметричних криптосистемах, таких як RSA, атака з вибором відкритого тексту має обмежену ефективність через складність математичних операцій, необхідних для зламу системи. Однак у деяких випадках, якщо криптосистема має вразливості або недостатній рівень ключової складності, така атака може бути використана для виявлення певних слабких місць. Сучасні алгоритми, як правило, включають додаткові механізми захисту від таких атак, зокрема, використання додаткових випадкових компонентів при шифруванні. Приклад адаптивної атаки з вибором відкритого тексту можна навести на прикладі класичної криптосистеми RSA. У такій атаці зловмисник може вибирати конкретні відкриті тексти, які хоче зашифрувати, і отримувати відповідні шифротексти, що дозволяє йому спробувати виявити деякі властивості шифру. Наприклад, якщо зловмисник може надіслати кілька вибраних повідомлень на шифрування та отримати їх зашифровані варіанти, він може спробувати здійснити статистичний аналіз або побудувати математичні моделі для відновлення секретного ключа.

У випадку з RSA, атака може бути ефективною в тому випадку, якщо криптосистема неправильно реалізована або використовує слабкі ключі. Наприклад, якщо під час шифрування використовується недостатньо велика кількість бітів для ключа, або якщо алгоритм має вразливості до

таких атак, це може дозволити зловмиснику побудувати відповідність між відкритим текстом і шифротекстом, що дає можливість зрештою відновити частину секретної інформації або знайти секретний ключ.

Сучасні реалізації RSA і інших асиметричних алгоритмів захищені від таких атак через використання додаткових заходів, таких як padding (додавання випадкових бітів), що робить шифротекст більш випадковим і таким чином ускладнює атаку з вибором відкритого тексту.

2. Атака з перевіркою тексту (verifiable-text attack)

Якщо можливі відкриті тексти обмежені, зловмисник, знаючи публічний ключ, може підготувати криптограми для кожного можливого відкритого тексту та порівняти їх з перехопленими. Цей тип атаки застосовується до ситуацій, коли обсяг можливих відкритих текстів невеликий або обмежений. Зловмисник може перерахувати всі можливі варіанти відкритих текстів і за допомогою публічного ключа зашифрувати їх, створюючи відповідні криптограми. Після цього він порівнює ці криптограми з тими, що були перехоплені, і, знайдавши збіги, отримує відповідний відкритий текст. Хоча цей тип атаки може бути ефективним у випадку обмеженого простору відкритих текстів, сучасні криптосистеми часто використовують великі простори ключів та додаткові механізми захисту для ускладнення такого підходу. Приклад атаки з перевіркою тексту можна продемонструвати на простому випадку з криптосистемою RSA, де обсяг можливих відкритих текстів обмежений, наприклад, через використання обмеженого словника. У такому випадку зловмисник, знаючи публічний ключ, може перерахувати всі можливі повідомлення з цього словника та зашифрувати їх за допомогою цього публічного ключа, отримуючи відповідні шифротексти. Після цього зловмисник порівнює ці зашифровані варіанти з перехопленими шифротекстами, і якщо він знаходить збіг, це означає, що відповідний зашифрований текст є копією одного з перехоплених. Оскільки простір можливих відкритих текстів обмежений, такий підхід може бути ефективним для відновлення оригінального відкритого тексту. Наприклад, якщо зловмисник знає, що повідомлення є одним із кількох стандартних повідомлень або має певний шаблон (наприклад, вхідний код або ідентифікаційний номер), він може створити криптограми для всіх можливих варіантів і порівняти їх з перехопленим шифротекстом, що дозволить знайти відповідний відкритий текст. Сучасні криптосистеми, як правило, використовують великі простори ключів і значні обсяги даних для зашифрування, що значно ускладнює або робить неможливим проведення такої атаки.

Типи загроз для криптосистем

▲ Часткове розкриття

Зловмисник отримує часткову інформацію про секретний ключ або відкритий текст, що може бути корисно для наступних атак. Це може відбутися, наприклад, через витoki інформації в процесі обробки даних або через зловживання недоліками криптосистеми. Часткове розкриття може дозволити зловмиснику застосувати методи криптоаналізу, зокрема атаки на основі статистики або навіть часткових знань про структуру ключа. Зловмисник може поступово збирати часткову інформацію, що з часом наближає його до розкриття повного секретного ключа або відновлення відкритого тексту. Для захисту від таких загроз використовуються додаткові заходи, як, наприклад, частіше оновлення ключів і використання складніших алгоритмів шифрування.

▲ Розкриття тексту

Зловмисник повністю відновлює відкритий текст, що є серйозною загрозою для безпеки. Таке розкриття може статися через уразливості в криптосистемі або через невірно реалізовані алгоритми шифрування. У разі повного розкриття тексту зловмисник може отримати доступ до конфіденційної інформації, що призведе до серйозних наслідків, таких як витік даних або зловживання приватними даними. Розкриття тексту може стати результатом атаки з вибором шифртекстів або зловживання уразливістю в криптографічних протоколах. Для мінімізації цієї загрози необхідно регулярно оновлювати алгоритми шифрування та застосовувати методи захисту, які ускладнюють отримання відкритого тексту з шифртексту.

▲ Повне розкриття

Зловмисник отримує доступ до секретного ключа або знаходить алгоритм розшифрування без необхідності знати цей ключ. Повне розкриття може виникнути через слабкі алгоритми шифрування або недостатньо сильні методи захисту ключів. Коли зловмисник отримує доступ до секретного ключа, він може дешифрувати будь-які дані, що були захищені цим ключем, що робить систему вразливою до подальших атак. У разі знаходження алгоритму розшифрування без знання ключа, зловмисник може успішно обробляти зашифровану інформацію без необхідності доступу до конфіденційних даних. Для запобігання повному розкриттю необхідно застосовувати складніші шифри, постійну ротацію ключів та механізми додаткового захисту, такі як багатофакторна аутентифікація та апаратні модулі безпеки.

Специфічні загрози для систем ЕЦП

1. Екзистенціальна підrobка

Зловмисник підробляє підпис хоча б для одного повідомлення, яке не було підписано під час атаки. Екзистенціальна підробка є серйозною загрозою, оскільки зловмисник може згенерувати підроблений підпис для будь-якого повідомлення, навіть якщо це повідомлення не було створено оригінальним відправником. Така атака може призвести до серйозних наслідків, якщо зловмисник використає підроблений підпис для введення в оману одержувача або системи. Для запобігання екзистенціальній підробці важливо використовувати криптографічні методи, що забезпечують незворотність підпису та ускладнюють його підробку. Наприклад, це можуть бути алгоритми з використанням сильних хеш-функцій та асиметричних ключів, що робить підробку підпису практично неможливою без знання секретного ключа.

2. Селективна підробка

Підробка підпису для конкретного повідомлення, обраного зловмисником до початку атаки. Селективна підробка дозволяє зловмиснику створювати підроблені підписи для конкретних повідомлень, які він обирає до початку атаки. Така атака є більш цілеспрямованою та специфічною, оскільки зловмисник має можливість вибрати лише певні повідомлення для підробки, що дозволяє уникнути широкого охоплення. Однак, навіть за умов селективної підробки, можна виявити вразливість у криптографічній системі, якщо вона не забезпечує належного захисту підписів. Для запобігання селективній підробці важливо використовувати методи, які ускладнюють вибір конкретних повідомлень для атаки, зокрема шляхом застосування криптографічних протоколів, що забезпечують непередбачуваність у виборі підписуваних даних.

3. Універсальна підробка

Зловмисник знаходить алгоритм, що еквівалентний алгоритму обчислення підпису без знання секретного ключа. Універсальна підробка є серйозною загрозою, оскільки зловмисник може підробити підпис для будь-якого повідомлення, не маючи доступу до секретного ключа. Це можливо завдяки тому, що зловмисник знаходить або обчислює алгоритм, який дозволяє йому генерувати підписи без знання ключа підпису. Така вразливість може виникнути, якщо криптографічний алгоритм має слабкі місця, які можна експлуатувати для обчислення підписів без авторизації. Для захисту від універсальної підробки необхідно використовувати стійкі до атак криптографічні протоколи та алгоритми, які забезпечують належний рівень безпеки навіть за наявності потенційно небезпечних вразливостей.

Оцінка стійкості

Практична стійкість криптосистем залежить від складності математичних задач, на яких вони ґрунтуються. Наприклад, стійкість системи базується на таких задачах, як факторизація чисел або дискретний логарифм. Однак важливо враховувати, що ефективність криптосистеми повинна бути адекватною до потенційних ризиків і вартості витрат на криптоаналіз. Крім того, на стійкість системи впливає ймовірність розв'язання цих математичних задач за допомогою сучасних обчислювальних потужностей, що постійно зростають. З розвитком квантових обчислень, задачі, на яких ґрунтуються традиційні криптосистеми, можуть стати вразливими до нових методів розв'язування. Тому важливо враховувати не лише математичну складність, а й потенційні нові технології криптоаналізу. Таким чином, постійна перевірка і адаптація криптосистем до нових загроз є необхідною умовою забезпечення їх стійкості в умовах швидкого розвитку технологій.

16.3. Властивості елементарних шифрів

Шифрувальні системи (шифрсистеми) відіграють важливу роль у забезпеченні інформаційної безпеки, дозволяючи захищати дані від несанкціонованого доступу під час їх передачі або зберігання. Вони поділяються на кілька типів залежно від різних критеріїв.

Шифрувальні системи (шифрсистеми) — це сукупність методів, алгоритмів і засобів, призначених для перетворення інформації з метою приховування її змісту від несанкціонованого доступу. Основним завданням шифрсистем є забезпечення конфіденційності, цілісності та автентичності даних під час їх зберігання або передачі через інформаційні канали.

Принцип роботи шифрсистем полягає в перетворенні вихідного тексту (відкритого) у шифротекст за допомогою спеціального алгоритму та ключа. Розшифрування виконується у зворотному порядку для відновлення початкової інформації. Залежно від типу ключа шифрсистеми поділяються на симетричні та асиметричні. Симетричні шифри використовують один ключ для шифрування та розшифрування (AES, DES), тоді як асиметричні (RSA, ECC) передбачають використання двох ключів — відкритого та закритого.

Крім того, шифрсистеми класифікуються за типом операцій з даними (потоківі та блочні), за призначенням (для конфіденційності, цифрового підпису або гешування), а також за стійкістю до квантових атак. Завдяки цьому вони широко застосовуються для захисту інформації в мережах

зв'язку, базах даних, банківських системах та інших критично важливих сферах.

Одним із ключових критеріїв класифікації є тип ключа, який використовується для шифрування та розшифрування інформації. Симетричні шифрсистеми передбачають використання одного й того ж ключа обома сторонами комунікації. Вони мають високу швидкість роботи, однак складні у керуванні ключами. Прикладами таких систем є AES та DES. Натомість асиметричні шифрсистеми використовують пару ключів — відкритий для шифрування та закритий для розшифрування. Це полегшує процес обміну ключами, але робить процес шифрування повільнішим. Серед відомих асиметричних алгоритмів можна виділити RSA та алгоритми на основі еліптичних кривих.

Ще одним важливим критерієм є спосіб обробки даних. Поточкові шифри, такі як RC4, шифрують інформацію побітно або побайтно, що робить їх ефективними для поточкових передавань даних. Натомість блочні шифри, наприклад AES або Blowfish, працюють із блоками фіксованого розміру, що забезпечує високу стійкість до атак за правильного вибору режиму шифрування.

Важливим аспектом класифікації є призначення шифрсистем. Вони можуть забезпечувати конфіденційність інформації, як це роблять класичні шифри (AES, DES), або ж гарантувати автентифікацію та цілісність повідомлень через використання цифрових підписів, таких як DSA. Окрему категорію становлять системи гешування, що дозволяють контролювати цілісність даних (SHA-256).

Залежно від алгоритмічної основи, шифрсистеми поділяються на шифри перестановки, де символи міняються місцями, шифри підстановки, де символи замінюються іншими, та комбіновані методи, що поєднують обидва підходи. Наприклад, класичний шифр Цезаря належить до шифрів підстановки.

Окремо виділяються шифрсистеми за стійкістю до квантових обчислень. Класичні шифри є вразливими до атак квантових комп'ютерів, тому сучасна криптографія активно розробляє квантово-стійкі алгоритми, наприклад на основі решіток.

Таким чином, класифікація шифрсистем дозволяє зрозуміти їх різноманіття, особливості використання та вибрати найкращі рішення для захисту інформації залежно від конкретних потреб підприємства або іншої сфери застосування.

Шифрувальні системи (шифрсистеми) є основою криптографії та забезпечення інформаційної безпеки. Вони використовуються для захисту конфіденційності інформації під час її передачі або зберігання.

Шифрсистеми можна класифікувати за різними критеріями

✳ За типом ключа:

- **Симетричні шифрсистеми**

Відправник і отримувач використовують один і той самий ключ для шифрування та розшифрування інформації. Приклади: AES, DES, Triple DES. Особливості: висока швидкість шифрування, але складність управління ключами.

- **Асиметричні шифрсистеми**

Використовуються два різних ключі — відкритий для шифрування та закритий для розшифрування. Приклади: RSA, ElGamal, ECC (еліптичні криві). Особливості: простота обміну ключами, але нижча швидкість порівняно з симетричними методами.

2. За типом операції з даними

- **Потокові шифри**

Шифрують дані побітно або побайтно в режимі потоку. Приклади: RC4, Salsa20. Особливості: ефективні для поточкових передавань інформації.

- **Блочні шифри**

Шифрують інформацію блоками фіксованого розміру (наприклад, 128 біт). Приклади: AES, DES, Blowfish. Особливості: висока стійкість до атак за умови правильного режиму шифрування.

3. За призначенням

- **Класичні шифрувальні системи**

Призначені для забезпечення конфіденційності даних. Приклади: DES, AES.

- **Криптографічні системи цифрового підпису**

Забезпечують автентифікацію та цілісність повідомлень. Приклади: DSA, ECDSA.

- **Системи хешування**

Забезпечують контроль цілісності даних. Приклади: SHA-256, MD5.

4. За алгоритмічною основою:

- **Шифри перестановки**

Міняють місцями символи повідомлення за визначеним правилом.

- **Шифри підстановки**

Заміщають символи повідомлення іншими символами. Приклад: Шифр Цезаря.

- **Комбіновані шифри**

Поєднують методи перестановки та підстановки.

5. За стійкістю до квантових атак:

- **Класичні шифри**

Вразливі до атак квантових обчислювачів.

- **Квантово-стійкі шифри**

Розроблені для протидії квантовим атакам. Приклади: алгоритми на основі решіток (Lattice-based cryptography).

Класифікація шифрсистем дозволяє краще розуміти їх властивості та вибирати оптимальні рішення для забезпечення інформаційної безпеки. Залежно від цілей захисту та контексту використання важливо правильно обирати між симетричними, асиметричними чи комбінованими методами шифрування.

Системи шифрування класифікуються залежно від синхронізації процедур шифрування-розшифрування та організації передачі зашифрованих даних у каналі зв'язку.

Види систем шифрування

1. Попереднє шифрування

Цей підхід передбачає попереднє криптографічне перетворення інформації перед її передачею. Момент передачі повідомлення визначає передавач. Попереднє шифрування широко використовується у випадку електронної пошти, хмарних сховищ та месенджерів із функцією наскрізного шифрування, таких як Signal або ProtonMail. Попереднє шифрування дозволяє значно підвищити рівень безпеки інформації навіть у разі компрометації каналу зв'язку. Зашифровані дані можуть зберігатися тривалий час без ризику їх розкриття, поки не буде надано відповідний ключ для розшифрування. Цей підхід є особливо актуальним для захисту конфіденційних документів та приватного листування. Завдяки попередньому шифруванню повідомлення стає недоступним для несанкціонованого доступу навіть під час передачі через загальнодоступні мережі. Протоколи, які реалізують попереднє шифрування, зазвичай використовують асиметричні алгоритми, такі як RSA або сучасні квантово-стійкі алгоритми. Важливим аспектом цього підходу є можливість автентифікації відправника через цифровий підпис. Попереднє шифрування також дозволяє забезпечити цілісність даних, захищаючи їх від модифікацій під час передачі.

2. Лінійне засекречування (синхронні потокові шифри)

Ця система базується на узгодженій роботі шифрувальних пристроїв та засобів зв'язку. Вона забезпечує синхронну роботу генераторів поточкових

шифрів на обох кінцях зв'язку, що є важливим для захисту телефонних розмов або інших реального часу комунікацій, таких як VoIP. Лінійне засекречування забезпечує високу швидкість шифрування, оскільки обробка даних відбувається потоком без необхідності розбивки на блоки. Цей підхід є ефективним для захисту голосових дзвінків, відеоконференцій та потокової передачі мультимедійних даних. Система використовує генератори псевдовипадкових чисел для створення ключового потоку, який змішується з відкритим текстом для отримання шифротексту. Синхронізація генераторів є критично важливою, оскільки навіть незначні збої можуть призвести до втрати синхронізації та спотворення переданих даних. Для відновлення синхронізації використовуються спеціальні механізми повторного узгодження ключів. Вразливістю цього підходу є можливість перехоплення даних під час моментів синхронізації, тому додаткові механізми автентифікації можуть підвищити безпеку. Лінійне засекречування знаходить широке застосування в мобільних мережах і захищених каналах корпоративного зв'язку.

Загалом, для забезпечення роботи таких систем використовуються генератори поточкових шифрів, які ініціалізуються за допомогою ключової інформації та даних синхронізації. У разі збою на лінії зв'язку система автоматично перезапускає генератори для збереження синхронізації.

Переваги та недоліки

Перевагою лінійного засекречування є ефективне використання пропускної здатності каналу зв'язку та швидке шифрування даних у режимі реального часу. Водночас системи попереднього шифрування дозволяють зберігати повідомлення у зашифрованому вигляді на тривалий час і надійно захищати їх до моменту розшифрування.

Сучасні тенденції

Із розвитком квантових обчислень і нових видів загроз актуальними стають квантово-стійкі шифрувальні системи, які базуються на алгоритмах, стійких до атак квантових комп'ютерів (наприклад, алгоритми на основі решіток). Крім того, активно розвиваються гібридні системи шифрування, що поєднують переваги симетричних та асиметричних алгоритмів для підвищення безпеки й продуктивності.

Засоби шифрування дедалі частіше інтегруються у програмне забезпечення та апаратні пристрої, дозволяючи автоматизувати процеси захисту даних і мінімізувати ризики компрометації інформації.

Властивості елементарних шифрів

Елементарні шифри є базовими криптографічними операціями, які забезпечують основу для створення складних шифрувальних систем. До

основних типів таких шифрів належать перестановка та підстановка, кожна з яких має свої властивості й особливості використання. Перестановка змінює порядок символів у тексті без їх заміни, що дозволяє рівномірно розподілити інформацію у зашифрованому повідомленні. Однак цей метод не змінює частотного розподілу символів відкритого тексту, тому залишається вразливим до статистичних атак. Перестановка часто використовується як один із етапів блокового шифрування, як, наприклад, у DES.

Підстановка, на відміну від перестановки, замінює символи тексту за визначеним ключем або правилом. Цей метод змінює статистичний розподіл символів, що значно ускладнює криптоаналіз. Підстановка може бути простою, коли кожен символ замінюється одним іншим символом, або складною, коли заміні підлягає блок символів. Сучасні симетричні алгоритми, такі як AES, активно використовують цей метод.

Для підвищення надійності шифрування найчастіше застосовується комбінація підстановки та перестановки. Це дозволяє поєднати їх переваги та створити складні криптографічні перетворення. У блокових шифрах послідовне застосування підстановок і перестановок є основою для забезпечення високого рівня стійкості до атак.

Однією з ключових властивостей елементарних шифрів є реверсивність — можливість виконати зворотне перетворення для розшифрування даних. Важливою є також відповідність довжини тексту, особливо для поточкових шифрів, де довжина повідомлення після шифрування має залишатися незмінною. Елементарні шифри також характеризуються ефективністю, оскільки їх операції виконуються швидко, що дозволяє використовувати їх для захисту великих обсягів інформації в режимі реального часу.

Завдяки властивостям композиційності елементарні шифри можуть комбінуватися у різних конфігураціях, створюючи сучасні криптографічні алгоритми, які відповідають високим вимогам безпеки. Саме тому їх вивчення та використання залишаються актуальними в сучасній криптографії.

16.4. ТЕОРЕТИЧНА ТА ПРАКТИЧНА СТІЙКІСТЬ, АБСОЛЮТНО СТІЙКИЙ ШИФР

Теоретична стійкість шифру означає його здатність витримувати математичні атаки при ідеальних умовах, коли атакуюча сторона має доступ лише до зашифрованого тексту і не має додаткової інформації

(наприклад, до ключа або частини відкритого тексту). Теоретична стійкість визначається на основі криптографічної складності, яка включає в себе кількість можливих варіантів для атаки (наприклад, кількість можливих ключів) і складність відновлення відкритого тексту при застосуванні стандартних методів криптоаналізу.

Практична стійкість — це здатність шифру залишатися захищеним у реальних умовах, з урахуванням обмежень на обчислювальні ресурси та час, доступних зломиснику. Тут важливі не тільки математичні принципи, але й апаратні та програмні засоби, а також можливості для реалізації атак на конкретні реалізації алгоритму. Практична стійкість може бути знижена через слабкості у впровадженні або через недостатньо довгі ключі, що дозволяють зломиснику виконати атаку методом перебору або через вразливості в конкретному криптографічному протоколі.

Абсолютно стійкий шифр — це ідеальний шифр, стійкий до будь-яких видів атак, навіть якщо атакуючий має необмежену обчислювальну потужність і доступ до необмеженої кількості зашифрованих повідомлень. Такий шифр має дві основні характеристики:

1. Невизначеність

Кожне зашифроване повідомлення має рівноцінні ймовірності для кожного можливого відкритого тексту. Тобто, неможливо однозначно виявити відкритий текст за допомогою лише зашифрованого тексту.

2. Невідповідність між шифром і відкритим текстом

Ідеальний шифр не дає жодної додаткової інформації про структуру відкритого тексту або його властивості, що робить неможливим криптоаналіз навіть при значній кількості зашифрованих повідомлень.

Приклад абсолютно стійкого шифру — це шифр Вернама (також відомий як одноразовий блокнот). У цьому шифрі ключ має таку ж довжину, як і повідомлення, і використовується лише один раз. Ключ генерується випадковим чином і повністю покриває текст повідомлення, що робить шифр абсолютно стійким до всіх атак. Однак через вимоги до довжини ключа та необхідність його секретного обміну, на практиці такий шифр рідко використовується в реальних системах. Шифр Вернама забезпечує ідеальну криптографічну стійкість, оскільки кожен біт ключа використовується тільки один раз, і його можна легко знищити після використання, що виключає можливість повторного використання. Це гарантує, що навіть якщо зломисник перехопить зашифроване повідомлення, без доступу до ключа він не зможе здійснити розшифрування, оскільки немає жодної закономірності, за якою можна було б відновити текст. Одноразовий блокнот є теоретичним ідеалом безпеки в криптографії, який не піддається жодним відомим методам

криптоаналізу. Проблеми виникають через необхідність забезпечення безпеки і обміну великими ключами, що обмежує його використання в реальному світі. У випадку великої кількості повідомлень, для кожного з яких потрібно генерувати новий ключ, забезпечити надійність обміну стає складним завданням. Крім того, через вимоги до довжини ключа, шифр може стати неефективним для систем з великою кількістю даних, оскільки ключі будуть дуже великими та складними для зберігання та передачі. Тим не менше, шифр Вернама продовжує використовуватися в особливих випадках, таких як захист високочутливої інформації в критичних системах або в умовах, де можна забезпечити безпечний обмін ключами.

Загалом, абсолютно стійкий шифр є ідеалом у теоретичній криптографії, але в реальному світі такі шифри є складними для реалізації та мають обмеження щодо практичності використання.

Теоретична стійкість

Теоретична стійкість криптосистеми визначається на основі математичних принципів і алгоритмів, на яких вона ґрунтується. Вона полягає в складності вирішення криптографічних задач, що використовуються в системі, таких як факторизація великих чисел або вирішення дискретного логарифму. Якщо ці задачі є складними для класичних обчислювальних машин, то теоретично система може вважатися стійкою. Теоретична стійкість залежить від математичної моделі і припускає, що не існує швидких алгоритмів для розв'язання цих задач. Теоретична стійкість також враховує припущення щодо обмеженості обчислювальних ресурсів і часу, необхідного для проведення криптоаналізу. Вона оцінюється за допомогою формальних доказів, що підтверджують, що проблема, на основі якої будується криптографічна система, є складною з математичної точки зору. Крім того, теоретична стійкість залежить від можливості існування нових методів чи технологій, які можуть змінити оцінку складності задачі. Вона також враховує вірогідність можливих поліпшень у розв'язуванні задач за допомогою нових наукових відкриттів або обчислювальних підходів. Важливо зазначити, що теоретична стійкість не завжди гарантує захист у реальних умовах, оскільки практична реалізація криптосистеми може мати вразливості, які не відображаються в теоретичних моделях. Крім того, теоретична стійкість не враховує фактори, такі як атаки на основі людського фактора чи фізичні вразливості системи. Тому важливо проводити оцінку криптосистеми не тільки з теоретичної точки зору, але й у реальних умовах експлуатації.

Теоретична стійкість криптосистеми оцінюється на основі складності математичних задач, на яких вона ґрунтується, і визначається здатністю цих задач залишатися важкими для розв'язання, навіть з використанням найбільш потужних класичних обчислювальних методів. Тобто, теоретична стійкість передбачає, що для зловмисника неможливо швидко розв'язати ключові криптографічні задачі, на яких базується шифрування або підписування, без наявності секретного ключа.

Одним з основних критеріїв теоретичної стійкості є математична складність задач, таких як факторизація великих чисел (для RSA) або обчислення дискретного логарифму (для систем, що використовують алгоритми на основі дискретного логарифму). Якщо наукове співтовариство не змогло знайти ефективний алгоритм для розв'язання цих задач за розумний час, криптосистема вважається теоретично стійкою.

Крім того, теоретична стійкість також враховує відсутність ефективних методів для проведення атак на криптографічні алгоритми в контексті певної криптографічної моделі (наприклад, атаки з вибором відкритих текстів або криптографічного аналізу). Однак теоретична стійкість не завжди відповідає реальним умовам, оскільки нові теореми або алгоритми можуть змінити оцінку складності задач, а також нові обчислювальні потужності або алгоритми квантових обчислень можуть вплинути на стійкість криптосистем.

Практична стійкість

Практична стійкість криптосистеми полягає в її здатності витримати реальні атаки за допомогою доступних обчислювальних потужностей. Вона враховує не лише складність математичних задач, але й ефективність застосовуваних криптоаналітичних методів, а також можливості сучасних обчислювальних засобів, таких як суперкомп'ютери та квантові обчислення. Практична стійкість залежить від того, як швидко зловмисники можуть розв'язати криптографічні задачі за допомогою існуючих технологій. Вона також враховує фактори, як довжина ключа, швидкість алгоритмів шифрування та розшифрування, а також рівень захисту від атак на фізичному рівні. Практична стійкість визначається також здатністю криптосистеми протистояти атакувальним методам, таким як атаки на основі вибору тексту або шифртексту, а також потенціалу нових уразливостей, що можуть виникнути в результаті розвитку технологій. Важливим аспектом є також наявність стандартів та протоколів, які забезпечують додатковий рівень захисту в умовах реальних атак. Практична стійкість з часом може змінюватися в залежності від розвитку нових методів криптоаналізу та потужностей для проведення

атак, зокрема в епоху квантових комп'ютерів, що можуть порушити багато сучасних криптографічних алгоритмів. Оцінка практичної стійкості криптосистеми також включає її здатність адаптуватися до нових умов і методів атак, що робить її важливою частиною загальної стратегії кібербезпеки. Це вимагає регулярного оновлення алгоритмів і протоколів з урахуванням нових досягнень в галузі криптографії та комп'ютерних наук. Врахування цих факторів дозволяє організаціям ефективно забезпечувати безпеку своїх систем у умовах постійних змін. Окрім того, важливою є роль апаратного забезпечення та його вплив на здатність криптосистеми витримувати атаки в реальному світі.

Отже, теоретична стійкість є основою для оцінки надійності криптосистеми в теорії, а практична стійкість — це її реальний захист від атак у конкретних умовах.

Практична стійкість криптосистеми оцінюється на основі її здатності витримати реальні атаки, зокрема, з використанням доступних на даний момент обчислювальних ресурсів. Це означає, що навіть якщо криптографічна задача, на якій ґрунтується система, є теоретично складною, криптосистема може бути вразливою до практичних атак, якщо існуючі технології дозволяють швидко розв'язувати ці задачі в реальному часі. Оцінювання практичної стійкості враховує кілька ключових факторів, таких як обчислювальні потужності, довжина ключа, квантові обчислення та атакуювальні методи.

Обчислювальні потужності, зокрема швидкість, з якою сучасні комп'ютери, суперкомп'ютери або спеціалізовані апаратні засоби (наприклад, ASIC) можуть обробляти криптографічні операції, визначають, чи є атака реалістичною. Чим більша довжина ключа в криптосистемі, тим більше часу знадобиться зловмисникові для проведення атаки методом перебору (brute force). Враховується, що з розвитком технологій довжина ключа повинна збільшуватися, щоб залишатися надійною в умовах зростаючих обчислювальних потужностей. Крім того, з розвитком квантових комп'ютерів багато сучасних криптосистем можуть стати уразливими до нових типів атак, таких як алгоритм Шора для факторизації чисел або обчислення дискретного логарифму, тому практична стійкість повинна також враховувати майбутні виклики, пов'язані з квантовими обчисленнями.

Оцінка також враховує існуючі та потенційні методи криптоаналізу, включаючи методи з вибором відкритих текстів, атаки на фізичному рівні (фізичний криптографічний аналіз) та інші методи, які можуть використовувати зловмисники. Практична стійкість оцінюється на основі того, скільки часу зловмисники зможуть витратити на успішне

дешифрування повідомлення або розкриття секретного ключа з використанням доступних ресурсів. Якщо за час, необхідний для виконання атак, можна легко зламати криптосистему, то вона вважається нестійкою з практичної точки зору. Такий підхід до оцінки практичної стійкості був запропонований Діффі та Хеллманом, які наголосили на необхідності враховувати реальні обчислювальні можливості та технологічний прогрес при розробці стійких криптографічних систем.

Абсолютно стійкий шифр (або ідеальний шифр)

Абсолютно стійкий шифр (або ідеальний шифр) — це такий шифр, який не дозволяє зловмиснику отримати жодної інформації про відкритий текст, навіть якщо він має доступ до шифртексту. Для такого шифру ймовірність відновлення відкритого тексту з шифртексту є рівною ймовірності кожного можливого варіанту відкритого тексту, тобто кожен шифртекст має однакову ймовірність відповідати будь-якому з можливих відкритих текстів.

Ідеальний приклад абсолютно стійкого шифру — це шифр Віженера, якщо ключ довший або рівний за довжину відкритого тексту і використовується лише один раз (так званий шифр "one-time pad"). У цьому випадку кожен символ відкритого тексту буде зашифрований випадковим чином, що унеможливило б відновлення відкритого тексту без знання ключа. Для абсолютної стійкості ключ повинен бути повністю випадковим, мати довжину, рівну довжині повідомлення, та використовуватись лише один раз, тобто не повторюватися в майбутньому.

Однак, на практиці абсолютна стійкість є важко досяжною через обмеження в безпечному обміні ключами та зберіганні великих випадкових ключів. Більшість сучасних криптографічних систем не досягають абсолютної стійкості через різноманітні обмеження, але вони пропонують достатній рівень захисту для більшості застосувань.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 16

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне

модельовання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.

4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.

5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

6. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

7. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

8. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.

9. Шевченко, С., Жданова, Ю., Спасітелєва, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

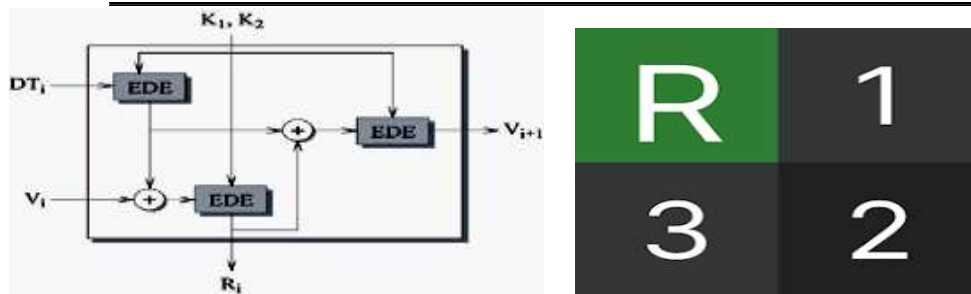
10. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.

11. Шевченко , С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до модельовання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.

12. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, *Cybersecurity Providing in Information and Telecommunication Systems* Vol. 3421 (2023) 56–66.
13. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 25–37. Спасітелева, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(21), 193–210.
14. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об’єктів критичної інфраструктури. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(17), 145–158.
15. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: *Workshop on Classic, Quantum, and Post-Quantum Cryptography*, vol. 3504 (2023) 12–25.
16. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3288 (2022) 142-148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in *Cybersec. Prov. Inf. Telecom. Syst. II*, vol. 3187, 2021, pp. 251–259.
17. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 2923 (2021) 117–124.
18. Y. Dreis, et al., Restricted Information Identification Model, in: *Cybersecurity Providing in Information and Telecommunication Systems* Vol. 3288 (2022) 89–95.
19. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, *Cryptography* 8(3), iss. 38 (2024) 1–17.

РОЗДІЛ 17

ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ І МЕТОДИ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ



17.1. Дані для формування ключової інформації

17.2. Статистичне тестування псевдовипадкових послідовностей

17.3. Генератори псевдовипадкових послідовностей

"Ідея використання псевдовипадкових чисел у криптографії є основою для безпечного обміну ключами, оскільки вони дозволяють створювати такі послідовності, які є складними для прогнозування, навіть коли їх частина відома."

Bruce Schneier, експерт з безпеки

17.1. Дані для формування ключової інформації

Формування ключової інформації для криптосистеми вимагає врахування кількох важливих факторів та даних, що забезпечують надійність і стійкість генерації ключів. До таких даних відносяться:

1. Справжня випадковість

Ключі мають бути створені з використанням джерел справжньої випадковості, таких як фізичні процеси, які неможливо передбачити, наприклад, шум в електронних пристроях або процеси, що виникають у навколишньому середовищі. Справжня випадковість забезпечує високу ентропію і непередбачуваність ключів, що важливо для криптографічної безпеки. Для отримання справжньої випадковості використовуються

фізичні явища, такі як тепловий шум або процеси, які важко моделювати чи відтворювати злоумисниками. Проте один з недоліків таких джерел полягає в необхідності наявності спеціального обладнання, що може зробити їх використання складним та дорогим. Однак, при належному використанні, справжня випадковість є однією з найбільш надійних основ для формування криптографічних ключів.

2. Псевдовипадкові числа

У разі неможливості забезпечити справжню випадковість, використовуються псевдовипадкові генератори, які повинні мати великі внутрішні стани і використовувати високоякісні алгоритми, щоб згенеровані числа виглядали випадковими. Проте важливо, щоб початкове значення або "насіння" (seed) для таких генераторів було достатньо випадковим і важким для передбачення. Псевдовипадкові генератори зазвичай працюють за допомогою детермінованих алгоритмів, що дозволяють відтворювати одну і ту ж послідовність чисел з однаковим насінням. Однак, якщо насіння слабке або передбачуване, псевдовипадкові числа можуть стати вразливими для атак. Для підвищення безпеки використовується комбінування кількох джерел випадковості, щоб зменшити ймовірність відновлення насіння злоумисниками. Псевдовипадкові генератори є економічно вигідними і достатньо ефективними для багатьох криптографічних застосувань, але їх надійність значною мірою залежить від якості використовуваних алгоритмів та механізмів генерації насіння.

3. Зовнішні джерела випадковості

Для покращення якості генерації ключів, можна використовувати комбінацію різних джерел випадковості, таких як системні таймери, рухи миші, натискання клавіш, показники температури чи інші фізичні величини. Ці джерела надають додаткову непередбачуваність у процесі генерації випадкових чисел, що знижує ризик виявлення шаблонів або повторень у створених ключах. Комбінація різних джерел також допомагає покращити стійкість до атак, що спрямовані на передбачення значень генератора. Для підвищення надійності часто використовують апаратні генератори випадкових чисел, які працюють безпосередньо з фізичними процесами в апаратному забезпеченні. Однак важливо, щоб збір таких даних був добре контрольований і зашифрований, аби запобігти їх маніпуляції або зловживанню злоумисниками.

4. Довжина ключа

Розмір ключа є важливим параметром, оскільки більші ключі зазвичай забезпечують більшу стійкість до атак. Для асиметричних систем, таких як

RSA, для досягнення високої стійкості потрібна велика довжина ключа, в той час як для симетричних шифрів можуть бути достатніми менші ключі, але з достатньою ентропією. Однак, з часом та з розвитком обчислювальних потужностей необхідно коригувати довжину ключа для підтримки надійності системи. Зокрема, для забезпечення довгострокової стійкості слід брати до уваги зростання обчислювальних потужностей і можливість майбутніх атак, таких як квантові обчислення. У багатьох випадках довжина ключа визначається стандартами і рекомендаціями криптографічних організацій, щоб забезпечити баланс між стійкістю та ефективністю системи. Важливо також, щоб система могла гнучко масштабувати довжину ключа відповідно до змін умов і нових викликів у сфері безпеки.

5. Використання криптографічних хеш-функцій

Для забезпечення цілісності і недоступності ключа для зломисників часто використовуються хеш-функції, що дозволяють перетворювати вихідні дані в унікальні короткі представлення. Це також є важливим етапом у процесі генерації ключів, де ключі часто проходять через багато етапів хешування для забезпечення їх стійкості. Хеш-функції допомагають забезпечити захист від атаки на базу даних, де зломисники можуть спробувати відновити оригінальний ключ або інші важливі дані. Використання солі (salt) разом з хешуванням додає додатковий рівень безпеки, ускладнюючи відновлення початкових даних навіть при наявності доступу до хешованих значень. Окрім цього, хеш-функції використовуються для створення цифрових підписів, де важливим є забезпечення унікальності та неможливості відновлення оригінальних даних з хешу. Вибір правильної криптографічної хеш-функції є критичним для забезпечення надійності та безпеки всієї криптосистеми.

6. Методи генерації ключів

Методи генерації ключів визначають спосіб створення криптографічних ключів, що використовуються для шифрування та дешифрування даних. Одним із популярних методів є використання псевдовипадкових генераторів чисел, які, на основі початкових значень (насіння), генерують послідовності чисел, що наближаються до випадкових. Однак для підвищення якості генерації ключів часто комбінують декілька джерел випадковості, щоб забезпечити більшу ентропію і меншу передбачуваність результатів. Іншим методом є використання криптографічних хеш-функцій, які застосовуються для перетворення великих обсягів даних у короткі та стійкі представлення, що використовуються як ключі. Для асиметричних систем, таких як RSA, ключі генеруються через складні

математичні операції, що включають обрання великих простих чисел і подальше їх використання для створення публічних та приватних ключів. Симетричні системи, на відміну від асиметричних, зазвичай використовують алгоритми генерації з меншою складністю, але з високою швидкістю роботи. У сучасних криптосистемах також можуть використовуватися спеціалізовані апаратні пристрої, які генерують ключі на основі фізичних процесів, що додає додатковий рівень безпеки.

Ключі можуть бути згенеровані за допомогою різних методів, зокрема:

- ✓ **Генератори на основі часу** - використання поточного часу для формування ключа.
- ✓ **Методи хешування** - пропускання даних через криптографічні хеш-функції.
- ✓ **Алгоритми дифузії** - створення ключів за допомогою складних математичних операцій, що забезпечують стійкість.

Ці елементи забезпечують ключову інформацію, яка необхідна для безпечного функціонування криптографічних алгоритмів і протистояння можливим атакам.

Значна кількість атак на криптосистеми базується на особливостях ключових даних. Невідповідний розподіл випадкових величин під час генерації ключів може створити вразливості, що дозволяють здійснити ефективні атаки, зокрема за допомогою часткового перебору найбільш ймовірних значень.

Ключовим аспектом для забезпечення стійкості криптографічних систем є генерація випадкових чисел із високою ентропією, що забезпечує непередбачуваність та стійкість до атак. Для цього використовуються апаратні генератори випадкових чисел, засновані на фізичних процесах (наприклад, квантовий шум), які забезпечують максимальну ентропію та ускладнюють прогнозування.

Враховуючи розвиток квантових технологій, традиційні криптографічні системи, такі як RSA та ECC, можуть стати вразливими до атак, здійснених за допомогою квантових алгоритмів, зокрема алгоритму Шора. Це призводить до пошуку нових підходів, таких як постквантова криптографія, яка передбачає використання алгоритмів, стійких до квантових атак.

Наразі активно досліджуються альтернативи традиційним схемам цифрового підпису, таким як ECDSA, з метою забезпечення більшої стійкості до атак. Особливу увагу привертає криптографія на решітках, яка, згідно з прогнозами, може стати основою для захисту від квантових атак.

Використання методів машинного навчання для криптографічного аналізу й пошуку вразливостей у криптографічних алгоритмах набирає популярності. Ці методи дозволяють швидко виявляти нові уразливості, які могли б бути непоміченими традиційними способами аналізу. Зокрема, на сьогодні активно розвиваються методи використання глибоких нейронних мереж для прогнозування ймовірності існування вразливостей.

Технології блокчейн і криптовалюти потребують удосконалення криптографічних алгоритмів для забезпечення стійкості до атак. Використання zk-SNARKs (Zero Knowledge Succinct Non-Interactive Arguments of Knowledge) є одним із таких підходів, що дозволяє забезпечити анонімність і конфіденційність при збереженні високої швидкості транзакцій.

Таким чином, сучасні тенденції у криптографії спрямовані на підвищення стійкості систем до нових типів атак, зокрема через розвиток квантово-стійких алгоритмів і використання новітніх методів для генерації випадкових чисел та аналізу вразливостей.

17.2. СТАТИСТИЧНЕ ТЕСТУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Статистичне тестування псевдовипадкових послідовностей є важливим етапом у забезпеченні безпеки криптографічних систем, оскільки воно дозволяє оцінити їх відповідність ключовим вимогам щодо випадковості, рівномірності, незалежності елементів і непередбачуваності. Псевдовипадкові послідовності повинні мати властивості, які забезпечують надійність криптографічних алгоритмів. Однією з основних характеристик є рівномірний розподіл символів, при якому кожен елемент має однакову ймовірність появи. Якщо цей розподіл порушується, це може спричинити уразливості, які злоумисники можуть використати для атак. Іншою важливою властивістю є незалежність елементів послідовності, тобто відсутність залежності між елементами, що дає змогу уникнути передбачуваності.

Для оцінки якості псевдовипадкових послідовностей використовуються різноманітні статистичні тести. Один із найбільш поширених тестів — тест на рівномірний розподіл, відомий як Chi-square test, який дозволяє перевірити, чи символи в послідовності з'являються з однаковою ймовірністю. Якщо результат тесту показує значне відхилення від рівномірного розподілу, це свідчить про потенційну небезпеку використання такого генератора в криптографічній системі. Інший

важливий тест — тест на автокореляцію, який перевіряє залежність між елементами послідовності. Якщо виявляються регулярні закономірності або цикли, це вказує на те, що елементи послідовності не є незалежними, що знижує стійкість системи до атак.

Тест Монобіт використовується для перевірки кількості нулів та одиничних бітів у послідовності, оскільки в ідеалі їх має бути порівну. Нерівномірний розподіл цих бітів може вказувати на проблеми з випадковістю генератора. Тест на довгі послідовності (Runs test) перевіряє, чи існують в послідовності надмірні або занадто короткі послідовності однакових бітів, оскільки криптографічні послідовності повинні мати помірну кількість таких повторень. Такі тести допомагають виявити слабкі місця в генераторах випадкових чисел і забезпечити їх відповідність вимогам криптографічної стійкості.

Окрім стандартних статистичних тестів, використовується також тест на взаємозв'язок (Permutation test), який перевіряє наявність прихованих закономірностей у великих масивах даних. Додатково застосовуються методи енергетичних функцій для аналізу статистичних властивостей псевдовипадкових послідовностей, що дозволяє оцінити їх стійкість до атак.

В криптографії для тестування псевдовипадкових послідовностей часто використовуються стандарти, такі як набір тестів NIST (Національний інститут стандартів і технологій США), які включають в себе різноманітні перевірки, зокрема, на рівномірність, автокореляцію та інші статистичні характеристики. Ці тести дозволяють переконатися, що генератор випадкових чисел відповідає високим вимогам безпеки і стійкості до атак.

У результаті статистичне тестування є невід'ємною частиною процесу забезпечення криптографічної стійкості систем. Воно дозволяє виявити недоліки в генераторах випадкових чисел та забезпечити їх максимальну ефективність і безпеку. Точні та комплексні методи тестування є необхідними для збереження надійності сучасних криптографічних систем, особливо в умовах постійного розвитку нових атак і технологій.

17.3. ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Генератори псевдовипадкових послідовностей (ГПП) — це математичні алгоритми, що створюють послідовності чисел або символів, які виглядають випадковими, але насправді є детермінованими, тобто їх можна відтворити, знаючи початкове значення (вихідну умову) та сам

алгоритм. Псевдовипадкові послідовності відіграють ключову роль у криптографії, оскільки використовуються для генерації ключів, цифрових підписів, маскування даних та інших криптографічних операцій. Однак, через свою детермінованість, псевдовипадкові послідовності можуть бути вразливими до атак, якщо генератор не має належної стійкості. Для забезпечення криптографічної стійкості генератори псевдовипадкових послідовностей повинні відповідати високим вимогам до ентропії та непередбачуваності. Зокрема, важливо, щоб вони не були передбачуваними навіть у випадку обмеженого доступу до деяких елементів вихідних даних. Одним із підходів до підвищення безпеки є використання комбінованих методів генерації, які поєднують псевдовипадкові та фізичні джерела випадковості. У сучасній криптографії особливу увагу приділяють регулярному тестуванню генераторів для виявлення потенційних слабкостей та забезпечення їх стійкості до атак.

Фізичні генератори випадкових чисел, зокрема на основі оптичних явищ, такі як генератори випадкових чисел на основі оптичних випадкових процесів (ORB — Optical Random Bit Generators), раніше вважалися новаторськими і мали потенціал у забезпеченні високої ентропії та стійкості до атак. Ці генератори використовують принципи квантової механіки або оптичні ефекти, такі як шум, що виникає в процесі розсіювання світла чи інших фізичних явищ.

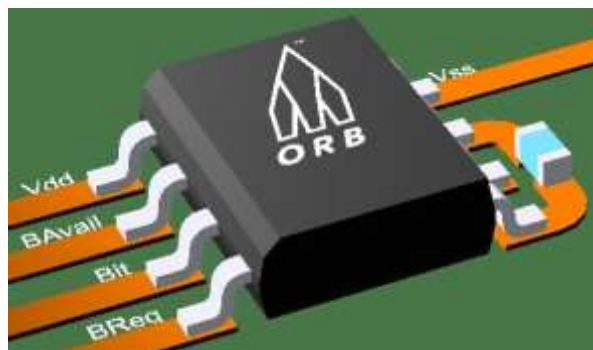


Рис. 17.1. Генератор випадкових чисел ORB

Джерело: побудовано на основі джерела [8]

ORB працюють, засновані на непередбачуваних квантових або статистичних процесах, що дозволяє генерувати насправді випадкові послідовності чисел. Наприклад, це може бути генерація випадкових бітів за допомогою детекції флуктуацій світла, що проходить через спеціалізовані оптичні системи.

Проте, із розвитком технологій та квантових обчислень, деякі фізичні генератори на основі оптичних процесів (таких як ORB) стали менш популярними або їх вважають застарілими в порівнянні з більш сучасними технологіями, такими як квантові генератори випадкових чисел, що забезпечують ще більшу стійкість і надійність. Наприклад, квантові генератори використовують явища квантової суперпозиції та ентропії для створення випадкових бітів, і вони надають більшу криптографічну стійкість.

Загалом, хоча ORB-генератори фізичних випадкових чисел колись були значним кроком уперед, сьогодні вони поступаються місцем новим методам, таким як квантові генератори, які забезпечують ще більш високий рівень випадковості та криптографічної стійкості. Це пов'язано з їх здатністю генерувати більш передбачувані та швидкі процеси, що вимагають менше фізичних ресурсів для створення випадкових чисел.

Одним з найпоширеніших типів генераторів є лінійні конгруентні генератори (LCG), які використовують рекурентне співвідношення для отримання наступного числа в послідовності. Формула виглядає так: $X_n = (aX_{n-1} + b) \bmod N$, де X_0 – випадкове початкове значення, a – множник, b – приріст, N – модуль.

Хоча цей метод є досить простим і швидким, він має деякі обмеження, зокрема послідовність може швидко повторюватися або бути передбачуваною при виборі певних параметрів.

Іншим поширеним генератором є Мережевий генератор (Mersenne Twister), який має дуже великий період (більше $2^{19937} - 1$), що робить його стійким до передбачення та повторення послідовності чисел. Мережевий генератор часто використовується в криптографії та статистичних обчисленнях завдяки високій швидкості генерації та якості послідовностей. Однак, хоча Mersenne Twister є потужним генератором для багатьох застосувань, його не можна використовувати в криптографії без додаткових заходів безпеки, оскільки він не має достатньої криптографічної стійкості. Для криптографічних цілей зазвичай використовуються генератори, які включають фізичні джерела випадковості або спеціалізовані алгоритми, що враховують непередбачуваність. Попри це, Mersenne Twister широко застосовується в статистичних моделях, симуляціях та в інших задачах, де потрібна швидка генерація великих обсягів псевдовипадкових чисел. Сучасні реалізації цього генератора оптимізовані для роботи на різних платформах і мають високу ефективність при генерації послідовностей.

Ще одним методом є генератори на основі хеш-функцій, таких як SHA-256 або SHA-512. Вони використовуються для створення псевдовипадкових послідовностей, де кожен хеш є унікальним для кожного вхідного значення. Хеш-функції забезпечують високий рівень безпеки, оскільки їх складно передбачити або зворотно розрахувати. Ці генератори широко використовуються у криптографії для створення ключів, цифрових підписів і маскування даних. Проте варто зазначити, що хеш-функції не є ідеальними генераторами випадковості, оскільки їх результат може бути передбачуваним, якщо злоумисник знає вхідні дані. Незважаючи на це, комбінація хеш-функцій із іншими криптографічними техніками дозволяє підвищити стійкість до атак. Хеш-функції також часто застосовуються в протоколах аутентифікації та забезпечення цілісності даних завдяки своїй здатності створювати однозначні й незворотні послідовності.

Для високої криптографічної стійкості особливо важливо використовувати апаратні генератори випадкових чисел (AGG), які використовують фізичні джерела випадковості, такі як шум, що генерується електронними компонентами або квантовими ефектами. Апаратні генератори здатні створювати числа, які мають максимальну ентропію, і тому є більш стійкими до прогнозування в порівнянні з псевдовипадковими генераторами. Незалежно від типу генератора, всі вони повинні відповідати певним вимогам до якості послідовностей. По-перше, послідовність повинна бути випадковою і не мати будь-яких передбачуваних закономірностей. По-друге, числа в послідовності повинні бути незалежними, тобто не повинно бути кореляції між сусідніми елементами. По-третє, розподіл чисел має бути рівномірним, щоб забезпечити правильну роботу криптографічних алгоритмів. І, по-четверте, період генератора має бути якомога більшим, що дозволяє уникнути повторення послідовностей.

Для перевірки якості генераторів псевдовипадкових послідовностей використовуються різноманітні статистичні тести, такі як тест на рівномірність, тест на автокореляцію, монобіт тест, тест на довгі послідовності та тест на пермутацію. Ці тести допомагають оцінити, чи відповідає послідовність вимогам до випадковості, незалежності та рівномірного розподілу, а також чи є в ній потенційні слабкі місця, що можуть бути використані при атаках. Тест на рівномірність перевіряє, чи рівномірно розподілені числа в межах допустимого діапазону, а тест на автокореляцію виявляє наявність кореляцій між елементами послідовності на різних відстанях. Монобіт тест оцінює, наскільки добре генератор створює послідовності, де кожен біт має рівну ймовірність бути 0 або 1.

Тест на довгі послідовності перевіряє, чи немає у послідовності повторюваних або регулярних шаблонів, а тест на пермутацію оцінює різноманітність послідовностей чисел або бітів у згенерованих наборах. Ці тести є необхідними для забезпечення надійності та безпеки криптографічних систем, що використовують псевдовипадкові послідовності.

Завдяки розвитку криптографії та необхідності забезпечення безпеки даних у сучасному світі, роль генераторів псевдовипадкових послідовностей стає дедалі важливішою. Високоякісні генератори є основою для криптографічних протоколів, а їх тестування та оцінка є важливим кроком у забезпеченні надійності та стійкості криптосистем до потенційних атак.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 17

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.

2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.

4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.

5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

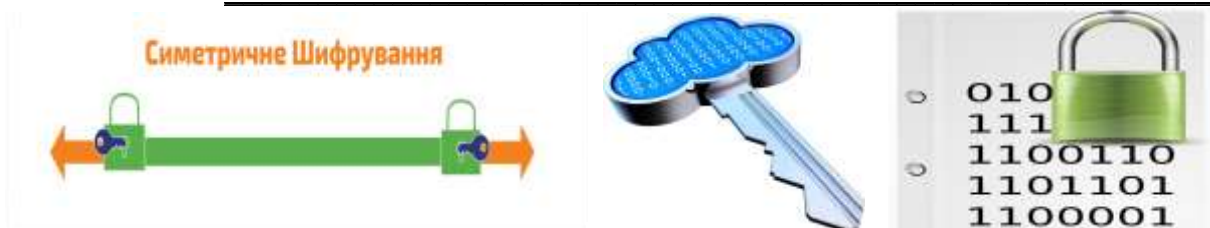
6. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

7. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.
8. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.
9. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.
10. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.
11. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.
12. Шевченко , С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.
13. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.
14. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.
15. Спасітелева, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.
16. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об’єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.

17. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.
18. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.
19. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.
20. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.
21. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.
22. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

РОЗДІЛ 18

КЛАСИЧНІ МЕТОДИ СИМЕТРИЧНОГО ШИФРУВАННЯ



- 18.1. Шифри перестановок**
- 18.2. Шифри підстановок**
- 18.3. Гамування**
- 18.4. Аналітичні методи**
- 18.5. Поточкові шифри**
- 18.6. Блокові складені шифри**

"Безпечний шифр — це той, який залишається захищеним навіть тоді, коли все про нього відомо, крім ключа."

Керкгоффс, Принцип Керкгоффса (1883)

18.1. ШИФРИ ПЕРЕСТАНОВОК

Шифрування є важливим процесом захисту інформації, який передбачає перетворення вихідного тексту у зашифрований вигляд, недоступний для розуміння сторонніми особами. Основна мета шифрування полягає у забезпеченні конфіденційності переданих чи збережених даних. Процес дешифрування, що є оберненим до шифрування, дозволяє відновити вихідну інформацію за допомогою спеціального ключа. Ключ, як набір символів або параметрів, відіграє критично важливу роль, адже саме від його складності та секретності залежить стійкість криптографічного захисту.

Криптографічні алгоритми повинні відповідати ряду вимог для забезпечення надійного захисту даних. Однією з основних вимог є конфіденційність, тобто зашифрований текст має бути доступним для прочитання лише при наявності правильного ключа. Сучасні методи

криптоаналізу ставлять високу планку для алгоритмів шифрування, тому стійкість до зламу є ще однією ключовою характеристикою. Важливо, щоб навіть знання алгоритму не знижувало рівень безпеки — надійність системи має повністю залежати від секретності ключа. Крім того, невелика зміна ключа або вихідного тексту повинна суттєво змінювати шифрований текст, забезпечуючи стійкість до статистичного аналізу.

Шифрування — це процес перетворення вихідного тексту в шифрований вигляд, щоб захистити інформацію від несанкціонованого доступу.

Дешифрування — обернений процес, який дозволяє відновити вихідний текст із шифрованого, використовуючи відповідний ключ.

Ключ — це критично важливий набір символів або параметрів, необхідних для шифрування та дешифрування інформації. Надійність криптографічної системи значною мірою залежить від секретності та складності ключа.

Текст — набір символів, що передає певний логічний зміст.

Алфавіт — скінченна множина символів, які використовуються для представлення інформації у текстовій формі.

Процеси шифрування і розшифрування здійснюються в рамках деякої криптосистеми (набір інструкцій, апаратні засоби, комплекс програм, що дозволяють зашифровувати відкритий текст та розшифровувати шифротекст різним способом за допомогою ключа. Характерною рисою симетричної криптосистеми є застосування того самого секретного ключа як при шифруванні, так і при розшифруванні повідомлень.



Рис. 18.1. Використання симетричного методу шифрування
Джерело: побудовано автором на основі [8-9]

Залежно від принципів функціонування шифри поділяються на симетричні та асиметричні. Симетричні алгоритми, такі як AES,

використовують один і той самий ключ для шифрування та дешифрування. Вони характеризуються високою швидкістю роботи та ефективністю, що робить їх популярними для масового шифрування даних. Натомість асиметричні алгоритми, як-от RSA, передбачають використання пари ключів — відкритого для шифрування та закритого для дешифрування. Такий підхід забезпечує підвищену безпеку, але є більш ресурсомістким.

У сучасних умовах стрімкого розвитку технологій виникає необхідність у гібридних системах шифрування, які поєднують переваги обох підходів. Наприклад, протокол TLS забезпечує ефективну передачу даних із використанням симетричних шифрів, але попередньо встановлює ключі через асиметричне шифрування. З розвитком квантових обчислень актуальною стає розробка квантово-стійких алгоритмів, здатних протистояти загрозам майбутнього.

Таким чином, шифрування є невід'ємною складовою сучасної інформаційної безпеки. Постійне вдосконалення криптографічних алгоритмів та систем захисту інформації дозволяє ефективно протидіяти новітнім кіберзагрозам, зберігаючи конфіденційність і цілісність даних.

Шифри перестановки

Шифри перестановки належать до класу симетричних методів шифрування, де однаковий ключ використовується як для шифрування, так і для дешифрування повідомлень. В основі таких методів лежить перестановка символів у тексті відповідно до певного алгоритму чи ключа, що значно ускладнює зрозумілість інформації для сторонніх осіб. Основна ідея шифрів перестановки полягає у зміні послідовності символів повідомлення без зміни їхнього значення. В результаті початковий текст (відкритий текст) перетворюється на шифротекст, який стає нечитабельним без знання ключа.

Шифрування перестановкою — один із базових методів криптографії, який полягає у зміні порядку символів вихідного тексту за визначеним правилом у межах певного блоку даних. Суть цього підходу полягає у переставленні символів таким чином, щоб зашифрований текст виглядав хаотичним і важким для розуміння без знання правил перестановки.

Незважаючи на свою простоту, шифрування перестановкою все ще знаходить застосування у навчальних цілях та деяких простих криптографічних задачах. Його ефективність може бути підвищена шляхом використання великих блоків для перестановки та складних неповторюваних схем перестановки символів. Однак сучасні вимоги до інформаційної безпеки значно перевищують можливості таких примітивних методів шифрування.

Шифри перестановки належать до найдавніших криптографічних методів. Відомі історичні приклади включають шифр Скитала, що використовувався у Стародавній Греції, де текст наносився на стрічку, яка оберталася навколо циліндра для створення перестановок. Однак із розвитком технологій та появою більш складних алгоритмів, таких як AES (Advanced Encryption Standard), прості методи перестановки втратили практичну цінність для захисту сучасних інформаційних систем.

Сьогодні шифрування перестановкою може бути використане лише як частина складніших криптографічних схем у поєднанні з іншими методами, такими як підстановки та багатоступеневі блокові алгоритми. Це дозволяє підвищити стійкість шифру та адаптувати його до сучасних вимог кібербезпеки.

Методи шифрування, засновані на перестановці символів, відіграють важливу роль у забезпеченні інформаційної безпеки. Одним із найпростіших таких методів є шифр «Частоколу», що базується на розташуванні символів повідомлення у рядках певної висоти. Шифротекст утворюється шляхом зчитування символів із кожного рядка по черзі. Наприклад, якщо шифрувати слово «за шифрування» з висотою частоколу 2, текст записується у два рядки, а результатом стає послідовність символів «аирвнязшфуан». Цей метод відзначається простотою реалізації, але має низьку стійкість до злому.

а и р в н я
з ш ф у а н

Інший підхід до шифрування полягає у використанні табличних або матричних методів, де текст розташовується в таблиці за визначеними правилами. У методі простої перестановки повідомлення записується по рядках, а шифротекст зчитується по стовпцях. Наприклад, якщо шифрувати текст «завтра пишемо контрольну роботу» у таблиці розміром 5x7, шифротекст формується шляхом зчитування символів по рядках, що дозволяє значно ускладнити його розуміння для злоумисників.

Заповнення таблиці з 5 рядків і 7 стовпців

з	р	ш	к	р	н	б
а	а	е	о	о	у	о
в	п	м	н	л	р	т
т	и	о	т	ь	о	у

Більш складним варіантом є перестановка за ключем. У цьому методі текст спочатку записується у таблицю, після чого стовпці переставляються відповідно до порядку букв ключового слова. Наприклад, якщо ключем є слово «ПЕЛІКАН», визначається порядок перестановки стовпців, і шифротекст утворюється шляхом послідовного зчитування символів із нової таблиці. Такий підхід значно підвищує рівень безпеки порівняно з простою перестановкою.

п	е	л	і	к	а	н
7	2	5	3	4	1	6
з	р	ш	к	р	н	б
а	а	е	о	о	у	о
в	п	м	н	л	р	т
т	и	о	т	ь	о	у

Перестановка стовпців

1	2	3	4	5	6	7
н	р	к	р	ш	б	з
у	а	о	о	е	о	а
р	п	н	л	м	т	в
о	и	т	ь	о	у	т

Для додаткової стійкості використовується метод подвійної перестановки. Спочатку здійснюється перестановка стовпців за одним ключем, а потім — перестановка рядків за іншим ключем. Цей підхід ускладнює розшифрування тексту, навіть якщо злоумисник володіє частиною інформації про таблицю.

Цікавим методом є використання магічних квадратів. Тут застосовується спеціальна таблиця з прорізними віконцями. Під час шифрування накладають маску на таблицю та записують символи через віконця. Потім маску повертають на 90 градусів і повторюють процес. Цей метод вимагає точного узгодження маски між відправником і одержувачем, але забезпечує достатньо високий рівень безпеки. Цей метод був популярний у давнину, оскільки дозволяв здійснювати шифрування без використання складних математичних алгоритмів. Для посилення рівня захисту, маски можуть бути змінювані після кожного сеансу зв'язку або за певними правилами, що ускладнює криптоаналіз. Магічні квадрати також дозволяють проводити шифрування одночасно кількох повідомлень, що додає до системи додатковий рівень складності для потенційного

зловмисника. Хоча цей метод є досить простим, він все ж має свої обмеження в умовах сучасних технологій криптографії.



Загалом, табличні методи шифрування мають свої переваги завдяки гнучкості у виборі розмірів таблиць і ключів, а також простоті реалізації. Однак їхнім недоліком є відносно низька стійкість до сучасних атак порівняно з такими криптографічними алгоритмами, як AES чи RSA. Попри те, що шифри перестановки поступаються сучасним методам симетричного шифрування, таким як AES чи DES, вони все ще можуть використовуватись як частина багатошарових систем захисту інформації або у навчальних цілях для демонстрації основ криптографії.

18.2. Шифри підстановок

Шифри підстановок є важливим класом методів симетричного шифрування, основною ідеєю яких є заміна символів відкритого тексту на інші символи відповідно до певного алгоритму або ключа. Вони забезпечують базовий рівень захисту інформації, перетворюючи текст у незрозумілу форму, яку неможливо прочитати без знання методу шифрування.

Шифрування заміною, або підстановкою, є методом криптографії, де символи вихідного тексту замінюються іншими символами за певною схемою. Шифри підстановки поділяються на кілька типів: моноалфавітні, поліалфавітні та гомофонічні. Кожен з цих методів має свої особливості та рівень стійкості до криптоаналізу.

Моноалфавітні шифри

Моноалфавітні шифри базуються на заміні кожної букви вихідного тексту на іншу букву того ж алфавіту за фіксованим правилом. Найвідомішим моноалфавітним шифром є шифр Цезаря, який полягає в тому, що кожна буква замінюється на іншу, зміщену на певну кількість позицій у алфавіті. Наприклад, для англійського алфавіту з ключем $K=3$ буква "A" змінюється на "D", "B" на "E" і так далі. Якщо зміщення досягає

кінця алфавіту, то здійснюється циклічний перехід на початок, тобто після "Z" йде "A". Таким чином, текст "HELLO" зашифрується як "KHOOR".

Перевагами шифру Цезаря є його простота у використанні як для шифрування, так і для дешифрування. Однак цей метод має суттєві недоліки: він не маскує частоти появи символів у тексті, що дозволяє легко провести криптоаналіз за допомогою частотного аналізу. Крім того, кількість можливих ключів обмежена, і для англійського алфавіту вона складає лише 26 варіантів зсуву.

Для підвищення стійкості шифру можна використати модифікацію шифру Цезаря із ключовим словом. У цьому випадку ключове слово визначає новий порядок символів, який використовується для зміщення букв у тексті. Наприклад, якщо ключове слово — "ДИПЛОМАТ" і значення $K=5$, то заміна букв здійснюється за допомогою модифікованого алфавіту. Для англійського алфавіту, це виглядатиме наступним чином:

a bcdefghijklmnopqrstuvwxyz
vwxyz**diplomat**bcefg hijknqrsu

Таким чином, текст "send more money" зашифрується як "hzby tcgd tcbzs". Цей метод підвищує стійкість шифру, оскільки використання ключового слова додає випадковості в процес заміни символів і зменшує ефективність стандартного частотного аналізу. Шифри підстановки залишаються популярними завдяки своїй простоті, але для досягнення більш високого рівня безпеки сучасні криптографічні системи використовують складніші поліалфавітні та гомофонічні методи, які значно ускладнюють процес дешифрування.

Поліалфавітні шифри

Поліалфавітні шифри є важливим різновидом шифрів заміни, де для шифрування використовуються кілька алфавітів заміни, які змінюються протягом процесу шифрування. Це дозволяє значно ускладнити криптоаналіз, оскільки кожен символ відкритого тексту може бути зашифрований за допомогою різного алфавіту, що знижує ефективність атак, заснованих на аналізі частоти символів. Одним з найвідоміших прикладів поліалфавітного шифру є шифр Віженера. Шифр Віженера, винайдений французьким криптографом Блезом Віженером у 16 столітті, є класичним поліалфавітним шифром.

Механізм шифрування за шифром Віженера полягає в тому, що кожній літері відкритого тексту відповідає буква з ключового слова, і для кожної пари символів (літера відкритого тексту та відповідна літера з ключа) визначається зміщення, яке використовуватиметься для

шифрування. Ключове слово повторюється так, щоб його довжина відповідала довжині відкритого тексту. Це дозволяє кожному символу отримати інше зміщення, що значно ускладнює його дешифрування без знання ключа. Наприклад, якщо відкритий текст — це "HELLO", а ключове слово — "KEY", то шифрування відбуватиметься таким чином: перша літера "H" зміщується відповідно до букви "K" у ключі, друга літера "E" зміщується відповідно до букви "E" і так далі.

Завдяки використанню декількох алфавітів такі шифри значно стійкіші до частотного аналізу. У процесі шифрування і дешифрування використовувалася таблиця Віжінера (квадрат), що утворена наступним чином: у перший рядок виписується весь алфавіт, в наступних рядках вводиться зсув на 1 літеру вліво, так отримується квадратна таблиця; щоб зашифрувати повідомлення, вибирають лозунг, який підписують під текстом; потім у стовпчику шукаємо літеру повідомлення, а у рядку — ключа, на їх перетині знаходиться наша підстановка. Також цю криптосистему можна розглядати як шифр гамування із використанням періодичної гами малого періоду

	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я
А	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я
Б	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А
В	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б
Г	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В
Д	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г
Е	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д
Є	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е
Ж	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є
З	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж
И	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З
І	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ц	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ч	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Ш	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Щ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ъ	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ю	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Я	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю

Рис. 18.2. Таблиця Віжінера

Джерело: [8-9]

Хоча шифр Віженера є більш складним за моноалфавітні шифри, його криптоаналіз все ж можливий. Важливими недоліками є те, що ключове слово, яке повторюється, може бути виявлене при досить довгому тексті, що дозволяє застосувати частотний аналіз до кожного з алфавітів,

використовуваних для шифрування. Однак, шифр Віженера все ж забезпечує вищий рівень безпеки в порівнянні з моноалфавітними шифрами, оскільки кожен символ тексту має різне зміщення залежно від букви в ключовому слові.

Окрім цього, існує шифр Плейфера, де заміна символів відбувається парами, використовуючи спеціальний квадрат 5x5 із ключовим словом. Якщо текст містить дві однакові літери поспіль, для збереження правильності підстановки додають спеціальний символ-вставку, наприклад «X».

Система шифрування методом Вернама, також відома як одноразовий блокнот або шифр Вернама, є криптографічною технікою, яка базується на використанні випадкових ключів для забезпечення абсолютної секретності повідомлень. Цей метод був запропонований американським інженером Гілбертом Вернамом у 1926 році, і він є частинним випадком шифру Віженера, коли алфавіт складається лише з двох символів (0 і 1). Таким чином, шифр Вернама використовує бінарний код для обробки тексту.

Принцип роботи шифру Вернама полягає в наступному: кожен символ відкритого тексту (наприклад, символи в англійському алфавіті або в бінарному вигляді) XOR-иться з відповідним символом з випадково згенерованого ключа такої ж довжини. Ключ у шифрі Вернама є випадковим і повністю секретним. Один з важливих аспектів цього методу — ключ використовується лише один раз і ніколи не повторюється, що забезпечує максимальний рівень безпеки.

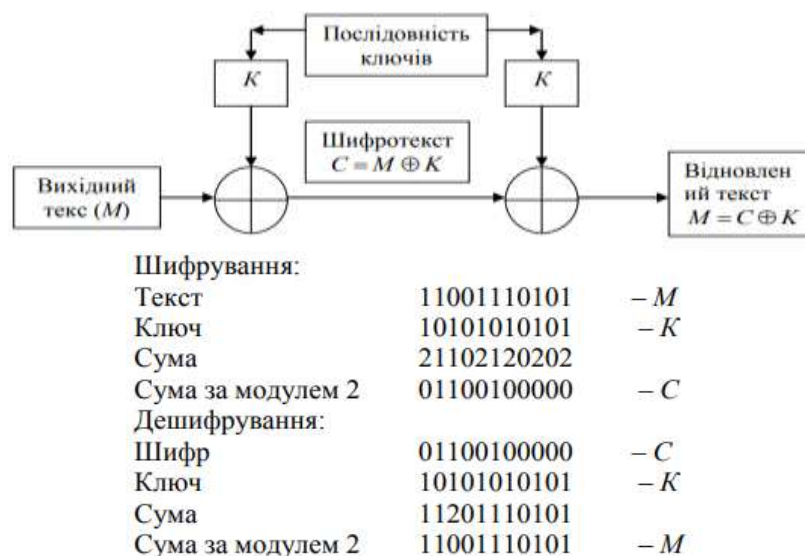


Рис. 18.3. Система шифрування за методом Вернама
Джерело: [8-9]

Наприклад, припустимо, що ми шифруємо повідомлення, яке складається з бінарних символів. Якщо відкритий текст (наприклад, текст повідомлення) представлений у вигляді бітів, і якщо ключ також представлений випадковими бітами такої ж довжини, то кожен біт відкритого тексту XOR-иться з відповідним бітом ключа. Операція XOR (де $0 \text{ XOR } 0 = 0$, $1 \text{ XOR } 1 = 0$, а $0 \text{ XOR } 1 = 1$) є основою цього шифру.

Шифр Вернама є ідеальним, якщо виконуються два важливих правила:

1. Ключ має бути абсолютно випадковим - ключ для шифрування не можна генерувати за допомогою будь-яких алгоритмів, що можуть бути передбачуваними. Він повинен бути суто випадковим і згенерованим на основі джерела випадковості.

2. Ключ має бути рівної довжини з повідомленням - якщо довжина повідомлення є N , то і ключ має бути рівний N , щоб кожен біт повідомлення міг бути зашифрований за допомогою одного біта ключа.

Однією з ключових особливостей методу Вернама є його теоретична незламність за умови, що ключ є абсолютно випадковим, використовується лише один раз, і його зберігання та передача є повністю безпечними. Однак на практиці основними проблемами є забезпечення безпеки та управління великими ключами, оскільки довжина ключа повинна бути такою ж, як і довжина самого повідомлення.

Метод Вернама також знайшов застосування в ряді інших криптографічних систем, наприклад, у роторних машинах, таких як SIGABA (США), ENIGMA (Німеччина) і PURPLE (Японія), де принципи шифрування, подібні до методів заміни та зміщення символів, використовувалися для створення складних криптографічних систем у часи Другої світової війни. У сучасних криптографічних системах, хоча метод Вернама застосовується рідше, його основи використовуються у більш складних алгоритмах симетричного шифрування, таких як AES, що забезпечує високий рівень безпеки для сучасних криптографічних додатків.

Шифри підстановок також можуть базуватися на числових ключах, як у шифрі Гронсфельда, де для підстановки використовується цифрова послідовність. Інший підхід полягає у використанні гамування, коли до кожного символу тексту додається псевдовипадкова послідовність, що забезпечує додатковий рівень захисту.

Попри їх історичну значущість, прості шифри підстановок мають низку недоліків. Зокрема, моноалфавітні шифри легко піддаються частотному аналізу, що дозволяє визначити відповідності між символами

тексту та шифру. Поліалфавітні шифри є стійкішими, однак потребують складнішого управління ключами.

Незважаючи на це, принципи шифрів підстановок стали основою для сучасних криптографічних систем, таких як DES і AES, де використовуються складні комбінації підстановок і перестановок для забезпечення високого рівня безпеки. Таким чином, шифри підстановок залишаються важливими як для розуміння базових принципів захисту інформації, так і для побудови сучасних систем криптографічного захисту.

У сучасних криптографічних системах, хоча принципи поліалфавітних шифрів є вже застарілими, їх ідеї знайшли своє застосування в більш складних системах. Наприклад, у роторних машинах, таких як ENIGMA, використовувалися принципи поліалфавітного шифру для забезпечення складного шифрування, яке ускладнювало криптоаналіз. Роторні машини працювали на основі багатоалфавітної заміни символів з використанням змінюваних ключів, що дозволяло значно підвищити рівень безпеки.

Сучасні криптографічні алгоритми, такі як AES (Advanced Encryption Standard) або RSA, хоча і не є класичними поліалфавітними шифрами, також застосовують принципи, схожі на поліалфавітне шифрування. Вони використовують багатоетапні заміни та складні математичні операції для забезпечення безпеки. Наприклад, у системі AES для шифрування використовуються кілька раундів заміни та пермутацій, що аналогічно змінюванам алфавітам у поліалфавітних шифрах.

Загалом, поліалфавітні шифри, зокрема шифр Віженера, відіграли важливу роль у розвитку криптографії, оскільки вони значно ускладнили криптоаналіз у порівнянні з моноалфавітними шифрами. Хоча сучасні криптографічні методи значно складніші, принципи, закладені в поліалфавітних шифрах, і сьогодні залишаються основою для більш складних алгоритмів і систем шифрування.

18.3. Гамування

Шифрування гамування — це криптографічний метод, який використовується для захисту інформації шляхом заміни символів відкритого тексту випадковими значеннями, які отримуються із так званої "гами шифру". Гама шифру являє собою випадкову послідовність, що використовується для перетворення вихідного повідомлення в зашифрований текст. Важливим моментом є те, що ця гама повинна бути абсолютно випадковою, і її довжина повинна бути щонайменше такою ж, як і довжина самого повідомлення, що шифрується.

Під час процесу шифрування кожен символ тексту по черзі комбінується з відповідним символом гами за допомогою операції XOR (побітової операції додавання за модулем 2). Ця операція перетворює відкритий текст у зашифрований таким чином, що для кожного символу відкритого тексту результат буде залежати від випадкової послідовності гами. Оскільки операція XOR є комутативною і оберненою (якщо зашифрований текст знову застосувати до гами через XOR, отримаємо початковий текст), цей метод дозволяє здійснювати і шифрування, і дешифрування за допомогою одного і того ж ключа — гами.

Одним із важливих аспектів гамування є те, що при достатньо великій довжині гами та її високій випадковості, стійкість шифрування стає дуже високою. Оскільки гама використовується лише один раз для кожного повідомлення і має бути абсолютно випадковою, це унеможливорює передбачення або вгадування ключа зловмисником. Тому, якщо період гами набагато перевищує довжину повідомлення і кожен блок зашифровується окремо, то такий шифр стає надзвичайно стійким до криптоаналітичних атак.

Основний виклик, пов'язаний з гамуванням, полягає в необхідності забезпечити абсолютно випадкову та достатньо довгу гаму. Якщо гама буде повторюватися або бути недостатньо випадковою, це значно знизить криптографічну стійкість шифру, адже зловмисник може виявити закономірності в зашифрованому тексті. Ось чому дуже важливо забезпечити надійне генерування гами та її безпечну передачу між сторонами.

Одним з класичних застосувань шифрування гамування є одноразова система шифрування (так званий одноразовий блокнот), який був винайдений в 1917 році американськими вченими Дж. Моборном і Г. Вернамом. У цій системі використовується спеціальний блокнот, що містить таблицю випадкових чисел або символів. Кожен лист блокнота є унікальним і використовується лише один раз для шифрування одного повідомлення. Після використання листа його знищують, і для наступного повідомлення використовують новий лист. Важливо, що для гарантування безпеки кожен символ відкритого тексту шифрується за допомогою унікального символу з таблиці, тому повторне використання будь-якого листа або ключа є неприпустимим.

Одноразова система шифрування вважається теоретично абсолютно надійною. Це означає, що вона не може бути розкрита або зламана навіть при використанні необмежених обчислювальних потужностей, якщо ключова послідовність є справді випадковою і використовується тільки один раз. Однак на практиці цей метод має суттєві обмеження. Зокрема,

для передачі ключів (листів блокнота) необхідно мати захищений канал зв'язку, оскільки передача ключів може бути перехоплена або розкрита. Крім того, одноразова система шифрування вимагає наявності великої кількості випадкових ключів, що може стати проблемою при шифруванні великих об'ємів даних.

З розвитком обчислювальної техніки і криптографії гамування стало основою для створення нових, більш ефективних методів шифрування, таких як поточні шифри, що використовують генератори псевдовипадкових чисел для створення ключових потоків. В таких системах, як AES або ChaCha, використовуються схеми гамування для генерації ключових послідовностей, які потім комбінуються з відкритим текстом для отримання зашифрованого повідомлення. Таким чином, принцип гамування продовжує бути важливою складовою криптографії в сучасних інформаційних системах.

18.4. АНАЛІТИЧНІ МЕТОДИ

Аналітичні методи шифрування є основою криптографії, де для перетворення відкритого тексту в зашифрований використовуються математичні операції, що ґрунтуються на певних аналітичних правилах. Ці методи дозволяють забезпечити конфіденційність інформації та її захист від несанкціонованого доступу. Один з таких методів — шифр Хілла, що використовує лінійні перетворення за допомогою матриць. У цьому методі текст розбивається на біграми, які потім підлягають перетворенню за допомогою матриці ключа. Це дозволяє перетворювати символи в числові значення, що залежить від алфавітного порядку букв, а потім проводити математичні операції, що дають можливість здійснити шифрування.

Шифр Хілла застосовує матрицю, яка виконує роль ключа шифрування. Ключова матриця повинна бути оберненою, а також її визначник не повинен ділитись на прості числа, що ділять розмір алфавіту (наприклад, 26 для латинського алфавіту). Сам процес шифрування починається з того, що текст розбивається на біграми — пари літер. Кожен символ в біграмі переводиться у числовий код, і ці числа множаться на матрицю ключа. Результат перетворення дає нові числові значення, які потім перетворюються назад у символи.

Для прикладу, якщо взяти текст «рауmоgетmоnеu», то кожна буква цього тексту замінюється її порядковим номером в алфавіті, що дає числову послідовність. Потім ця послідовність множиться на матрицю, яка виступає як ключ шифрування, і результат дає зашифровані символи.

Такий підхід дозволяє отримати досить складне шифрування, яке може бути розшифроване лише за наявності правильного ключа.

Дешифрування за допомогою шифру Хілла відбувається за зворотною формулою, де використовуються обернена матриця та модульне ділення. При цьому для успішного дешифрування необхідно мати саме ту матрицю, яку використовували під час шифрування, інакше відновити оригінальний текст неможливо.

Хоча шифр Хілла має свої переваги, такі як простота реалізації та ефективність, в сучасній криптографії він рідко використовується. Це пояснюється тим, що метод вразливий до криптоаналітичних атак, таких як атака з вибором тексту або аналіз частотності. У результаті були розроблені більш стійкі методи шифрування, такі як RSA, ElGamal та криптографія з відкритим ключем. Ці методи забезпечують набагато більший рівень безпеки, оскільки для їх розкриття потрібно значно більше часу і ресурсів, що робить їх ефективними в сучасних інформаційних системах.

З розвитком технологій криптографія також не стоїть на місці. Вона продовжує еволюціонувати, і зараз активно вивчаються методи квантового шифрування, що обіцяють революційні зміни в забезпеченні безпеки інформації. Використання комбінованих методів шифрування, що поєднують класичні та новітні технології, дозволяє створювати потужні системи захисту даних, здатні протистояти навіть найбільш складним атакам. Вибір методу шифрування завжди залежить від конкретних вимог до безпеки та обчислювальних ресурсів, що доступні в тій чи іншій ситуації.

18.5.Потокові шифри

Потокові шифри не мають фіксованого розміру блоку, як блокові шифри. Вони працюють з потоком даних і обробляють інформацію найчастіше на рівні:

1. Бітів (1 біт) — де кожен біт відкритого тексту комбінується з відповідним бітом ключового потоку. Цей підхід забезпечує максимально гнучке шифрування.
2. Байтів (8 біт) — найпоширеніший варіант обробки, оскільки байт є базовою одиницею інформації для більшості комп'ютерних систем.
3. Слів (16 або 32 біти) — іноді використовується для оптимізації продуктивності в певних реалізаціях потокових шифрів.

Прикладом є алгоритм RC4, який обробляє дані побайтово, тоді як інші алгоритми, такі як Salsa20 або ChaCha20, можуть працювати зі словами або більшими одиницями.

Потокові шифри відрізняються від блокових тим, що обробляють дані не блоками фіксованого розміру, а окремими потоками інформації, байтами або навіть бітами. Вони не мають фіксованого розміру блоку, як, наприклад, блокові шифри (64 чи 128 біт). Замість цього, потік ключових даних (ключовий потік) генерується динамічно і комбінується з відкритим текстом для отримання шифрованого тексту. Ця особливість робить потокові шифри ефективними для застосувань, де розмір даних може бути довільним або де важлива низька затримка, наприклад у бездротових комунікаціях або потоковій передачі відео. Вони дозволяють шифрувати та дешифрувати інформацію поступово, без необхідності чекати накопичення цілих блоків даних. Вибір розміру оброблюваних одиниць (байтів або бітів) залежить від алгоритму шифрування та конкретних вимог до системи. Саме гнучкість у виборі обсягу шифрованих даних робить потокові шифри незамінними у багатьох сучасних криптографічних рішеннях.

Поточний розвиток криптографії та інформаційної безпеки привів до удосконалення та широкого використання поточкових шифрів, що є невід'ємною частиною сучасних систем захисту інформації. Поточковий шифр — це симетричний шифр, де кожен символ відкритого тексту перетворюється на зашифрований, виходячи не тільки з ключа, а й з його позиції в потоці даних. Суть поточкових шифрів полягає в тому, що генератор ключових послідовностей створює потік бітів, який поєднується з відкритим текстом за допомогою операції XOR (модуль два). Ключове завдання генератора — забезпечити високу стійкість системи, що багато в чому залежить від якості і періоду генерації ключової послідовності. Якщо генератор має короткий період, це значно знижує стійкість шифру, оскільки повторення ключа дозволяє зловмисникам прорвати захист.

У більшості випадків потоки бітів виглядають випадковими, хоча насправді є детермінованими, що дозволяє відтворювати їх на приймаючій стороні за допомогою однакового секретного ключа. Це виключає можливість простого розшифрування, навіть якщо перший біт шифрованого тексту став відомим. Поточкові шифри здатні ефективно шифрувати безперервні потоки інформації, що важливо для таких сфер, як мережі передачі даних, де важлива висока швидкість шифрування та низькі затримки. Крім того, використання поточкових шифрів дозволяє мінімізувати витрати на пам'ять і ресурси процесора, що робить їх привабливими для мобільних пристроїв і вбудованих систем. Проте, при

некоректному управлінні ключами, таких шифрів можуть виникати уразливості, оскільки однаковий ключ для шифрування декількох повідомлень може призвести до компрометації безпеки. Важливим аспектом є використання додаткових механізмів захисту, таких як синхронізація ключів і застосування спеціальних алгоритмів для перешкодження повторному використанню одного і того ж ключа. Тому, хоча поточкові шифри мають численні переваги, вони вимагають уважного управління та надійної інфраструктури для забезпечення високого рівня безпеки.

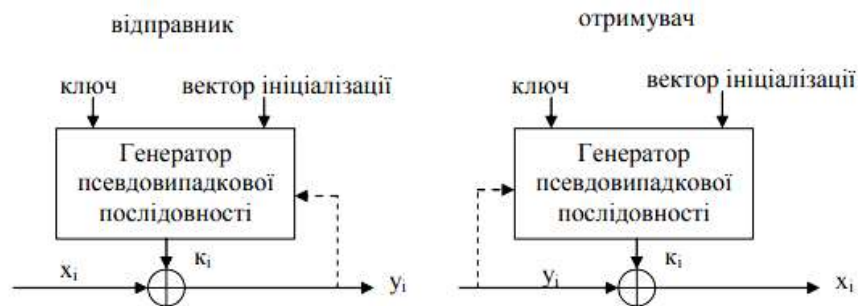


Рис. 18.4. Схема потокового шифрування

Джерело: [8-9]

Ідея поточкових шифрів була вперше запропонована у 1946 році в США в патенті на шифр з авто-ключем (Cipher Text Auto Key, або СТАК). Вони стали основою для шифрів, що використовують алгоритми синхронізації, де внутрішній стан генератора є функцією попередніх бітів зашифрованого тексту, що дозволяє синхронізувати відправника та одержувача. Важливою характеристикою є здатність генератора "відновлюватися" після синхронізації за допомогою передачі невеликої частини зашифрованого тексту, хоча помилка в одному бітові може поширитися на кілька бітів.

Одним із важливих кроків у розвитку поточкових шифрів стало доведення стійкості шифру Вернама, опублікованого Клодом Шенноном у 1949 році. Він доказав, що якщо ключ для шифрування вибирається випадково і має таку ж довжину, як і повідомлення, то такий шифр є абсолютно стійким. При цьому, якщо ключ не повторюється і складається із випадкових бітів, криптографічна стійкість забезпечується. Однак практична реалізація такого шифру потребує передачі ключа такої ж довжини, що накладає обмеження на його використання в реальних умовах.

Потокові шифри можна класифікувати на синхронні та самосинхронізовані. Синхронні поточкові шифри мають значну перевагу в

тому, що для їх реалізації не потрібно великого обсягу пам'яті, а сам процес шифрування та розшифрування досить швидкий. Вони застосовуються, коли необхідно шифрувати інформацію у реальному часі, наприклад, в телекомунікаційних мережах, проте мають вразливість до атак на основі помилок синхронізації. Оскільки синхронізація між відправником і одержувачем повинна бути точною, будь-яка втрата даних або затримка може призвести до розсинхронізації і, як наслідок, до збоїв в роботі системи. Рішенням є використання додаткових механізмів синхронізації, що дозволяє уникнути таких проблем.

Самосинхронізовані потокові шифри використовують механізми, де кожен біт шифротексту залежить від декількох попередніх бітів шифрованого тексту. Такі шифри здатні відновлювати синхронізацію після втрати або пошкодження кількох бітів, що робить їх менш чутливими до помилок в передаванні. Вони також не страждають від деяких обмежень, притаманних синхронним шифрам, але вимагають більш складної обробки на стороні приймача, оскільки процес дешифрування залежить від фіксованої кількості попередніх бітів.

До сьогоднішнього дня розроблено багато алгоритмів потокового шифрування, серед яких можна виділити такі як RC4, A3, A5, eSTREAM, SEAL, PIKE, а також багато інших. RC4 був широко використаний у практиці до останніх років, коли виявилися його вразливості до криптографічних атак. Водночас, новіші алгоритми, такі як елементи з сімейства eSTREAM, забезпечують більшу криптографічну стійкість і підвищену ефективність при забезпеченні високого рівня захисту інформації в умовах сучасних кіберзагроз.

Оскільки потокові шифри стали невід'ємною частиною забезпечення безпеки інформації, вони знайшли застосування не тільки в телекомунікаційних системах, але й в області фінансових технологій, систем захисту інформації в урядових установах і на підприємствах з високим рівнем вимог до конфіденційності.

Алгоритм RC4

RC4 (Rivest Cipher 4) — це один з найвідоміших і найпоширеніших поточкових шифрів, розроблений Рівом Рівестом у 1987 році для компанії RSA Data Security. Він використовує змінну довжину ключа і працює в режимі оберненого зв'язку. Однією з його особливостей є простота реалізації та швидкодія, завдяки чому RC4 широко використовувався в різних протоколах і системах, таких як WEP для бездротових мереж, Skype для захисту трафіку та навіть в документах PDF.

Структура алгоритму включає блоки заміни, розмір яких складає 256 елементів. Ініціалізація починається з масиву, що містить всі можливі значення байтів (від 0 до 255), після чого кожен елемент цього масиву змінюється в залежності від ключа. Далі в алгоритмі використовуються два лічильники, що визначають зміни індексів елементів масиву для генерування псевдовипадкових байтів. В результаті XOR цього байта з відкритим текстом отримується зашифрований потік.

Слабкість алгоритму RC4 була виявлена з часом через недостатньо сильні властивості щодо стійкості до атак, що зробило його менш популярним у порівнянні з новими шифрами. Однак він все ще використовується в деяких старих системах та протоколах.

ПОТОКОВІ ШИФРИ НА БАЗІ РЕГІСТРІВ ЗСУВУ

Потокові шифри на базі регістрів зсуву (Shift Registers) використовують принцип генерації псевдовипадкових послідовностей бітів через послідовне зміщення елементів у реєстрі з певним зворотним зв'язком. Одним із таких шифрів є Лінійний регістр з зворотнім зв'язком (LFSR), що є основою для багатьох криптографічних алгоритмів, завдяки своїй швидкості і простоті реалізації.

У 1965 році Ернст Селмер розробив теорію послідовностей зсувних регістрів, яка пізніше була доповнена іншими дослідниками, зокрема Соломоном Голомбом. Алгоритм LFSR має просту структуру і високу швидкодію, що робить його ідеальним для використання в реальному часі. Однією з його переваг є використання лише базових операцій додавання і множення, що дозволяє реалізувати його навіть на простих обчислювальних пристроях.

Потоковий шифр A5, який використовує LFSR, застосовується в GSM-зв'язку для шифрування голосових та даних в каналах зв'язку між мобільними телефонами та базовими станціями. A5 складається з трьох LFSR з довжинами 19, 22 та 23 біта, і для генерації шифрованого потоку використовуються операції XOR між їх виводами. Однак A5 має відомі вразливості і, зважаючи на розвиток криптоаналітичних методів, він вважається не досить безпечним. Тому для нових поколінь мобільних мереж були розроблені нові, більш стійкі варіанти цього шифра.

АЛГОРИТМ SEAL

SEAL (Software-optimized Encryption Algorithm) — це програмно оптимізований симетричний потоковий шифр, розроблений у 1991 році Ральфом Мерклом. Основна мета алгоритму полягала у створенні

високопродуктивного шифру для програмної реалізації, який би працював на 32-бітних процесорах і мінімум з 8 регістрами загального призначення та кешем не менше 8 КБ. В 1993 році була представлена перша версія шифру SEAL 1.0.

Він використовує ключову послідовність, яка генерується на основі певних модифікацій, де зміни в значеннях регістрів виконуються залежно від таблиць, отриманих з ключа. Після численних ітерацій значення цих регістрів додаються до ключової послідовності, яка потім використовується для шифрування даних. Одна з особливостей алгоритму SEAL полягає в тому, що замість самого ключа для шифрування використовуються спеціальні таблиці, що дозволяє значно підвищити швидкість шифрування.

Однак, незважаючи на високу швидкодію, SEAL 1.0 виявився уразливим до криптоаналітичних атак, і тому були розроблені нові версії SEAL 2.0 і SEAL 3.0, в яких були вдосконалені методи генерації таблиць і використовувалися більш стійкі до атак алгоритми, такі як SHA-1.

Хоча старі потокові шифри, такі як RC4 і A5, залишаються частково актуальними в деяких старих системах, сучасні криптографічні алгоритми зазвичай орієнтовані на більш високу стійкість до криптоаналітичних атак. Сучасні потокові шифри, як правило, використовують складніші структури, що забезпечують більшу безпеку і меншу вразливість до атак, таких як атаки на вибірку або атаки на базі статистичних властивостей псевдовипадкових послідовностей.

До теперішнього часу шифри на основі регістрів зсуву, таких як LFSR, залишаються основними інструментами для генерації псевдовипадкових послідовностей, але застосовуються в нових і вдосконалених формах, що враховують новітні криптографічні вимоги безпеки.

18.6.Блокові складені шифри

Блокові складені шифри є одними з найефективніших інструментів для захисту інформації, оскільки вони поєднують простоту виконання операцій з високим рівнем безпеки. Один з найбільш відомих методів у цьому контексті — шифр Фейстеля, розроблений на основі ідеї перетворення даних через багаторазові раунди з використанням простих математичних операцій. Підхід, запропонований К. Шенноном, полягає у застосуванні двох основних типів операцій — перемішування та розсіювання — для досягнення високого рівня криптографічної стійкості.

Принцип блокових шифрів полягає в тому, що дані (відкритий текст) розбиваються на блоки фіксованої довжини, і кожен блок піддається перетворенню за допомогою декількох раундів. В результаті цього перетворення відбувається не тільки заміна окремих частин тексту, а й зміна їх розташування. Тому для зламування таких шифрів необхідно враховувати взаємозалежність між блоками та складні математичні операції, що ускладнює статистичний аналіз.

Блокові шифри працюють з фіксованими розмірами блоків даних, що визначає ефективність і безпеку процесу шифрування.

Типові розміри блоків:

1. 64 біти (8 байтів) — використовуються у старіших алгоритмах, таких як DES (Data Encryption Standard) та Triple DES (3DES).
2. 128 бітів (16 байтів) — є сучасним стандартом у шифрах, таких як AES (Advanced Encryption Standard).
3. 256 бітів та більше — іноді використовуються для підвищення стійкості до криптоаналізу, хоча надмірно великі блоки можуть уповільнювати шифрування.

Вплив розміру блоку на безпеку

- Маленький блок (64 біти) може створювати ризик колізій, коли однакові блоки шифруються однаково, що полегшує криптоаналіз.
- Великі блоки (128 бітів і більше) значно знижують ймовірність таких колізій і підвищують криптографічну стійкість.

Вибір розміру блоку залежить від алгоритму та вимог до безпеки системи. AES зі 128-бітним блоком став загальноприйнятим стандартом завдяки оптимальному балансу між продуктивністю та безпекою.

Проблема, що виникає при застосуванні простих шифрів заміни, полягає в тому, що вони стають уразливими при шифруванні великих обсягів тексту. Якщо розмір шифрованого тексту значно перевищує розмір абетки, то злом таких шифрів за допомогою статистичного аналізу стає можливим. Для підвищення стійкості шифрів заміни застосовують два підходи: збільшення абетки (реалізоване в багатозначних замінах та блокових шифрах) і зменшення кількості знаків, що шифруються за одну операцію (як це робиться у потокових шифрах).

Шифр Фейстеля, що є класичним прикладом складеного шифру, реалізує принцип перемішування через багаторазове застосування криптографічних операцій. В рамках цього підходу текст розбивається на два півблоки, і кожен з них піддається модифікаціям із використанням раундових ключів. Операція шифрування відбувається шляхом перетворення лівої частини блоку за допомогою правої частини та

раундових ключів, що дає можливість перетворити вхідний текст в іншу форму, що не дозволяє легко відновити відкритий текст без ключа.

Розглянемо приклад операції перемішування за допомогою функції XOR. Якщо для цього вибирається вектор a , то операція XOR між вектором x і a може змінити область векторів, забезпечуючи перетасування та ускладнюючи відновлення вихідного тексту. Такий підхід дозволяє створити складні схеми шифрування, де кожен раунд перетворює блоки тексту через комбінацію заміни та перестановки, що сприяє високому рівню безпеки.

Ключовою перевагою блокових складених шифрів є їх симетричність: одна й та сама операція застосовується як для шифрування, так і для дешифрування, що дозволяє реалізувати такі шифри на одному пристрої. Перехід між шифруванням і дешифруванням забезпечується простою зміною порядку раундових ключів.

Водночас сучасні криптографічні стандарти, такі як AES (Advanced Encryption Standard), також базуються на подібних принципах, але використовують більш складні методи перетворення для забезпечення високого рівня безпеки. Вони застосовують багато раундів з операціями заміни та перестановки, а також варіативні ключі, що значно ускладнюють можливість злому.

Блокові шифри, зокрема шифр Фейстеля, стали основою для багатьох сучасних криптографічних протоколів і систем, зокрема у фінансових, урядових та військових додатках, де важливі висока безпека та ефективність. Вони продовжують розвиватися, вдосконалюючи методи шифрування для відповіді на нові виклики в сфері кібербезпеки та криптографії.

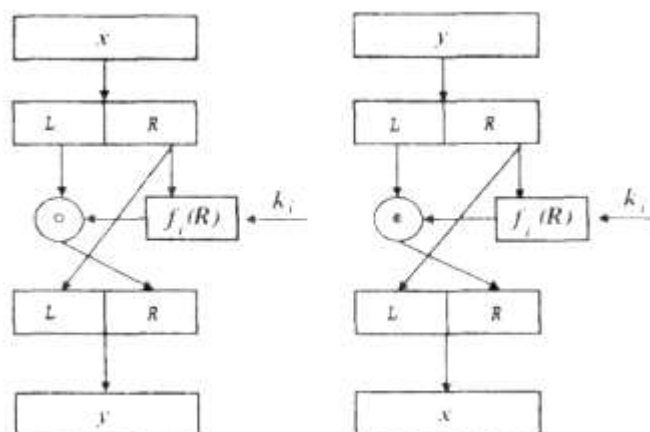


Рис. 18.5. Петля Фейстеля

Джерело: [8-9]

Шифр Фейстеля є одним із класичних прикладів блокових шифрів, структура якого лягла в основу багатьох сучасних алгоритмів, таких як DES (Data Encryption Standard). Його ключовою особливістю є симетричність процесів шифрування та дешифрування, що досягається завдяки застосуванню однакових функцій із реверсуванням порядку ключів. Основна структура складається з декількох раундів обробки даних, де кожен раунд включає розбиття блоку на дві частини, обчислення функції на одній із них та обмін місцями частин. Петля Фейстеля дозволяє створити стійку криптографічну систему навіть із використанням простих функцій у кожному раунді. Такий підхід забезпечує високу гнучкість у виборі функцій шифрування та дозволяє легко масштабувати кількість раундів залежно від вимог до стійкості шифру. Шифр Фейстеля залишається важливим етапом у розвитку криптографії та демонструє ефективний підхід до проєктування стійких блокових шифрів. Завдяки своїй архітектурі цей тип шифру забезпечує високу надійність навіть за умов обмежених обчислювальних ресурсів.

Режим електронної кодової книги (ЕСВ)

Блокові шифри є ключовим інструментом у криптографії для захисту інформації, забезпечуючи обробку фіксованих розмірів блоків даних із використанням симетричних ключів. Їх ефективність багато в чому залежить від обраного режиму шифрування. Зазвичай, розмір блоку дорівнює 64 бітам, отже, в «кодовій книзі» досить багато записів - 2^{64} . Структура кожної «кодової книги» визначається своїм ключем.

Перевагою ЕСВ є незалежне шифрування блоків. Це важливо для шифрування сукупності файлів з довільним (випадковим) доступом, наприклад, бази даних. Шифровані записи можна видаляти і додавати в будь-яку довільну ділянку БД, якщо вважати, що запис складається з цілого числа блоків.

Найпростішим із них є режим електронної кодової книги (ЕСВ), де кожен блок відкритого тексту шифрується незалежно від інших. Простота реалізації та можливість працювати з файлами довільного доступу є основними перевагами цього режиму. Однак однакові блоки відкритого тексту шифруються однаково, що створює ризики, такі як аналіз повторюваних структур та атаки повторення блоків. Наприклад, у системах електронних платежів зловмисник може повторно надіслати зашифроване повідомлення про транзакцію, що призведе до несанкціонованої виплати.

Режим зчеплення шифрованих блоків (СВС)

Більш захищеним варіантом є режим зчеплення шифрованих блоків (CBC), де кожен блок перед шифруванням комбінується із зашифрованим попереднім блоком або випадковим вектором ініціалізації (IV). Зчеплення забезпечується шляхом застосування результату шифрування попереднього блоку для шифрування поточного блоку. Таким чином, будь-який блок шифртексту залежить від усіх попередніх блоків вихідного тексту.

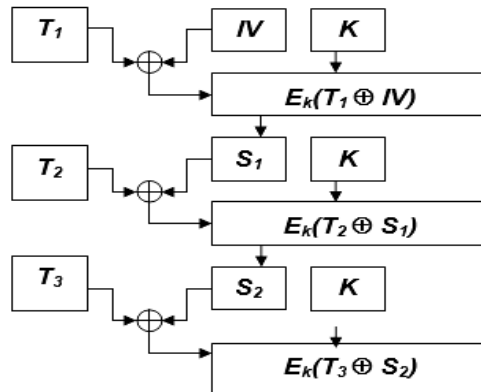


Рис. 18.6. Режим шифрування CBC для трьох символів тексту
Джерело: [8-9]

Такий підхід забезпечує залежність між блоками, ускладнюючи криптоаналіз і підвищуючи унікальність шифрування. Водночас цей режим чутливий до втрати синхронізації: зміна одного біта шифртексту впливає на розшифрування всіх наступних блоків. Крім того, останній блок може потребувати заповнення (padding), що ускладнює роботу з даними.

Більшість повідомлень не ділиться без остачі на 64-бітові блоки, зазвичай залишається короткий блок в кінці тексту. Можна по-різному боротися з цим.

Найпростіший метод - це доповнення до повного блоку (padding) несуттєвим набором символів. Для видалення «сміття» при відновленні повідомлення достатньо в останньому байті вказати кількість зайвих символів. Також з цією метою можна використовувати як останній байт тексту символ кінця файлу, але іноді це неможливо реалізувати, наприклад, у випадку, коли розшифрований блок негайно відправляється в пам'ять.

Тоді застосовується така схема шифрування: припустимо, останній блок складається з j бітів. Після шифрування останнього цілого блоку, зашифруємо шифрований блок ще раз, виберемо j початкових бітів отриманого тексту і додамо за mod 2 з останнім блоком вихідного тексту.

Це і є шифр для неповного блоку.

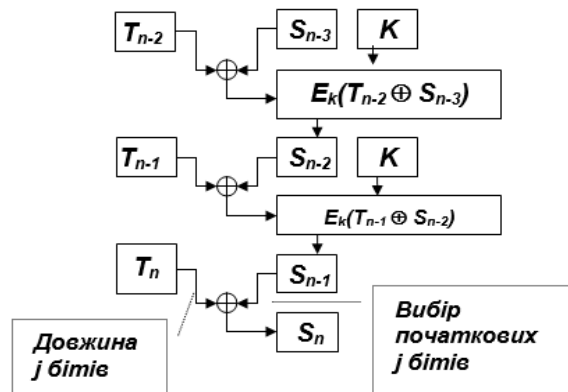


*Рис. 18.7. Шифрування останнього короткого блоку
Джерело: [8-9]*

Ця схема дозволяє ефективно обробляти повідомлення, довжина яких не є кратною розміру блоку. Оскільки після шифрування останнього блоку здійснюється додавання початкових бітів до попереднього блоку, це забезпечує додатковий рівень безпеки та ускладнює аналіз шифрованого тексту. Крім того, така операція дозволяє мінімізувати ризик виникнення шаблонів у зашифрованих даних, що важливо для запобігання криптоаналізу. Після цього отриманий результат стає остаточним шифрованим блоком, який можна передавати одержувачу. Важливим моментом є синхронізація між відправником і отримувачем, щоб обидві сторони мали однакову інформацію про шифрування неповного блоку. Такі методи шифрування застосовуються в багатьох сучасних криптографічних протоколах, де потрібна висока швидкість і ефективність при роботі з великими обсягами даних. Однак для забезпечення максимального рівня захисту потрібно застосовувати додаткові механізми, такі як обробка ключів та регулярне їх оновлення.

Режим зворотного зв'язку з шифром (CFB)

Для шифрування даних меншими одиницями, наприклад, байтами чи бітами, часто використовують режим зворотного зв'язку з шифром (CFB). Цей режим забезпечує потокове шифрування та не вимагає заповнення блоків, але схильний до поширення помилок: одна помилка в шифртексті призводить до пошкодження відповідного біта у відкритому тексті. CFB дозволяє шифрувати дані поступово, що робить його зручним для передачі інформації в реальному часі, наприклад, у потокових відео- та аудіосервісах. Однією з важливих переваг цього режиму є його сумісність із пристроями, які мають обмежені ресурси пам'яті. Водночас критичним

недоліком є те, що навіть невелика зміна в зашифрованих даних може вплинути на розшифрування наступних сегментів. Це ускладнює виправлення помилок при передачі інформації через нестабільні канали зв'язку. Через свою гнучкість CFB залишається популярним у певних криптографічних застосуваннях, хоча і поступається за рівнем захисту іншим сучасним режимам. Сьогодні, аби зменшити вплив помилок, рекомендовано поєднувати цей режим із механізмами контролю та корекції помилок. Попри свої обмеження, CFB продовжує знаходити застосування завдяки здатності ефективно шифрувати потоки даних.

Режим CFB (Cipher Feedback Mode) передбачає можливість шифрування даних записами, меншими, ніж цілий блок. Ми розглянемо варіант шифрування одного символу в коді ASCII (так званий 8-бітовий CFB), але його можна узагальнити і на випадок одного біта. На рис. показаний 8-бітовий режим CFB у випадку 64-бітового блокового алгоритму. У цьому варіанті блоковий алгоритм працює з чергою (стеком) з розміром, що дорівнює довжині вхідного блоку - 64 біти. Перед початком шифрування стек, як і в режимі CBC, заповнюється вектором ініціалізації IV.

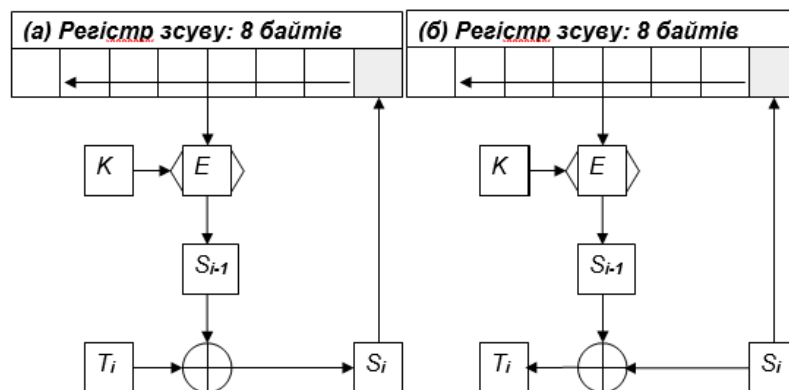


Рис. 18.8. Режим 8-бітовий CFB-mode, (а) зашифрування,
(б) розшифрування

Джерело: [8-9]

У кожному такті шифрується вміст стека, а крайні ліві 8 бітів результату складаються за модулем два з першим 8-бітовим символом тексту, в результаті отримуємо 8 бітів шифрованого тексту, готових для передачі. Потім вміст стека зсувається вліво на 8 бітів, крайні ліві 8 бітів при цьому відкидаються. Раніше отриманий символ шифрованого тексту заміщає крайні праві 8 бітів стека. Потім процес повторюється. Таким чином, по суті, реалізується генератор поточкового шифру. Розшифрування

здійснюється в зворотному порядку. Відзначимо, що на обох сторонах блоковий алгоритм працює в режимі зашифрування.

Сучасні тенденції у використанні блокових шифрів свідчать про поступову заміну класичних алгоритмів, таких як DES та 3DES, більш стійкими стандартами, зокрема AES (Advanced Encryption Standard). Крім того, у контексті загроз від квантових обчислень активно розробляються квантово-стійкі шифри, здатні забезпечити належний рівень захисту інформації.

Для безпечного використання блокових шифрів важливо дотримуватися кількох рекомендацій. Перевагу слід віддавати сучасним режимам шифрування, таким як GCM (Galois/Counter Mode), які не лише шифрують дані, а й забезпечують їх автентифікацію. Часта зміна ключів дозволяє знижувати ризик успішних атак, а використання випадкових векторів ініціалізації (IV) забезпечує унікальність шифртекстів. Не менш важливими є контроль цілісності повідомлень та впровадження механізмів виправлення помилок.

Таким чином, блокові шифри залишаються критично важливим компонентом захисту інформації. Їх ефективність напряму залежить від правильного вибору режиму роботи, дотримання сучасних криптографічних практик і своєчасного впровадження інноваційних рішень для протидії новітнім загрозам.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 18

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.

2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

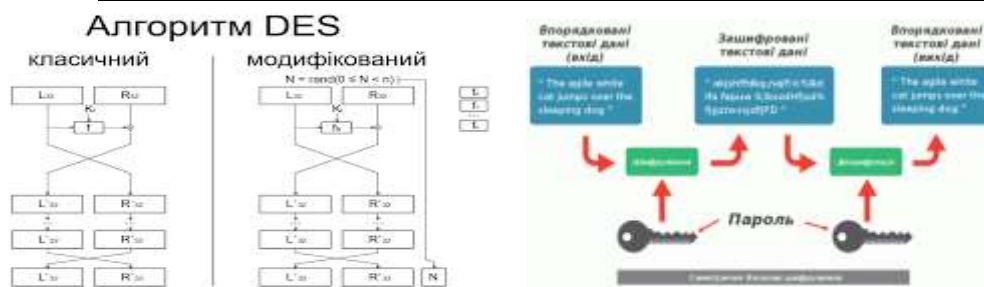
3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.

4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
6. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
7. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.
8. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.
9. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.
10. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.
11. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.
12. Шевченко , С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.
13. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.
14. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.

15. Спасітелєва, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.
16. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.
17. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.
18. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142–148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.
19. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.
20. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.
21. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.
22. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.
23. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

РОЗДІЛ 19

СИМЕТРИЧНІ КРИПТОАЛГОРИТМИ



19.1. Алгоритм DES

19.2. Основні режими роботи алгоритму DES

19.3. Стійкість та модифікація DES

19.4. Алгоритм шифрування IDEA

19.5. Алгоритм AES

"Симетричні криптографічні системи є ефективними для шифрування даних, але їх безпека залежить від одного ключа, що створює уразливість в разі його компрометації."

Bruce Schneier, експерт з безпеки

19.1. АЛГОРИТМ DES

DES (Data Encryption Standard) був одним з найпопулярніших симетричних криптоалгоритмів у 20 столітті і використовувався як федеральний стандарт шифрування в США до початку 2000-х років. Хоча DES вже давно вважається застарілим через короткий розмір ключа (56 біт), він залишався важливим у криптографії до того часу, поки не був замінений більш потужними алгоритмами, такими як AES. Проте, DES продовжує використовуватися в певних випадках, де швидкість обробки даних є критично важливою і не потребується надзвичайно високий рівень криптостійкості.

Незважаючи на свою історичну значущість, DES піддався численним атакам, зокрема за допомогою brute-force (перебору всіх можливих ключів), що стало можливим із розвитком обчислювальних потужностей.

Після публікації спеціалізованих атак на DES, таких як диференційний криптоаналіз і атаки на основі перебору ключів, були розроблені більш сучасні варіанти шифру, такі як Triple DES (3DES), який використовує тричі повторене шифрування з трьома різними ключами, щоб компенсувати короткий розмір ключа.

Враховуючи сучасний розвиток обчислювальних технологій і криптографії, DES вважається ненадійним для використання в нових системах безпеки, однак залишається важливим історичним етапом у розвитку сучасних криптографічних стандартів. Сьогодні рекомендується використовувати інші більш потужні алгоритми, такі як AES, для забезпечення високої криптостійкості в інформаційних системах.

Алгоритм DES також використовує комбінацію підстановок і перестановок. DES здійснює шифрування 64-бітових блоків даних за допомогою 64-бітового ключа, у якому значущими є 56 біт (інші 8 бітперевірочні біти для контролю на парність). Дешифрування в DES є операцією, зворотною шифруванню, і виконується шляхом повторення операцій шифрування в зворотній послідовності. Узагальнена схема процесу шифрування в алгоритмі DES показана на рис.9.1. Процес шифрування полягає в початковій перестановці бітів 64-бітового блоку, шістнадцятих циклах шифрування і, нарешті, у кінцевій перестановці бітів.



Рис. 19.1. Узагальнена схема шифрування в алгоритмі DES
Джерело: [8-9]

Узагальнена схема шифрування в алгоритмі DES включає кілька етапів, які забезпечують перетворення відкритого тексту (plain text) в зашифрований текст (cipher text).

Основні етапи цього процесу:

1. Початкова перестановка (Initial Permutation, IP)

Спочатку 64-бітовий блок відкритого тексту піддається початковій перестановці. Ця перестановка є фіксованою, тобто вона завжди однакова для всіх повідомлень. Вона дозволяє змішати біти тексту перед подальшою

обробкою. Початкова перестановка не змінює загальний обсяг даних, але забезпечує певний рівень криптографічної безпеки, ускладнюючи атакувальнику прямий доступ до структури тексту. Цей етап є лише першим кроком у складному процесі шифрування, що включає подальші операції з підстановками і перестановками на більш глибоких етапах.

2. Розподіл на дві частини (L_0, R_0)

Після початкової перестановки 64 біти відкритого тексту поділяються на дві рівні частини: ліву (L_0) і праву (R_0), кожна з яких має 32 біти. Ці частини будуть оброблятися окремо на кожному з етапів шифрування. Такий поділ дозволяє ефективно використовувати операції з XOR на кожному раунді, створюючи заплутану структуру шифру. Це також дозволяє застосовувати паралельну обробку обох частин, що сприяє підвищенню швидкості шифрування.

3. 16 раундів шифрування (16 Rounds)

На кожному раунді ліву частину L і праву частину R обробляють через функцію фейстеля, де відбувається підставлення та перестановка. Результати цих операцій XOR-уються з відповідними частинами, після чого ліву та праву частину міняють місцями перед наступним раундом. Кожен з 16 раундів шифрування виконується однаково і складається з наступних кроків:

- ➔ Розширення правої частини (Expansion): 32 біти правої частини (R) розширюються до 48 бітів за допомогою таблиці розширення (E). Це робиться для того, щоб підготувати частину даних для подальшої обробки.
- ➔ Застосування ключа (Key Mixing): Розширена права частина змішується з 48-бітовим раундовим ключем, який генерується з основного ключа за допомогою спеціальної процедури (сувора трансформація та циклічні зсуви).
- ➔ Шифрування за допомогою S-блоків: Змішаний результат передається через 8 S-блоків (підстановочних таблиць), кожен з яких зменшує 48 біт до 32 бітів, надаючи нелінійне перетворення.
- ➔ Перестановка (Permutation P): Результат з S-блоків піддається фіксованій перестановці (P), яка забезпечує подальше змішування бітів.
- ➔ Комбінація з лівою частиною (XOR): Отриманий результат XOR-ується з лівою частиною (L), створюючи нову праву частину для наступного раунду. Ліва частина (L) переходить до правої частини на наступний раунд.

4. Фінальна перестановка (Final Permutation, FP)

Після завершення 16 раундів ліва та права частини об'єднуються в один 64-бітовий блок, який піддається фінальній перестановці. Ця фінальна перестановка є зворотною до початкової перестановки IP, що дозволяє повернути біти до їх правильного порядку. Фінальна перестановка завершує процес шифрування, забезпечуючи, щоб всі зміни, внесені на попередніх етапах, були остаточно застосовані до блоку даних. Це також допомагає підвищити криптографічну стійкість алгоритму, оскільки в результаті перестановок складніше відновити оригінальні дані без знання ключа.

5. Результат шифрування

Отриманий результат після фінальної перестановки є зашифрованим текстом (cipher text). Для дешифрування використовується зворотний процес з тими ж операціями, але в зворотному порядку і з використанням зворотних раундових ключів. Цей процес забезпечує, що зашифрований текст можна відновити тільки за допомогою правильного секретного ключа, виконуючи операції дешифрування поетапно. Важливою особливістю є те, що всі операції, включаючи перестановки та функції Фейстеля, виконуються в зворотному порядку, що гарантує правильне відновлення оригінальних даних.

Ця схема є основою для алгоритму DES, який ефективно працює для шифрування великих обсягів даних, хоча через застарілість і короткий розмір ключа він вже не вважається повністю безпечним для сучасних застосувань.

Алгоритм DES відноситься до класу блокових шифрів, де вихідні дані та результати шифрування подаються у вигляді 64-бітових блоків. Шифрування та розшифрування виконуються за однаковими схемами, зокрема, основною відмінністю є порядок використання ключів. Ключ шифрування є випадковим числом довжиною 56 бітів, доповненим вісьмома бітами перевірки парності, що дає загальну довжину 64 біти.

Алгоритм використовує схему Фейстеля, яка передбачає ітераційну обробку двох частин блоку даних. Кожен із 16 раундів шифрування складається з операцій підстановки та перестановки, що реалізують функції розсіювання (дифузії) та перемішування. Перш ніж почати шифрування, 64-бітовий блок даних піддається початковій перестановці, після чого він розбивається на дві частини по 32 біти, які обробляються окремо на кожному етапі.

У кожному раунді правий півблок даних розширюється до 48 бітів за допомогою перестановки розширення, після чого додається за модулем 2 з 48 бітами ключа відповідного раунду. Далі застосовується серія замінів за допомогою S-блоків, де 48 бітів вхідних даних перетворюються в 32 біти.

Після підстановок відбувається перестановка результату, і правий півблок комбінується з лівим для наступного раунду.

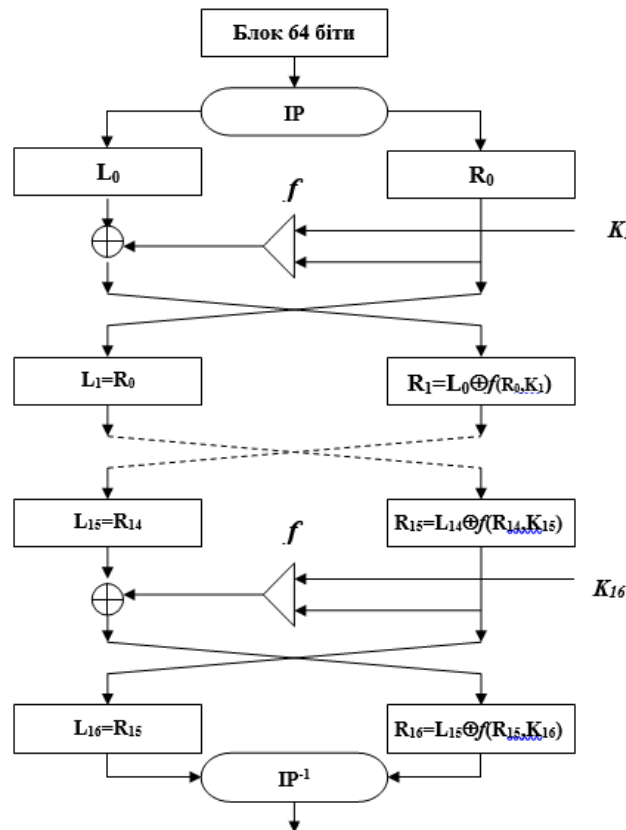


Рис. 19.2. Загальна схема алгоритму DES

Джерело: [8-9]

Процес розшифрування є зворотним до процесу шифрування, але з використанням раундових ключів у зворотному порядку. Окрім цього, ключі для кожного раунду генеруються за допомогою циклічних зсувів півблоків початкового 56-бітного ключа, після чого вони піддаються перестановці для отримання 48-бітових ключів. Перестановки та підстановки в DES забезпечують його стійкість до криптоаналізу, зокрема, до диференціального аналізу, що ускладнює відновлення оригінального тексту без знання ключа.

Загалом, DES є класичним прикладом блокового шифру, але через його вразливість до сучасних методів атак, таких як методи перебору ключів, його використання вважається застарілим, і він був замінений більш безпечними алгоритмами, наприклад, AES.

Алгоритм DES (Data Encryption Standard) має кілька значних слабких місць, основним з яких є недостатня довжина ключа. Оскільки ключ у DES складає лише 56 біт, це робить його вразливим до атаки методом повного

перебору ключів, яка стає реальною через потужність сучасних обчислювальних систем.

Згідно з оцінками, ще в 1979 році було визначено, що для побудови спеціального обчислювача для перебору ключів за одну добу потрібно близько 20 мільйонів доларів, а у 1981 році — не більше 50 мільйонів доларів. Однак, для сучасних спеціальних служб і з урахуванням прогресу в обчислювальних потужностях, перебір ключів у DES є цілком реальним.

Крім того, одна з важливих особливостей DES — це кількість раундів шифрування. Алгоритм використовує 16 раундів, оскільки після 8 ітерацій блок шифрування набуває властивостей практично випадкової функції. Однак зменшення числа раундів, як показав А. Конхейм, значно знижує стійкість алгоритму, а виведення результатів криптоаналізу для 4- і 6-раундових версій DES вказує на їхню вразливість.

У 1990 році Е. Біхам і А. Шамір розробили методи диференціального криптоаналізу, які показали, що для меншої ніж 16 кількості раундів алгоритм можна розкрити за допомогою атаки типу known-plaintext (атака на основі відомих відкритих текстів) з меншою складністю, ніж за допомогою методу повного перебору.

Крім того, DES має схему генерації ключів, що допускає наявність слабких ключів. Наприклад, деякі ключі можуть бути однаковими для всіх раундів або навіть мати парні ключі, що використовуються багато разів, що знижує складність криптоаналізу. Існують також так звані напівслабкі ключі, де пара ключів дає однакові результати при шифруванні, що також є уразливістю в системі.

Іншою важливою вразливістю є так звані доповнювальні (інверсні) ключі, що можуть скоротити кількість варіантів для перебору на половину. Це дозволяє певним атакам типу chosen-plaintext знижувати складність криптоаналізу.

У результаті, хоча DES досі застосовується у деяких випадках, його слабкість, зокрема через короткий ключ і кількість раундів, робить його вразливим до сучасних криптоаналітичних атак. Актуальним є перехід до нових стандартів шифрування, таких як AES, які забезпечують значно більшу стійкість до атак.

Потрійне шифрування за допомогою DES (Triple DES, або 3DES) — це вдосконалена версія алгоритму DES, яка дозволяє підвищити безпеку шляхом багаторазового застосування стандартного DES для одного блоку даних. 3DES була розроблена для того, щоб компенсувати обмеження DES, зокрема, його коротку довжину ключа (56 біт), яка робить алгоритм вразливим до атак методом перебору ключів.

У 3DES застосовуються три ключі, кожен з яких має довжину 56 біт. Алгоритм працює за принципом послідовного шифрування:

1. **Перше шифрування** - перший ключ (K_1) використовується для зашифрування блоку даних за допомогою стандартного алгоритму DES.
2. **Розшифрування** - потім дані розшифровуються за допомогою другого ключа (K_2), знову за допомогою DES.
3. **Перше шифрування (повторно)** - наостанок блок шифрується вдруге за допомогою третього ключа (K_3) в алгоритмі DES.

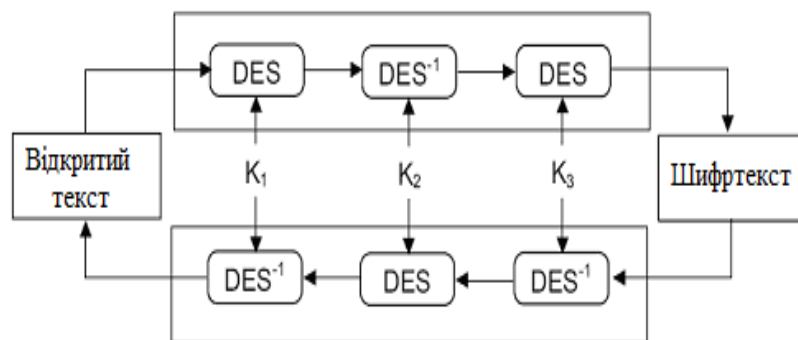


Рис. 19.3. Потрійне шифрування за допомогою DES

Джерело: [8-9]

Таким чином, 3DES використовує три ключі для шифрування та розшифрування інформації, що забезпечує набагато вищу стійкість порівняно з одним шифруванням DES. Довжина ключа в 3DES складає 168 біт (3×56 біт), хоча в деяких реалізаціях, якщо два ключі однакові ($K_1 = K_3$), ефективна довжина ключа буде знижена до 112 біт.

Процес потрійного шифрування виглядає так:

1. Зашифрувати текст за допомогою ключа K_1 .
2. Розшифрувати результат за допомогою ключа K_2 .
3. Зашифрувати отриманий результат за допомогою ключа K_3 .

У результаті, навіть якщо зломисник має можливість зламати один етап (наприклад, за допомогою атаки на DES), йому буде набагато складніше здійснити це для трьох етапів, що робить 3DES значно більш безпечним.

Попри це, 3DES теж має свої недоліки. Він набагато повільніший за інші сучасні алгоритми шифрування, такі як AES, і в результаті його використовують менш часто в сучасних системах, хоча він все ще може використовуватися для збереження сумісності з старими стандартами.

19.2. ОСНОВНІ РЕЖИМИ РОБОТИ АЛГОРИТМУ DES

Алгоритм DES (Data Encryption Standard) добре підходить як для шифрування, так і для аутентифікації даних. Він дозволяє перетворювати 64-бітовий відкритий текст в 64-бітовий шифрований текст. Однак, для вирішення різних криптографічних задач, зокрема коли дані не обмежуються 64 бітами, розроблені чотири основні режими роботи алгоритму:

- електронна кодова книга ECB (Electronic Code Book);
- зчеплення блоків шифру CBC (Cipher Block Chaining);
- зворотний зв'язок за шифром CFB (Cipher Feed Back);
- зворотний зв'язок за виходом OFB (Output Feed Back).

✱ **Електронна кодова книга (ECB)** – у цьому режимі великий файл розбивають на 64-бітові блоки, і кожен з них шифрується окремо за допомогою одного і того ж ключа. Хоча цей режим є простим в реалізації, він має слабку стійкість проти криптоаналізу, оскільки однакові блоки відкритого тексту призводять до однакових блоків шифротексту, що дозволяє зловмисникам отримати інформацію про вміст повідомлення.

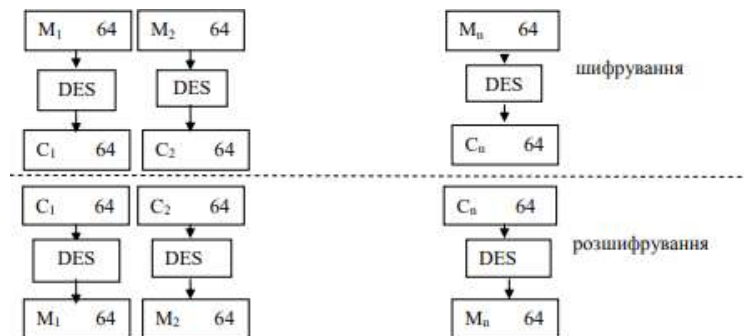


Рис. 19.4. Схема алгоритму DES в режимі електронної кодової книги
Джерело: [8-9]

Через фіксований характер шифрування при обмеженій довжині блоку 64 біти можливе проведення криптоаналізу «зі словником». Блок такого розміру може повторитися в повідомленні внаслідок великої надмірності в тексті природної мови. Це приводить до того, що ідентичні блоки відкритого тексту в повідомленні будуть представлені ідентичними блоками шифротексту, що дає криптоаналітику деяку інформацію про зміст повідомлення.

✱ **Зчеплення блоків шифру (CBC)** – у цьому режимі кожен блок шифрується за допомогою попереднього блоку, що забезпечує більшу стійкість до криптоаналізу. Перший блок з'єднується з 64-бітовим

початковим вектором (IV) перед шифруванням. Це дозволяє уникнути повторення блоків у шифротексті та забезпечує високу стійкість до атак за допомогою словників. Крім того, помилки при передачі впливають лише на два блоки повідомлення, що підвищує надійність.

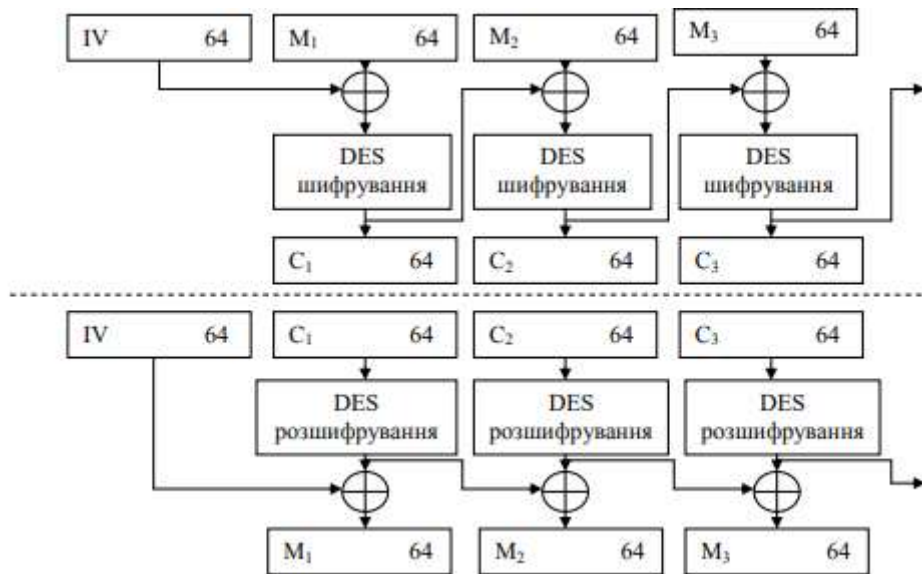


Рис. 19.5. Схема алгоритму DES у режимі зчеплення блоків шифру
Джерело: [8-9]

✱ **Зворотний зв'язок за шифром (CFB)** – цей режим перетворює блочний шифр на поточковий шифр, що самосинхронізується. Шифрування схоже на режим CBC, але за основу береться не попередній шифротекст, а зашифрований попередній блок. При цьому, на відміну від CBC, втрата одного байту або біту не руйнує всі наступні блоки шифротексту, що дозволяє краще справлятися з помилками в передаванні. Описаний вище найпростіший спосіб використання CFB ані трохи не більш самосинхронізовний ніж інші режими на кшталт CBC. Якщо губиться цілий блок шифротексту, то обидва CBC і CFB синхронізуються, тоді як втрата IV 64 M1 64 M2 64 M3 64 DES шифрування DES шифрування DES шифрування C1 64 C2 64 C3 64 IV 64 C1 64 C2 64 C3 64 DES розшифрування DES розшифрування DES розшифрування M1 64 M2 64 M3 64 100 одного байту або біту остаточно відкине розшифрування. Для уможливлення синхронізації після втрати одного байту або біту, за раз треба шифрувати один байт або біт. CFB можна таким чином використовувати разом з зсувним регістром на вході до блочного шифру. Подібно до режиму CBC, зміни в відкритому тексті поширюються на весь шифротекст, і шифрування не можна упаралелити. Також подібно до CBC,

розшифрування упаралельнюване. При розшифруванні, зміна одного біту в шифротексті впливає на два блоки відкритого тексту: однобітова зміна в відповідному блоці відкритого тексту і повне пошкодження наступного блоку. Подальші блоки розшифровуються нормально. Через це, якщо зломисник знає відкритий текст, він може змінити біти в блоці шифротексту як він захоче і призвести до отримання потрібного йому блоку відкритого тексту, наступний блок буде перетасовано, але на той час вже може бути заподіяна шкода. CFB разом з режимами поточкових шифрів (OFB) поділяє дві переваги над CBC режимом: блок шифр використовується лише в напрямку шифрування, і повідомлення не потребує доповнення до розміру кратного розміру блоку (хоча також можна використати викрадення шифротексту і таким чином зробити доповнення необов'язковим).

✱ **Зворотний зв'язок за виходом (OFB)** – у цьому режимі використовуються попередні виходи блочного шифру для формування потоку ключа, який додається за модулем 2 до блоків відкритого тексту. Це робить OFB синхронним поточковим шифром, де кожен біт відкритого тексту перетворюється у відповідний біт шифротексту. Цей режим є особливо підходящим для передачі даних у реальному часі (наприклад, відео та голосу) завдяки високій швидкодії і здатності зменшувати помилки при передачі.

Для кожного нового повідомлення треба використовувати новий IV, інакше повідомлення будуть шифруватись за тим самим потоком ключа. IV можна відправляти у відкритому вигляді, однак, якщо зломисник підмінив IV, тоді на відміну від CFB режиму, отримати відкритий текст з шифротексту неможливо. Кожен блок на виході залежить від усіх попередніх, отже неможливе паралельне виконання. Однак, через те, що відкритий текст і шифр використовуються лише в фінальному XOR, операції блочного шифру можна виконати наперед, що дозволить виконання фінального кроку паралельно щойно відкритий або шифротекст стане доступним. Можна отримати потік ключа для режиму OFB із рядком нулів на вході. Це може бути корисним, бо уможливорює використання швидкого апаратного забезпечення, що втілює CBC для шифрування в режимі OFB. На відміну від CFB, помилка в одному біті відкритого тексту зачіпає лише відповідний біт в шифротексті, наступні блоки залишаються неушкодженими. Ця властивість разом із можливістю високої швидкодії OFB робить його підходящим для шифрування потоків даних на 101 кшталт голосу і відео, особливо на каналах с завадами де поширення помилок може легко перетворити зашифроване передавання в майже неможливе. З іншого боку OFB вимагає від двох учасників бути синхронізованими. Як

варіант розв'язання цієї проблеми пропонується відправлення синхронізаційних сигналів в узгоджені проміжки часу.

Переваги та недоліки кожного режиму:

- ECB: простота реалізації, але слабка стійкість до криптоаналізу, оскільки однакові блоки відкритого тексту шифруються однаково.
- CBC: стійкий до атак, але неможливо паралельно шифрувати.
- CFB: самосинхронізується і не потребує попереднього шифротексту для наступних блоків, але можливі проблеми з синхронізацією при втраті даних.
- OFB: відмінний для поточкових даних і забезпечує високу швидкість, однак потребує синхронізації між учасниками.

Кожен з цих режимів має свої переваги залежно від вимог до шифрування і типу переданих даних.

ОБЛАСТІ ЗАСТОСУВАННЯ АЛГОРИТМУ DES

Кожному з розглянутих режимів (ECB, CBC, CFB, OFB) властиві свої переваги і недоліки, що визначає сфери їхнього застосування. Режим ECB добре підходить для шифрування ключів, режим CFB зазвичай застосовується для шифрування окремих символів, а режим OFB широко використовується для шифрування в супутникових системах зв'язку.

Режими CBC і CFB є ефективними для аутентифікації даних. Ці режими дозволяють використовувати алгоритм DES для:

- інтерактивного шифрування під час обміну даними між терміналом і головною ЕОМ;
- шифрування криптографічних ключів у практиці автоматизованого поширення ключів;
- шифрування файлів, поштових відправлень, даних супутників і інших практичних задач.

Спочатку стандарт DES був розроблений для шифрування і дешифрування даних ЕОМ. Однак його використання було розширене й на аутентифікацію. Звичайні коди для виявлення помилок не підходять, оскільки, якщо алгоритм утворення коду відомий, супротивник може сформувати правильний код після внесення змін у дані. Однак алгоритм DES дозволяє створити криптографічну контрольну суму, яка забезпечує захист як від випадкових, так і навмисних змін даних. Це описано в стандарті для аутентифікації даних ЕОМ (FIPS 113), який передбачає, що дані шифруються в режимі зворотного зв'язку по шифротексту (CFB) або в режимі зчеплення блоків шифру (CBC), що дає в результаті блок шифру, який є функцією всіх розрядів відкритого тексту.

Застосування цього процесу дозволяє використовувати шифрування для захисту даних від несанкціонованого доступу та аутентифікацію для виявлення змін. Алгоритм аутентифікації може бути застосований до як відкритих, так і зашифрованих даних. У фінансових операціях, де реалізуються і шифрування, і аутентифікація, остання зазвичай застосовується й до відкритого тексту.

Шифрування та аутентифікація використовуються для захисту даних, що зберігаються в ЕОМ. Зокрема, паролі часто зашифровуються необоротним способом і зберігаються в пам'яті комп'ютера. Коли користувач вводить пароль, він шифрується та порівнюється з тим, що зберігається. Якщо значення співпадають, користувач отримує доступ до системи, в іншому випадку йому відмовляється в доступі.

Одним із важливих застосувань алгоритму DES є захист повідомлень в електронних системах платежів, таких як операції між банками та при роботі з широкою клієнтурою. Алгоритм DES активно використовується в банківських автоматах, терміналах торговельних центрів та інших автоматизованих системах. Різноманітність застосувань алгоритму DES дозволяє ефективно захищати широке коло даних, від малих платежів до великих трансакцій.

Стійкість DES

Обговорюючи DES, не можна не згадати про питання безпеки цього алгоритму та потенційні атаки, які можуть бути на нього здійснені. Багаторічний досвід використання DES і його відкритість зробили його об'єктом ретельного аналізу з боку криптоаналітиків, що дозволило виявити багато його слабкостей. Варто зауважити, що деякі атаки є теоретичними та припускають, що злоумисник має доступ до певних обчислювальних або часових ресурсів. Водночас, з розвитком комп'ютерної техніки та криптології, деякі з цих атак можуть бути реалізовані на практиці.

Основні недоліки DES такі:

- ➔ ***Наявність слабких ключів*** – існують 4 слабкі та 12 напівслабких ключів. Ці слабкості виникають через структуру генерації ключів, зокрема через використання двох незалежних регістрів зсуву для генерування ключової послідовності. Наприклад, для слабкого ключа 1F1F1F1F0E0E0E0E, результатом є однакові ключові послідовності в усіх 16 раундах.
- ➔ ***Невелика довжина ключа*** – довжина ключа в 56 бітів, на сучасному етапі розвитку комп'ютерних технологій, вже недостатньо захищена для деяких типів інформації. Це дозволяє проводити атаки методом

«повного перебору» ключів, зокрема через використання потужних комп'ютерних систем.

➔ **Надмірність ключа** – DES використовує біти контролю парності, що може створювати вразливості. Атаки, запропоновані Біхамом і Шаміром, можуть бути ефективними для атаки на реалізації DES у смарт-картах або банківських криптографічних модулях, що зберігають ключі в EEPROM-пам'яті. Наявність бітів контролю парності дозволяє відновити ключ при втраті частини інформації в пам'яті.

➔ **Статичні підстановки в S-блоках** – незважаючи на великий кількість раундів, використання статичних підстановок у S-блоках дозволяє здійснювати атаки на алгоритм. Наприклад, атака, запропонована М. Хеллманом, може за допомогою робочої станції SUN4 визначити 10 бітів ключа за 10 секунд. З вибором 512 відкритих текстів ймовірність успіху атаки складає 80%, а при виборі 768 відкритих текстів – 95%. Відновивши 10 бітів ключа, решту можна знайти методом повного перебору.

Отже, сьогодні використання DES для захисту критично важливої інформації є небезпечним, і криптологи давно працюють над модифікаціями цього алгоритму для підвищення його криптостійкості. До таких модифікацій належать:

- 3DES (Triple DES) – застосовує тричі виконане шифрування DES з трьома різними ключами для підвищення безпеки.
- DESX – вдосконалена версія DES, що використовує додаткові ключі для розширення простору ключів.
- S-DES – спрощена версія DES, яка зазвичай використовується в освітніх цілях для демонстрації принципів роботи шифрування.

Ці модифікації, незважаючи на покращення рівня безпеки, все ж не здатні гарантувати належний рівень захисту для надзвичайно важливої інформації, і тому рекомендується застосовувати більш сучасні алгоритми, такі як AES.

19.3. СТІЙКІСТЬ ТА МОДИФІКАЦІЯ DES

Стійкість DES

Обговорюючи DES, не можна не згадати про питання безпеки цього алгоритму та потенційні атаки, які можуть бути на нього здійснені. Багаторічний досвід використання DES і його відкритість зробили його об'єктом ретельного аналізу з боку криптоаналітиків, що дозволило

виявити багато його слабкостей. Варто зауважити, що деякі атаки є теоретичними та припускають, що зломисник має доступ до певних обчислювальних або часових ресурсів. Водночас, з розвитком комп'ютерної техніки та криптології, деякі з цих атак можуть бути реалізовані на практиці.

Основні недоліки DES такі:

➔ Наявність слабких ключів – існують 4 слабкі та 12 напівслабких ключів. Ці слабкості виникають через структуру генерації ключів, зокрема через використання двох незалежних регістрів зсуву для генерування ключової послідовності. Наприклад, для слабкого ключа 1F1F1F1F0E0E0E0E, результатом є однакові ключові послідовності в усіх 16 раундах.

➔ Невелика довжина ключа – довжина ключа в 56 бітів, на сучасному етапі розвитку комп'ютерних технологій, вже недостатньо захищена для деяких типів інформації. Це дозволяє проводити атаки методом «повного перебору» ключів, зокрема через використання потужних комп'ютерних систем.

➔ Надмірність ключа – DES використовує біти контролю парності, що може створювати вразливості. Атаки, запропоновані Біхамом і Шаміром, можуть бути ефективними для атаки на реалізації DES у смарт-картах або банківських криптографічних модулях, що зберігають ключі в EEPROM-пам'яті. Наявність бітів контролю парності дозволяє відновити ключ при втраті частини інформації в пам'яті.

➔ Статичні підстановки в S-блоках – незважаючи на великий кількість раундів, використання статичних підстановок у S-блоках дозволяє здійснювати атаки на алгоритм. Наприклад, атака, запропонована М. Хеллманом, може за допомогою робочої станції SUN4 визначити 10 бітів ключа за 10 секунд. З вибором 512 відкритих текстів ймовірність успіху атаки складає 80%, а при виборі 768 відкритих текстів – 95%. Відновивши 10 бітів ключа, решту можна знайти методом повного перебору.

Отже, сьогодні використання DES для захисту критично важливої інформації є небезпечним, і криптологи давно працюють над модифікаціями цього алгоритму для підвищення його криптостійкості. До таких модифікацій належать:

- 3DES (Triple DES) – застосовує тричі виконане шифрування DES з трьома різними ключами для підвищення безпеки.
- DESX – вдосконалена версія DES, що використовує додаткові ключі для розширення простору ключів.

- S-DES – спрощена версія DES, яка зазвичай використовується в освітніх цілях для демонстрації принципів роботи шифрування.

Ці модифікації, незважаючи на покращення рівня безпеки, все ж не здатні гарантувати належний рівень захисту для надзвичайно важливої інформації, і тому рекомендується застосовувати більш сучасні алгоритми, такі як AES.

Модифікації DES

3DES

Потрійний DES (3DES) є однією з найбільш відомих модифікацій класичного алгоритму DES. У цій схемі використовуються три ключі: K1, K2 і K3, що дозволяє суттєво збільшити рівень безпеки в порівнянні з оригінальним DES. Сумарна довжина ключа в 3DES становить 168 біт, оскільки кожен з ключів має довжину 56 біт. Процес шифрування відбувається в три етапи: перше шифрування за допомогою ключа K1, потім розшифрування за допомогою ключа K2 і повторне шифрування за допомогою ключа K3. Така схема забезпечує додаткову стійкість до атак, оскільки навіть якщо один із ключів порушений, криптографічний захист все одно зберігається завдяки використанню трьох різних ключів. Для розшифрування застосовують зворотний порядок операцій. Однак варто зазначити, що хоча 3DES значно посилює безпеку порівняно з оригінальним DES, він все одно має деякі вразливості, особливо у випадку з великою кількістю даних. Завдяки своїй складній структурі, алгоритм 3DES є значно повільнішим, ніж сучасні криптографічні алгоритми, такі як AES, що обмежує його ефективність у багатьох реальних застосуваннях. У зв'язку з цим, багато організацій поступово відмовляються від використання 3DES, переходячи на більш ефективні та стійкі до атак алгоритми, такі як AES, особливо після того, як DES був офіційно визнаний за слабкий для сучасних стандартів безпеки. Попри це, 3DES продовжує застосовуватися у старих системах, де його заміна на новіший стандарт є економічно та технічно складною.

DESX

Зважаючи на те, що 3DES є послідовним застосуванням DES тричі, його швидкість значно нижча за оригінальний алгоритм. Це може бути проблемою в реальних застосуваннях, де важлива швидкість обробки великих обсягів даних. Існує й альтернативна модифікація — DESX, запропонована Роном Рівестом у 1984 році. Вона дозволяє поліпшити стійкість без значних витрат часу, додавши два операції XOR до стандартного алгоритму DES, що значно ускладнює криптоаналіз. В результаті, DESX має більшу стійкість до атак, таких як перебір ключів, а

також до диференційного та лінійного криптоаналізів. DESX забезпечує покращену безпеку за рахунок використання додаткових операцій XOR з випадковими ключами перед і після основного процесу шифрування. Це ускладнює атакуючим процес знаходження слабких точок у алгоритмі, адже додаткові операції змішують вихідні дані. Однак, незважаючи на покращення стійкості, DESX все ще не відповідає сучасним вимогам безпеки через обмежену довжину ключа і слабкість основного DES. Тому, подібно до 3DES, DESX поступово втрачає популярність на користь більш нових та ефективних алгоритмів, таких як AES.

S-DES

Іншою спрощеною версією DES є S-DES — алгоритм, що використовується в основному в навчальних цілях для демонстрації принципів симетричного шифрування. Він працює з 8-бітними блоками даних та 10-бітними ключами. Алгоритм складається з п'яти основних етапів, включаючи початкову та кінцеву перестановку, дві операції заміни, а також застосування циклічних зсувів і XOR для генерування раундових підключів. Хоча S-DES не має практичного застосування через свою обмежену криптографічну стійкість, він є зручним для розуміння основ роботи з блоковими шифрами. S-DES використовує два раунди шифрування, кожен з яких включає заміну та перестановку, що забезпечує певний рівень змішування і дифузії. Хоча цей алгоритм не підходить для використання в реальних системах через свою вразливість до атак, таких як перебір ключів, він є чудовим інструментом для навчання основам криптографії. Завдяки своїй простоті S-DES дозволяє зрозуміти принципи роботи блокових шифрів, заміни, перестановки та генерування раундових ключів. Однак для забезпечення надійної безпеки в сучасних умовах використовують більш складні і стійкі алгоритми, як AES чи 3DES.

19.4. АЛГОРИТМ ШИФРУВАННЯ IDEA

Алгоритм шифрування IDEA (International Data Encryption Algorithm) є актуальним, оскільки цей алгоритм, хоча й не так широко використовується сьогодні, є важливою частиною історії криптографії та залишається цікавим з точки зору вивчення теорії шифрування. IDEA був розроблений в 1991 році як альтернативний алгоритм для заміни DES, який вже в той час вважався недостатньо безпечним.

IDEA використовує 128-бітовий ключ для шифрування даних, розділених на 64-бітові блоки, і застосовує 8 раундів обробки з комбінацією операцій XOR, множення за модулем $2^{16} + 1$ та

перестановок. Це дозволяє забезпечити високий рівень стійкості до атак, таких як атака вибором тексту чи диференційний криптоаналіз.

Хоча IDEA не є так популярним в сучасних системах (зокрема через патенти, які обмежують його безкоштовне використання), він все ж залишається важливим прикладом ефективного блочного шифру для тих, хто вивчає криптографію.

Також IDEA був використаний у різних протоколах, зокрема у PGP (Pretty Good Privacy), і через це він має значний внесок у розвиток сучасної криптографії.

Алгоритм шифрування IDEA (International Data Encryption Algorithm) є одним з найбільш відомих блочних шифрів, розроблених для захисту інформації. Він оперує 64-бітовими блоками даних і використовує ключ довжиною 128 біт. Алгоритм був розроблений в 1991 році і за своєю структурою значно складніший, ніж його попередники, такі як DES. IDEA застосовує вісім раундів шифрування, в кожному з яких здійснюються кілька операцій, таких як множення за модулем, додавання за модулем та порозрядне додавання (XOR). Ці операції проводяться над 16-бітовими субблоками, що дозволяє створювати складні перетворення, що значно ускладнює криптоаналіз і підвищує безпеку шифрування.

Першим етапом роботи алгоритму є розбиття 64-бітового блоку на чотири 16-бітових субблоки: X_1, X_2, X_3, X_4 . Потім кожен з цих субблоків піддається серії операцій протягом восьми раундів. У кожному раунді виконуються такі математичні операції, як множення за модулем модулем $2^{16}+1$, додавання за модулем 2^{16} , а також операція XOR між результатами множення і додавання. Підключі, які використовуються для цих операцій, генеруються з початкового 128-бітного ключа, розбитого на вісім 16-бітових підключів. Ключ циклічно зсувається, що дозволяє кожному раунду використовувати різні підключі, забезпечуючи додатковий рівень безпеки.

У ході кожного з восьми раундів вихідні субблоки змінюються через ряд математичних операцій, після чого проводиться перестановка внутрішніх субблоків, за винятком останнього циклу. Після виконання восьми раундів залишається заключне перетворення результатів знову з використанням операцій множення та додавання за модулем. Це перетворення дає кінцевий шифротекст. Таким чином, кожен раунд і заключне перетворення використовують комбінацію математичних операцій, що значно ускладнює відновлення відкритого тексту без знання ключа.

Процес розшифрування в алгоритмі IDEA майже ідентичний до процесу шифрування, з тією лише відмінністю, що підключі

використовуються в зворотному порядку. Це дозволяє відновити оригінальний текст, використовуючи зворотні операції.

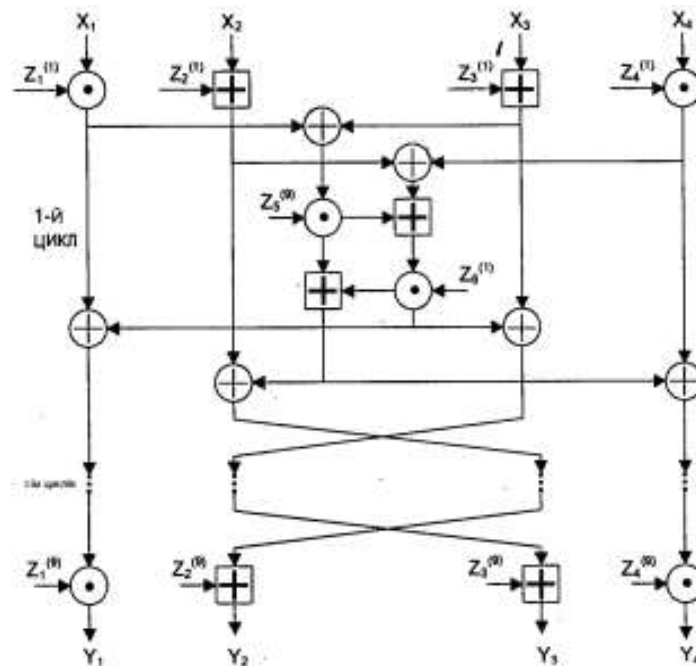


Рис. 19.6. Схема алгоритму IDEA (режим шифрування)
Джерело: [8-9]

IDEA відомий своєю високою стійкістю до різних видів криптоаналізу, зокрема до диференційного і лінійного аналізу. Це досягається завдяки складній структурі алгоритму, комбінуванню різних математичних операцій і застосуванню довгих ключів. Алгоритм є значно безпечнішим за DES, оскільки має набагато більшу довжину ключа (128 біт проти 56 біт у DES) і використовує складнішу структуру для перетворення даних. IDEA забезпечує високий рівень захисту даних і може ефективно працювати як на апаратних, так і на програмних засобах.

Однак з часом IDEA поступився місцем більш сучасним алгоритмам шифрування, таким як AES (Advanced Encryption Standard), які пропонують ще більшу ефективність і безпеку. Незважаючи на це, IDEA залишається важливим етапом у розвитку криптографії і досі використовується в деяких специфічних областях, таких як PGP (Pretty Good Privacy), де потреба в високому рівні захисту даних є критично важливою. Цей алгоритм має свою важливу роль в історії криптографії і служить основою для розуміння принципів роботи з блочними шифрами.

19.5. АЛГОРИТМ AES

AES (Advanced Encryption Standard) є одним з найвідоміших та найбільш широко використовуваних алгоритмів симетричного шифрування в сучасному світі, розробленим як заміна застарілого DES і затвердженим як національний стандарт США в 2001 році. Основною характеристикою AES є використання блоку даних розміром 128 біт (16 байт), що дозволяє забезпечити високу ефективність при шифруванні великих обсягів інформації. AES підтримує три варіанти довжини ключа: 128, 192 та 256 біт, що визначає кількість раундів, необхідних для шифрування. Для ключа 128 біт алгоритм виконує 10 раундів, для 192 біт — 12 раундів, а для 256 біт — 14 раундів.

Процес шифрування AES заснований на серії трансформацій, які виконуються над блоками даних. Кожен блок обробляється за допомогою таких основних етапів: початкове додавання раундового ключа (Add Round Key), побайтова заміна байтів за допомогою заміщувальної таблиці S-Box (Sub Bytes), зсув рядків (Shift Rows), змішування стовпців (Mix Columns) та знову додавання раундового ключа в кінці кожного раунду. АК (Add Round Key) – додавання раундового ключа. Просте побітне додавання кожного байта масиву і відповідного байта ключа. Ключі ітерацій отримуються із ключа шифру за допомогою алгоритму обробки ключа, а саме розширення і вибору. Як стандарт Rijndael криптологи пропонують використовувати 128 бітний блок тексту. Якщо ключ брати 128 біт, то використовувати 10 раундів, для 192 біт ключа – 12 раундів, для 256 біт ключа – 14 раундів. Під час цих операцій використовуються математичні операції в полі Галуа $GF(2^8)$, що дозволяє здійснювати ефективні операції множення та знаходження зворотних елементів, важливих для змішування та забезпечення криптографічної стійкості. Дослідження показали, що криптоаналіз 16-раундового DES у принципі реальний, однак вимагає великої кількості вихідних даних. Криптоаналіз при 20-24 циклах стає навіть теоретично неможливим. За оцінками розробників Rijndael, вже на чотирьох раундах шифрування цей алгоритм досить стійкий для сучасних використань. Теоретичною межею вважається 6-8 раундів. Отже, 10-14 раундів, передбачених в цьому алгоритмі, мають значний запас щодо криптостійкості. До недоліків алгоритму можна віднести нетрадиційність, недостатньо вивчену схему, яка може містити приховані вразливості, невідомі на час конструювання алгоритму.

Але однією з основних особливостей AES є його здатність працювати з різними довжинами ключа. Це дає можливість вибору між безпекою та швидкістю: чим довший ключ, тим більше раундів і, відповідно, більша криптостійкість алгоритму. Наприклад, використання ключа довжиною

128 біт забезпечує швидше шифрування, але з меншим рівнем безпеки в порівнянні з 256-бітним ключем, який забезпечує високий рівень захисту від криптографічних атак.

Незважаючи на те, що AES забезпечує високу стійкість до різноманітних атак, таких як диференційний та лінійний криптоаналіз, його ефективність також підтверджена підтримкою на апаратному рівні. Наприклад, інструкції AES-NI (AES New Instructions) в процесорах Intel дозволяють значно прискорити операції шифрування та розшифрування, що робить алгоритм надзвичайно ефективним навіть у вимогливих високопродуктивних системах. Ці апаратні оптимізації дають змогу використовувати AES в таких сферах, як захист урядових і фінансових даних, шифрування електронних платежів, а також захист каналів зв'язку, зокрема в HTTPS-протоколі.

У свою чергу, незважаючи на свою високу криптостійкість, AES має певні обмеження та вразливості, пов'язані з деякими теоретичними атаками на більш короткі ключі та проблемами з безпекою на деяких апаратних платформах. Наприклад, певні модифікації алгоритму можуть бути уразливими до атак зі зниженим рівнем складності, хоча на практиці це не становить серйозної загрози за умови правильного використання довгих ключів. Існують також побоювання щодо безпеки апаратних реалізацій AES, особливо у випадках, коли є можливість маніпулювання на рівні апаратних інструкцій, як це було продемонстровано у випадку з розкриттям інформації про діяльність агентів спецслужб, таких як Едвард Сноуден.

З огляду на ці обмеження, деякі компанії та дослідники шукають альтернативи AES. Наприклад, алгоритм ChaCha20, який є шифром потоку, поступово замінює AES у деяких мобільних пристроях на базі Android, оскільки він може бути більш стійким до апаратних атак. ChaCha20 використовує принципи шифрування, які забезпечують більшу стійкість до атак з боку сторонніх урядів чи організацій, і вважається більш ефективним на деяких пристроях, де апаратна підтримка AES відсутня або недостатня.

Висока ефективність і криптографічна стійкість AES забезпечили йому популярність у багатьох критичних сферах, зокрема в фінансових і урядових системах. Він використовується для захисту інформації в хмарних обчисленнях, для шифрування мобільних пристроїв, а також для забезпечення безпеки при передачі даних через Інтернет. Завдяки своєму широкому застосуванню та постійній підтримці у вигляді оновлень та вдосконалення стандартів AES, цей алгоритм продовжує бути основним

вибором для забезпечення безпеки цифрових даних навіть у найбільш складних умовах.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 19

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.
4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
6. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
7. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.
8. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

9. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: *Advances in Computer Science for Engineering and Education IV* (2021) 374–388.

10. Шевченко, С., Жданова, Ю., Спасітелєва, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

11. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: *Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421*. (2023) 266–271.

12. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.

13. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, *Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421* (2023) 56–66.

14. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 25–37.

15. Спасітелєва, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.

16. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.

17. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: *Workshop on Classic, Quantum, and Post-Quantum Cryptography*, vol. 3504 (2023) 12–25.

18. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3288 (2022) 142–148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in *Cybersec. Prov. Inf. Telecom. Syst. II*, vol. 3187, 2021, pp. 251–259.

19. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: *Workshop on Cybersecurity Providing*

in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.

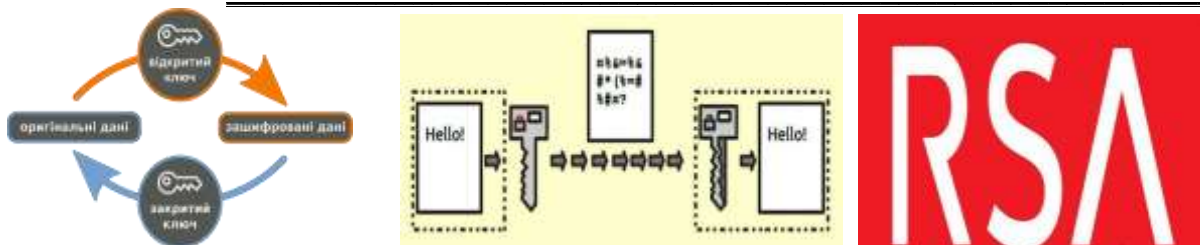
20. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

21. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.

22. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

РОЗДІЛ 20

АСИМЕТРИЧНІ КРИПТОСИСТЕМИ



20.1. Основні поняття

20.2. Кристоосистема RSA

20.3. Кристоосистема Ель-Гамал

20.4. Кристоосистеми на основі еліптичних кривих

"Краса криптографії з публічним ключем полягає в тому, що вона дозволяє безпечну комунікацію між двома сторонами, які ніколи не зустрічалися раніше, без необхідності довіряти третій стороні."

Рональд Рівест

20.1. Основні поняття

Асиметричні кристоосистеми, або кристоосистеми з відкритим ключем, є одним з основних методів криптографічного захисту даних. Ці системи використовують два різних ключі: відкритий, який може бути публічно доступним, і закритий, який зберігається в секреті у власника. Така структура дозволяє ефективно забезпечити безпеку даних, адже розшифрування за допомогою відкритого ключа неможливе, а лише власник закритого ключа має змогу доступити шифровану інформацію.

Ідея асиметричного шифрування була вперше запропонована в середині 1970-х років, коли Уїтфілд Діффі та Мартін Хеллман представили концепцію криптографії з відкритим ключем. Вони запропонували метод обміну секретними ключами через публічний канал, що дозволяло уникнути попередніх домовленостей про спільний секретний ключ. Цей підхід став основою для подальших розробок у галузі криптографії.

У 1973 році британський математик Кокс розробив кристоосистему з відкритим ключем, що ґрунтувалась на складності розкладу чисел на

прості множники. Ця криптосистема збігалася з алгоритмом RSA, який став широко застосовуваним і залишався засекреченим до 1977 року, коли був розсекречений. У 1977 році Рональд Рівест, Аді Шамір і Леонард Адлеман розробили алгоритм RSA, який став основним стандартом для шифрування та цифрових підписів. Цей алгоритм використовує властивість математичних задач, таких як розклад числа на прості множники, що робить його надзвичайно складним для зворотного виконання без знання секретного ключа.

Перевага асиметричних криптосистем полягає в можливості безпечного обміну даними без попереднього обміну секретними ключами, що суттєво знижує ризик компрометації ключів. Це дозволяє ефективно передавати конфіденційну інформацію навіть між сторонами, які не мали спільних секретів до початку взаємодії.

Сучасні реалізації асиметричних криптосистем використовують односторонні функції з секретом, які забезпечують захист від обчислення закритого ключа з відкритого. Одним з таких прикладів є алгоритм RSA, що базується на складності розкладу великих чисел на множники. Інші системи, наприклад, ElGamal, використовують інші складні математичні задачі, такі як дискретне логарифмування.

Попри численні переваги, асиметричні криптосистеми мають певні недоліки, зокрема, вони значно повільніші за симетричні алгоритми. Тому на практиці часто використовуються гібридні системи, де асиметричне шифрування застосовується для обміну ключами, а для шифрування великих обсягів даних використовуються симетричні алгоритми, які є більш швидкими.

Асиметричні криптосистеми широко застосовуються в сучасних протоколах безпеки, таких як HTTPS для захищених з'єднань в Інтернеті, а також в системах цифрових підписів, які забезпечують автентичність і цілісність переданої інформації. Вони є основою для захисту інформації в різних сферах, включаючи електронну комерцію, аутентифікацію користувачів і поширення ключів.

Особливо актуальною є проблема розподілу ключів у симетричних криптосистемах, зокрема в системах захищеного електронного документообігу, електронних банківських платежів та електронної торгівлі. Для забезпечення обміну конфіденційною інформацією між двома абонентами телекомунікаційної мережі необхідно згенерувати ключ, який може бути створений одним з абонентів, а потім переданий через захищений канал. Однак безпечний обмін таким ключем стає складнішим, коли неможливо попередньо описати склад мережі.

Для вирішення цієї проблеми були розроблені криптосистеми з відкритим ключем. У таких системах для шифрування використовуються публічні ключі, які можуть бути доступними для всіх, а секретні ключі необхідні лише для розшифрування. Одним із основних елементів таких систем є використання однонаправлених функцій з секретом, які є легкими для обчислення, але складними для зворотного виконання без секретної інформації.

На сьогодні алгоритм RSA є стандартом для шифрування з відкритим ключем і широко застосовується в інформаційних системах, зокрема в електронній комерції через Інтернет. В його основі лежить принцип, що кожен абонент генерує пару ключів — відкритий та секретний, де відкритий ключ публікується і доступний для всіх для шифрування повідомлень, а секретний зберігається в таємниці і використовується для розшифрування повідомлень.

В наш час алгоритми шифрування з відкритим ключем отримали широке розповсюдження в інформаційних системах. Так, алгоритм RSA фактично став стандартом для відкритих систем і рекомендований міжнародною організацією зі стандартизації ISO, відповідні додатки лежать в основі електронної комерції, здійснюваної через Internet. Суть їх полягає в тому, що кожним абонентом мережі генеруються два ключі, зв'язані між собою за певним математичним законом. Один ключ оголошується відкритим, а інший закритим (секретним). Відкритий ключ опубліковується і доступний будь-кому, хто бажає послати повідомлення власнику секретного ключа. Секретний ключ зберігається в таємниці. Вихідний текст шифрується відкритим ключем Одержувача і передається йому. Зашифрований текст в принципі не може бути розшифрований тим же відкритим ключем. Розшифрувати повідомлення можна тільки з використанням секретного ключа, який відомий лише самому адресату.

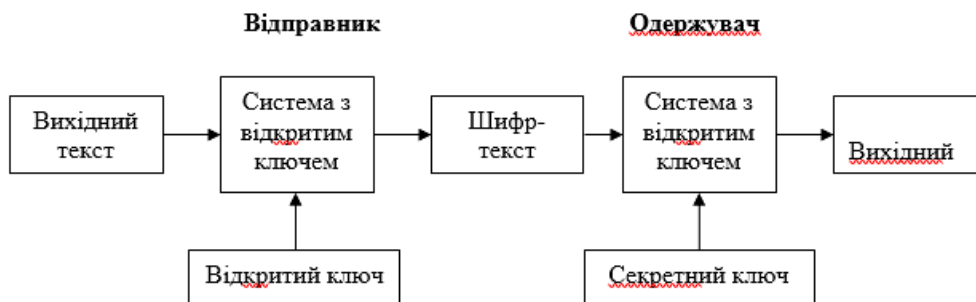


Рис. 20.1. Криптосистема з відкритим ключем
Джерело: [8-9]

Таким чином, одностороння функція з секретом, що використовується в асиметричній системі, є взаємооднозначною, але разом з тим має властивості необерненості. Необерненість, звичайно, розуміється не в загальноприйнятому значенні, а як практична неможливість обчислити обернену функцію, використовуючи сучасні обчислювальні засоби за досяжний інтервал часу.

Сучасні криптосистеми з відкритим ключем продовжують вдосконалюватися для забезпечення високого рівня безпеки та ефективності в умовах розвитку технологій і зростання вимог до захисту інформації.

20.2. Криптосистема RSA

Криптосистема RSA є однією з найбільш популярних і надійних асиметричних криптосистем, яка широко використовується для забезпечення конфіденційності, автентичності та цілісності інформації. Вона була розроблена в 1977 році Рональдом Рівестом, Аді Шаміром і Леонардом Адлеманом, і отримала свою назву від перших літер прізвищ авторів. RSA працює на основі використання двох різних ключів: відкритого та закритого. Відкритий ключ публічно доступний і використовується для шифрування даних, тоді як закритий ключ зберігається в таємниці і застосовується для їх розшифрування. Основна ідея, що лежить в основі RSA, полягає в складності задачі розкладу великих чисел на прості множники. Завдяки цьому, хоча зашифроване повідомлення можна легко створити за допомогою відкритого ключа, розшифрувати його можна тільки володіючи відповідним закритим ключем.

Ключова пара (відкритий і закритий ключі) генерується за допомогою кількох математичних кроків. Спочатку вибираються два великі прості числа p і q , які повинні бути секретними. Потім обчислюється їхній добуток $n = p \times q$, що використовується як модуль для обох ключів. Розмір числа n визначає рівень безпеки системи, оскільки чим більше це число, тим складніше його розкласти на прості множники. Далі обчислюється функція Ейлера $\varphi(n) = (p-1)(q-1)$, яка використовується для вибору відкритого ключа. Відкритий ключ e має бути взаємно простим з $\varphi(n)$, а закритий ключ d знаходиться як обернене число до e за модулем $\varphi(n)$. Таким чином, отримується пара ключів, які є основою роботи криптосистеми RSA.

Шифрування повідомлення відбувається за допомогою відкритого ключа. Повідомлення перетворюється на число, яке є меншим за n , і шифрується за допомогою формули $C = M^e \bmod n$, де M — це оригінальне повідомлення, а C — зашифроване повідомлення. Для розшифрування використовують закритий ключ, застосовуючи формулу $M = C^d \bmod n$, що дозволяє відновити початкове повідомлення. Важливою властивістю RSA є те, що зашифроване повідомлення неможливо розшифрувати без доступу до закритого ключа, що забезпечує високий рівень безпеки.

RSA має низку переваг, зокрема, це високий рівень безпеки завдяки складності розкладу великих чисел на прості множники. Крім того, відсутність необхідності обміну секретними ключами перед початком комунікації робить цю систему зручнішою для користувачів. Однак, RSA має й недоліки, основним з яких є низька швидкість шифрування, оскільки операції з великими числами потребують значних обчислювальних ресурсів. Тому RSA зазвичай використовується для шифрування коротких повідомлень або для обміну ключами, після чого для шифрування великих обсягів даних застосовуються більш швидкі симетричні алгоритми.

Сьогодні криптосистема RSA є основою для багатьох криптографічних протоколів, таких як HTTPS, TLS і цифрові підписи, що забезпечують безпеку онлайн-комунікацій. Вона також застосовується в електронній комерції, системах захисту електронних платежів і багатьох інших галузях. Проте з розвитком квантових технологій з'являється загроза для RSA, оскільки квантові комп'ютери можуть значно спростити задачу розкладу великих чисел. Тим не менше, на сьогоднішній день RSA залишається однією з найбільш надійних і широко використовуваних криптосистем, що гарантує безпеку інформації в сучасному цифровому світі.

Криптостійкість RSA

Криптостійкість RSA залежить від складності задачі розкладу великих чисел на прості множники, що є основною математичною основою цієї криптосистеми. В RSA, безпека алгоритму зводиться до обчислювальної складності цієї задачі. Якщо зломисник має можливість швидко розкласти на прості множники велике число n , яке є добутком двох простих чисел p і q , то він зможе обчислити закритий ключ d і, відповідно, розшифрувати зашифровані повідомлення.

Криптостійкість RSA базується на кількох ключових факторах:

1. Розмір ключа

Розмір числа n , (добуток двох простих чисел p і q) визначає криптостійкість системи. Чим більший розмір n , тим складніше зломиснику здійснити розклад чисел на прості множники. У сучасних криптографічних системах рекомендований мінімальний розмір ключа для RSA становить 2048 біт, а для високого рівня безпеки часто використовують ключі 3072 біт або більше. Однак з розвитком обчислювальних потужностей, вимоги до розміру ключів зростають.

2. *Методи факторизації*

Найбільш відомими методами факторизації є методи, такі як решето Ератосфена, метод числових решіток та алгоритм Коха. Але всі ці методи мають експоненційну складність, і на даний момент не існує швидких алгоритмів для факторизації великих чисел, що робить RSA стійким до атак на традиційних комп'ютерах. Однак з розвитком квантових обчислень ситуація може змінитися.

3. *Квантові обчислення*

Основною загрозою для криптостійкості RSA в майбутньому є розвиток квантових комп'ютерів. Квантовий алгоритм Шора, який був розроблений для квантових комп'ютерів, здатен розкласти великі числа на прості множники значно швидше, ніж класичні алгоритми. За допомогою квантових комп'ютерів можна буде ефективно зламати систему RSA навіть при використанні великих розмірів ключів (2048 біт і більше), оскільки квантовий алгоритм має поліноміальну складність.

4. *Атаки на слабкі ключі*

Крім атак на факторизацію, криптостійкість RSA також залежить від правильної генерації ключів. Якщо обрані прості числа p і q будуть занадто близькими або якщо виявляться математичні зв'язки між ними, це може значно спростити факторизацію числа npq і знизити стійкість системи. Тому важливо використовувати високоякісні методи генерації випадкових чисел і правильно вибирати прості числа для створення ключів.

5. *Проблеми з деякими типами атак*

RSA також вразлива до деяких типів атак, таких як атаки на основі аналізу часу виконання (наприклад, атаки на базі часового аналізу). Зломисники можуть використовувати час виконання операцій для відновлення секретного ключа.

У результаті, хоча RSA є дуже надійною криптосистемою, його криптостійкість в значній мірі залежить від розміру ключа, методів факторизації та наявності квантових комп'ютерів у майбутньому. Для забезпечення тривалої стійкості RSA необхідно продовжувати збільшувати

розміри ключів і стежити за розвитком квантових технологій, а також використовувати додаткові методи захисту від атак.

20.3. Криптосистема Ель-Гамал

Криптосистема ElGamal, заснована на складності обчислення дискретного логарифма у скінченних групах, була розроблена в 1985 році і забезпечує високу криптостійкість завдяки математичним властивостям дискретних логарифмів. Алгоритм має дві основні складові: генерування пари ключів та сам процес шифрування і розшифрування повідомлень. На відміну від RSA асиметрична криптосистема Ель-Гамал заснована на проблемі дискретного логарифма, що дозволяє забезпечити складність розв'язання цієї задачі навіть за наявності публічного ключа. Процес шифрування включає використання випадкового числа, що додає додатковий рівень безпеки шляхом застосування різних шифрів для одного і того ж повідомлення, зменшуючи ймовірність атак. Розшифрування в ElGamal також вимагає використання приватного ключа, що забезпечує захист від несанкціонованого доступу до інформації. З точки зору стійкості, криптосистема ElGamal дуже ефективно протистоїть атакам на основі обчислення дискретного логарифма, однак для неї потрібні великі обсяги даних та значна обчислювальна потужність, що може обмежувати її використання в деяких випадках. Завдяки своїм властивостям ElGamal є основою для кількох сучасних криптографічних протоколів і використовується в таких сферах, як цифрові підписи та захищене шифрування в різних протоколах безпеки.

Відповідна одностороння функція є показниковою функцією за простим модулем p : секретні параметри входять в показники степенів.

Піднесення числа до степеня в скінченному полі виконується легко, тоді як відновлення показника степеня за значенням функції (тобто знаходження дискретного логарифма) при великих p є складною обчислювальною задачею.

Особливістю цієї криптосистеми є те, що дискретний логарифм не є односторонньою функцією з секретом. Тому для її обернення відправник повідомлення формує додаткову інформацію на основі разового ключа, яку одержувач може використовувати для читання повідомлення захищеним від просочування інформації способом.

В криптосистемі Ель-Гамал для побудови пари асиметричних ключів вибирається велике просте число p і два псевдовипадкові числа, менші $p-1$.

Одне з них, g , повинно бути елементом великого порядку за модулем p , скажімо, первісним коренем. Друге число, x , вибирається як секретний ключ. Вважається, що повідомлення – лишки за модулем p .

Відкритим ключем є трійка чисел $p, g, y = g^x \bmod p$.

Для кожного повідомлення формуються додаткові дані, що грають роль лазівки для конкретного сеансу шифрування.

Для зашифрування повідомлення m вибирається псевдовипадкове число k (рандомізатор, разовий ключ) з умовою $\text{НСД}(k, p-1)=1$. Рандомізатори не повинні повторюватися і повинні триматися в секреті.

Потім обчислюються числа $a = g^k \bmod p$ – лазівка і $b = y^x m \bmod p$ – шифртекст. Криптограмою є пара блоків даних a, b .

Для розшифрування достатньо одержати співмножник y^k , що можна зробити за допомогою секретного ключа, обчисливши значення $a^x = g^{kx} \bmod p$.

Дійсно, $y^k = g^{xk} \bmod p$, тому $m = a^{-x} b \bmod p$.

Таким чином, забезпечується захищений інформаційний обмін без попереднього розсилання секретних ключів. Криптосистема ElGamal забезпечує надійний захист інформації завдяки використанню складних математичних задач і здатна забезпечити конфіденційність при передачі даних через незахищені канали зв'язку. Оскільки алгоритм ґрунтується на складності обчислення дискретного логарифма, його безпека залежить від розміру використовуваних чисел та складності вирішення цієї задачі. Завдяки цьому криптосистема є стійкою до атак, таких як атаки з вибором відкритого тексту або атаки на основі аналізу шифртексту. Крім того, ElGamal забезпечує можливість цифрового підпису, що додає додатковий рівень автентифікації та цілісності даних. Однак, як і будь-яка криптосистема, вона має обмеження на швидкість виконання, особливо при використанні великих ключів. Враховуючи це, для досягнення високої продуктивності часто використовуються гібридні підходи, які комбінують переваги як симетричних, так і асиметричних алгоритмів.

Головне в криптографії з відкритим ключем – потенційно велика безпека. Однак є недоліки: генерація ключів заснована на генерації нових великих простих чисел, а перевірка на ці властивості займає багато процесорного часу; процес шифрування і дешифрування громіздкі. Криптосистема з відкритим ключем застосовується для шифрування і передачі та подальшого розшифрування секретного ключа симетричної криптосистеми. Симетрична криптосистема використовується для шифрування і розшифрування самого вихідного відкритого тексту.

Асиметрична криптосистема доповнює симетричну криптосистему, підвищуючи її стійкість, оскільки вона дозволяє забезпечити безпеку навіть при зберіганні і передачі ключів по відкритих каналах. Система з відкритим ключем забезпечує безпеку обміну даними без необхідності попередньо обмінюватися секретними ключами. Однак для забезпечення оптимальної продуктивності і зменшення часу на шифрування та дешифрування необхідно застосовувати гібридні системи, що поєднують переваги обох криптографічних методів.

20.4. КРИПТОСИСТЕМИ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Криптосистеми на основі еліптичних кривих (Elliptic Curve Cryptography, ECC) — це тип криптографічних систем, які використовують математику еліптичних кривих для створення більш ефективних і безпечних алгоритмів шифрування та підпису порівняно з традиційними методами, такими як RSA та DSA. Вони базуються на складності розв'язання задачі дискретного логарифмування в групі точок на еліптичній кривій, що забезпечує високий рівень безпеки при значно менших розмірах ключів. Для побудови СВК можуть бути використані еліптичні криві — математичні об'єкти, визначені над скінченними полями, що дозволяє зменшити необхідні ресурси для досягнення необхідного рівня безпеки. Використання еліптичних кривих дозволяє створювати криптосистеми з коротшими ключами, що робить їх менш вимогливими до пам'яті та часу обчислень, зберігаючи при цьому високу стійкість до атак. Економія на розмірі ключа при збереженні рівня безпеки робить ECC особливо привабливими для мобільних пристроїв та інших обмежених ресурсів. Крім того, еліптичні криві використовуються для цифрових підписів, шифрування даних та реалізації аутентифікації, що забезпечує широкий спектр застосувань у сучасних криптографічних протоколах, таких як TLS/SSL. Однак вибір еліптичної кривої та параметрів для конкретної криптосистеми потребує ретельного підходу, оскільки деякі криві можуть бути вразливими до специфічних атак. Різні стандарти, такі як NIST (Національний інститут стандартів і технологій) та SECG (Security Engineering Task Force), визначають еліптичні криві, які є рекомендованими для використання в сертифікованих криптосистемах. Одним із головних переваг еліптичних кривих є їх здатність забезпечувати більшу безпеку з меншою кількістю обчислень, що є ключовим для сучасних розподілених систем та інтернет-технологій. Застосування ECC в блокчейн-технологіях, криптовалютах і платіжних системах дозволяє

покращити ефективність та безпеку при передачі і зберіганні криптографічних ключів.

Принцип криптосистем на основі еліптичних кривих (Elliptic Curve Cryptography, ECC) базується на використанні математичних властивостей еліптичних кривих для створення ефективних і безпечних криптографічних алгоритмів. Еліптичні криві є геометричними об'єктами, які визначаються рівнянням типу $y^2 = x^3 + ax + b$, де a та b — це параметри, що задають конкретну криву, а x і y — змінні, що представляють точки на кривій. Принцип їх використання полягає в тому, що задача пошуку дискретного логарифму в групі точок на еліптичній кривій є математично складною і обчислювально важкою, що забезпечує високий рівень безпеки. Ключові елементи криптосистем ECC включають генерацію пари ключів (публічного та приватного), де приватний ключ є випадковим числом, а публічний ключ отримується шляхом множення генератора точки на кривій на приватний ключ. Завдяки складності розв'язання задачі дискретного логарифмування, навіть при знанні публічного ключа, неможливо зворотно відновити приватний ключ, що забезпечує конфіденційність і цілісність передачі даних.

Основні переваги криптосистем на основі еліптичних кривих полягають у тому, що для забезпечення такої ж безпеки, як у традиційних методах (наприклад, RSA), еліптичні криві вимагають значно коротших ключів. Це зменшує витрати на зберігання ключів і час обчислень, роблячи їх ідеальними для мобільних пристроїв і ресурсно обмежених систем. Важливим моментом є також використання стандартів, які визначають безпечні еліптичні криві (наприклад, NIST P-256, P-384), що гарантує стабільність і надійність криптографічних операцій. ECC використовується в таких криптографічних протоколах, як TLS/SSL для захищених з'єднань, цифрових підписах, а також в криптовалютах для підтвердження транзакцій і забезпечення безпеки блокчейн-технологій.

Еліптичні криві є рівняннями вигляду $y^2 = x^3 + ax + b$, де a і b — це сталі, що визначають форму кривої, а x та y — координати точок, які належать кривій. На відміну від традиційних криптографічних схем, що використовують операції на великих простих числах, еліптичні криві працюють в рамках групи точок цієї кривої, що дозволяє досягати високого рівня безпеки за допомогою менших за розміром ключів.

Для випадків характеристик поля $p=2$, $p=3$, $p>3$ алгоритми обчислення значень, пов'язаних з реалізацією подібних СВК, істотно різні. Разом з тим, основні принципи, на основі яких побудовані СВК на еліптичних кривих, в ідейному значенні однакові.

Цікаво відзначити, що, на відміну від розглянутих раніше криптосистем, побудова відкритих параметрів для систем на еліптичних кривих є складною алгоритмічною проблемою. В даному випадку ефект від стандартизації криптоалгоритмів особливо відчутний.

Для спрощення викладу розглянемо еліптичні криві над простим полем характеристики $p > 3$.

Еліптична крива (ЕК) над полем лишків за модулем $p > 3$ безпосередньо пов'язана з розв'язками порівняння $y^2 = x^3 + ax + b \pmod{p}$ за так званої умови невідродженості кривої $4a^3 + 27b^2 \neq 0$.

Вказане порівняння називається рівнянням кривої в афінних координатах.

Кожний розв'язок (x, y) порівняння $y^2 = x^3 + ax + b \pmod{p}$ називається точкою кривої $P(x, y)$.

Множину розв'язків порівняння $y^2 = x^3 + ax + b \pmod{p}$ можна розширити таким чином, що розширена множина стане комутативною групою E . Ця група називається групою точок на еліптичній кривій.

Груповий закон в групі E називається додаванням. Основною причиною, що дозволяє побудувати групу E , є можливість побудови нових рішень рівняння кривої, виходячи з вже відомих. Виявляється, якщо дані розв'язки $P_1(x_1, y_1)$ і $P_2(x_2, y_2)$, то «практично завжди» можна знайти третій розв'язок, використовуючи знання координат перших двох.

Операція, що зіставляє двом (можливо, однаковим) точкам їх «суму», в афінних координатах записується у вигляді дробових виразів, тому при обчисленнях може виникнути особливість, якщо у відповідному знаменнику з'явиться нульове значення (за модулем p).

Очевидно, це єдина ситуація, коли виникає особливість. Отже, їй можна зіставити деяке позначення (O) і розширити множину розв'язків рівняння кривої, додавши символ O , імітуючи тим самим існування додаткового елемента, званого нескінченно віддаленою точкою.

Можна показати, що якщо для операції «+» вважати O нейтральним елементом, то розширена множина точок кривої перетворюється на комутативну групу, а сама операція – в груповий закон.

Насправді, для аналітичного опису розширеної множини точок кривої слід використовувати так звані проєктивні координати, в яких точки кривої будуть задаватися не парою, а трійкою чисел.

Виявляється, в цьому випадку всі точки кривої будуть рівноправними і будуть підкорятися більш загальному груповому закону.

Груповий закон в афінних координатах був відкритий при дослідженнях еліптичних кривих на звичайному полі дійсних чисел, що «підказало» вид відповідних перетворень над скінченними полями.

Додавання двох точок ЕК над полем дійсних чисел можна сформулювати у вигляді геометричної побудови, що зв'язує координати точок-доданків з координатами точки-суми (рис. 20.2).

Для цього слід враховувати, що якщо пряма перетинає ЕК в двох точках розширеної кривої, то вона перетинає криву в третій точці (точка дотику вважається подвійною точкою).

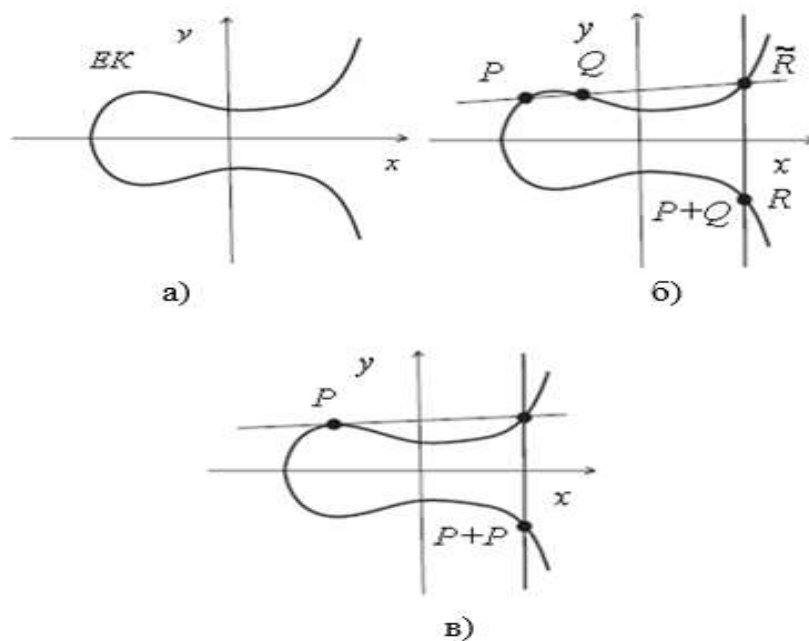


Рис. 20.2. Графік еліптичної кривої $y^2 = x^3 - 3x + 4$ (а), додавання двох точок (б), кратна точка (в)

Джерело: [8-9]

Для складання точок P і Q кривої (рис. 20.2, б) проводимо через P і Q пряму. Вона перетне ЕК в деякій третій точці $\tilde{R}$. Проведемо через $\tilde{R}$ пряму, паралельну осі ординат, яка перетне ЕК в деякій точці R , яку приймемо за суму точок кривої: $R = P + Q$.

Якщо $P = Q$, то точка $\tilde{R}$ є перетином кривої і дотичної до кривої в точці P . У відповідних випадках вважаємо, що прямі, паралельні осі ординат, проходять через нескінченно віддалену точку O .

Вказана геометрична побудова називається методом січних і дотичних.

Нехай $P = (u, v)$. Позначимо $\tilde{P} = (u, -v)$. Очевидно, що при нашій побудові $R = (x, y)$, а $\tilde{R} = (x, -y)$. Розглянемо точку $R + \tilde{P}$. Користуючись геометричною побудовою, легко прослідкувати, що $R + \tilde{P} = Q$. Іншими словами, додавання до точки $R = P + Q$ точки $\tilde{P}$ еквівалентно «відніманню» точки P з точки R . Таким чином, для визначення операції віднімання, оберненої додаванню, прийнемо $(-P(u, v)) = P(u, -v)$.

Нехай $G_1 = G$, $G_2 = G + G$ і т. д. Виходячи з точки G , можна побудувати послідовність точок $G_1, \dots, G_{n-1}, G_n = O$ деякої довжини n .

Якщо записувати подібне k -кратне додавання на кривій у вигляді kG , прийнявши $0G = O$, то, очевидно, коефіцієнт k можна приводити за модулем n і розглядати вирази вигляду $uP + vQ$ і $u(vP)$. Операція kG називається скалярним множенням точки на k . Найменше ціле n , для якого $nG = O$, називається порядком точки G .

Використовуючи аналітичну геометрію, можна показати, що груповий закон $P_1(x_1, y_1) + P_2(x_2, y_2) = P_3(x_3, y_3)$ відповідає деяким правилам, які, у разі скінченного поля характеристики $p > 3$, зводяться до нижчевикладеного.

1. $x_3 = \lambda^2 - x_1 - x_2 \bmod p$, $y_3 = \lambda(x_1 - x_3) \bmod p$, де
 $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$, якщо $P_1 \neq P_2$ і $\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p$, якщо $P_1 = P_2$.
2. Якщо знаменник λ перетворюється в нуль, то $P_1(x_1, y_1) + P_2(x_2, y_2) = O$.
3. Операція, обернена додаванню: $-P(x, y) = P(x, -y)$
4. Для будь-якої точки P розширеної кривої: $O \pm P = P$.

Як правило, при побудові СВК на еліптичній кривій використовується точка G великого простого порядку n . Всі операції в СВК здійснюються над точками вигляду kG , які утворюють циклічну підгрупу групи E .

Покажемо, як можна побудувати аналог алгоритму Діффі-Хеллмана на еліптичній кривій. Вихідними параметрами є сама крива E над скінченним полем і точка G великого простого порядку n .

Користувачі криптосистеми незалежно генерують секретні великі числа m_A і m_B , які є параметрами для формування спільного секретного ключа. На їх основі обчислюються відкриті ключі $Q_A = m_A G$ і $Q_B = m_B G$.

Провівши обмін відкритими ключами, кожний з абонентів може сформувати загальний ключ $K_{AB} = m_A m_B G = m_A Q_B = m_B Q_A$.

Стійкість СВК заснована на складності задачі дискретного логарифмування на кривій. Ця задача полягає в знаходженні скалярного множника із співвідношення $P = kG$ і, в загальному випадку, є обчислювано недоступною.

Найбільш трудомістким етапом обчислення відкритих параметрів еліптичної кривої є визначення простого числа n , яке є дільником кількості $\#E$ елементів в групі E .

Як правило, обчислення n зводиться до обчислення $\#E$ з його подальшою факторизацією. Для обчислення $\#E$, взагалі кажучи, використовуються складні алгоритми. Відомі прості обмеження на коефіцієнти рівняння ЕК, при яких або $\#E = n$, або факторизація $\#E$ здійсненна.

Теоретично група E складається з не більш, ніж двох циклічних підгруп. Зазвичай параметри кривих такі, що порядок n_2 однієї з підгруп дуже малий і визначається порівняно легко. Після чого n обчислюється у вигляді $n = \#E : n_1$.

Спільні алгоритми обчислення $\#E$ існують, але є складними і трудомісткими.

Для числа $\#E$ є оцінки. Наприклад, нерівність Хассе: $q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q}$, де $q = p^r$ – кількість елементів в полі характеристики p . Таким чином, $\#E = q + 1 - t$, де $|t| \leq 2\sqrt{q}$.

Для деяких кривих число $\#E$ можна обчислити теоретично.

Криві, для яких $\#E = p$, називаються аномальними, а криві, для яких $t = 0(p)$, – суперсингулярними.

Для кривих цих типів відомі ефективні методи дискретного логарифмування.

Проте існує клас криптопротоколів, в яких істотно використовуються властивості саме суперсингулярних еліптичних кривих.

Цікаво відзначити, що багато криптографічних систем, розроблених на основі системи RSA, породжують аналоги на еліптичних кривих над кільцем лишків Z/nZ для складеного числа, де p, q — різні прості числа.

Еліптична крива E_n над Z/nZ задається тими ж алгебраїчними рівняннями, що і у разі простого модуля. Наприклад, крива задається як множина розв'язків основного порівняння $y^2 = x^3 + ax + b \bmod n$, при НСД $(4a^3 + 27b^2, n) = 1$ з нескінченно віддаленою точкою O .

Операції на E_n виконуються за формулами, відповідними методу січних і дотичних. На жаль, такий об'єкт не є групою.

Тому замість E_n розглядається так звана пряма сума кривих $\tilde{E}_n = E_p + E_q$: інший об'єкт, який «мало» відрізняється від E_n .

Кожний елемент $\tilde{E}_n$ – чотиривимірний вектор, що складається з двох точок кривих E_p і E_q .

Якщо пара (x, y) задовольняє основне рівняння для E_n , то пари лишків $(x \bmod p, y \bmod p)$ і $(x \bmod q, y \bmod q)$ автоматично задовольняють те ж рівняння за модулями p і q відповідно.

Нагадаємо, що Китайською теоремою про лишки називається наведене нижче твердження.

Нехай числа $m_1, m_2, \dots, m_k$ попарно взаємно прості і $M = m_1 m_2 \cdots m_k$.

Тоді єдиний за модулем M розв'язок системи порівнянь $x = c_i \bmod m_i, \quad i = 1, \dots, k$ має вигляд: $x = \sum_{i=1}^k c_i M_i N_i \bmod M$, де

$$M_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k, \quad N_i = M_i^{-1} \bmod m_i.$$

Дійсно, у вказаному виразі для x доданок $c_i M_i N_i$ порівнянний з c_i за модулем m_i , а всі інші порівнянні за цим модулем з нулем.

Враховуючи Китайську теорему про лишки, x і y однозначно відновлюються за значеннями $(x \bmod p, x \bmod q)$ і $(y \bmod p, y \bmod q)$.

Проте, разом з нескінченно віддаленою точкою O , група $\tilde{E}_n$ містить сукупність точок виду $\{(O_p, y), (x, O_q)\}$. Тому $\tilde{E}_n$ складається з точок кривої E_n і деякої множини особливих точок.

Наведемо основні властивості $\tilde{E}_n$, близькі до властивостей E_n , що дозволяє будувати RSA-подібні криптосистеми.

1. Метод січних і дотичних у разі, коли він визначений для E_n , збігається з груповою операцією в $\tilde{E}_n$.

Таким чином, якщо виконується додавання конкретних точок в E_n , то воно виконується без факторизації n .

2. При великих p і q з ймовірністю, близькою до одиниці, множення точки на скаляр в $\tilde{E}_n$ поводить як аналогічна операція в E_n .

Суть цього твердження така.

Приймемо $N = \text{НСД}(\#E_p, \#E_q)$. Тоді $(kN + 1)P = P$ для переважного числа точок і будь-яких цілих k .

Розглянемо аналог системи RSA з використанням еліптичної кривої. Відкритим ключем є пара N, e , де $N = \text{НСД}(\#E_p, \#E_q)$, $(N, e) = 1$, секретним – число d таке, що $ed = 1 \bmod N$.

Шифртекст повідомлення m , яке зіставляється наперед вибраним способом деякій точці M кривої E_n , Відправник одержує з допомогою скалярного множення у вигляді $C = eM$. Одержувач, знаючи число d , відновлює $M = deM = dC$.

Виявляється, однак, що зіставлення $m \Leftrightarrow M$ може вимагати факторизацію n , тобто вказана схема шифрування, взагалі кажучи, не є коректною. Проте існує ряд більш досконалих RSA-подібних криптосистем, наприклад, криптосистема Демітко (для кривих загального вигляду), або криптосистема Кувакадо-Кояма для кривих вигляду $y^2 = x^3 + b \bmod n$.

Основні переваги криптосистем на основі еліптичних кривих:

1. Менші розміри ключів

Для досягнення того ж рівня безпеки, що й традиційні методи, ECC вимагає набагато менших за розміром ключів. Наприклад, для забезпечення рівня безпеки, еквівалентного 2048-бітному RSA, достатньо використовувати ключі довжиною 256 біт у системі на основі еліптичних кривих.

2. Ефективність

Завдяки меншій довжині ключів, алгоритми на основі еліптичних кривих зазвичай працюють швидше та з меншими витратами на обчислення, що робить їх ідеальними для ресурсозбережних середовищ, таких як мобільні пристрої, сенсори та інші вбудовані системи.

3. Забезпечення високої безпеки

Оскільки задачі на еліптичних кривих, такі як обчислення дискретного логарифму, значно складніші порівняно з аналогічними задачами в класичних криптосистемах, еліптичні криві можуть запропонувати більш високий рівень криптостійкості при тих самих розмірах ключів.

Основні застосування криптосистем на основі еліптичних кривих:

- ✓ Шифрування використовуються для захисту передавання даних у відкритих мережах, таких як Інтернет.
- ✓ ECC застосовується для створення цифрових підписів у таких протоколах, як ECDSA (Elliptic Curve Digital Signature Algorithm), що гарантують автентичність і цілісність даних.
- ✓ Алгоритми на основі еліптичних кривих, такі як ECDH (Elliptic Curve Diffie-Hellman), використовуються для безпечного обміну

ключами між сторонами без необхідності попереднього обміну секретами.

Завдяки цим властивостям, криптосистеми на основі еліптичних кривих знаходять широке застосування в сучасних системах безпеки, включаючи протоколи для безпечних з'єднань (наприклад, TLS/SSL для HTTPS) і мобільні платформи, де ефективність і безпека є критично важливими.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 20

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.
4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
6. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
7. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і

протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

8. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

9. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.

10. Шевченко, С., Жданова, Ю., Спасітелєва, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

11. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.

12. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.

13. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.

14. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.

15. Спасітелєва, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.

16. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.

17. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

18. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.
19. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.
20. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.
21. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.
22. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

РОЗДІЛ 21
ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС



- 21.1. Проблема аутентифікації даних і електронний цифровий підпис**
- 21.2. Хеш-функція**
- 21.3. Алгоритми електронного цифрового підпису**
- 21.4. Стандарти алгоритмів формування і перевірки ЕЦП**
- 21.5. Протоколи взаємодії і сертифікати в стандарті X.509**
- 21.6. Структура сертифіката відкритих ключів**

21.1. ПРОБЛЕМА АУТЕНТИФІКАЦІЇ ДАНИХ І ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

У сучасному цифровому середовищі забезпечення автентичності даних є однією з найважливіших задач інформаційної безпеки. Відсутність фізичних носіїв у процесі обміну інформацією значно ускладнює перевірку справжності автора повідомлення та цілісності переданих даних. Якщо у паперовому документообігу цю проблему вирішують за допомогою рукописних підписів і печаток, то в електронних системах такі методи є непридатними. Ця проблема є особливо критичною для банківських установ, комерційних підприємств та державних органів, де помилка у встановленні справжності даних може призвести до значних фінансових втрат або компрометації конфіденційної інформації.

Одними з основних загроз під час обміну електронними документами є перехоплення та модифікація даних, коли зловмисник змінює зміст документа, маскарад — ситуація, коли відправник видає себе за іншу особу, а також відмова від авторства, коли відправник заперечує факт передачі документа. Додатковими ризиками є підміна документів отримувачем і так звані реплей-атаки, коли зловмисник повторно відправляє раніше перехоплений документ.

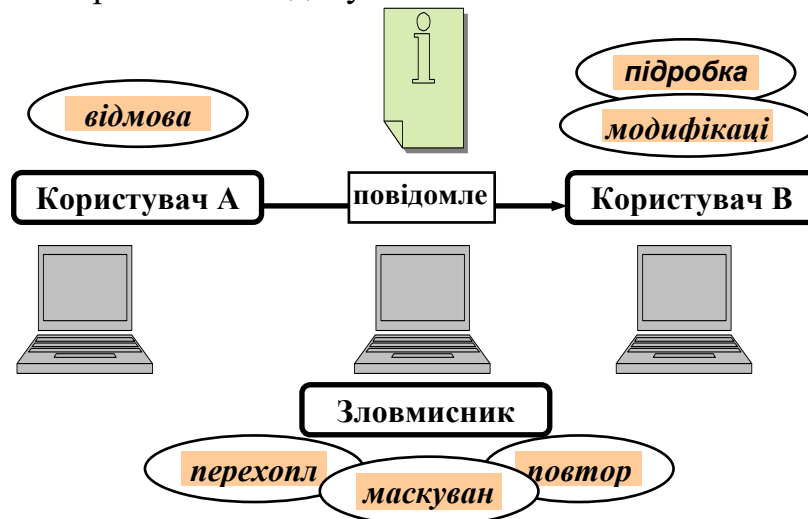


Рис. 21.1. Загрози безпеки повідомлень

Джерело: [8-9]

Загрози безпеки повідомлень виникають під час передачі інформації через мережі або зберігання її на різних носіях, що може призвести до втрати конфіденційності, цілісності чи доступності даних. Однією з основних загроз є перехоплення (Eavesdropping), коли зловмисник отримує доступ до повідомлення без відома відправника або отримувача, що може бути досягнуто через перехоплення мережевого трафіку або витік даних з ненадійних каналів зв'язку. Іншою загрозою є фальсифікація (Forgery), що передбачає створення підроблених повідомлень або цифрових підписів, які вводять отримувача в оману, змушуючи його вірити в автентичність підробленої інформації, що може призвести до помилкової перевірки авторства або змісту повідомлення. Колізії (Collision) також становлять серйозну загрозу для хеш-функцій, адже вони виникають, коли два різних повідомлення мають однаковий хеш, що може спричинити помилкову перевірку цілісності даних. У разі модифікації (Modification) повідомлення перед його доставкою отримувачу, може змінюватися зміст чи значення переданої інформації, що створює ризик її ненавмисної або навмисної спотвореності. Загроза повторного відправлення (Replay Attack) має місце,

коли зломисник перехоплює повідомлення і відправляє його знову, намагаючись отримати той самий результат, що може призвести до невірної інтерпретації чи повторного використання вже переданого запиту. Атаки типу "чоловік посередині" (Man-in-the-Middle) є ще однією серйозною загрозою, коли зломисник перехоплює та змінює повідомлення між двома сторонами без їхнього відома, що дозволяє йому маніпулювати переданими даними. Не менш важливою загрозою є відмова від послуг (Denial of Service, DoS), яка спрямована на переривання доступу до сервісів чи повідомлень, що призводить до втрати доступності важливих даних або комунікаційних каналів. Останньою загрозою є використання слабких ключів (Key Weakness), коли для шифрування повідомлень використовуються слабкі або зламані ключі, що дає зломисникам можливість дешифрувати або отримати доступ до переданих даних. Щоб захистити повідомлення від цих загроз, використовуються різноманітні криптографічні методи, включаючи шифрування, цифрові підписи, а також протоколи для захисту цілісності та автентичності даних.

Іноді немає необхідності зашифровувати повідомлення, що передається, але його потрібно завірити електронним цифровим підписом.

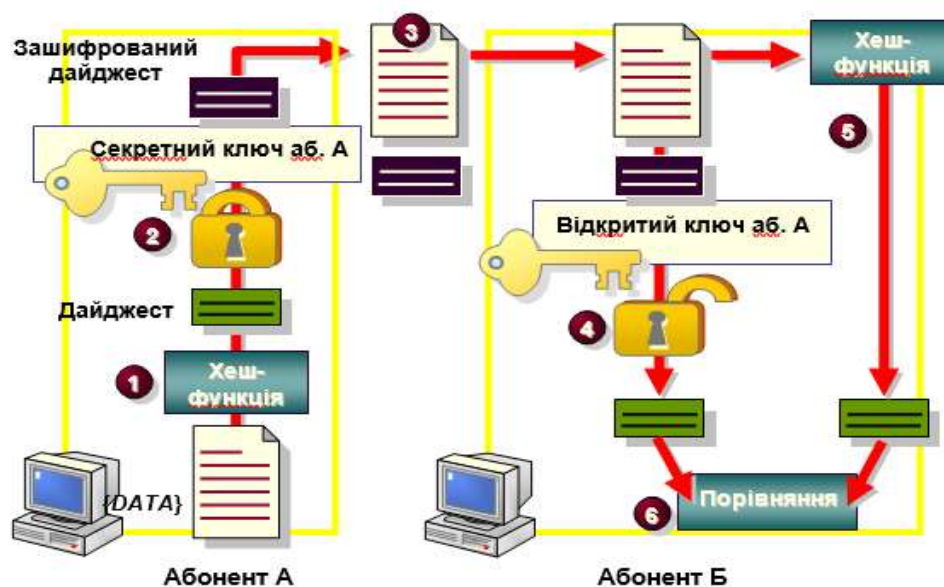


Рис. 21.2. Схема ЕЦП без шифрування повідомлення
Джерело: [8-9]

Першим кроком обчислюється дайджест повідомлення за допомогою хеш-функції. Далі (крок 2) цей дайджест шифрується секретним ключем відправника. Отримана послідовність символів — електронний цифровий

підпис — об'єднується з вихідним документом і відправляється абоненту Б (крок 3). Одержувач, використовуючи відкритий ключ відправника, розшифровує дайджест (крок 4) і обчислює хеш-код прийнятого повідомлення (крок 5). Набуті значення порівнюються (крок 6). У разі збігу вважається підтвердженням авторство абонента А і відсутність спотворень (цілісність) повідомлення.

Механізм електронного цифрового підпису (ЕЦП), що ґрунтується на принципах асиметричної криптографії. ЕЦП забезпечує три ключові функції: підтвердження автентичності відправника, гарантування цілісності даних та юридичне підтвердження авторства. Завдяки цьому ЕЦП функціонально аналогічний рукописному підпису, але має значно ширші можливості у цифровому просторі.

Механізм роботи ЕЦП передбачає використання хеш-функції для створення унікального значення, яке характеризує весь документ. Це значення шифрується секретним ключем відправника, формуючи цифровий підпис. Отримувач документа за допомогою відкритого ключа відправника розшифровує підпис і перевіряє відповідність хеш-значення. Такий підхід дозволяє гарантувати, що документ не було змінено під час передачі, а також підтверджує його авторство.

Сучасні системи електронного цифрового підпису мають низку переваг. Вони дозволяють швидко перевіряти автентичність документів, ефективно передавати дані завдяки використанню хешування, забезпечують високий рівень безпеки завдяки використанню передових криптографічних алгоритмів, таких як алгоритми на основі еліптичних кривих. Крім того, вони відповідають вимогам міжнародного та національного законодавства, що робить їх юридично значущими.

Таким чином, електронний цифровий підпис є ключовим інструментом для забезпечення надійного та безпечного обміну інформацією у цифровому середовищі. Його впровадження дозволяє захистити дані від зловмисних дій, забезпечити їхню цілісність та підтвердити авторство документів, що є важливим аспектом сучасного інформаційного суспільства.

Використання електронного цифрового підпису (ЕЦП) у сучасному цифровому середовищі стало ключовим елементом забезпечення автентичності та цілісності електронних документів. Його роль особливо важлива в умовах зростаючої кількості електронних угод, дистанційного укладення контрактів та передачі чутливої інформації через мережу Інтернет.

ЕЦП дозволяє вирішити основні проблеми ідентифікації автора документа та захисту від змін під час передачі. Це забезпечується завдяки

використанню сучасних криптографічних алгоритмів та хеш-функцій. На відміну від традиційних методів аутентифікації, де інформація пов'язана з фізичними носіями (наприклад, паперовими документами з рукописними підписами), ЕЦП надає можливість створювати юридично значущі електронні документи.

Важливою перевагою сучасних систем ЕЦП є використання хеш-функцій для оптимізації обсягу переданої інформації. Під час створення підпису спершу обчислюється хеш тексту документа, після чого він шифрується секретним ключем відправника. Це дозволяє значно скоротити обсяг даних, що передаються мережею, порівняно з прямим шифруванням усього документа.

Актуальні види атак на інформаційні системи, де використовується ЕЦП, включають:

- Фальсифікація підпису: спроби злочинців створити підпис без доступу до секретного ключа відправника.
- Атаки на хеш-функції: спроби підібрати інший документ з тим самим хеш-значенням (колізії хешу).
- Атаки типу "людина посередині" (MITM): підміна електронних підписів при передачі.

Щоб забезпечити належний рівень безпеки, сучасні криптографічні системи використовують стійкі алгоритми шифрування та хеш-функції, наприклад, SHA-3 та алгоритми на основі еліптичних кривих. Ці технології дозволяють підвищити ефективність та безпеку роботи з ЕЦП.

Законодавчі ініціативи та стандарти (наприклад, EU eIDAS) стимулюють поширення електронного підпису як легального інструмента для укладання контрактів та захисту цифрової ідентичності. Таким чином, сучасні інформаційно-інтелектуальні системи активно впроваджують ЕЦП як невід'ємну частину захисту електронного документообігу та аутентифікації користувачів.

21.2. ХЕШ-ФУНКЦІЯ

Хеш-функція — це математичний алгоритм, який перетворює дані довільного розміру у фіксовану послідовність символів, відому як хеш-код. Основна мета такого перетворення полягає у створенні унікального цифрового відбитка для кожного набору даних. Це дозволяє ефективно перевіряти цілісність інформації, оскільки навіть найменша зміна у вхідних даних суттєво змінює хеш-код.

Однією з ключових властивостей хеш-функцій є їхня односторонність, тобто неможливість відновити оригінальні дані за хеш-кодом. Ця особливість робить хеш-функції важливими для криптографічних задач, таких як зберігання паролів та створення електронних цифрових підписів (ЕЦП). Завдяки цьому механізму у системах ЕЦП підписується не весь документ, а лише його хеш-код, що суттєво знижує обсяг передаваних даних та прискорює процес перевірки підпису.

Хеш-функції забезпечують цілісність інформації під час передачі даних у телекомунікаційних мережах. Наприклад, при отриманні електронного документа одержувач може обчислити його хеш-код і порівняти його з тим, що був надісланий разом із документом. Якщо значення співпадають, це підтверджує, що документ не було змінено під час передачі.

Крім того, хеш-функції широко застосовуються для зберігання паролів у захищеному вигляді. Замість самого пароля у базі даних зберігається лише його хеш-код. Навіть якщо база даних буде скомпрометована, відновити оригінальні паролі буде вкрай складно.

Іншим важливим застосуванням є боротьба з реплей-атаками. У системах автентифікації хешування дозволяє створювати одноразові токени, які неможливо повторно використати. Завдяки цьому злоумисники не можуть скористатися перехопленими даними для отримання несанкціонованого доступу.

Популярними алгоритмами хешування є SHA-256 та SHA-3, які вважаються надійними та широко використовуються для захисту інформації. Водночас старіші функції, такі як MD5 і SHA-1, вже визнані ненадійними через можливість виникнення колізій, коли різні набори даних генерують однаковий хеш-код.

Загалом хеш-функції є незамінним інструментом у сучасній криптографії та інформаційній безпеці. Вони забезпечують надійний захист інформації, підтримують автентифікацію даних, зберігають цілісність документів та підвищують стійкість інформаційних систем до кіберзагроз.

Функції хешування відіграють ключову роль у забезпеченні цілісності та безпеки даних у сучасних інформаційних системах, сприяючи підвищенню їх ефективності та захищеності від злоумисних атак.

Забезпечення цілісності даних є одним із основних застосувань хеш-функцій. Під час передачі документів або файлів через мережу інтернет, хеш-функція дозволяє створити унікальний цифровий "відбиток" документа, який можна використовувати для перевірки його цілісності.

Після отримання документу, обчислюється його хеш-код, і цей код порівнюється з початковим значенням, надісланим разом з документом. Якщо хеш-коди співпадають, це підтверджує, що файл не було змінено або пошкоджено під час передачі. Таким чином, хешування дозволяє переконатися, що дані залишаються незмінними й надійними.

Функції хешування та їхнє детальне застосування

✱ Забезпечення цілісності даних

Хеш-функції відіграють ключову роль у перевірці цілісності інформації під час її зберігання або передачі через мережі. Під час передачі документів або файлів через мережу інтернет, хеш-функція дозволяє створити унікальний цифровий "відбиток" документа, який можна використовувати для перевірки його цілісності. Після отримання документу, обчислюється його хеш-код, і цей код порівнюється з початковим значенням, надісланим разом з документом. Якщо хеш-коди співпадають, це підтверджує, що файл не було змінено або пошкоджено під час передачі. Таким чином, хешування дозволяє переконатися, що дані залишаються незмінними й надійними.

✱ Електронний цифровий підпис (ЕЦП)

Іншим важливим застосуванням хеш-функцій є їх використання в електронних цифрових підписах (ЕЦП). У системах ЕЦП хешування дозволяє підписувати не весь документ, а лише його хеш-код. Це значно знижує обсяг передаваних даних і дозволяє швидше перевіряти підпис. Підписання хеш-коду замість всього документа дозволяє швидше обробляти інформацію, зберігаючи при цьому високу ступінь захищеності. Крім того, завдяки хешуванню можна гарантувати, що документ не був змінений після того, як він був підписаний.

✱ Криптографія та захист паролів

Криптографія та захист паролів — ще одна важлива сфера застосування хеш-функцій. У сучасних системах автентифікації паролі не зберігаються у вигляді тексту, а зберігається лише їхній хеш. Це дозволяє захистити паролі в разі витоку баз даних, оскільки злоумисники не зможуть відновити самі паролі з їхніх хеш-кодів. Крім того, для підвищення безпеки хешування часто комбінується з технікою "соління" — додавання випадкового значення до пароля перед його хешуванням, що ускладнює атаки на бази даних.

✱ Цифрові підписи та сертифікати безпеки

Хеш-функції також застосовуються для створення цифрових підписів та сертифікатів безпеки. Завдяки хешуванню, можна створювати унікальні відбитки документів, що використовуються для захисту та автентифікації цифрових сертифікатів, таких як SSL/TLS. Ці сертифікати підтверджують

автентичність вебсайтів і забезпечують захищене з'єднання між користувачем та сервером. Хешування в цьому контексті дозволяє підтвердити, що сертифікат не був змінений, і що він дійсно належить заявленому власнику.

✱ *Захист від реплей-атак*

Одним із важливих застосувань хешування є захист від реплей-атак. У таких атаках зловмисники можуть перехопити й повторно використовувати старі дані для несанкціонованого доступу. Хешування дозволяє створювати одноразові токени для кожної сесії чи операції, що робить неможливим повторне використання старих даних. Кожен запит або операція стає унікальним, що ускладнює їхнє повторне використання зловмисниками.

✱ *Інформаційні пошукові системи*

Завдяки хешуванню можна значно покращити інформаційні пошукові системи. Хеш-функції дозволяють швидко індексувати та знаходити інформацію в базах даних та файлових системах. Вони дозволяють створювати короткі унікальні ідентифікатори для великих обсягів даних, що значно прискорює пошук та доступ до інформації. Це застосовується, наприклад, у системах пошуку документів, де хеші використовуються для швидкої ідентифікації та отримання потрібної інформації.

Таким чином, хеш-функції є основою для безпеки та ефективного оброблення даних у сучасних інформаційних технологіях. Вони забезпечують цілісність переданих даних, захищають паролі, а також підтримують високий рівень захисту в різноманітних сферах, від криптографії до пошукових систем.

АЛГОРИТМИ ХЕШУВАННЯ СІМЕЙСТВА MD

Сімейство алгоритмів хешування MD (Message Digest) було розроблене Роналдом Рівестом для створення 128-бітних хеш-образів. Ці алгоритми відіграють важливу роль у забезпеченні цілісності даних та створенні цифрових підписів. Незважаючи на те, що MD5 залишається одним із найбільш відомих алгоритмів, його безпека сьогодні викликає серйозні сумніви через вразливість до криптографічних колізій.

Вимоги до сучасних хеш-алгоритмів:

- **Безпека** - складність знаходження двох різних повідомлень із однаковими хешами.
- **Пряма безпека** не залежить від складних математичних припущень (наприклад, розкладу чисел на прості множники).
- **Швидкість** - оптимізовані для швидкої програмної реалізації на різних архітектурах.

- Стійкість до колізій: неможливість підібрати дані з однаковими хешами.

Алгоритм MD2

MD2 був розроблений у 1989 році для 8-розрядних процесорів. Він формує 128-бітний хеш-образ і використовує контрольні суми та випадкові перестановки, засновані на числі π . Незважаючи на цікаву архітектуру, алгоритм повільний і застарілий для сучасних криптографічних задач. MD2 забезпечує сумісність із апаратною архітектурою 1980-х років і був оптимізований для роботи з обмеженими обчислювальними ресурсами. Алгоритм виконує доповнення повідомлень до довжини, кратної 16 байтам, та додає контрольні суми для забезпечення цілісності даних. Однією з ключових особливостей MD2 є використання 48-байтного блоку для обробки даних із застосуванням випадкових перестановок, що робить його стійким до деяких типів атак того часу. Випадкові перестановки базуються на цифрах числа π , що додає додатковий рівень ентропії у процес хешування. Незважаючи на це, MD2 не забезпечує високої криптографічної стійкості, необхідної для сучасних інформаційних систем. Сьогодні цей алгоритм вважається вразливим до колізій та повністю застарілим. У більшості випадків його замінено більш сучасними алгоритмами, такими як SHA-2 та SHA-3.

Алгоритми MD4 та MD5

MD4 став основою для багатьох сучасних хеш-функцій, але його безпека була поставлена під сумнів через успішні атаки. MD5, як удосконалена версія MD4, має чотири етапи обробки повідомлення та використовує унікальні константи у кожному циклі. Однак навіть MD5 вразливий до колізій, що робить його непридатним для критичних застосувань, таких як цифрові підписи та захист паролів. MD4 був розроблений для швидкої обробки даних на 32-бітних процесорах і став важливим етапом у розвитку хеш-функцій. Його трьохетапна структура забезпечувала високу продуктивність, але мала низьку стійкість до криптоаналітичних атак. MD5, як його наступник, намагався виправити ці недоліки шляхом додавання четвертого етапу обробки та використання унікальних констант. Попри це, MD5 також не витримав перевірки часом через вразливість до колізій, які стали відомими вже у 2004 році. Це призвело до відмови від його використання для захищених криптографічних задач. Наразі MD5 все ще використовується для контрольних сум файлів та перевірки цілісності даних, але не для захисту конфіденційної інформації. Сучасні стандарти, такі як SHA-2 та SHA-3, стали безпечнішою альтернативою.

Сучасний стан:

- Недоліки: MD5 уже не вважається безпечним через можливість колізій. З 2004 року було знайдено методи для ефективного генерування колізій.

- Замінники: У сучасній криптографії MD5 та MD4 були витіснені алгоритмами сімейства SHA (Secure Hash Algorithm), такими як SHA-256 та SHA-3, які пропонують значно вищий рівень безпеки.

- Використання: MD5 все ще можна зустріти для контрольних сум файлів, але не для криптографічних цілей.

Алгоритм SHA-1

Алгоритм SHA-1 (Secure Hash Algorithm 1) був розроблений Національним інститутом стандартів і технологій США (NIST) у 1993 році та став наступником SHA-0. Його основне призначення — формування 160-бітного хеш-образу, що забезпечувало високу щільність хешування та певну стійкість до колізій на момент розробки. SHA-1 обробляє дані блоками по 512 біт і використовує п'ять 32-бітних регістрів для зберігання проміжних результатів. У процесі обробки кожен блок проходить через 80 раундів перетворень, де використовуються логічні операції XOR, додавання за модулем 2^{32} та циклічні зсуви.

Попри тривалу популярність алгоритму, у 2005 році були виявлені перші серйозні вразливості, які дозволяли проводити атаки на колізії ефективніше, ніж передбачалося. У 2017 році Google та CWI Amsterdam публічно продемонстрували реальну колізію SHA-1, довівши, що цей алгоритм більше не може вважатися безпечним для криптографічних цілей. Зокрема, використання SHA-1 стало неприйнятним для цифрових підписів, захисту паролів та сертифікаційних систем.

На сьогодні SHA-1 вважається застарілим, і більшість підприємств та розробників перейшли на безпечніші алгоритми, такі як SHA-256 або SHA-3. Хоча SHA-1 все ще іноді використовується для перевірки цілісності даних у старих системах, його застосування категорично не рекомендується для захищених інформаційних процесів.

Алгоритм SHA-2

SHA-2 (Secure Hash Algorithm 2) — це сімейство криптографічних хеш-функцій, розроблене Національним інститутом стандартів і технологій США (NIST) у 2001 році. Алгоритм став покращенням свого попередника SHA-1 і значно підвищив рівень безпеки завдяки більшій довжині хеш-образів та вдосконаленій структурі.

Основні версії SHA-2:

- ✓ SHA-224: генерує 224-бітний хеш;

- ✓ SHA-256: формує хеш довжиною 256 біт;
- ✓ SHA-384: створює 384-бітний хеш;
- ✓ SHA-512: генерує 512-бітний хеш;
- ✓ SHA-512/224 та SHA-512/256: оптимізовані варіанти для специфічних задач.

Входом алгоритму може бути повідомлення довільної довжини, а виходом є хеш з фіксованою довжиною залежно від версії. SHA-2 базується на структурі Merkle–Damgård із функцією стиснення, яка використовує побітові операції, додавання за модулем 2^{32} або 2^{64} , та нелінійні функції, що забезпечують високу стійкість до колізій і криптоаналітичних атак.

Переваги SHA-2 включають його високу стійкість до атак порівняно з SHA-1, оптимізацію для апаратної та програмної реалізації, а також широку підтримку в сучасних криптографічних протоколах, таких як TLS, SSL, PGP, SSH та IPsec. Проте деякі версії, зокрема SHA-512, є ресурсомісткими через великий обсяг обчислень. З часом SHA-2 поступово витісняється сімейством SHA-3, яке має іншу архітектуру та ще вищий рівень безпеки.

SHA-256 залишається найбільш популярним для цифрових підписів, перевірки цілісності даних і криптовалют (наприклад, Bitcoin). SHA-512 часто застосовується в системах з високими вимогами до безпеки. Хоча SHA-2 є сучасним і безпечним алгоритмом, рекомендується звертати увагу на SHA-3 як стандарт нового покоління.

SHA-256 (Secure Hash Algorithm 256-bit) є одним із членів сімейства алгоритмів SHA-2, розробленого Національним інститутом стандартів і технологій США (NIST) у 2001 році. Основною метою цього алгоритму є створення надійного хеш-образу довжиною 256 біт, що забезпечує високу стійкість до колізій та криптографічну безпеку.

SHA-256 обробляє повідомлення блоками по 512 біт. На початковому етапі повідомлення доповнюється, щоб його довжина стала кратною 512 бітам, після чого додається 64-бітне представлення початкової довжини повідомлення. Алгоритм використовує вісім 32-бітних регістрів для накопичення проміжних значень і проходить 64 раунди обробки даних із застосуванням математичних та логічних операцій, включаючи додавання за модулем 2^{32} , логічні функції XOR і циклічні зсуви.

Використання унікальних констант та ретельно підібраних нелінійних перетворень значно підвищує безпеку SHA-256, роблячи його стійким до відомих атак, таких як колізії та підбір першого образу. Завдяки цьому алгоритм активно застосовується у криптографії, цифрових підписах, блокчейн-системах та для захисту паролів.

Порівняно зі своїм попередником SHA-1, алгоритм SHA-256 має значно вищий рівень безпеки. Він широко підтримується сучасними протоколами шифрування та сертифікації, такими як TLS, SSL та PKI. Завдяки своїй ефективності та стійкості SHA-256 став стандартом у багатьох критично важливих інформаційних системах.

Алгоритм SHA-3

SHA-3 (Secure Hash Algorithm 3) — це сімейство криптографічних хеш-функцій, яке було розроблено як частина ініціативи NIST з створення стандартів для криптографічних алгоритмів. Відрізняючись від попередників SHA-2, SHA-3 побудований на принципах, що використовують іншу архітектуру — конструкцію Sponge (губка), яка забезпечує вищу стійкість до атак.

Основні характеристики SHA-3:

- Алгоритм використовує конструкцію Sponge, що дозволяє адаптувати довжину хеш-образу залежно від конкретних вимог (наприклад, SHA3-224, SHA3-256, SHA3-384, SHA3-512).
- SHA-3 може працювати з різними довжинами вихідного хешу, що надає більшу гнучкість порівняно з SHA-2.
- Він включає в себе додаткові варіанти: SHAKE128 та SHAKE256, які є динамічними хеш-функціями з змінною довжиною вихідних значень.

Переваги:

- Вищий рівень безпеки, оскільки SHA-3 не має тих самих криптографічних слабкостей, які були виявлені в SHA-1 і SHA-2.
- Побудова на конструкції Sponge дозволяє реалізовувати SHA-3 для численних криптографічних завдань, таких як підписування, генерація випадкових чисел та забезпечення цілісності даних.
- SHA-3 розроблений для того, щоб бути стійким до нових типів атак, таких як атаки на основі бічних каналів.

Недоліки:

- Хоча SHA-3 має високу безпеку, на сьогодні він має більші вимоги до ресурсів, ніж SHA-2, що робить його менш ефективним в деяких застосуваннях.
- SHA-3 ще не отримав такого широкого застосування, як SHA-2, тому його інтеграція в існуючі системи може бути складною.

Застосування: SHA-3 активно використовується в нових криптографічних протоколах і системах, таких як захищена передача даних, цифрові підписи та криптовалюти. Завдяки своїй гнучкості та безпеці він має велике майбутнє в нових криптографічних стандартах.

Висновок: SHA-3 є надійним і сучасним алгоритмом хешування, що пропонує високий рівень безпеки, але вимагає більше ресурсів і ще не отримав такої широкої підтримки, як SHA-2.

АЛГОРИТМ RIPEMD (RACE INTEGRITY PRIMITIVES EVALUATION MESSAGE DIGEST)

Алгоритм RIPEMD (Race Integrity Primitives Evaluation Message Digest) був розроблений у 1996 році дослідниками Хансом Доббертіном, Антом Босселарсом та Бартом Пренелем як частина європейського проєкту RIPE. Основна мета алгоритму полягала у створенні криптографічного хеш-функції з високою стійкістю до колізій. RIPEMD став альтернативою алгоритмам MD5 і SHA-1, які на той час мали певні недоліки. RIPEMD був розроблений з урахуванням потреби у більшій безпеці та надійності криптографічних алгоритмів для різних застосувань, таких як цифрові підписи та перевірка цілісності даних. Він має різні версії, зокрема RIPEMD-128 та RIPEMD-160, з різною довжиною хеш-образу, що дозволяє обирати оптимальний варіант залежно від вимог до безпеки. Однак, з часом було виявлено, що RIPEMD також має деякі вразливості до атак, що ставить під сумнів його ефективність для високо захищених систем. Попри це, RIPEMD досі залишається корисним у деяких випадках, зокрема в старих системах або для забезпечення сумісності з існуючими протоколами.

Основні версії алгоритму:

- RIPEMD-128 формує хеш-образ довжиною 128 біт,
- RIPEMD-160 створює хеш довжиною 160 біт.

Пізніше були розроблені удосконалені варіанти RIPEMD-256 і RIPEMD-320, але вони не стали такими популярними, як основна версія RIPEMD-160.

Актуальність: RIPEMD-160 вважається стійкішим і безпечнішим порівняно з MD5 та SHA-1, але на сьогодні він втрачає актуальність через впровадження алгоритмів сімейства SHA-2 (SHA-256, SHA-512) та новітніх SHA-3. Попри це, деякі криптографічні системи та блокчейн-проєкти (наприклад, деякі старі криптовалюти) продовжують використовувати RIPEMD-160.

RIPEMD-128 вже не відповідає сучасним вимогам безпеки через недостатню довжину хеш-образу. Алгоритм має нижчу ефективність порівняно з SHA-2. Оскільки він не може забезпечити належний рівень захисту від сучасних криптографічних атак, його використання в критичних застосуваннях є ризикованим. Крім того, RIPEMD-128 не має тих же рівнів безпеки та гнучкості, як новіші алгоритми хешування. Щодо

переваг, то алгоритм добре оптимізований для програмної реалізації, що робить його доступним для різних застосувань в обмежених ресурсах. Також варто відзначити високу стійкість до відомих атак на час свого створення, що дозволяє використовувати його у деяких старих системах. Загалом, RIPEMD-160 ще може використовуватися для сумісності у спадкових системах, але для нових проєктів рекомендовано обирати сучасніші алгоритми, такі як SHA-256 або SHA-3, що пропонують кращу безпеку та ефективність.

21.3.АЛГОРИТМИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Технологія застосування системи ЕЦП припускає наявність мережі абонентів, що посилають один одному підписані електронні документи. Для кожного абонента генерується пара ключів: секретний і відкритий. Секретний ключ зберігається абонентом у таємниці і використовується ним для формування ЕЦП. Відкритий ключ відомий всім іншим користувачам і призначений для перевірки ЕЦП одержувачем підписаного електронного документа. Інакше кажучи, відкритий ключ є необхідним інструментом, що дозволяє перевірити дійсність електронного документа й автора підпису. Відкритий ключ не дозволяє обчислити секретний ключ.

Алгоритми електронного цифрового підпису (ЕЦП) є важливою частиною криптографії і забезпечують захист цілісності, автентичності та неоспоримості повідомлень. Вони використовують асиметричне шифрування для підписання і перевірки підпису.

Основні алгоритми для створення ЕЦП:

RSA (Rivest–Shamir–Adleman)

Це один з найвідоміших алгоритмів для генерації електронного підпису. Він використовує пару ключів: відкритий (для перевірки підпису) і закритий (для підписання). Алгоритм RSA базується на математичних операціях з великими простими числами та їх добутках. Підпис RSA є дуже безпечним, але з обмеженнями на розмір повідомлення, яке може бути підписано.

Узагальнена схема цифрового підпису RSA складається з кількох етапів. Спочатку генеруються два ключі: відкритий і закритий. Відправник використовує свій закритий ключ для підписання повідомлення, створюючи підпис за допомогою хеш-функції, яка генерує унікальне значення для повідомлення. Підпис разом з повідомленням відправляється одержувачу. Одержувач використовує відкритий ключ відправника для перевірки підпису, обчислюючи хеш повідомлення та порівнюючи його з

отриманим значенням. Якщо вони співпадають, підтверджується, що повідомлення не було змінено і воно дійсно походить від вказаного відправника. Це забезпечує цілісність та автентичність переданої інформації.

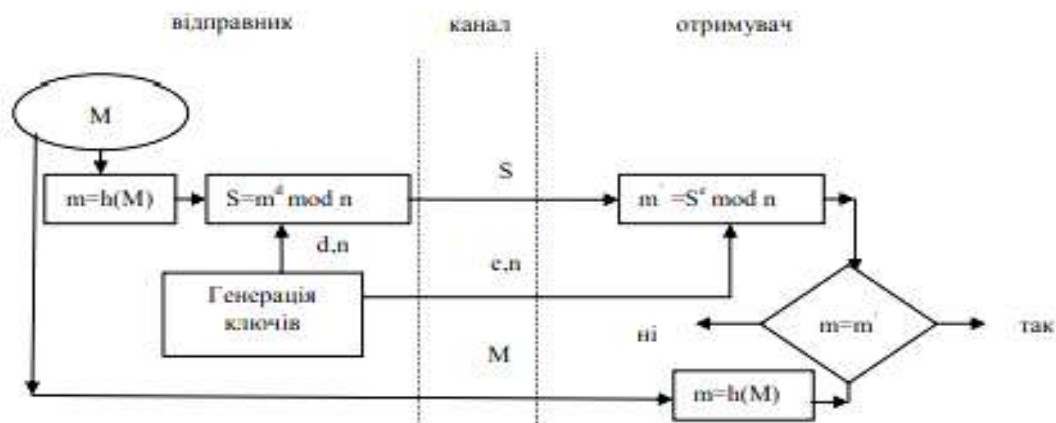


Рис. 21.3. Узагальнена схема цифрового підпису RSA

Джерело: [8-9]

Алгоритм RSA є одним з найстаріших і найбільш широко використовуваних методів криптографії з відкритим ключем. Його безпека ґрунтується на складності факторизації великих чисел, що робить його дуже стійким до атак за допомогою сучасних методів обчислень. Однак RSA вимагає великих обсягів пам'яті та часу для обробки великих повідомлень, що може бути проблемою для ресурсозалежних систем. Сучасні варіанти RSA використовують збільшені розміри ключів (2048 біт і більше), щоб забезпечити належний рівень безпеки в умовах зростаючої обчислювальної потужності.

1. DSA (Digital Signature Algorithm)

Алгоритм, який був розроблений Агентством національної безпеки США (NSA) та стандартизований NIST. DSA використовує криптографічний алгоритм з відкритим ключем і має схожу функціональність із RSA. Проте на відміну від RSA, DSA використовує інший тип математичних операцій для генерування та перевірки підписів, зокрема, операції на полях з великою кількістю елементів. Основна перевага DSA полягає в тому, що він забезпечує швидше генерування підписів, що робить його більш ефективним для застосувань, де важлива швидкість. Однак DSA має обмеження на довжину підпису та не дозволяє використовувати підпис для шифрування даних, як це робить RSA. Для забезпечення надійності підпису в DSA використовуються великі прості числа, що дозволяє

уникати атак типу "перевірка за допомогою brute-force". Як і RSA, безпека DSA залежить від складності математичних задач, зокрема, від проблеми дискретного логарифмування.

2. *ECDSA (Elliptic Curve Digital Signature Algorithm)*

Це варіант DSA, який застосовує еліптичні криві для генерації підписів. Використання еліптичних кривих забезпечує більшу ефективність та безпеку з меншим обсягом даних. Вона широко використовується в сучасних криптографічних протоколах, таких як Bitcoin, TLS, а також у мобільних додатках, що потребують високої безпеки. Основною перевагою ECDSA є те, що для досягнення того ж рівня безпеки, що і у традиційних алгоритмах, таких як RSA або DSA, вона вимагає значно меншого розміру ключа. Це знижує вимоги до обчислювальних потужностей і економить пам'ять, що особливо важливо для мобільних пристроїв і обмежених систем. Завдяки своїй високій ефективності та безпеці, ECDSA є стандартом для цифрових підписів у багатьох сучасних криптографічних застосунках. Однак її безпека також залежить від правильного вибору еліптичної кривої та параметрів, що використовуються в алгоритмі.

3. *EdDSA (Edwards-curve Digital Signature Algorithm)*

Алгоритм на основі еліптичних кривих, який є більш ефективним і захищеним, ніж ECDSA, завдяки використанню кривих Едвардса. EdDSA застосовується в таких системах, як OpenSSH, WireGuard та інші сучасні криптографічні рішення, що вимагають високої швидкості і безпеки. Однією з ключових переваг EdDSA є його стійкість до атак типу бокових каналів, завдяки використанню детерміністичних методів генерації підписів, що виключає ризики, пов'язані з вибором випадкових чисел. Алгоритм також швидший, оскільки має більш прості та ефективні операції порівняно з ECDSA, що дозволяє досягти більш високої продуктивності при менших витратах ресурсів. EdDSA забезпечує більш високу безпеку при менших розмірах ключів, що робить його ідеальним для мобільних пристроїв і розподілених систем. Цей алгоритм набуває все більшої популярності в сучасних криптографічних застосунках завдяки своїй ефективності та здатності забезпечити надійний рівень захисту.

4. *ElGamal*

Алгоритм, заснований на проблемі дискретного логарифмування в групі чисел. Він використовується для підпису повідомлень і може бути налаштований для різних рівнів безпеки. Хоча ElGamal є дуже безпечним, його реалізація менш поширена через більшу складність порівняно з іншими алгоритмами, такими як RSA. ElGamal забезпечує високий рівень безпеки завдяки використанню великих простих чисел і складних математичних операцій, що робить його стійким до атак типу "підробки

підпису". Однак він має один великий недолік: більший розмір підпису порівняно з RSA або DSA, що може бути важливим фактором у системах з обмеженими ресурсами. Попри це, ElGamal застосовується в специфічних криптографічних рішеннях, таких як в криптовалютних протоколах для забезпечення анонімності та безпеки транзакцій. Алгоритм також використовується в схемах шифрування з відкритим ключем, що дозволяють здійснювати як підписування, так і захист повідомлень.

Загальні етапи роботи алгоритмів електронного цифрового підпису:

1. Генерація ключів: створення пари ключів — приватного для підписання і публічного для перевірки.
2. Підписання: повідомлення хешується, потім підписується приватним ключем відправника.
3. Перевірка: отримувач хешує повідомлення і використовує публічний ключ для перевірки підпису.

Переваги електронних підписів:

- ✓ Цілісність: будь-яка зміна повідомлення після підписання призведе до того, що перевірка підпису не пройде.
- ✓ Автентичність: підпис підтверджує, що повідомлення було створене конкретною особою.
- ✓ Неоспоримість: підписувач не може заперечити своє підписання повідомлення.

Недоліки:

- ✓ Висока обчислювальна складність для великих повідомлень (особливо RSA).
- ✓ Можливість атаки на коротші ключі або слабкі варіанти реалізації (зокрема у старих версіях RSA і DSA).

Завдяки своїй безпеці і широкому застосуванню, електронні цифрові підписи є критично важливими для багатьох сучасних цифрових систем, зокрема для забезпечення безпеки фінансових операцій, електронного урядування, цифрових контрактів тощо.

21.4. СТАНДАРТИ АЛГОРИТМІВ ФОРМУВАННЯ І ПЕРЕВІРКИ ЕЦП

Стандарти алгоритмів формування та перевірки електронного цифрового підпису (ЕЦП) визначають правила для забезпечення криптографічної безпеки, автентичності та цілісності повідомлень у різних системах. Основні стандарти:

1. **FIPS PUB 186-4 (DSA, RSA, ECDSA)**

Стандарт, розроблений Національним інститутом стандартів і технологій США (NIST), визначає використання алгоритмів для цифрових підписів, зокрема DSA, RSA та ECDSA. Це офіційний стандарт для підписів у федеральних урядових організаціях США, який забезпечує криптографічну стійкість і стандартні підходи для перевірки підписів.

2. ISO/IEC 14888 (Digital Signatures)

Цей стандарт охоплює три частини: загальні вимоги до алгоритмів ЕЦП, схеми підпису на основі асиметричних алгоритмів і методи використання відкритих ключів для перевірки підписів. Він визначає параметри для алгоритмів на основі дискретного логарифмування, включаючи DSA та інші криптографічні схеми.

3. X.509 (Public Key Infrastructure - PKI)

X.509 є міжнародним стандартом для систем управління сертифікатами та цифровими підписами. Важливою частиною цього стандарту є визначення формату сертифікатів та алгоритмів, які використовуються для підпису та перевірки автентичності.

4. RFC 3279 (Cryptographic Algorithms for Internet Security)

Цей стандарт, що містить рекомендації щодо криптографічних алгоритмів для використання в інтернет-протоколах, включає визначення алгоритмів для цифрових підписів. Він описує використання DSA, RSA та ECDSA в контексті забезпечення безпеки передачі даних в інтернеті.

5. ECDSA (Elliptic Curve Digital Signature Algorithm)

Частина стандартів, що використовує еліптичні криві для генерації і перевірки цифрових підписів, забезпечуючи високий рівень безпеки за допомогою менших ключів. ECDSA є частиною FIPS PUB 186-4 та широко застосовується в сучасних криптографічних протоколах, таких як TLS і Bitcoin.

Ці стандарти забезпечують ефективну інтеграцію алгоритмів цифрового підпису в різноманітні системи та служать основою для криптографічної безпеки, а також для автентифікації та захисту даних.

21.5. Протоколи взаємодії і сертифікати в стандарті X.509

Криптосистеми з відкритим розподілом ключів та електронним цифровим підписом (ЕЦП) є важливим інструментом для забезпечення високого рівня безпеки при обміні повідомленнями, оскільки вони дозволяють здійснювати захист конфіденційності та автентичності без необхідності обміну секретними ключами через канали зв'язку. Однак однією з основних загроз є можливість підміни відкритих ключів, коли

зловмисник може втручатися в процес обміну і замінити відкриті ключі на свої власні, що дозволяє йому читати зашифровані повідомлення. Для захисту від таких атак використовуються сертифікати, що підписуються центром сертифікації ключів (ЦСК), які дозволяють перевірити достовірність відкритого ключа. У такій системі відправник перевіряє сертифікат отримувача за допомогою відкритого ключа ЦСК і, після підтвердження його дійсності, здійснює шифрування сеансового ключа та повідомлення.

Для компенсації обмежень асиметричного шифрування, яке є повільним, використовується гібридна криптосистема, де для кожного сеансу генерується симетричний сеансовий ключ, що шифрує основне повідомлення, а сам сеансовий ключ шифрується відкритим ключем отримувача. Ключове завдання в таких системах — забезпечити відповідність рівня безпеки між асиметричними та симетричними ключами, оскільки навіть якщо асиметричні ключі є сильними, слабкість сеансового ключа може призвести до компрометації всієї системи. Крім того, необхідно ретельно обробляти процес передачі відкритих ключів, оскільки перехоплення запитів для отримання відкритого ключа є типовою атакою. Для цього використовуються різноманітні сертифікаційні механізми, проте жоден із них не може гарантувати 100% захист від підміни ключів, що є однією з головних вразливостей.

Система забезпечує перевірку кожного отриманого повідомлення за допомогою хеш-функцій та електронного підпису, що дозволяє підтвердити цілісність і автентичність повідомлення. Всі ці заходи забезпечують надійний захист при використанні систем з відкритим розподілом ключів, проте критичним є забезпечення безпеки роботи з центром сертифікації та запобігання його компрометації, оскільки вона може призвести до скомпрометування всієї системи.

Стандарт X.509 є важливою частиною криптографічних систем з відкритим розподілом ключів, забезпечуючи механізм для верифікації відкритих ключів за допомогою сертифікатів. Сертифікати X.509 містять відкритий ключ власника, а також додаткову інформацію, таку як ідентифікація власника, термін дії сертифіката та підпис центру сертифікації (ЦСК), що підтверджує його достовірність. Процес видачі сертифікатів включає подачу запиту користувачем до ЦСК, яке перевіряє надану інформацію, а після успішної перевірки підписує сертифікат своїм власним секретним ключем. Це дозволяє користувачам здійснювати перевірку достовірності відкритих ключів через сертифікати, запобігаючи атакувачам, які можуть спробувати підмінити відкритий ключ.

Протоколи взаємодії в стандарті X.509, такі як Protocol for Revocation of Certificates (CRL) та Online Certificate Status Protocol (OCSP), дають змогу перевіряти, чи не був сертифікат відкликаний або чи є він дійсним в реальному часі. Також стандарт передбачає ієрархічну модель сертифікації, де кожен сертифікат підписується більш високим рівнем сертифікації, забезпечуючи тим самим довіру в межах цілої системи сертифікаційних ланцюгів. Зокрема, кореневі сертифікати, які є основою цієї ієрархії, можуть підтверджувати достовірність сертифікатів на нижчих рівнях, що дає можливість користувачам перевіряти дійсність сертифікатів інших осіб чи організацій.

Ці сертифікати X.509 та протоколи взаємодії є основою для побудови безпечних криптографічних каналів зв'язку, забезпечуючи надійний захист даних у системах з відкритим розподілом ключів.

21.6. СТРУКТУРА СЕРТИФІКАТА ВІДКРИТИХ КЛЮЧІВ

Сертифікат відкритого ключа, відповідно до стандарту X.509, є важливим елементом для забезпечення безпеки та автентичності в інфраструктурах відкритих ключів (PKI). Він служить для підтвердження зв'язку між відкритим ключем та його власником, забезпечуючи захист від атак на підміну ключів. Структура сертифіката містить кілька ключових елементів, що визначають його функціональність та надають можливість перевірки його дійсності. Основними складовими є версія сертифіката, яка визначає, який стандарт X.509 був використаний (версії 1, 2 або 3), та унікальний ідентифікатор сертифіката, що дозволяє однозначно визначити його в межах інфраструктури PKI.

Сертифікат містить ідентифікаційні дані власника, що включають ім'я особи або організації, а також інші атрибути, які використовуються для точного визначення користувача. Крім того, він включає відкритий ключ власника, який використовується для перевірки підписів або шифрування. Важливою частиною сертифіката є також інформація про центр сертифікації, який видав цей сертифікат, що гарантує його автентичність через цифровий підпис, що створюється приватним ключем цього центру.

Термін дії сертифіката вказує на період, протягом якого цей сертифікат є дійсним, що дозволяє уникнути використання застарілих або скомпрометованих ключів. Крім цього, сертифікат може містити поля, що визначають політику його використання, тобто конкретні обмеження або дозволи на застосування сертифіката для певних криптографічних операцій. Завершує структуру сертифіката підпис центру сертифікації, який підтверджує, що сертифікат не був змінений після його випуску, а

також є дійсним для використання в заданий період. Термін дії сертифіката також є важливим аспектом для своєчасного поновлення та перевірки актуальності ключів, що використовуються в системах безпеки. По закінченню цього терміну, сертифікат стає недійсним, що знижує ризики використання старих або зламаних криптографічних даних. Сертифікати можуть містити додаткову інформацію про політику сертифікації, яка регулює умови їх використання, наприклад, для яких типів криптографічних операцій вони підходять. Це дозволяє обмежити використання сертифіката лише для певних цілей, що підвищує рівень безпеки. У разі, якщо сертифікат використовувався для аутентифікації або підпису, наявність таких обмежень дає змогу чітко контролювати доступ до важливих даних. Завершуючи процес сертифікації, підпис центру сертифікації гарантує, що сертифікат був створений згідно з певними стандартами і не піддався жодним змінам з моменту його видачі. Це підписання є засобом доказу його легітимності в рамках всієї інфраструктури відкритих ключів. В результаті, перевірка підпису є важливою частиною перевірки автентичності сертифіката, що дозволяє уникнути підробок і підвищити довіру до системи безпеки.

Версія
Реєстраційний номер сертифіката
Ідентифікатор алгоритму підпису
Назва засвідчувального центру
Термін дії (з . по .)
Ім'я власника відкритого ключа
Значення відкритого ключа
Унікальний ідентифікатор центру сертифікації ключів
Унікальний ідентифікатор власника відкритого ключа
Розширення
Підпис

Рис. 21.4. Формат сертифіката відкритого ключа
Джерело: [8-9]

Такий підхід до структури сертифікатів дозволяє забезпечити високий рівень безпеки та довіри при використанні відкритих ключів для електронного підпису, шифрування і аутентифікації в різних

інформаційно-комунікаційних системах. Завдяки чітко визначеним політикам використання та обмеженням на конкретні криптографічні операції, сертифікати забезпечують контроль за правильністю та безпекою кожної транзакції чи дії, що здійснюється через систему. Це дозволяє мінімізувати можливості для зловмисників, а також забезпечує легкість у верифікації дійсності сертифікатів, що використовуються в різних організаціях та установах. Оскільки сертифікати підписуються центром сертифікації, їх можна перевіряти за допомогою публічних ключів сертифікаційних організацій, що підвищує рівень довіри до всіх учасників електронного обміну даними. Таким чином, інфраструктура відкритих ключів стає основою для ефективної та надійної організації процесів захисту інформації в будь-яких сферах, де використовуються криптографічні методи.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 21

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. — Електронні текстові дані (1 файл: 2,04 Мбайт). — Київ : КПІ ім. Ігоря Сікорського, 2018. — 162 с.
3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. — Київ : НУБіП України, 2023.
4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. — К.: ЦП «Компринт», 2021. — 296 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. — Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. — 213 с.

6. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
7. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.
8. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.
9. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.
10. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.
11. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.
12. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.
13. Спасітельєва, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.
14. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об’єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.
15. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.
16. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148. Y. Ivanichenko, et al.,

Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.

17. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.

18. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

19. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.

20. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

РОЗДІЛ 22

КРИПТОГРАФІЧНІ ПРОТОКОЛИ



22.1. Поняття криптографічного протоколу

22.2. Розподіл ключів і аутентифікація

22.3. Протоколи розподілу секрету

22.4. Стандарти криптопротоколів

22.5. Формальний аналіз криптографічних протоколів

"Криптографія – це не просто наука або техніка, це фундаментальна частина будь-якої системи безпеки."

Bruce Schneier, експерт з безпеки

22.1. Поняття КРИПТОГРАФІЧНОГО ПРОТОКОЛУ

Криптографічний протокол – це набір правил і процедур, які використовуються для забезпечення безпеки передачі або зберігання даних шляхом застосування криптографічних методів. Він визначає, як сторони повинні взаємодіяти, які алгоритми використовувати та як обробляти інформацію для досягнення конкретних цілей безпеки, таких як конфіденційність, цілісність, автентифікація чи незаперечність.

Ключові характеристики криптографічних протоколів:

1. **Мета протоколу** – визначає, яку саме проблему безпеки він вирішує (наприклад, забезпечення захищеного обміну ключами, автентифікація сторін, підпис даних тощо). Використання криптографічних примітивів — протоколи будуються на основі базових

механізмів, таких як симетричне та асиметричне шифрування, хешування та цифрові підписи. Розподіл ролей між учасниками — кожен учасник виконує визначені функції, наприклад генерацію ключів, шифрування або перевірку автентичності. Захист від загроз — криптографічні протоколи мають механізми протидії різним типам атак, таким як атаки посередника, підміна даних або повторні атаки. Надійність та масштабованість — протоколи повинні ефективно функціонувати як у невеликих системах, так і в масштабних мережах з великою кількістю учасників.

2. **Учасники** — сторони, які взаємодіють у межах протоколу. Учасники криптографічного протоколу можуть бути як людьми, так і програмними або апаратними системами. Кожен з учасників має свою роль і набір операцій, які він виконує для забезпечення коректної взаємодії. Для ідентифікації та забезпечення безпеки обміну даними кожен учасник зазвичай володіє власними ключами та сертифікатами. Ефективність і надійність криптографічного протоколу значною мірою залежать від правильної поведінки та довіри між усіма учасниками.

3. **Алгоритми шифрування** — основа криптографічного протоколу, яка забезпечує захист даних від несанкціонованого доступу. Алгоритми шифрування можуть бути симетричними, де використовується один і той самий ключ для шифрування та розшифрування, або асиметричними, де застосовуються пари відкритого і закритого ключів. Вибір конкретного алгоритму залежить від вимог безпеки, продуктивності та типу даних, що обробляються. Для додаткового захисту криптографічні протоколи часто комбінують кілька алгоритмів, створюючи гібридні схеми шифрування. Такі підходи забезпечують оптимальний баланс між швидкістю обробки інформації та її надійною криптографічною безпекою.

4. **Формати повідомлень** — порядок і структура даних, які передаються між учасниками. Формати повідомлень визначають, як саме інформація структурується та передається між учасниками протоколу. Це може включати поля для ідентифікації відправника та одержувача, криптографічні хеші, ключі шифрування та цифрові підписи. Коректно визначений формат повідомлень забезпечує сумісність між різними системами та гарантує цілісність даних. Стандартизовані формати повідомлень, як-от ASN.1 у сертифікатах X.509, сприяють їх широкому впровадженню та взаємодії.

5. **Механізми автентифікації** — перевірка ідентичності учасників, щоб уникнути підміни чи несанкціонованого доступу. Механізми аутентифікації забезпечують підтвердження справжності учасників перед початком обміну даними. Вони можуть включати паролі, цифрові сертифікати, біометричні дані або протоколи багатофакторної

аутентифікації. Коректна реалізація аутентифікації дозволяє захистити інформаційну систему від атак типу "людина посередині" (MITM) та несанкціонованого доступу. Сучасні криптографічні протоколи, такі як TLS і IPSec, широко використовують механізми аутентифікації для захисту мережевого трафіку.

6. **Захист від атак** – враховує потенційні загрози, такі як атаки на повтор, атаки "людина посередині" (MITM) або атаки на підбір ключів. Захист від атак є критичним аспектом криптографічних протоколів, який забезпечує їх надійність і стійкість до зовнішніх загроз. Для протидії атакам на повтор часто застосовують механізми одноразових ключів або метки часу. Атаки типу "людина посередині" (MITM) ефективно нейтралізуються за допомогою сертифікатів і перевірки автентичності учасників. Криптографічні протоколи також мають вбудовані механізми для ускладнення підбору ключів, зокрема використання алгоритмів із високою ентропією ключів.

Протоколи взаємодії в моделі OSI

Криптографічні протоколи є складовою частиною протоколів взаємодії в моделі відкритих систем OSI (Open Systems Interconnection). Вони забезпечують захист інформації на різних рівнях моделі та сприяють безпечній передачі даних у мережах.

Роль криптографічних протоколів у рівнях моделі OSI:

✱ **Фізичний рівень (Physical Layer)** – криптографія на цьому рівні практично не використовується, але можливі рішення для захисту сигналів від перехоплення (наприклад, захист через спектральне розширення).

✱ **Канальний рівень (Data Link Layer)** – протоколи, такі як MACsec (Media Access Control Security), забезпечують шифрування та контроль цілісності на рівні локальних мереж (LAN).

✱ **Мережевий рівень (Network Layer)** – IPSec (Internet Protocol Security) є класичним прикладом криптографічного протоколу, який шифрує пакети та забезпечує цілісність даних під час їх передачі.

✱ **Транспортний рівень (Transport Layer)** – на цьому рівні працюють протоколи SSL/TLS (Secure Sockets Layer/Transport Layer Security), які забезпечують захищений обмін даними між клієнтами та серверами.

✱ **Сеансовий рівень (Session Layer)** – криптографічні протоколи можуть використовуватися для управління захищеними сеансами зв'язку.

✱ **Рівень представлення (Presentation Layer)** – шифрування та дешифрування даних, цифрові підписи, сертифікація відкритих ключів.

✱ **Прикладний рівень (Application Layer)** – захищені протоколи передачі даних, такі як HTTPS, S/MIME (для електронної пошти), SSH (для віддаленого доступу), PGP (для захисту файлів і повідомлень).

Таким чином, криптографічні протоколи інтегруються в архітектуру OSI для забезпечення конфіденційності, автентифікації та цілісності даних, створюючи багаторівневий підхід до інформаційної безпеки в комп'ютерних мережах.

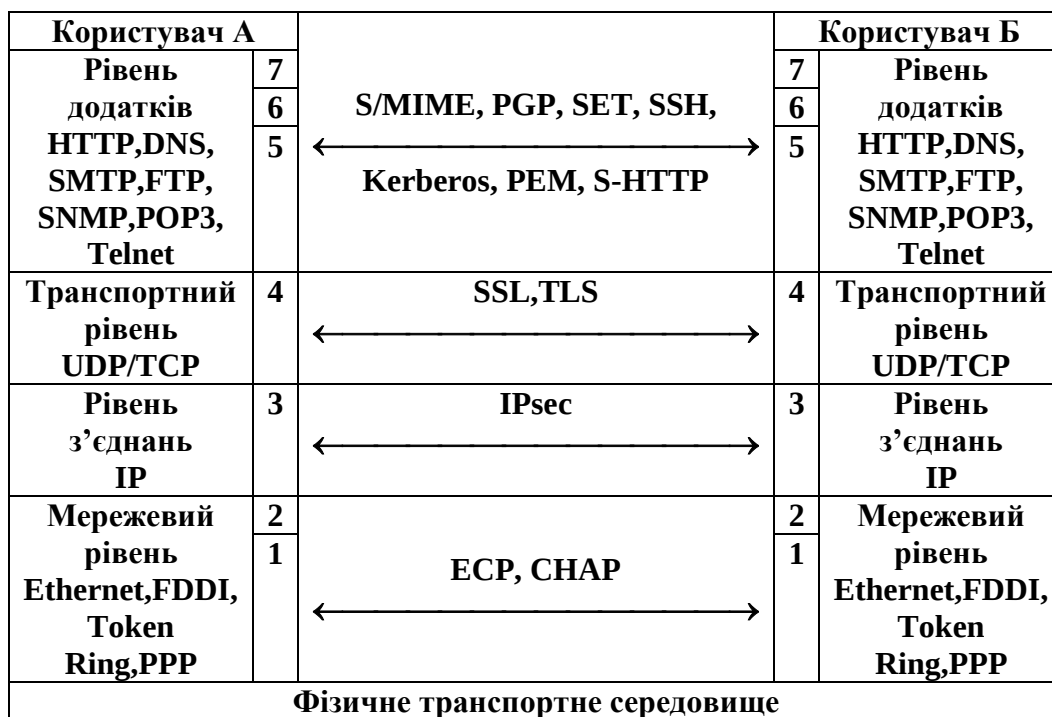


*Рис. 22.1. Схема протоколів взаємодії в моделі OSI
Джерело: [8-9]*

Приклади криптографічних протоколів:

• SSL/TLS (Secure Sockets Layer/Transport Layer Security)

використовується для захищених інтернет-з'єднань. SSL/TLS забезпечує шифрування переданих даних між клієнтом і сервером, що захищає їх від перехоплення сторонніми особами. Цей протокол також підтримує автентифікацію учасників, використовуючи сертифікати відкритих ключів. Важливою особливістю SSL/TLS є можливість домовленості про шифрувальний алгоритм і параметри сесії на етапі рукошлякування. Протокол широко використовується для забезпечення безпеки веб-сайтів, електронної пошти та VPN-з'єднань.

• **IPSec (Internet Protocol Security)**

забезпечує безпечну передачу даних через мережі. IPSec використовує різні криптографічні алгоритми для шифрування та аутентифікації даних, що передаються через Інтернет або приватні мережі. Він функціонує на рівні мережевого протоколу і може забезпечувати як тунелювання, так і транспортування даних в зашифрованому вигляді. IPSec забезпечує цілісність даних, автентифікацію джерела і захист від атак на мережевому рівні, таких як підміна пакунків. Протокол є основою для створення віртуальних приватних мереж (VPN) і забезпечує надійний захист при з'єднаннях між віддаленими мережами.

• **Kerberos**

протокол автентифікації в розподілених системах. Kerberos використовує систему квитків для автентифікації користувачів та сервісів у мережах, що забезпечує високий рівень безпеки без необхідності передавати паролі через мережу. Протокол базується на принципах симетричного шифрування, де клієнт отримує тимчасові квитки для доступу до ресурсів системи. Kerberos також забезпечує взаємну автентифікацію, що дозволяє переконатися, що як користувач, так і сервер є дійсними та не підробленими. Це робить Kerberos важливим компонентом у захищених корпоративних мережах і служить основою для таких технологій, як Active Directory.

• **Diffie–Hellman**

протокол обміну ключами. Протокол Diffie–Hellman дозволяє двом сторонам безпечним чином обмінюватися криптографічним ключем через відкритий канал зв'язку, не передаючи сам ключ. Він базується на математичних обчисленнях, що використовують принципи складності дискретного логарифмування, забезпечуючи таким чином захист від атак на підбір ключа. Завдяки цьому протоколу обидві сторони можуть отримати спільний секретний ключ, який використовуватиметься для подальшого шифрування даних. Diffie–Hellman також є основою для багатьох сучасних криптографічних стандартів, таких як IPsec і TLS.

• **RSA**

протокол для шифрування й підпису даних. Протокол RSA заснований на використанні пари ключів: публічного та приватного, для забезпечення шифрування та цифрового підпису. Публічний ключ використовується для шифрування даних, а приватний — для їх розшифрування, забезпечуючи конфіденційність. Крім того, RSA дозволяє створювати цифрові підписи для перевірки автентичності та цілісності даних. RSA є одним з основних криптографічних алгоритмів,

що використовуються в інтернет-безпеці, зокрема в таких протоколах як SSL/TLS для захищених з'єднань.

Ефективність криптографічного протоколу залежить від його стійкості до атак, таких як перехоплення даних, підміна повідомлень або компрометація ключів. Тому розробка та аналіз таких протоколів є важливим напрямом у сфері інформаційної безпеки. Таким чином, криптографічні протоколи є важливим компонентом сучасної інформаційної безпеки, забезпечуючи захист даних у цифрових системах.

22.2. Розподіл ключів і аутентифікація

Розподіл ключів та аутентифікація є важливими складовими частинами систем безпеки в криптографії. Вони забезпечують конфіденційність, цілісність і автентичність даних, що передаються через небезпечні мережі. Розподіл ключів дозволяє встановити надійні канали для обміну секретною інформацією між учасниками комунікації. Аутентифікація, у свою чергу, гарантує, що кожен учасник може бути ідентифікований та перевірений перед виконанням будь-якої операції. Для забезпечення цих процесів використовуються різноманітні протоколи, такі як симетричне та асиметричне шифрування, а також цифрові підписи. Це дозволяє створити надійні системи захисту даних, що мінімізують ризики атак, зокрема, Man-in-the-Middle.

Розподіл ключів — це процес обміну криптографічними ключами між сторонами для того, щоб вони могли здійснювати зашифровану комунікацію або виконувати інші криптографічні операції. У криптографії розподіл ключів може здійснюватися кількома методами, зокрема через використання асиметричної криптографії (наприклад, RSA або Diffie–Hellman), коли один з учасників передає публічний ключ, а приватний залишається в нього. Інші методи включають використання симетричних ключів, що мають бути збережені в таємниці і передаватися через захищені канали зв'язку.

Аутентифікація — це процес перевірки ідентичності користувачів або систем, що взаємодіють у межах протоколу. Це забезпечує захист від несанкціонованого доступу, підміни або фальсифікації даних. Найпоширенішими методами аутентифікації є використання пароля, біометричних даних або криптографічних засобів, таких як цифрові підписи або аутентифікаційні протоколи (наприклад, Kerberos). Окрім цього, для зміцнення безпеки аутентифікації застосовуються

багатофакторні методи, які вимагають підтвердження ідентичності через кілька незалежних елементів.

Таким чином, процеси розподілу ключів і аутентифікації працюють разом, забезпечуючи надійність і безпеку передачі даних та захист від різноманітних атак, таких як підробка особи або крадіжка ключів.

Основою криптографічного протоколу є криптоалгоритм, при цьому на відміну від шифрування, окрім наявності зловмисника, в криптопротоколах передбачається недовіра між учасниками.

Криптопротоколи можуть бути класифіковані за такими основними напрямками:

- ***Генерація ключів*** - це протоколи для пересилання або узгодження ключів (наприклад, протокол Діффі-Хеллмана).
- ***Аутентифікація*** – підтвердження достовірності джерела, даних або ключів.
- ***Підпис*** – електронний підпис, включаючи звичайний, затемнений чи конфіденційний.
- ***Електронні гроші*** – системи для забезпечення захищених розрахунків.
- ***Протоколи голосування*** – для проведення виборів та перевірки результатів.
- ***Конфіденційні обчислення*** – обчислення функцій з обмеженням доступу до приватних даних учасників.

У протоколах електронних грошей ключова задача — забезпечити неможливість підробки та невідстежуваність транзакцій. Невідстежуваність досягається через механізм сліпих підписів, де банк не може зв'язати підписану купюру з конкретною транзакцією чи користувачем.

Протоколи голосування забезпечують анонімність виборців та правильність підрахунку голосів. Протоколи для конфіденційних обчислень дозволяють кільком учасникам обчислювати спільну функцію, не розкриваючи при цьому приватні дані один одному.

Розрізняють кілька типів атак на протоколи:

1. ***Пасивні атаки*** — націлені на аналіз або підслуховування даних протоколу для отримання необхідної інформації. Це відповідає типу атак на криптосистеми, зокрема, ciphertext-only attack.
2. ***Активні атаки*** — спрямовані на зміну протоколу на користь зловмисника, включаючи вставку, видалення чи зміну повідомлень.
3. ***Пасивне шахрайство*** — коли учасники протоколу намагаються здобути більше інформації, порушуючи умови протоколу.

4. *Активне шахрайство* — включає зміну протоколу з метою досягнення вигоди через підробку повідомлень.

Захист від пасивного шахрайства є обов'язковим для будь-якого протоколу, незалежно від умов, в яких працюють його учасники. Захист від активних шахраїв потребує більш складних механізмів і, інколи, дозволяє своєчасно виявляти підозрілі дії.

У разі утруднень при передачі ключів через захищений канал, можна використовувати певні алгоритми для економії ключів або їх обміну через незахищені канали зв'язку. Наприклад, можна використовувати симетричне шифрування разом з генераторами випадкових чисел для формування сеансового ключа через обмін зашифрованими повідомленнями, що включають випадкові числа та ідентифікатори абонентів.

Захищений обмін ключами через алгоритм рукописання, як-от Діффі-Хеллман, дозволяє учасникам безпечним чином встановлювати спільний сеансовий ключ через відкриті канали зв'язку, спираючись на складність дискретного логарифмування. Однак, цей метод вразливий до атаки типу "агент посередині", що може бути усунено шляхом впровадження систем аутентифікації для учасників протоколу.

Важливою частиною безпеки є ідентифікація користувачів системи, що часто здійснюється через паролі. Для уникнення збереження самих паролів, використовуються хеш-функції, що дозволяють зберігати лише хеш пароля в пам'яті комп'ютера, забезпечуючи більшу безпеку в разі компрометації системи.

Для захисту від таких атак в криптопротоколах застосовуються різні методи, в тому числі використання секретних ключів та механізмів підтвердження ідентичності учасників. Важливим елементом є також створення механізмів для захищеного обміну ключами, наприклад, через протоколи типу Діффі-Хеллмана.

22.3. ПРОТОКОЛИ РОЗПОДІЛУ СЕКРЕТУ

Протоколи розділення секрету є важливими інструментами в криптографії, що дозволяють поділити секрет (наприклад, ключ або пароль) на кілька частин таким чином, що лише певна кількість учасників може відновити оригінальний секрет. Ці протоколи використовуються в ситуаціях, де важливо забезпечити безпеку даних, не дозволяючи жодному учаснику мати повний доступ до секрету, але водночас дозволяючи групі учасників відновити його шляхом комбінування їхніх частин. Одним із

найвідоміших і широко застосовуваних методів є протокол Шаміра, що базується на поліноміальних рівняннях. У цьому протоколі секрет є константним членом полінома, а кожен учасник отримує точку на цьому поліномі. Для відновлення секрету потрібно знати мінімальну кількість точок (зазвичай це кількість учасників, визначених у протоколі, наприклад, 2 з 3 або 3 з 5). Перевагою цього підходу є простота реалізації та висока безпека, оскільки навіть при компрометації кількох частин секрету неможливо відновити сам секрет без необхідної кількості точок.

Іншим варіантом є протокол Басса і Шенкмана, який використовує геометричний підхід. В цьому випадку секрет розділяється на кілька частин, що є точками перетину гіперплощин у просторі. Кожен учасник має свою гіперплощину, і лише при перетині достатньої кількості площин можна відновити секрет. Цей підхід також забезпечує високу надійність і захищає від компрометації секрету. У випадках, коли потрібне розділення секрету між лише двома учасниками, застосовуються методи двочастинного розподілу, де секрет ділиться між ними, і для відновлення необхідно, щоб обидва учасники надали свої частини. Це може бути корисним, наприклад, у ситуаціях, де двоє партнерів повинні спільно приймати рішення або отримувати доступ до системи.

Протокол розділення секрету за допомогою порогових значень є ще одним поширеним підходом, у якому секрет ділиться на кілька частин, і для його відновлення потрібно зібрати певну кількість частин. Це дозволяє знижувати ризик витоку секрету у разі компрометації кількох учасників. Протоколи розділення секрету широко застосовуються в різних сферах, таких як резервне копіювання та відновлення даних, керування доступом до чутливих систем, а також у багатофакторній аутентифікації. Однак для забезпечення безпеки частин секрету важливо належно захищати ці частини, адже їх компрометація або втрата може призвести до втрати доступу до оригінального секрету. Тому правильне зберігання та управління частинами секрету є критично важливим для ефективного функціонування таких протоколів.

22.4. СТАНДАРТИ КРИПТОПРОТОКОЛІВ

Стандарти криптопротоколів є важливими для забезпечення сумісності, безпеки та ефективності криптографічних систем. Вони встановлюють правила для взаємодії між різними системами, забезпечуючи стандартизовані методи шифрування, автентифікації, а також безпечного обміну даними. Серед основних стандартів, що регулюють криптопротоколи, можна виділити кілька основних напрямків:

1. SSL/TLS (Secure Sockets Layer / Transport Layer Security) — це набір криптографічних протоколів, призначених для забезпечення захищеного зв'язку в Інтернеті. SSL був розроблений компанією Netscape, а згодом був замінений на TLS. TLS використовується для шифрування даних, які передаються між клієнтом та сервером, наприклад, у веб-браузерах, при підключенні до вебсайтів через HTTPS. Стандарти TLS визначають процедури для встановлення шифрованих з'єднань, автентифікації учасників і забезпечення конфіденційності.

2. IPsec (Internet Protocol Security) — це набір протоколів для захисту передачі даних на рівні мережі, що використовує криптографію для забезпечення конфіденційності, автентифікації та цілісності даних. IPsec застосовується для захищених VPN-з'єднань (Virtual Private Network), що дозволяє шифрувати та аутентифікувати трафік, що передається через публічні мережі, такі як Інтернет.

3. PGP (Pretty Good Privacy) та GPG (GNU Privacy Guard) — це протоколи для шифрування електронної пошти та забезпечення цифрових підписів. PGP використовує симетричне і асиметричне шифрування для захисту повідомлень. GPG є вільною альтернативою PGP і сумісний з ним. Стандарти PGP/GPG дозволяють користувачам захищати свою кореспонденцію і перевіряти автентичність отриманих повідомлень.

4. Kerberos — це протокол автентифікації, який використовується для забезпечення безпеки в розподілених системах. Він дозволяє користувачам безпечно автентифікуватися в мережі, використовуючи принципи симетричного шифрування. Kerberos застосовується для контролю доступу до мережевих ресурсів, зокрема у великих корпоративних мережах.

5. SHA (Secure Hash Algorithm) — це набір криптографічних хеш-функцій, який використовується для створення унікальних і фіксованих розмірів хеш-значень з вхідних даних. SHA-2 та SHA-3 є сучасними стандартами, що широко застосовуються для цифрових підписів, автентифікації, перевірки цілісності даних та інших криптографічних операцій.

6. RSA (Rivest-Shamir-Adleman) — це один з найпопулярніших криптографічних протоколів для асиметричного шифрування. Він широко застосовується для захищеного обміну ключами та цифрових підписів. RSA базується на складності факторизації великих чисел і забезпечує високу ступінь безпеки при належній довжині ключа.

7. ECDSA (Elliptic Curve Digital Signature Algorithm) — це протокол для створення цифрових підписів, заснований на еліптичних кривих. Він забезпечує ту саму безпеку, що і RSA, але при меншій довжині ключа, що робить його більш ефективним для використання в мобільних пристроях і системах з обмеженими ресурсами.

8. Diffie-Hellman (DH) — це протокол для обміну криптографічними ключами між двома сторонами. В основі його роботи лежить складність обчислення дискретного логарифму. Протокол дозволяє двом сторонам згенерувати спільний секретний ключ через публічний канал зв'язку, не обмінюючись самим секретом.

9. X.509 — це стандарт для цифрових сертифікатів, які використовуються для підтвердження ідентичності учасників у протоколах аутентифікації, таких як SSL/TLS. Сертифікат X.509 містить публічний ключ, підписаний сертифікаційним центром, що підтверджує його справжність.

10. FIPS (Federal Information Processing Standards) — це серія стандартів, встановлених урядом США для використання криптографічних алгоритмів і протоколів в урядових та національних безпекових системах. Наприклад, FIPS 140-2 визначає вимоги до апаратних і програмних засобів для шифрування, а FIPS 197 описує стандарт AES (Advanced Encryption Standard).

Ці стандарти є основою для розробки безпечних комунікаційних протоколів і широко застосовуються у всіх сферах діяльності, де необхідно забезпечити захист інформації, від фінансових установ до урядових організацій. Вони гарантують, що всі учасники обміну даними можуть використовувати надійні методи шифрування, аутентифікації та перевірки цілісності, що є важливими для забезпечення безпеки і конфіденційності.

22.5. ФОРМАЛЬНИЙ АНАЛІЗ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Формальний аналіз криптографічних протоколів є важливою частиною процесу забезпечення безпеки в інформаційних системах. Це метод, який полягає у вивченні криптографічних алгоритмів та протоколів за допомогою математичних і логічних методів з метою виявлення потенційних вразливостей та забезпечення високого рівня захисту інформації. Завдяки формальному аналізу можна значно знизити ймовірність несанкціонованого доступу до важливих даних, а також мінімізувати можливість атак на криптографічну систему.

Першим етапом у формальному аналізі є створення математичної моделі криптографічного протоколу. Це дозволяє описати всі етапи обміну інформацією між учасниками, зокрема процеси шифрування, дешифрування, генерації ключів, автентифікації та підписів. Створення такої моделі є необхідним для подальшої перевірки протоколу на коректність та безпеку. Паралельно з моделлю необхідно сформулювати припущення щодо безпеки, які протокол має забезпечити. Це можуть бути такі вимоги, як конфіденційність, цілісність, автентифікація та відсутність вразливостей до різноманітних атак, зокрема до атак типу *man-in-the-middle*, *replay*-атак або атак на відмову в обслуговуванні.

Наступним етапом є визначення потенційних загроз і атак, які можуть бути спрямовані на систему. Для цього досліджуються різні варіанти атак, наприклад, атаки на шифрування, на автентифікацію, атаки на цілісність або на доступність. Можна також врахувати вразливості в реальних реалізаціях криптографічних алгоритмів, як це було виявлено в багатьох випадках з використанням недостатньо сильних ключів або помилками у впровадженні протоколів. Оцінка ймовірності кожної з таких атак дозволяє виявити найбільш небезпечні уразливості та адаптувати протокол для запобігання таким загрозам.

Завершенням цього етапу є перевірка протоколу на коректність, що включає в себе математичне доведення того, що він виконує необхідні функції без жодних недоліків. Це може включати доказ того, що протокол не дозволяє третім особам дізнаватися конфіденційну інформацію або змінювати передані дані без виявлення. Для цього використовуються різні математичні методи, зокрема теорії складності обчислень, автоматні моделі або формальні системи доказів. Одним із ключових інструментів є використання програмних засобів, таких як ProVerif або AVISPA, які автоматизують перевірку коректності криптографічних протоколів і можуть виявити уразливості на ранніх етапах.

Останнім етапом є виявлення вразливостей у протоколі. Це може бути здійснено через застосування методів аналізу на основі теорії графів, де протокол описується у вигляді графа, або за допомогою спеціалізованих інструментів для пошуку атак. Наприклад, для виявлення слабких місць в алгоритмах шифрування можна використати атаки на факторизацію великих чисел або атаки на дискретний логарифм. З метою забезпечення більшого рівня безпеки протоколу можна скоригувати його таким чином, щоб усунути виявлені вразливості.

Формальний аналіз дозволяє значно підвищити рівень безпеки криптографічних протоколів. Вони можуть бути використані для захисту важливих даних у різних сферах, таких як фінансові системи, державні

інформаційні структури, системи обміну даними між підприємствами. Важливою перевагою формального аналізу є можливість прогнозувати потенційні загрози на етапі проектування, що дозволяє своєчасно вносити необхідні корективи та уникнути можливих катастрофічних наслідків у майбутньому.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 22

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.
4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
6. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
7. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

8. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.
9. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.
10. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.
11. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.
12. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.
13. Спасітельєва, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.
14. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об’єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.
15. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.
16. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142–148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.
17. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.
18. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

19. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.

20. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

РОЗДІЛ 23

АРХІТЕКТУРА СИСТЕМИ ЕЦП



23.1. Основні характеристики архітектури системи ЕЦП

23.2. Управління сертифікатами і ключами

23.3. Управління інфраструктурою відкритих ключів (PKI)

"Безпека інформаційних систем не є результатом випадкових заходів, вона має бути інтегрована в саму архітектуру системи з моменту її створення, щоб забезпечити довіру та надійність всіх електронних операцій."

Bruce Schneier, експерт з безпеки

23.1. ОСНОВНІ ХАРАКТЕРИСТИКИ АРХІТЕКТУРИ СИСТЕМИ ЕЦП

Архітектура системи електронного цифрового підпису (ЕЦП) включає в себе набір механізмів та принципів, які забезпечують створення, перевірку та валідацію цифрових підписів для підтвердження автентичності та цілісності електронних документів. Основною метою архітектури є надання правової сили електронним підписам, що дозволяє забезпечити довіру до електронного документообігу, а також захистити від підробок і змін інформації.

Ключовою складовою системи є інфраструктура управління ключами, що включає сертифікаційні центри (ЦС), які відповідальні за

видачу сертифікатів відкритих ключів та їх перевірку. Приватні ключі підписантів використовуються для створення підписів, а публічні – для їх перевірки. Важливою частиною є зберігання та захист приватних ключів, що здійснюється через спеціальні апаратні засоби, такі як смарт-карти або токени, або через програмні рішення з високим рівнем безпеки.

Процес підписання в системі ЕЦП базується на криптографічних алгоритмах, які включають алгоритми хешування для генерації унікального ідентифікатора документа та підпису його приватним ключем підписанта. Перевірка підпису здійснюється шляхом застосування публічного ключа, що забезпечує перевірку цілісності документа та підтвердження, що підпис був поставлений конкретною особою.

Система також включає сертифікаційні механізми для встановлення довіри між учасниками. Сертифікати, видані сертифікаційними центрами, підтверджують автентичність публічних ключів, що використовуються для перевірки підпису. Це забезпечує правову силу електронних підписів в судових і юридичних справах.

Інтеграція з іншими інформаційними системами, такими як системи аутентифікації та захисту даних, є важливою характеристикою архітектури системи ЕЦП. Крім того, архітектура повинна забезпечувати масштабованість для роботи з великими обсягами даних та великою кількістю користувачів, що робить її адаптивною до змінних умов і вимог.

Одним із важливих аспектів є аудит та прозорість. Система повинна мати механізми для фіксації всіх операцій, пов'язаних із цифровими підписами, що дозволяє здійснювати перевірку дій у разі виникнення спірних ситуацій або спроб несанкціонованого доступу до ключів або підписів.

В цілому, архітектура системи ЕЦП є комплексною і багатофункціональною системою, яка повинна забезпечувати високу ступінь захисту, масштабованість, а також відповідність правовим вимогам для використання в електронному документообігу та електронних транзакціях.

Архітектура системи електронного цифрового підпису (ЕЦП) передбачає принципи побудови апаратно-програмних комплексів, що забезпечують функціонування засвідчувальних центрів, через які корпоративні та індивідуальні користувачі можуть працювати з сертифікатами відкритих ключів. Для цього надаються комплексні рішення, що включають інфраструктуру відкритих ключів (PKI), яка була описана робочою групою PKIX (Public Key Infrastructure Working Group). Система ЕЦП складається з кількох основних компонентів, зокрема

сертифікаційних центрів, користувачів, а також апаратних та програмних засобів для генерації і перевірки підписів.

Сучасні характеристики архітектури системи ЕЦП включають модульність, масштабованість та модель довіри. Вони є критеріями для оцінки якості рішень, представлених на ринку. Серед найбільш відомих і широко використовуваних програмних рішень у світі можна виділити такі системи, як Entrust Authority, iPlanet Certificate Management System, Microsoft Certificate Server, RSA Keon та UNICERT PKI.

Модульність системи ЕЦП означає наявність окремих сервісів, що забезпечують функціонування інфраструктури відкритих ключів. Вони включають сервіси реєстрації, сертифікації, ведення баз даних, статусу сертифікатів (OCSP), фіксації часу, блокування та відміни сертифікатів. Система реєстрації дозволяє перевіряти дані користувачів, аутентифікацію та контролювати повноваження, а також здійснювати консультаційну підтримку. Сервіс сертифікації відповідає за перевірку запитів на сертифікацію та формування сертифікатів, тоді як сервіс ведення баз даних займається зберіганням та публікацією сертифікатів. Важливим елементом є сервіс фіксації часу, що дозволяє засвідчити існування документа на певний момент часу.

Моделі довіри

Моделі довіри визначають, як сертифікаційні центри взаємодіють між собою та забезпечують довіру до видаваних сертифікатів. Ієрархічна модель створює єдину точку довіри, з якої виходять довірчі зв'язки до підпорядкованих сертифікаційних центрів. Ця модель є найбільш традиційною і широко використовуваною, оскільки забезпечує чітку ієрархію довіри, де один центр може виступати як корінь для всіх інших. Мережева модель, з іншого боку, дозволяє встановлювати прямі довірчі зв'язки між кількома ЦСК, що може призвести до більш гнучкої та динамічної інфраструктури. Вибір між цими моделями залежить від конкретних вимог і цілей системи, таких як масштаб, безпека та гнучкість. Крім того, комбінація цих моделей може бути використана для досягнення оптимального рівня довіри та безпеки в складних інфраструктурах. Вони є основою для ефективного функціонування інфраструктури відкритих ключів, де кожна модель довіри може бути адаптована під потреби конкретного підприємства або організації. Моделі довіри є основою для взаємодії різних систем PKI. Існує кілька основних моделей довіри, серед яких найпоширенішими є *ієрархічна модель* та *мережева модель*.

Ієрархічна модель довіри передбачає встановлення єдиної точки довіри між кількома сертифікаційними центрами ключів (ЦСК).

Ієрархічна модель забезпечує наявність одного кореневого центру сертифікації (Root CA), який є головною точкою довіри для всіх підлеглих ЦСК. Кожен підлеглий ЦСК видає сертифікати для своїх підписувачів, базуючись на довірі до кореневого ЦСК. У разі, якщо кореневий ЦСК скасовує сертифікат, це може вплинути на довіру до всіх сертифікатів, що були видані підлеглими ЦСК. Така структура дозволяє централізовано управляти безпекою та надавати чіткі правила для сертифікації та перевірки цифрових підписів. У ієрархічній моделі довіра до одного ЦСК передається вниз по ланцюгу сертифікацій, що дозволяє забезпечити більшу контрольованість і надійність. Однак вона також створює певні ризики, оскільки компрометація кореневого ЦСК може порушити довіру до всієї інфраструктури. У разі потреби можна застосувати процедури відновлення довіри через перевипуск сертифікатів або впровадження додаткових заходів безпеки.



Рис. 23.1. Ієрархічна модель довіри

Джерело: [8-9]

Мережева модель довіри передбачає встановлення прямих довірчих зв'язків між ЦСК, що дозволяє реалізувати метод крос-сертифікації. Мережева модель дозволяє встановлювати прямі довірчі зв'язки між кількома ЦСК без необхідності проходження через кореневий ЦСК. У цьому випадку кожен ЦСК може прямо довіряти іншому ЦСК і використовувати взаємну сертифікацію для підтвердження достовірності сертифікатів. Крос-сертифікація передбачає, що кожен сертифікаційний центр видає сертифікат для іншого ЦСК, підтверджуючи його автентичність і надійність. Ця модель забезпечує більшу гнучкість, оскільки дозволяє організаціям та системам мати власні незалежні сертифікаційні центри, що можуть взаємодіяти між собою. Мережева модель знижує залежність від одного кореневого центру, що робить систему менш вразливою до єдиної точки відмови. Проте ця модель може бути складнішою в управлінні, оскільки вимагає точних домовленостей між всіма учасниками і забезпечення належного рівня довіри між ними. Вона також потребує ефективного контролю за процесами крос-сертифікації для запобігання компрометації довірчих зв'язків.

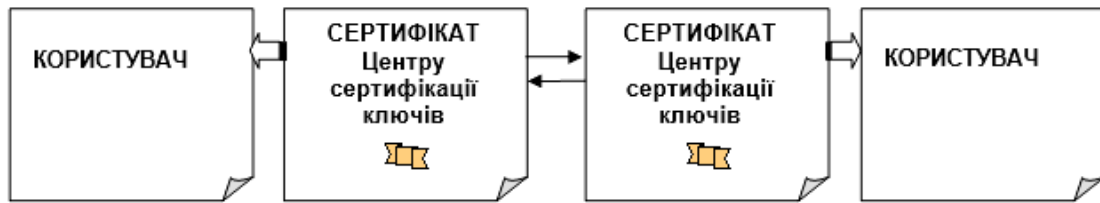


Рис. 23.2. Мережева модель довіри

Джерело: [8-9]

Однією з важливих характеристик архітектури є її **масштабованість**, що дозволяє системам ЕЦП підтримувати велику кількість користувачів і масштабуватися відповідно до зростання потреб у безпеці. Сучасні рішення, як-от Entrust і UNICERT, забезпечують високу масштабованість, що робить їх ідеальними для великих організацій та установ. Усі ці складові разом створюють ефективну систему для забезпечення електронного документообігу з високим рівнем безпеки та зручності для користувачів.

Основні відмінності між моделями довіри стосуються методів побудови ланцюгів сертифікатів і верифікації сертифікатів, виданих різними ЦСК. Ці фактори є важливими для інтеграції різних рішень PKI та визначають ефективність їх взаємодії, що є критичним для корпорацій, які використовують кілька рішень або мають великі інфраструктури. Продукти, що підтримують гібридну модель довіри, як Entrust, RSA і UniCert, забезпечують більш високу гнучкість, порівняно з тими, що підтримують лише ієрархічну модель, як MCS і iPlanet. В Україні, згідно з законом «Про електронний цифровий підпис», найбільш поширеною є ієрархічна модель сертифікації з єдиним коренем, що включає центральний засвідчувальний орган і центри сертифікації ключів. Також передбачена можливість створення трирівневої системи сертифікації для державних органів. Перевагою ієрархічної моделі є простота перевірки сертифікатів, але її недолік полягає в тому, що при порушенні роботи кореневого центру всі сертифікати, підписані цим центром, стають компрометованими. Масштабованість систем PKI часто оцінюється на основі можливості підтримувати велику кількість сертифікатів, а також наявності модульної структури, підтримки різних платформ і відкритих криптографічних стандартів. Крім того, для великих інфраструктур важливою вимогою є наявність механізмів для побудови довірчих відносин в реальному часі та управління привілеями. Оскільки масштаби інфраструктур PKI можуть значно варіюватися, рішення повинні забезпечувати високий рівень безпеки без компромісів щодо ефективності роботи. Важливою характеристикою є здатність інтегруватися з іншими

системами та підтримувати взаємодію з різними реалізаціями PKI, що забезпечує більшу гнучкість в управлінні довірою. У разі компрометації одного з елементів інфраструктури, система повинна мати механізми для оперативного реагування та мінімізації наслідків. Підтримка новітніх стандартів і технологій також є критично важливою для забезпечення довгострокової ефективності та безпеки рішень PKI.

23.2. УПРАВЛІННЯ СЕРТИФІКАТАМИ І КЛЮЧАМИ

Управління сертифікатами і ключами є важливою складовою інфраструктури відкритих ключів (PKI), оскільки забезпечує надійне використання криптографічних методів для захисту інформації в організаціях. Основні аспекти управління сертифікатами і ключами включають їх випуск, публікацію, відгук і припинення дії.

Випуск сертифікатів

Сертифікати видаються центром сертифікації (ЦСК) для ідентифікації суб'єктів та забезпечення їхньої аутентифікації в інформаційних системах. Випуск сертифікатів може бути автоматизований (auto-enrollment) або здійснюватися вручну. Багато сучасних рішень підтримують різні методи інтеграції сертифікатів, зокрема через веб-інтерфейс або e-mail. Наприклад, продукти таких постачальників, як Entrust, iPlanet, Microsoft, RSA, забезпечують зручне управління сертифікатами. Випуск сертифікатів передбачає перевірку заявленої ідентичності суб'єкта, що може включати верифікацію документів або інші методи підтвердження особи. Після успішної перевірки Центр сертифікації генерує сертифікат, що містить відкритий ключ та інформацію про його власника. Для забезпечення безпеки та автентичності сертифікатів часто використовується механізм підпису, де ЦСК підписує сертифікат своїм приватним ключем. Крім того, сертифікати можуть бути видані для різних цілей, таких як шифрування, підписування документів або забезпечення доступу до ресурсів у корпоративних мережах.

Публікація сертифікатів

Публікація сертифікатів здійснюється в каталогах або через сервіси директорій, таких як LDAP або Active Directory. Цей процес дозволяє користувачам доступ до актуальних сертифікатів для перевірки підписів і шифрування даних. Сучасні рішення, такі як Entrust і UNICERT, підтримують публікацію сертифікатів за допомогою DAP, а також LDAP для інтеграції з існуючими інфраструктурами. Публікація сертифікатів також включає забезпечення механізмів для пошуку та доступу до

сертифікатів в реальному часі, що дозволяє користувачам швидко перевіряти їх дійсність. Для підвищення безпеки можуть використовуватись списки відкликаних сертифікатів (CRL), що регулярно оновлюються для запобігання використанню недійсних сертифікатів. Деякі сервіси також підтримують механізм Online Certificate Status Protocol (OCSP), який дозволяє миттєво перевіряти статус сертифікатів без необхідності завантажувати весь список відкликаних сертифікатів. Завдяки цим інструментам забезпечується ефективний і безпечний доступ до сертифікатів в рамках корпоративних і зовнішніх комунікацій.

Відгук сертифікатів

Відгук сертифіката здійснюється у разі його компрометації або інших порушень. Інформація про відгук сертифіката публікується в списках відкликаних сертифікатів (CRL), які регулярно оновлюються для забезпечення доступу користувачів до актуальної інформації. Сучасні сертифікаційні служби використовують також Delta CRL для зменшення обсягу інформації та прискорення процесу оновлення. Крім того, відгук сертифікатів може бути здійснений через протокол OCSP, що дозволяє перевіряти їх статус в реальному часі без необхідності завантажувати весь список відкликаних сертифікатів. Відгук сертифіката є критично важливим етапом для підтримки безпеки, оскільки забезпечує припинення використання скомпрометованих або втрачених сертифікатів. Зазначені методи відгуку сертифікатів допомагають організаціям мінімізувати ризики, пов'язані з витоками інформації та забезпечити відповідність стандартам безпеки. Всі ці заходи сприяють підтримці довіри до системи цифрових сертифікатів, що є основою для безпечних електронних транзакцій та комунікацій.

Управління ключами

Важливою частиною управління сертифікатами є управління криптографічними ключами, що забезпечує захист шифрованих даних і підписів. У багатьох сучасних рішеннях для управління ключами використовуються спеціалізовані сервіси, такі як Key Management Server (KMS) або Hardware Security Modules (HSM), які гарантують безпечне зберігання та обробку криптографічних ключів. Продукти, наприклад, RSA, iPlanet і UniCERT, підтримують розподілене зберігання ключів для забезпечення надійної безпеки. Управління ключами також включає їх генерацію, розподіл, оновлення та відгук, що гарантує безперервність захисту протягом всього життєвого циклу сертифікатів. Крім того, важливою складовою є встановлення політик доступу до ключів, щоб обмежити їх використання лише авторизованими особами або системами.

Сучасні системи управління ключами забезпечують автоматичне оновлення ключів і підтримку багатофакторної аутентифікації для запобігання несанкціонованому доступу. Таким чином, ефективне управління ключами є основою для побудови надійної та безпечної інфраструктури цифрових сертифікатів.

Визначення статусу сертифікатів

Один з важливих аспектів управління сертифікатами — це визначення їхнього статусу в реальному часі. Для цього використовуються протоколи, такі як OCSP (On-line Certificate Status Protocol), який дозволяє в реальному часі перевіряти, чи є сертифікат дійсним. Деякі рішення, зокрема iPlanet, надають власний сервіс OCSP, що дозволяє перевіряти статус сертифікатів через HTTP-запити. Протокол OCSP дозволяє знизити навантаження на інфраструктуру, оскільки він не вимагає завантаження цілих списків відкликаних сертифікатів (CRL), а лише перевіряє статус конкретного сертифіката. Для більш високого рівня безпеки використовуються комбіновані методи, де OCSP може працювати в парі з CRL, щоб забезпечити комплексну перевірку статусу. Багато сертифікаційних центрів пропонують можливість налаштування частоти перевірок та визначення термінів дії сертифікатів для мінімізації ризиків. Це забезпечує не тільки високий рівень надійності, а й швидкість перевірки статусу сертифікатів у реальному часі.

Резервне зберігання пар ключів

Резервне зберігання пар криптографічних ключів є критичним для забезпечення доступу до зашифрованої інформації у випадку втрати або пошкодження ключів. Багато рішень, такі як Entrust, iPlanet і RSA, пропонують різні варіанти для резервного зберігання ключів, забезпечуючи доступ до зашифрованих даних навіть за умови технічних неполадок або зловмисних атак. Для резервного зберігання ключів використовуються як фізичні, так і віртуальні рішення, включаючи розподілені сервери та спеціалізовані сховища, такі як HSM (Hardware Security Module). Сучасні системи забезпечують автоматичне резервне копіювання ключів із шифруванням для запобігання несанкціонованому доступу. Також можливе використання мультифакторної автентифікації для доступу до резервних копій, що додає додатковий рівень безпеки. Окрім цього, важливо забезпечити регулярне оновлення та тестування резервних копій, щоб гарантувати їхню актуальність і цілісність у разі потреби відновлення.

Управління сертифікатами і ключами є комплексним процесом, який забезпечує цілісність, конфіденційність та автентичність інформації в

організаціях. Використання сучасних рішень для управління сертифікатами, таких як Entrust, iPlanet, RSA і UniCERT, дозволяє підприємствам оптимізувати цей процес і підвищити рівень безпеки своїх інформаційних систем.

Видалення або припинення дії сертифікатів у рішеннях iPlanet та RSA здійснюється через Web або адміністратора. MCS пропонує видаляти сертифікати лише через адміністративну консоль.

Усі продукти підтримують публікацію сертифікатів у сервісах каталогів і Active Directory за протоколом LDAP, а також UNICERT і Entrust підтримують DAP.

Користувачі інфраструктури відкритих ключів повинні бути впевнені, що сертифікат чинний. У разі компрометації сертифіката або криптографічних ключів, сертифікат має бути негайно відкликаний ЦСК та внесений до списку відкликаних сертифікатів, доступного для всіх користувачів. Перевірка статусу сертифіката може здійснюватися через списки відкликаних сертифікатів (CRL), змінені списки відкликаних сертифікатів (Delta CRL) або шляхом визначення статусу сертифіката в реальному часі.

Протокол визначення статусу сертифіката в реальному часі (OCSP – Online Certificate Status Protocol) дозволяє визначити актуальний статус сертифіката в реальному часі. Рішення iPlanet надає повноцінний сервіс OCSP, а RSA обмежується сервісом OCSP Responder. Інші продукти використовують додаткове програмне забезпечення для OCSP.

Резервне зберігання пар ключів є важливим аспектом у системах PKI. Всі рішення забезпечують можливість відновлення зашифрованих даних, але реалізація варіюється. Entrust, iPlanet і RSA підтримують резервне зберігання пар ключів для шифрування та електронного підпису, забезпечуючи підвищену безпеку.

Управління інфраструктурою відкритих ключів (PKI) є основним інструментом для спілкування між системою та адміністраторами. Рішення Entrust, UniCERT і iPlanet пропонують потужні інструменти для управління та моніторингу PKI, забезпечуючи зручний доступ до керування інфраструктурою через різні інтерфейси: адміністративні консолі, командний рядок, web-інтерфейси та спеціалізовані модулі.

Управління політиками в інфраструктурі відкритих ключів визначає правила щодо сертифікації та вмісту сертифікатів. Усі продукти надають можливість налаштування політик безпеки та забезпечення гнучкості при зміні існуючих політик на корпоративному рівні.

Аудит і зберігання налаштувань є невід'ємною частиною системи PKI. Продукти Entrust, UniCERT і RSA забезпечують повнофункціональні

засоби для аудиту та створення звітів, що дозволяє здійснювати контроль за станом системи та захищати її від несанкціонованого доступу.

23.3. УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ ВІДКРИТИХ КЛЮЧІВ (PKI)

Управління інфраструктурою відкритих ключів (PKI) є критичним елементом для забезпечення безпеки в сучасних інформаційних системах. PKI забезпечує засоби для створення, розповсюдження, управління, зберігання та відкликання сертифікатів і ключів, що використовуються для аутентифікації, шифрування та підпису даних. Основними складовими PKI є центр сертифікації (ЦС), реєстраційний орган, а також сертифікати та ключі, що використовуються для аутентифікації й забезпечення конфіденційності.

Система PKI забезпечує безпечне управління та обмін інформацією через відкриті канали шляхом використання відкритих і закритих ключів для підтвердження автентичності та цілісності даних. Важливою частиною управління PKI є створення та підтримка політик безпеки, що регламентують процеси видачі, управління та відкликання сертифікатів, а також впровадження процедур для належного моніторингу та аудиту безпеки інфраструктури.

Сучасні системи PKI підтримують інтеграцію з іншими компонентами корпоративних IT-структур, зокрема з системами управління доступом, і можуть працювати з різними протоколами, такими як SSL/TLS для забезпечення безпечного з'єднання між клієнтами та серверами. У свою чергу, впровадження автоматизації процесів у PKI дозволяє знизити ризики помилок і підвищити ефективність управління сертифікатами та ключами, що робить систему більш масштабованою та гнучкою.

Принцип управління інфраструктурою відкритих ключів (PKI) полягає в організації та управлінні всіма аспектами використання криптографії з відкритими ключами для забезпечення безпеки електронної комунікації, автентифікації, цілісності даних та конфіденційності. Це набір стандартів, політик, процедур, програмного забезпечення та апаратних засобів, які забезпечують створення, зберігання, розповсюдження, використання та відкликання цифрових сертифікатів, що підтверджують ідентичність користувачів і пристроїв у мережі. Один із основних елементів PKI — цифрові сертифікати, які містять публічний ключ, інформацію про власника та підпис сертифікаційного центру (CA), що гарантує їх достовірність. Сертифікаційний центр є довіреним суб'єктом, що видає і підписує сертифікати після перевірки ідентичності користувачів

або пристроїв, а реєстраційний центр (RA) виконує роль посередника, перевіряючи ідентичність перед відправленням запиту на отримання сертифіката до СА. Крім того, в PKI використовується довірна модель, яка визначає, хто і як буде довіряти сертифікатам, виданим різними сертифікаційними центрами, що зазвичай організовується через ієрархію, де головний СА має найвищий рівень довіри. Керування ключами є невід'ємною частиною PKI і включає процеси створення, зберігання, захисту, оновлення та відкликання ключів і сертифікатів, що також охоплює контроль за терміном їх дії. Протоколи обміну ключами, що використовуються в PKI, забезпечують безпечний обмін публічними ключами між користувачами та пристроями, гарантуючи конфіденційність і аутентифікацію учасників під час комунікацій у мережі. В результаті принципи PKI забезпечують конфіденційність через шифрування даних за допомогою публічного та приватного ключів, аутентифікацію для підтвердження ідентичності учасників, цілісність даних, перевіряючи їх на зміну під час передачі, і невідкличність, що запобігає запереченню дій користувача завдяки цифровим підписам. Тому PKI є основою для забезпечення безпеки електронних транзакцій, цифрових підписів, захищених з'єднань (наприклад, через SSL/TLS) та захисту даних у хмарних обчисленнях і на мобільних пристроях.

Засоби управління PKI

Засоби управління інфраструктурою відкритих ключів (PKI) включають набір інструментів і технологій, які дозволяють організаціям ефективно управляти сертифікатами, криптографічними ключами та іншими елементами інфраструктури безпеки. Ці засоби забезпечують підтримку всіх етапів життєвого циклу сертифікатів, включаючи їх видачу, відгук, публікацію та перевірку статусу. Вони також включають системи для моніторингу та аудиту, що дозволяють відстежувати стан безпеки та забезпечувати відповідність політикам організації. Важливими компонентами є інструменти для автоматизації процесів, які знижують навантаження на адміністрацію і покращують швидкість реагування на загрози. Засоби управління інфраструктурою відкритих ключів забезпечують надійний захист даних, зменшують ризики компрометації та сприяють збереженню високих стандартів безпеки в організаціях.

Основними компонентами засобів управління PKI є:

1. Центри сертифікації (ЦС) – це ключові елементи PKI, які відповідають за видачу, відкликання і перевірку сертифікатів. Центри сертифікації можуть бути внутрішніми або зовнішніми в залежності від

вимог організації. Вони використовують криптографічні алгоритми для підпису сертифікатів і підтримки довіри до них. Центри сертифікації здійснюють перевірку інформації, що надається суб'єктами сертифікації, перш ніж видати сертифікат. Вони мають важливу роль у забезпеченні безпеки в інфраструктурі відкритих ключів (PKI), гарантуючи, що сертифікати видаються лише тим суб'єктам, які відповідають визначеним вимогам. Вони також здійснюють процес відкликання сертифікатів через публікацію списків відкликаних сертифікатів (CRL) або через реалізацію протоколу OCSP (Online Certificate Status Protocol). Для забезпечення безпеки центр сертифікації зберігає закриті ключі в захищеному середовищі, використовуючи апаратні модулі безпеки (HSM). Центри сертифікації можуть також виконувати моніторинг активності користувачів і сертифікатів для виявлення можливих аномалій чи порушень. Крім того, вони забезпечують обслуговування сертифікатів на протязі їхнього життєвого циклу, оновлюючи сертифікати або замінюючи їх у разі необхідності. Таким чином, функціонування центрів сертифікації є основою для ефективного і безпечного використання інфраструктури відкритих ключів

2. Реєстраційні органи (РО) – відповідають за перевірку ідентичності суб'єктів, які просять сертифікати, а також за процес реєстрації нових користувачів у системі. РО є проміжною ланкою між користувачами та ЦС, що дозволяє гарантувати правильність даних, переданих до центру сертифікації. Реєстраційні органи здійснюють процедуру перевірки особистих даних, таких як паспортні дані, документи, що підтверджують право доступу або інші види ідентифікації, щоб підтвердити, що заявник є законним користувачем. Вони можуть використовувати як фізичні, так і електронні методи для ідентифікації, зокрема відеоконференції або засоби електронного підпису. Після успішної перевірки РО передає дані до центру сертифікації для видачі сертифіката. Крім того, РО має обов'язок перевіряти зміни у даних користувача, щоб забезпечити актуальність інформації в системі. Реєстраційні органи також забезпечують конфіденційність переданої інформації, застосовуючи політики безпеки, що відповідають вимогам законодавства і стандартам. У разі виявлення порушень або неправильних даних, РО може відмовити в реєстрації або відгукнути сертифікат. Цей процес є критичним для підтримки надійності та безпеки всієї інфраструктури відкритих ключів.

3. Системи управління ключами – забезпечують безпечне генерування, зберігання та розподіл криптографічних ключів. До таких

систем належать Hardware Security Modules (HSM) і сервіси типу Key Management Servers (KMS), які гарантують, що приватні ключі не потраплять до зломисників. Системи управління ключами активно використовують високоякісні алгоритми шифрування для забезпечення безпеки під час зберігання ключів, а також для їхнього обміну між користувачами чи іншими компонентами системи. HSM є апаратними пристроями, які спеціалізуються на захисті криптографічних операцій, таких як генерація та підписання даних, зберігаючи ключі в безпечному середовищі. Вони гарантують, що навіть якщо пристрій буде фізично скомпрометований, ключі залишаються захищеними від несанкціонованого доступу. KMS, у свою чергу, є централізованими рішеннями для керування ключами в масштабі організації, забезпечуючи їхнє ефективне використання та безпечне зберігання. Вони інтегруються з іншими компонентами PKI, такими як сертифікаційні центри або реєстраційні органи, для оптимізації процесів криптографії. Для забезпечення безпеки в таких системах часто використовуються додаткові методи контролю доступу, такі як багатофакторна аутентифікація або політики мінімізації привілеїв. Надійні системи управління ключами є невід'ємною частиною забезпечення безпеки в рамках інфраструктури відкритих ключів.

4. Системи публікації сертифікатів – дозволяють організаціям публікувати сертифікати і списки відкликаних сертифікатів (CRL) для забезпечення прозорості і доступності актуальної інформації про сертифікати. Наприклад, LDAP або HTTP сервери використовуються для публікації сертифікатів та надання інформації для перевірки їх статусу. Такі системи забезпечують централізований доступ до сертифікатів, що дозволяє користувачам перевіряти їх дійсність і статус через відкриті канали. Вони також автоматизують процеси публікації CRL, що дозволяє уникнути використання скомпрометованих сертифікатів. Багато сучасних рішень підтримують інтеграцію з іншими системами PKI для полегшення процесу моніторингу та оновлення інформації про сертифікати. Використання таких систем гарантує, що всі учасники можуть швидко і ефективно перевіряти актуальність сертифікатів та своєчасно реагувати на зміни в статусі.

5. Протоколи для перевірки статусу сертифікатів – такі як OCSP (Online Certificate Status Protocol) дозволяють користувачам і системам перевіряти, чи є сертифікат дійсним на момент його використання, що забезпечує вищий рівень безпеки у процесах аутентифікації та шифрування. Протокол OCSP дозволяє отримати

інформацію про статус сертифіката в реальному часі, що забезпечує швидке реагування на його відгук чи припинення дії. Це критично важливо для мінімізації ризиків, пов'язаних з використанням застарілих або скомпрометованих сертифікатів. Впровадження OCSP також допомагає зменшити обсяг даних у порівнянні з традиційними списками відкликаних сертифікатів (CRL). Багато сучасних інфраструктур PKI включають підтримку OCSP для інтеграції з різними сервісами та платформами для покращення безпеки комунікацій.

6. Інструменти моніторингу та аудиту – дозволяють відстежувати стан інфраструктури PKI, виявляти потенційні вразливості, а також забезпечувати дотримання політик безпеки. Регулярний аудит допомагає виявити порушення і швидко реагувати на можливі інциденти. Ці інструменти можуть включати спеціалізовані рішення для моніторингу сертифікатів, ключів та іншої критичної інформації, що дозволяє забезпечити безперервний контроль за їх станом. Вони також можуть відслідковувати доступ до критичних даних та реєструвати дії користувачів для виявлення потенційно небезпечних або несанкціонованих операцій. Важливою частиною моніторингу є автоматизація виявлення аномалій та запуску механізмів реагування на інциденти в реальному часі. Таким чином, системи моніторингу та аудиту є необхідними для підтримки належного рівня безпеки та дотримання нормативних вимог в інфраструктурах PKI.

7. Автоматизація процесів PKI – системи автоматизації можуть включати автоматичне оновлення сертифікатів, автоматичний відгук сертифікатів при виявленні компрометації, а також автоматичну генерацію та розповсюдження сертифікатів для великих організацій з високими вимогами до масштабованості. Це дозволяє значно зменшити навантаження на адміністративний персонал та забезпечити своєчасне реагування на зміни в безпековому середовищі. Автоматизація також включає інтеграцію з іншими інформаційними системами, що дозволяє забезпечити безперервну аутентифікацію і шифрування даних без ручного втручання. Багато рішень дозволяють програмно налаштовувати правила для автоматичного оновлення ключів та сертифікатів відповідно до політик організації. Це забезпечує високу ефективність управління сертифікатами в умовах великих, динамічних інфраструктур, де зміни можуть відбуватися часто. Ці засоби допомагають організаціям підтримувати належний рівень безпеки в інфраструктурі відкритих ключів, знижуючи ризики компрометації даних і забезпечуючи безпеку електронного обміну інформацією.

Управління політиками

Управління політиками застосування сертифікатів є ключовим аспектом для забезпечення безпеки в інфраструктурі відкритих ключів (PKI) та визначає умови і правила використання сертифікатів у різних сферах діяльності організації. Політики застосування сертифікатів дозволяють чітко визначити цілі, для яких видаються сертифікати, наприклад, для аутентифікації, цифрового підпису або шифрування даних, що є важливим для правильної організації криптографічних процесів. Одним з важливих аспектів є встановлення політик довіри, які регулюють, кому організація може довіряти при використанні сертифікатів, а також визначають вимоги до постачальників сертифікатів та криптографічних стандартів, що застосовуються у сертифікатах. Політики також включають правила ідентифікації та верифікації суб'єктів, що отримують сертифікати, зокрема процедури реєстрації та перевірки особистих даних, а також вимоги до багатофакторної аутентифікації.

Крім того, важливо встановити обмеження на використання криптографічних ключів, що забезпечують захист сертифікатів, наприклад, визначити, які операції можна виконувати з конкретними ключами (підписання, шифрування або автентифікація), а також обмеження щодо терміну їхньої дії. Для забезпечення безпеки також необхідно ввести моніторинг та аудит, що дозволяють відстежувати використання сертифікатів і виявляти порушення політик застосування, а також запровадити механізми для оперативного реагування на інциденти безпеки. Окрім того, політики повинні включати процеси оновлення та відгуку сертифікатів у разі компрометації або закінчення їхнього терміну дії, що забезпечить своєчасну адаптацію інфраструктури до нових вимог безпеки. Враховуючи динамічність технологічного середовища, політики повинні бути гнучкими і масштабованими, дозволяючи організації швидко реагувати на зміни в криптографічних стандартах та підтримувати безпеку на високому рівні навіть у великих і складних системах. Таким чином, ефективне управління політиками застосування сертифікатів є важливою складовою для забезпечення надійної та безпечної роботи з інформацією в рамках інфраструктури відкритих ключів.

Реалізація засобів аудиту і зберігання налаштувань в PKI

Реалізація засобів аудиту і зберігання налаштувань в інфраструктурі відкритих ключів (PKI) є критично важливою для забезпечення прозорості, відповідальності та виявлення потенційних загроз безпеці. Аудит в рамках

PKI дозволяє відстежувати всі дії, пов'язані з використанням сертифікатів і ключів, включаючи їх видачу, скасування, оновлення, а також використання для підпису та шифрування даних. Зазвичай це включає запис логів про всі операції, пов'язані з сертифікатами, що дозволяє виявляти можливі порушення політик безпеки або зловмисні дії. Для забезпечення належного аудиту застосовуються спеціалізовані інструменти та сервіси, які дозволяють реєструвати та аналізувати події в режимі реального часу, зокрема засоби для централізованого збору та аналізу логів, такі як SIEM (Security Information and Event Management).

Зберігання налаштувань у PKI також є важливим елементом безпеки, оскільки неправильне управління конфігураціями може призвести до зниження ефективності криптографічного захисту. Налаштування, що стосуються політик застосування сертифікатів, параметрів криптографії, списків відгуків сертифікатів (CRL), а також списків доступу та довіри, повинні бути надійно збережені і захищені від несанкціонованого доступу або змін. Для цього використовуються методи резервного копіювання та шифрування даних, а також забезпечується контроль за їхнім доступом. У великих організаціях може бути організовано централізоване зберігання налаштувань PKI з використанням технологій, таких як HSM (Hardware Security Modules), які забезпечують безпеку як криптографічних ключів, так і конфігураційних файлів. Ключову роль у зберіганні налаштувань також відіграють процедури моніторингу і тестування, що дозволяють визначити, чи відповідають налаштування актуальним вимогам безпеки та чи не відбуваються зміни, які можуть призвести до уразливостей у системі. Таким чином, правильно організований аудит та зберігання налаштувань в PKI є основою для забезпечення цілісності, доступності та конфіденційності даних у межах інфраструктури відкритих ключів.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 23

1. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім.

Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

3. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.

4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.

5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

6. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

7. Костюк , Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.

8. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

9. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.

10. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.

11. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.

12. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.

13. Спасітелева, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною

архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.

14. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.

15. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

16. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142–148. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.

17. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.

18. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

19. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.

20. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке криптографія та яка її роль у забезпеченні інформаційної безпеки?
2. Яка основна різниця між симетричним та асиметричним шифруванням?
3. Як працює алгоритм шифрування RSA і для чого він застосовується?
4. Що таке хеш-функції і яке їх значення в криптографії?

5. Як функціонує цифровий підпис та яку роль він відіграє в забезпеченні автентичності даних?
6. Поясніть, як працює алгоритм AES (Advanced Encryption Standard).
7. Що таке криптографічний протокол TLS і як він забезпечує безпеку даних в Інтернеті?
8. Як використовується концепція "ключів" в криптографії для забезпечення безпеки?
9. Яка роль сертифікаційних центрів у криптографії?
10. Які основні методи аутентифікації користувачів використовуються в сучасних криптографічних системах?
11. Що таке криптоаналіз і чим він відрізняється від криптографії?
12. Як працює метод "грубої сили" в криптоаналізі?
13. Які основні методи криптоаналізу застосовуються до симетричних шифрів?
14. Що таке атака "чорного ящика" в контексті криптоаналізу?
15. Як здійснюється криптоаналіз асиметричних шифрів, таких як RSA?
16. Що таке атака "мідлмен" і як вона загрожує криптографічним системам?
17. Як статистичний криптоаналіз може використовуватися для зламування класичних шифрів?
18. Що таке "диференційний криптоаналіз" і як він застосовується до блочних шифрів?
19. Які сучасні методи криптоаналізу використовуються для атак на алгоритм AES?
20. Як проводиться оцінка стійкості криптографічних алгоритмів до атак?
21. Що таке стеганографія і чим вона відрізняється від криптографії?
22. Як працює метод LSB (Least Significant Bit) у стеганографії для приховування інформації в зображеннях?
23. Які інші медіа, окрім зображень, можуть бути використані для стеганографії?
24. Як стеганографія може бути використана для забезпечення конфіденційності в бездротових мережах?
25. Які методи виявлення стеганографії існують і як вони працюють?

ТЕМА 6. ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ І АУДИТ ІКС

РОЗДІЛ 24 УПРАВЛІННЯ ДОСТУПОМ



24.1. Поняття і технології управління доступом

24.2. Форми подання обмежень доступу

24.3. Дискреційна модель розмежування доступу

24.4. Мандатна модель розмежування доступу

24.5. Рольова модель розмежування доступу

"Безпека системи не полягає в тому, щоб відмовити всім доступ, а в тому, щоб визначити, хто і з якою метою може до неї отримати доступ."

Bruce Schneier, експерт з безпеки

24.1. ПОНЯТТЯ І ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ

Управління доступом – це механізм безпеки, який управляє процесом взаємодії користувачів з ресурсами системи. Якщо цей процес взаємодії стає безконтрольним, то наслідки можуть бути вкрай негативними: це і витoki конфіденційних даних, і втручання у роботу системи з боку не маючих на це повноважень незареєстрованих користувачів, і порушення безпеки системи тощо.

Управління доступом є важливою частиною інформаційної безпеки, яка передбачає контроль за правами доступу користувачів до ресурсів системи, щоб забезпечити їх правильне використання та захист від несанкціонованого доступу. Метою управління доступом є гарантування того, що лише

авторизовані особи мають доступ до конфіденційної або важливої інформації, а також зменшення ризику її втрати чи розкриття.

Поняття управління доступом

Управління доступом включає в себе процеси, методи та технології, що дозволяють визначати, хто має право доступу до яких ресурсів у системі, а також які дії ці користувачі можуть здійснювати. Основні компоненти цього процесу включають:

1. Авторизація — процес надання або обмеження доступу до конкретних ресурсів або дій у системі після перевірки ідентичності користувача.

2. Аутентифікація — перевірка ідентичності користувача перед наданням доступу, що зазвичай здійснюється через паролі, біометричні дані, картки доступу тощо.

3. Аудит доступу — моніторинг і запис дій користувачів у системі, щоб виявити порушення безпеки чи зловживання.

Типи систем управління доступом

1. **Модель DAC (Discretionary Access Control)** — контроль доступу, при якому власник ресурсу самостійно визначає, хто має право доступу до нього. У DAC користувачі можуть передавати свої права доступу іншим особам. Ця модель є гнучкою, але менш безпечною, оскільки власник ресурсу може помилково надавати доступ до важливих ресурсів.

2. **Модель MAC (Mandatory Access Control)** — контроль доступу, при якому доступ до ресурсів обмежений політиками безпеки, визначеними адміністраторами системи або організацією. У цій моделі користувачі не можуть передавати права доступу іншим особам. Моделі MAC є більш безпечними, оскільки доступ до інформації визначається на основі чітких політик, що знижує ймовірність несанкціонованого доступу.

3. **Модель RBAC (Role-Based Access Control)** — контроль доступу на основі ролей користувачів. Кожен користувач отримує роль, яка визначає його права доступу до певних ресурсів. Це дозволяє централізовано керувати правами доступу, зменшуючи складність та підвищуючи ефективність управління. Ролі можуть бути присвоєні користувачам відповідно до їхніх посад чи обов'язків, а не індивідуальних потреб.

4. **Модель ABAC (Attribute-Based Access Control)** — модель доступу, що базується на атрибутах користувача, ресурсу та контексту. Замість того, щоб призначати доступ до конкретних ресурсів, система використовує набори атрибутів для визначення, чи має користувач право

доступу. Ця модель дозволяє застосовувати більш складні умови доступу на основі різних характеристик, таких як час доби, місце розташування або статус користувача.

Технології управління доступом

1. **Системи управління ідентичністю та доступом (Identity and Access Management, IAM)** — це набір технологій і політик, які дозволяють організаціям ефективно керувати доступом користувачів до ресурсів. Вони включають аутентифікацію користувачів, управління правами доступу, моніторинг і аудит доступу, а також інтеграцію з іншими системами безпеки.

2. **Багатофакторна аутентифікація (MFA)** — технологія, яка вимагає від користувача надати більше одного доказу його ідентичності перед тим, як надавати доступ до ресурсів. Це можуть бути комбінації пароля, картки доступу, біометрії, одноразових кодів або інших факторів.

3. **Технології шифрування доступу** — використовуються для захисту даних при їх передачі або зберіганні. Вони гарантують, що навіть у разі несанкціонованого доступу до даних, ці дані залишатимуться захищеними.

4. **Керування привілеями (Privileged Access Management, PAM)** — технології, що забезпечують управління доступом для користувачів з підвищеними привілеями (наприклад, адміністраторів). Це дозволяє мінімізувати ризики, пов'язані з неправомірним доступом до важливих ресурсів.

5. **Системи контролю доступу до фізичних об'єктів (Physical Access Control Systems, PACS)** — технології, що обмежують доступ до фізичних приміщень, зокрема картки доступу, біометричні системи або системи розпізнавання осіб.

6. **Єдиний вхід (Single Sign-On, SSO)** — технологія, яка дозволяє користувачам здійснювати вхід до кількох систем або сервісів за допомогою одного набору облікових даних. Це зручний спосіб централізованого управління доступом, що дозволяє зменшити кількість паролів, які користувачі повинні пам'ятати.

Управління доступом є критично важливим для забезпечення безпеки в організаціях та захисту важливої інформації. Використання відповідних моделей доступу та технологій допомагає забезпечити баланс між доступністю ресурсів і рівнем їх захисту від несанкціонованого доступу.

Модель контрольованого доступу

Важливим напрямом забезпечення безпеки ІКС є впровадження на підприємстві контрольованого доступу. У моделі контрольованого доступу визначаються **об'єкти, суб'єкти, операції і система управління доступом**.

Об'єкти являють собою фізичні ресурси ІКС (різноманітні пристрої, що входять до складу ІКС), а також і логічні ресурси ІКС (файли, мережеві сервіси, додатки), що потребують захисту. Кожен об'єкт має унікальне ім'я, що відрізняє його від інших об'єктів в системі.

Суб'єкт – активна сутність, яка запитує доступ до об'єкта або даним всередині об'єкта. Суб'єктом може бути користувач, програма або процес, який використовує доступ до об'єкта для виконання свого завдання.

Для кожного типу об'єктів існує власний набір **операцій**, які з ними може виконувати суб'єкт.

Сутність контрольованого доступу полягає в тому, щоб обмежити та чітко визначити, які операції (читання, редагування, видалення тощо) у системі може виконувати той чи інший легальний суб'єкт системи. Тобто це система, яка, з одного боку, визначає, кому з суб'єктів, що вже пройшли аутентифікацію, дозволений допуск до тих чи інших об'єктів, з іншого боку, обмежує можливі дії суб'єктів над об'єктами залежно від їх повноважень у системі.

Управління доступом, як правило, реалізується для вирішення таких завдань.

По-перше, це забезпечення конфіденційності інформації шляхом того, що тим суб'єктам, які не входять до кола легальних користувачів тієї чи іншої конфіденційної інформації, доступ до неї не надається.

По-друге, для забезпечення цілісності і доступності інформації шляхом того, що користувачам, які можуть завдати шкоди цілісності або доступності інформації, доступ до неї не надається.

По-третьє, управління доступом дозволяє забезпечувати контроль дій користувачів за рахунок того, що кожен користувач діє строго в рамках своїх повноважень у системі і не може їх ніяким чином перевищити.

По-четверте, управління доступом служить реалізацією принципів мінімізації повноважень і поділу обов'язків, тобто кожен із суб'єктів у системі володіє тільки певним набором прав, який відповідає його посадовим обов'язкам, або завданням, що вирішує даний суб'єкт.

Логічне управління доступом, на відміну від фізичного, реалізується програмними засобами і може бути вбудовано в операційну систему, додатки, додаткові пакети безпеки, бази даних або системи керування телекомунікаціями.

Існують наступні типи технологій управління доступом:

- ➔ використання каталогів (для локальних мереж);
- ➔ використання вебдоступу (для глобальних мереж).

Каталоги

Каталог містить інформацію про мережеві ресурси та користувачів системи, що попередньо були зареєстровані. Більшість каталогів засновані на стандарті **X.500** і мають протокол доступу **LDAP (Lightweight Directory Access Protocol)**, що дозволяє об'єктам і суб'єктам взаємодіяти в системі. Каталог, що містить інформацію про мережеві ресурси та користувачів системи, є важливим елементом для організації управління доступом. Такий каталог зазвичай використовує стандарти X.500, які визначають структуру даних і спосіб їх зберігання у вигляді ієрархічної структури, зокрема деревоподібної організації. Ця структура дозволяє ефективно управляти великою кількістю користувачів і ресурсів, а також забезпечувати зручний доступ до необхідної інформації.

Протокол LDAP (Lightweight Directory Access Protocol) є основним засобом для доступу до цього каталогу. Він дозволяє користувачам і мережевим ресурсам виконувати операції пошуку, оновлення та керування об'єктами в каталозі. Важливим аспектом є те, що LDAP забезпечує зручну та ефективну інтеграцію з іншими системами аутентифікації та авторизації, такими як Active Directory, що широко використовуються для управління обліковими записами в корпоративних мережах. Через LDAP можна реалізувати централізоване управління доступом, що дозволяє зменшити ризики несанкціонованого доступу, а також спростити адміністрування великих і складних мереж.

Об'єкти і суб'єкти в рамках каталогу керуються за допомогою служби каталогу (**directory service**), що дозволяє адміністратору ІКС налаштовувати і керувати процесом ідентифікації, аутентифікації, авторизації і доступом до мережі.

Наприклад, якщо комп'ютерна мережа компанії має доменну структуру, то всі об'єкти і суб'єкти системи реєструються на окремому сервері – контролері домену (**DC – Domain Controller**), на якому і зберігається каталог у вигляді ієрархічної бази даних. Ця база даних використовується службою каталогу (**AD – Active Directory**), що організовує мережеві ресурси і виконує функції керування доступом. Як тільки користувач успішно автентифікує себе на контролері домену, йому стануть доступні певні мережеві ресурси (сервер друку, файловий сервер, поштовий сервер і т. п.) відповідно до налаштувань **AD**.

Керування вебдоступом

Програмне забезпечення керування вебдоступом управляє доступом користувачів до активів компанії при зверненні за допомогою веббраузера. Зазвичай це плагін для вебсервера, що направляє запит на сервер аутентифікації. Після аутентифікації вебсервер відправляє веббраузеру кукі-файл (змістом якого є облікові дані і параметрами платформи з якої проходила аутентифікація) і потім постійно перевіряє, протягом всього сеансу з'єднання, щоб переконатися, що ніхто не перехопив сесію і що вебсервер постійно взаємодіє саме з автентифікованою системою.

Агрегатори медіаконтенту, що пропонують одночасний перегляд свого контенту на 5 пристроях, саме працюють по цій технології.

Якщо сесія зв'язку з вебсервером завершена, але виникає потреба взаємодіяти з ним знову, то повторно проходить аутентифікація, після чого браузеру висилається новий кукі-файл і все почнеться з початку. Ця технологія постійно вдосконалюється у міру поширення і збільшення кількості сервісів електронної комерції, інтернет-банкінгу, вебсервісів і т.п.

24.2. ФОРМИ ПОДАННЯ ОБМЕЖЕНЬ ДОСТУПУ

Після того як користувач, пройшовши аутентифікацію, довів свою легальність, йому надається певний набір прав по відношенню до захищених системою ресурсів. Наділення легальних користувачів правами доступу до ресурсів називається авторизацією. Процедура приведення авторизації в дію називається управлінням доступом (Access Control). Якщо, наприклад, суб'єкт намагається використовувати ресурс із забороненим для нього типом доступу, то механізм управління доступом повинен відхилити цю спробу і, можливо, повідомити систему про цей інцидент з метою генерації сигналу тривоги.

При вирішенні задачі управління доступом до інформаційних ресурсів важливо дотримуватися принципу мінімальних привілеїв, який передбачає, що кожному користувачеві надається лише той набір прав, який необхідний для виконання його функціональних обов'язків. Такий підхід мінімізує потенційні втрати, які можуть виникнути через помилки користувачів або несанкціоновані дії, забезпечуючи високий рівень

безпеки. Рішення щодо прав доступу користувачів повинні ґрунтуватися на політиці безпеки підприємства, яка може бути представлена у вигляді різноманітних правил доступу, зокрема на основі часових обмежень, категорії користувачів або контексту запиту.

Одним з основних принципів є правило «необхідно знати», що означає, що кожен користувач має доступ лише до тих ресурсів, які йому необхідні для виконання службових обов'язків. Це дозволяє значно знизити ризик несанкціонованого доступу до конфіденційної інформації. Окрім того, існують контентно-залежні правила, які обмежують доступ до ресурсів, що містять чутливу інформацію, наприклад, документи з поміткою «секретно», або контекстно-залежні правила, що враховують умови, в яких здійснюється запит, такі як час доби або кількість невдалих спроб аутентифікації.

Матриця прав доступу є універсальною формою подання політики контролю доступу, вона прямо («в лоб») описує для кожного користувача набір конкретних операцій, які йому дозволяється виконувати по відношенню до кожного об'єкту.

Суб'єкти Об'єкти	User 1	User 2	User 3
File 1	Читати і записувати	Читати і записувати	Читати
File 2	Читати і записувати	Немає доступу	Читати
File 3	Записувати	Немає доступу	Читати

Рис. 24.1. Матриця прав доступу

Джерело: [3-6]

Особливістю матриці прав доступу є не тільки її велика розмірність, але і наявність великого числа нульових елементів. Такий вид матриць в математиці називають розрідженими. Нульове значення тут говорить про те, що для даного поєднання {суб'єкт, об'єкт} права доступу не визначені, а саме такі поєднання складають більшість в реальних системах. Властивість розрідженості матриці може бути використано для більш компактного представлення правил доступу.

З кожним об'єктом можна зв'язати список управління доступом (Access Control List, ACL), в якому вказані тільки ті суб'єкти (користувачі), які мають дозвіл на доступ до даного об'єкту (ресурсу). Зрозуміло, що кількість суб'єктів в даному списку буде значно менше загального числа суб'єктів системи. Такі списки повинні бути створені для всіх ресурсів.



Рис. 24.2. Список управління доступом до об'єкту
Джерело: [3-6]

Спосіб опису прав доступу набором списків настільки ж універсальний і гнучкий, як матриця, але разом з тим має більш компактний вигляд, так як він не включає порожні елементи матриці. Список ACL складається з елементів управління доступом (Access Control Element, ACE), кожен з яких описує права доступу певного користувача до даного ресурсу. На рис. список ACL складається з трьох елементів ACE.

Ефективним засобом обмеження доступу є налаштування користувацького інтерфейсу, яке дозволяє адміністратору приховувати або обмежувати доступ до певних функцій або частин файлової системи, навіть не надаючи користувачу можливості побачити ці елементи на екрані. Крім того, в якості альтернативи використовується метод списків управління доступом (ACL), де для кожного ресурсу визначається, які конкретні користувачі мають доступ до нього. Такий підхід є більш компактным порівняно з використанням матриці прав доступу, яка в свою чергу може бути дуже громіздкою для великих систем.

Права доступу можуть бути визначені як по відношенню до ресурсів, так і по відношенню до користувачів. В останньому випадку його називають списком дозволів (Capability). На рис. показаний список дозволів, які має користувач User 1 по відношенню до ресурсів File 1, File 2 і File 3.



Рис. 24.3. Список дозволів користувача User 1
Джерело: [3-6]

Матриця прав доступу може бути дуже корисною для відображення всієї інформації про доступ до ресурсів, однак її реалізація часто

ускладнена через велику кількість елементів. В таких випадках використовуються більш компактні представлення, наприклад, збереження прав доступу в списках для кожного ресурсу або для кожного користувача. Ці списки мають ту ж саму інформацію, що й матриця прав доступу, але займають менше місця та не містять порожніх елементів. Інші варіанти «стиснення» матриці прав доступу включають групування прав для певних категорій користувачів, що дозволяє ще більше оптимізувати процес управління доступом.

Що стосується авторизації, то існують два основні підходи: централізований і децентралізований. При централізованій авторизації є єдиний орган, що приймає рішення щодо надання прав доступу до ресурсів, в той час як при децентралізованій авторизації функції управління правами доступу можуть бути делеговані окремим користувачам або групам. У залежності від потреб та архітектури системи можуть застосовуватися різні методи доступу, зокрема дискреційний доступ (DAC), мандатний доступ (MAC) і рольовий доступ (RBAC), або їх комбінація для забезпечення максимального рівня безпеки та гнучкості в управлінні доступом.

24.3. ДИСКРЕЦІЙНА МОДЕЛЬ РОЗМЕЖУВАННЯ ДОСТУПУ

Дискретна модель розмежування доступу (DAC) є одним із основних підходів до управління доступом у комп'ютерних системах, де власники ресурсів (файлів, баз даних, програм тощо) мають можливість самостійно визначати, хто має доступ до їхніх ресурсів і в якому обсязі. У такій моделі доступ до інформації чи ресурсів визначається за допомогою прав доступу, призначених власниками ресурсів. Власники можуть надавати різні права іншим користувачам, зокрема право на читання, запис, виконання або інші операції з ресурсом.

Однією з основних особливостей цієї моделі є можливість передачі прав доступу між користувачами, що забезпечує гнучкість, але також створює ризики для безпеки, оскільки користувачі можуть випадково або навмисно передавати доступ до чутливих ресурсів неналежним особам. Зазвичай у рамках DAC права доступу надаються на основі ієрархії прав, і доступ може бути наданий не лише окремим користувачам, але й групам або ролям. Це дозволяє створювати ефективні механізми управління доступом у невеликих або середніх мережах, де власники ресурсів можуть самостійно контролювати доступ до своїх файлів чи програм.

Однак дана модель має суттєві недоліки з точки зору безпеки, оскільки її гнучкість може призвести до несанкціонованого доступу чи зловживання правами. Саме тому для більш критичних та безпечних середовищ застосовуються більш строгі моделі, такі як обов'язковий контроль доступу (MAC), де доступ до ресурсів визначається на основі політик безпеки, а не на волі власника ресурсу. У підсумку, хоча дискретна модель розмежування доступу є широко використовуваною завдяки своїй простоті та зручності, її обмеження з точки зору безпеки призводять до потреби в більш строгих підходах у високозахищених системах.

Існує три принципових підходи до керованого управління доступом: дискреційне (виборче) розмежування доступу, мандатне розмежування доступу та рольове розмежування доступу. Кожен з цих підходів має свої особливості, переваги та недоліки.

- ➔ **Дискреційне розмежування доступу (DAC)** — це модель, в якій власник ресурсу (наприклад, файлу чи програми) має право самостійно визначати, хто і який доступ має до його ресурсу. Це дозволяє власнику ресурсу надавати або обмежувати доступ користувачів до ресурсів на свій розсуд. Права доступу можуть бути передані іншому користувачеві. Основною перевагою є гнучкість і зручність управління доступом, але є ризик несанкціонованого доступу через людський фактор або ненавмисне передавання прав.
- ➔ **Мандатне розмежування доступу (MAC)** — це більш строгий підхід, де доступ до ресурсів контролюється на основі політик безпеки, які визначають адміністратори системи, а не власники ресурсів. У цьому підході доступ обмежується на основі рівня конфіденційності або інших критеріїв, що зазвичай визначаються організацією. Користувачі не можуть змінювати або передавати права доступу, що забезпечує більш високий рівень безпеки, але й знижує гнучкість системи.
- ➔ **Рольове розмежування доступу (RBAC)** — це підхід, в якому доступ до ресурсів надається на основі ролей, які визначаються в організації. Кожен користувач отримує роль (наприклад, адміністратор, користувач, гість) і відповідно до цієї ролі йому надаються певні права доступу до системи. Це забезпечує централізоване управління доступом, зменшує кількість помилок і спрощує адміністрування, оскільки ролі можна легко оновлювати та змінювати.

Кожен з цих підходів має свої переваги в різних контекстах використання, і вибір між ними залежить від вимог до безпеки, гнучкості та зручності управління доступом у конкретній організації або системі.

		Об'єкти			
		O ₁	O ₂	O ₃	O ₄
Суб'єкти	S ₁	-	+	-	-
	S ₂	-	+	+	+
	S ₃	+	-	+	+
	S ₄	+	-	+	-

Рис. 24.4. Матриця доступу в дискреційній моделі
Джерело: [1-7]

Кожна з моделей використовує різні методи для управління доступом суб'єктів до об'єктів, кожна має свої переваги і обмеження. Вибір оптимальної моделі управління доступом слід проводити на основі цілей бізнесу і цілей безпеки компанії. Деякі компанії використовують тільки одну модель, інші комбінують їх для отримання необхідного рівня захисту. Ці моделі вбудовані в ядро різних операційних систем і в багатьох випадках підтримуються додатками.

Система, яка використовує дискреційне (виборче) управління доступом (**DAC – Discretionary Access Control**) дозволяє власнику ресурсу визначати, які суб'єкти можуть використовувати цей ресурс. Ця модель називається **дискреційною (виборчою)**, тому що управління доступом засновано на рішеннях власника.

Управління доступом по дискреційній моделі ґрунтується на формуванні так званої матриці прав доступу. Рядки і стовпці даної матриці відповідають відповідно суб'єктам і об'єктам ІКС, а на перетині цих рядків і стовпців записані операції, які можна здійснити над об'єктом, а також додаткові умови (наприклад, час і місце дії), тобто в клітинах матриці знаходяться права, які даний суб'єкт має стосовно даного об'єкта.

Існують такі дозволи доступу:

- ✱ «Неможливо отримати доступ» (*No Access*);
- ✱ «Читання» (*Read*);
- ✱ «Запис» (*Write*);
- ✱ «Виконання» (*Execute*);
- ✱ «Видалення» (*Delete*);
- ✱ «Зміна» (*Change*);
- ✱ «Повний доступ» (*Full Control*).

Наприклад, атрибут **«Читання»** дозволяє читати файл, але не вносити в нього зміни; атрибут **«Зміна»** дозволяє читати, записувати, виконувати і видаляти файл, але не змінювати його атрибути або власника

файла; атрибут **«Повний доступ»** дозволяє проводити будь-які дії з файлом, дозволами на доступ до нього і володінням ним.

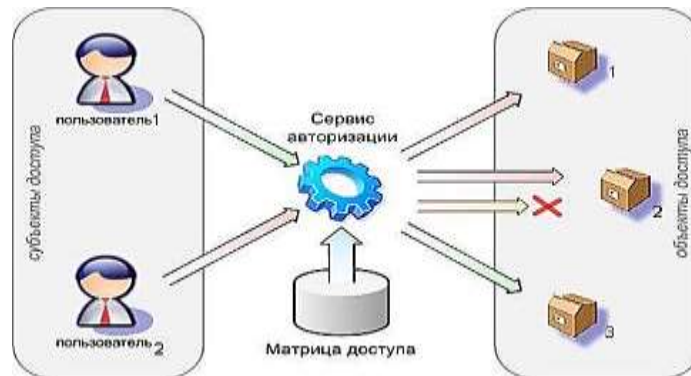


Рис. 24.5. Схема дискреційної моделі управління доступом.
(Суб'єкт доступу «Користувач № 1» має право доступу тільки до об'єкта доступу № 3, тому його запит до об'єкта доступу № 2 відхиляється. Суб'єкт «Користувач № 2» має право доступу як до об'єкта доступу № 1, так і до об'єкта доступу № 2, тому його запити до даних об'єктів не відхиляються)

Джерело: URL:

<https://www.netacad.com/courses/cybersecurity/cyberops-associate>

Отримавши запит на доступ до даних від користувача, дискреційна модель звіряє, чи представлений цей користувач у списку, і чи відповідає його рівень доступу тим даним, які він запитує.

Матриця доступу зберігається не у вигляді двовірного масиву, а по стовпцях, тобто для кожного об'єкта підтримується список «допущених» суб'єктів разом з їх правами (**список управління доступом ACL (Access Control List)**). За допомогою списків нескладно додати права або явним чином заборонити доступ. Переважна більшість операційних систем і систем управління базами даних реалізують саме виборче управління доступом.

При великій кількості користувачів виборчий доступ стає вкрай складним для адміністрування. У цьому випадку застосовують мандатний доступ.

24.4. МАНДАТНА МОДЕЛЬ РОЗМЕЖУВАННЯ ДОСТУПУ

Мандатна модель розмежування доступу (Mandatory Access Control, MAC) є потужним механізмом управління доступом, що базується на централізованому контролі доступу до інформаційних ресурсів. У рамках

цієї моделі доступ користувачів до різних об'єктів системи, таких як файли, бази даних або інші ресурси, визначається не волею власників об'єктів, а відповідно до заздалегідь заданих політик безпеки, які встановлюються адміністратором системи. Ці політики ґрунтуються на рівнях безпеки або мітках, які прикріплюються до кожного об'єкта і визначають, які користувачі мають доступ до цих об'єктів. Такі мітки, як «Конфіденційно», «Тайно» або «Загальнодоступно», вказують на рівень чутливості даних, а доступ до них можливий тільки для користувачів, які мають відповідний рівень дозволу.

Однією з ключових характеристик мандатної моделі є те, що користувачі не можуть змінювати рівні доступу або передавати свої права іншим користувачам, на відміну від дискреційної моделі. Усі права доступу визначаються центральною системою і строго контролюються, що забезпечує високий рівень безпеки. Система політик, яка регулює доступ, може бути побудована на таких принципах, як політика найменших привілеїв, де користувачам надається доступ лише до необхідних для виконання їх обов'язків ресурсів, а також політика обмеженого доступу, що передбачає, що користувачі можуть працювати лише з тими даними, які їм необхідні для їх функціонування.

Мандатний доступ є методикою, що забезпечує високий рівень безпеки даних і є найкращим вибором для організацій, де необхідно гарантувати найсуворіші умови захисту інформації. Це можуть бути урядові, військові установи або інші організації, для яких безпека інформації є критично важливою. Основною особливістю мандатного доступу є централізоване управління авторизацією та доступом, яке здійснюється повноважним органом, найчастіше операційною системою.

У системах мандатного доступу операційна система сама приймає рішення про надання доступу до об'єктів інформації, що дає змогу мінімізувати людський фактор у процесі управління безпекою. Рішення приймаються динамічно, ґрунтуючись на простих правилах, які розробляються відповідними уповноваженими особами, враховуючи політику безпеки організації.

Правила надання доступу зводяться до порівняння рівня секретності об'єкта та рівня допуску суб'єкта. Всі користувачі та об'єкти інформаційної системи розподіляються на групи, кожна з яких має свій рівень секретності або допуску. Об'єкти класифікуються за рівнем секретності (наприклад, «конфіденційно», «таємно», «цілком таємно»), а суб'єкти (користувачі) мають визначений рівень доступу, який відповідає певному рівню допуску.

Типове правило в мандатній системі полягає в тому, що суб'єкту дозволяється доступ до об'єкта лише в тому випадку, якщо рівень допуску

цього суб'єкта відповідає або перевищує рівень секретності об'єкта. Такі правила дозволяють системі автоматично контролювати доступ до інформації, не потребуючи додаткового втручання адміністраторів.

Наприклад, у матричній формі це правило може бути представлене наступним чином: для кожного об'єкта (наприклад, файлу чи документа) буде визначено його рівень секретності, а для кожного користувача — рівень допуску. Якщо рівень допуску користувача дорівнює або вищий за рівень секретності об'єкта, то доступ до нього дозволяється. В іншому випадку доступ блокується. Такий підхід дозволяє чітко контролювати і забезпечувати необхідний рівень безпеки в організації.

Мандатний доступ є ефективним механізмом для управління інформаційною безпекою, оскільки всі права доступу регулюються згідно з визначеними політиками безпеки, що дозволяє забезпечити захист інформації від несанкціонованого доступу та витоків даних.

Рівень секретності об'єктів \ Рівень допуску суб'єктів	Рівень від цілком таємно і нижче	Рівень від таємного і нижче	Рівень даних для службового використання
Цілком таємно	Доступ дозволений	0	0
Таємно	Доступ дозволений	Доступ дозволений	0
Дані для службового користування	Доступ дозволений	Доступ дозволений	Доступ дозволений

*Рис. 24.6. Правило мандатного доступу, представлене у вигляді матриці
Джерело: [1-6]*

У мандатній моделі доступу користувачі мають мітки, які відповідають певним рівням секретності, і для кожного рівня доступу визначені чіткі політики. Наприклад, є політика «Читання тільки з нижчого рівня» (Read Down, Write Up), де користувач може отримати доступ лише до даних, які мають більш низький або рівний рівень секретності, і може записувати інформацію тільки на більш високі рівні секретності. Іншою політикою є «Читання тільки з більш високого рівня» (Read Up, Write Down), де користувач може читати дані тільки з більш високих рівнів секретності, але може записувати лише на більш низькі рівні. Такі політики забезпечують захист даних від несанкціонованого доступу і дозволяють гнучко налаштовувати доступ до інформації.

Мандатна модель знаходить своє застосування в тих сферах, де забезпечення високого рівня безпеки є критично важливим, таких як державні та військові організації. Це дозволяє організувати чіткий контроль над інформацією, що має різні рівні секретності, і запобігти

витоку важливих даних. Завдяки строгим політикам контролю доступу, система може запобігти несанкціонованому доступу до критичної інформації, навіть якщо користувач має фізичний доступ до системи.



Рис. 24.7. Приклад реалізації мандатної моделі доступу
Джерело: [1-6]

У моделі мандатного управління доступом (**MAC – Mandatory Access Control**) користувачі і власники даних не можуть самостійно визначати, хто може мати доступ до файлів. Остаточне рішення приймає операційна система, і це рішення може не збігатися з бажаннями користувача. Ця модель є більш структурованою і жорсткою.

При **мандатному доступі** всі користувачі діляться на групи відповідно до дозволеного рівня доступу до ресурсів. Кількість груп істотно менше, ніж користувачів, оскільки в одну групу можна об'єднати багатьох користувачів. У той же час можливо, що один користувач може входити в кілька різних груп.

Доступ до ресурсів ІКС при такій моделі розмежування доступу заснований на використанні так званих **міток конфіденційності** об'єктів і **рівнів допуску** суб'єктів.

Мітки конфіденційності об'єктів

Під мітками конфіденційності мається на увазі рівень конфіденційності, який присвоюється об'єкту ІКС. Наприклад, для інформації можуть бути встановлені чотири типи міток конфіденційності – **несекретна інформація, інформація тільки для службового користування, секретна** і **цілком таємна інформація**, позначені відповідними мітками.

Рівні допуску суб'єктів

Відповідно, для суб'єктів вводиться поняття рівня допуску. Для того щоб визначити, чи може той чи інший суб'єкт отримати доступ до того чи іншого об'єкта, порівнюється рівень допуску суб'єкта і мітка конфіденційності об'єкта. Якщо рівень допуску не поступається мітці конфіденційності або перевершує її, то доступ надається. Наприклад, якщо суб'єкт має рівень доступу для службового користування, то він отримує доступ до всіх об'єктів з мітками секретності **«НЕ ТАЄМНО»** і **«ДЛЯ СЛУЖБОВОГО КОРИСТУВАННЯ»**, але при цьому не має доступу ні до яких об'єктів з іншими мітками.



Основною перевагою мандатної моделі є її здатність забезпечувати високу безпеку, оскільки доступ до ресурсів суворо контролюється за рівнями секретності і не залежить від волі користувачів. Однак, цим самим модель є менш гнучкою в порівнянні з іншими підходами, такими як дискреційне розмежування доступу. Її складність також полягає у впровадженні та адмініструванні, особливо в великих організаціях, де потрібно налаштувати велику кількість політик доступу. Зважаючи на це, мандатна модель розмежування доступу є надзвичайно корисною в умовах, де забезпечення конфіденційності та цілісності інформації є критичним, а контроль доступу має бути максимально жорстким.

З цих переваг, в свою чергу, слідують і недоліки. Доступ до об'єктів одного рівня секретності надається або обмежується спільно. Немає можливості ТЕМАити всю безліч об'єктів з рівнем секретності, наприклад, **«ДЛЯ СЛУЖБОВОГО ВИКОРИСТАННЯ»** на підмножини. Не можна надати будь-якому суб'єкту доступ до об'єктів з міткою конфіденційності рівня **«секретно»**, а частину, документів, допустимо, **«ДЛЯ СЛУЖБОВОГО КОРИСТУВАННЯ»** зробити для нього недоступними тому, що ці документи не відносяться до його сфери діяльності, а стосуються зовсім інших питань. Виходячи з принципу мінімізації повноважень, це було б важливо зробити, але мандатна модель розмежування доступу цього не дозволяє.

Ця модель застосовується в середовищі, в якій класифікація інформації та конфіденційність надзвичайно важливі, наприклад, у військових організаціях. На базі цієї моделі розроблені спеціалізовані версії *Unix-систем*, наприклад, *SE Linux, Trusted Solaris*. Компанії не можуть просто перемикатися між використанням *DAC* і *MAC*. Їм потрібно спеціально придбати для цього операційну систему, що спроектована та реалізує правила *MAC*.

24.5. Рольова модель розмежування доступу

Рольова модель розмежування доступу (RBAC) є важливою концепцією в управлінні безпекою, яка ґрунтується на наданні доступу до ресурсів в залежності від ролей користувачів у системі. Кожен користувач отримує одну або кілька ролей, що визначають його доступ до ресурсів і прав на виконання дій у системі. Цей підхід дозволяє централізовано та ефективно управляти доступом, спрощує адміністративні завдання та знижує ризики, пов'язані з помилками в налаштуванні доступу.

Основні компоненти рольової моделі включають ролі, користувачів, дозволи та ресурси. Ролі є абстракцією, що визначає набір дозволів для виконання певних дій, таких як читання, запис або зміна даних. Користувачі, в свою чергу, можуть бути прив'язані до однієї або кількох ролей, що дає їм можливість здійснювати різні операції в системі, залежно від їхніх обов'язків та функцій. Дозволи визначають конкретні права доступу, а ресурси — це елементи, до яких надається доступ, наприклад, файли, бази даних або сервери.

Переваги рольової моделі полягають у її простоті та ефективності. Адміністратор може легко призначати ролі користувачам, що значно знижує складність управління доступом у великих системах. Завдяки централізованому управлінню ролями знижується ймовірність помилок, пов'язаних з вручну налаштованими доступами для кожного окремого користувача. Крім того, ця модель забезпечує масштабованість, оскільки для додавання нових користувачів достатньо лише призначити їм відповідні ролі, не потребуючи кожного разу налаштування індивідуальних прав доступу.

Однак рольова модель не є універсальним рішенням для всіх типів організацій чи систем. Вона може бути обмеженою, коли необхідно впровадити більш гнучкі умови доступу або специфічні правила для окремих користувачів. Наприклад, у випадках, коли доступ до ресурсів залежить від комбінації кількох факторів, рольова модель може бути недостатньо ефективною. У таких випадках можуть використовуватись додаткові моделі доступу, такі як атрибутивне чи політико-орієнтоване управління доступом.

Попри ці обмеження, рольова модель є однією з найбільш використовуваних і перевірених на практиці моделей, адже вона забезпечує високий рівень безпеки, простоту адміністрування і ефективний контроль над доступом у багатьох інформаційних системах, від корпоративних мереж до хмарних сервісів та баз даних.

Рольова модель ґрунтується на так званих ролях суб'єктів ІКС. По суті, вона є оптимізацією дискреційного розмежування доступу. Під

роллю в даній моделі мається на увазі сукупність прав доступу суб'єкта до об'єктів ІКС. Тобто існує якесь еталонне значення цих прав доступу суб'єкта до об'єкта, яке одного разу зберігається та іменується якоюсь назвою. Ця назва далі називається **роллю**. Рольова модель розмежування доступу дійсно є оптимізацією дискреційного розмежування доступу і забезпечує ефективніше управління доступом до ресурсів інформаційно-комунікаційних систем (ІКС). В основі цієї моделі лежить поняття ролі, яка визначає набір прав доступу суб'єкта (користувача) до конкретних об'єктів ІКС. Роль, таким чином, є заздалегідь визначеним іменованим набором дозволених операцій або прав доступу, що приписуються певним категоріям користувачів відповідно до їхніх посадових обов'язків або функцій у системі.

Кожна роль в рамках рольової моделі обмежує доступ до ресурсів, базуючись на принципі мінімальних привілеїв, тобто надаючи користувачу лише ті права, які необхідні для виконання його функцій. Наприклад, роль "користувач" може передбачати лише права на перегляд інформації, роль "редактор" — додатково права на зміну інформації, а роль "адміністратор" може надавати права на керування всіма аспектами системи, включаючи налаштування і адміністрування користувачів та доступу.

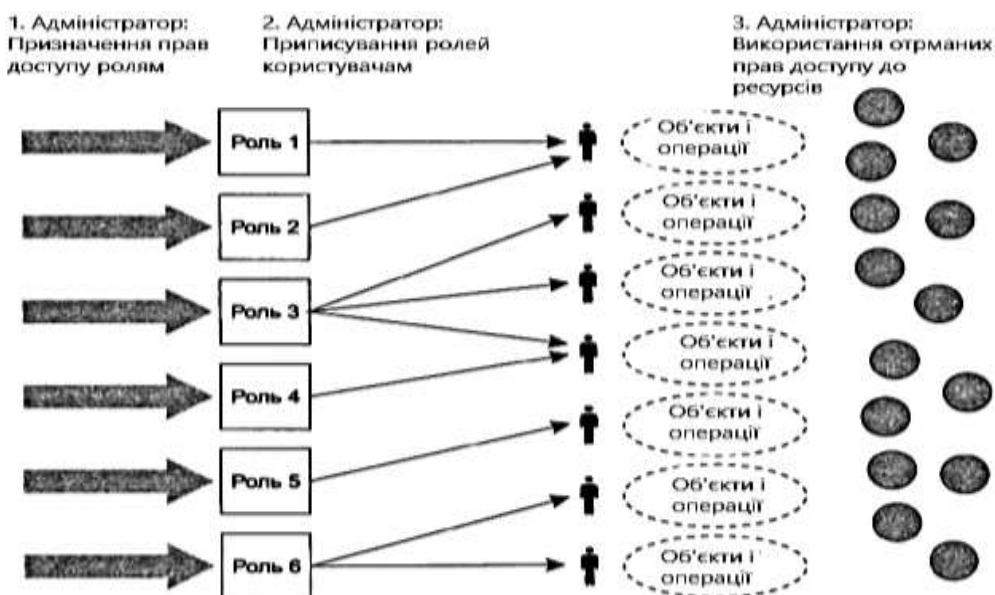


Рис. 24.8. Рольове розмежування доступу
Джерело: [1-6]

Один із головних аспектів рольової моделі полягає в тому, що вона централізує управління доступом, дозволяючи адміністраторам швидко та

ефективно налаштовувати і змінювати рівень доступу користувачів шляхом зміни ролей. Це знижує кількість помилок, які можуть виникнути через індивідуальні налаштування доступу, що характерно для дискреційного підходу. Крім того, рольова модель дозволяє легко адаптувати систему до змін у організаційній структурі або в обов'язках користувачів, оскільки для зміни прав доступу достатньо змінити роль, а не вручну коригувати доступ для кожного користувача.

Отже, рольова модель розмежування доступу забезпечує не лише ефективне управління правами користувачів, а й підвищує безпеку ІКС, зменшуючи можливості для зловживання та помилок у налаштуваннях доступу.

У контексті рольової моделі розмежування доступу, кожна роль в системі визначає набір прав доступу, що відповідають функціям та обов'язкам користувача в організації. Наприклад, роль "системний адміністратор" має стандартний набір прав, таких як доступ до конфігураційних файлів, можливість налаштування мережових з'єднань або управління користувацькими акаунтами. Ці права необхідні для того, щоб адміністратор міг підтримувати і управляти інфраструктурою та забезпечити безперебійну роботу системи.

Роль "начальника відділу" може включати права доступу до інформації, що стосується певного підрозділу організації, таких як перегляд і редагування звітів, доступ до специфічних баз даних або внутрішніх документів. Водночас, ця роль не передбачає прав на налаштування системи або доступ до критичних для безпеки елементів інфраструктури.

Роль "оператора" обмежується лише правами, необхідними для виконання своїх операційних завдань, таких як перегляд даних, виконання рутинних операцій або надання технічної підтримки, без можливості зміни налаштувань системи чи доступу до конфіденційної інформації.

Роль "бухгалтера" передбачає доступ до фінансової інформації, звітів і документів, але без права змінювати конфігурацію системи або керувати іншими користувачами. Зазвичай такій ролі надаються права для роботи з рахунками,

обліковими записами та іншими фінансовими документами, але без доступу до більш чутливих адміністративних функцій.

Таким чином, рольова модель дозволяє чітко визначити, який доступ має бути надано користувачам в залежності від їхніх посадових обов'язків. Це значно знижує ймовірність помилок або зловживань, оскільки кожен користувач має доступ тільки до тих ресурсів, які йому необхідні для виконання своїх завдань.

Роль у контексті систем управління доступом дійсно відображає діяльність користувача на підприємстві, а саме його трудові обов'язки та функції в межах організації. Кожен користувач отримує певну роль, яка чітко визначає його права та обов'язки в системі, що дозволяє ефективно організувати доступ до ресурсів і забезпечити їх захист.

Робота рольової системи передбачає, що кожен користувач в системі буде віднесений до конкретної ролі, що є набором прав доступу до різних об'єктів ІКС. Наприклад, роль "бухгалтер" надає доступ до фінансових документів і облікових записів, але не дозволяє змінювати системні налаштування, що характерно для ролі "системний адміністратор". Роль "менеджер" може включати доступ до звітів і стратегії, але обмежувати доступ до конфіденційної інформації, яка не відноситься до його функцій.

Після призначення ролі користувачеві, його доступ до інформації та можливості в системі будуть залежати лише від тієї ролі, яку йому присвоєно. Це дозволяє уникнути необхідності кожного разу вручну визначати права доступу для кожного окремого користувача, значно спрощуючи управління доступом та знижуючи ризики помилок або несанкціонованого доступу до чутливої інформації.

Таким чином, рольова модель дозволяє організації ефективно контролювати доступ до ресурсів, знижуючи ймовірність порушень безпеки та забезпечуючи більшу гнучкість в управлінні правами доступу. Вона дозволяє реалізувати принцип найменших привілеїв, надаючи користувачам лише ті права, які необхідні для виконання їхніх обов'язків.

Переваги у рольовій моделі розмежування доступу

У цьому випадку досягається ряд. По-перше, додавання нового суб'єкта не вимагає заповнення рядка матриці при наявності підходящої ролі. При цьому роль вільна від того недоліку, який є в мандатній моделі розмежування доступу. Можна ролі, наприклад адміністратора, надати

доступ

до файла з рівнем секретності «Секретно», але який має відношення до питань адміністрування системи і при цьому не надати їй права доступу до інших об'єктів, які в мандатної моделі мали б такі самі мітки конфіденційності.

Недоліки у рольовій моделі розмежування доступу

Проте є й свої недоліки у рольовій моделі розмежування доступу. У класичній рольовій моделі створюються ролі для суб'єктів, про групування об'єктів мови не йде, тобто об'єкти описуються незалежно окремими стовпцями в матриці, як в дискреційній моделі. По суті, при формуванні такої матриці різниця полягає в тому, що кожним рядком є не суб'єкт, а роль. Якщо для кожного суб'єкта потрібна окрема роль – всі вони такі незамінні, несхожі один на одного, абсолютно унікальні. Таке трапляється в невеликих організаціях, де кожен співробітник виконує ряд функцій, практично не маючи ніякої заміни, ніякої допомоги з боку інших користувачів. Тому що є, припустимо, один системний адміністратор, один бухгалтер, один генеральний директор, один менеджер з продажу і у кожного з них є свій унікальний набір прав в системі. У цьому випадку під кожного з них доводиться створювати окрему роль, а рольове розмежування доступу зводиться до дискреційної моделі, тобто ніякої оптимізації не відбувається.

Рольова система управління доступом поєднує в собі риси **мандатного** і **дискреційного методів** управління доступом, де доступ до ресурсів надається на основі ролей, що визначаються адміністраторами системи. Вона дозволяє централізовано керувати правами доступу, забезпечуючи більш ефективний контроль над великими обсягами користувачів і ресурсів. Користувачам надаються ролі, які відповідають їхнім функціональним обов'язкам, що дозволяє мінімізувати ризики від несанкціонованого доступу до чутливих даних. Крім того, рольова модель дозволяє знижувати адміністративні витрати на управління доступом, оскільки зміни в політиках доступу можна впроваджувати через оновлення ролей, не змінюючи прав кожного окремого користувача.

Яку модель управління доступом вибрати?



Вибір моделі управління доступом залежить від типу організації, її розміру, вимог до безпеки та особливостей роботи з інформацією.

Рольова модель є оптимальним вибором для великих підприємств, які мають складну організаційну структуру та великий штат співробітників,

зокрема, коли підприємство займається кількома видами економічної діяльності. Ця модель дозволяє значно спростити та автоматизувати процес управління доступом, що важливо для компаній з багаточисельним персоналом. У такій моделі доступ до ресурсів не залежить від конкретного користувача, а лише від ролі, яку йому надано. Це робить адміністрування більш ефективним, оскільки змінювати права доступу потрібно лише на рівні ролей, а не для кожного окремого користувача. Якщо співробітник звільняється, просто призначити роль новому співробітнику, і йому автоматично надаються відповідні права доступу. Цей підхід добре підходить для великих підприємств, де важливі швидкість і масштабованість.

Мандатна модель, у свою чергу, підходить для організацій, де безпека є пріоритетною. Це можуть бути закриті підприємства, державні органи або військові установи, де обробляється інформація з високим рівнем секретності. У такій моделі доступ до ресурсів базується на категорії безпеки користувача, і права доступу встановлюються централізовано та з урахуванням різних рівнів доступу. Це дозволяє створити чітку ієрархію доступу до інформації, що забезпечує високу безпеку та контроль за доступом. Однак, ця модель вимагає більшої уваги та складнішого адміністрування порівняно з рольовою.

Дискреційна модель є найпростішою в реалізації та використовується в організаціях з невеликим або середнім рівнем вимог до безпеки. Вона надає більше контролю самій особі або власнику ресурсу, який може самостійно визначати, хто має доступ до його даних. Однак, у випадку з великими підприємствами або організаціями, де контроль доступу потребує високого рівня централізації та стандартів безпеки, дискреційна модель може бути менш ефективною.

Таким чином, вибір моделі залежить від потреб організації в управлінні доступом і рівня вимог до безпеки. Для великих підприємств з різними видами діяльності та складною структурою перевагу краще надавати рольовій моделі, для закритих організацій, що потребують високого рівня контролю, — мандатній, а для менш вимогливих організацій або для менших за розміром підприємств підходить дискреційна модель.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 24

1. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. — Київ : Держ. торг.-екон. ун-т, 2023. — 376 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ;

ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

3. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.

4. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Порівняльний аналіз рішень для забезпечення контролю та управління привілейованим доступом в іт-середовищі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 98–112.

5. Shevchenko, S., Zhdanova Y., Skladannyi, P., & Boiko, S. (2022). Інсайтери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 175–185.

6. V. Shapoval, et al., Automation of Data Management Processes in Cloud Storage, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 410–418.

7. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233.

8. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 99–120.

9. Жданова, Ю., Шевченко, С., Спасітелєва, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.

10. P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 240–245.

11. F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021).

12. M. TajDini, et al., Wireless Sensors for Brain Activity—A Survey, Electronics 9(12), iss. 2092 (2020) 1–26.

13. V. Zhebka, et al., Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3288 (2022) 149–155.

14. V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.
15. Y. Sovyn, et al., Minimization of Bitsliced Representation of 4×4 S-Boxes based on Ternary Logic Instruction, in Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 12–24.
16. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 56–66.
17. N. Dovzhenko, et al., Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes, in: Cybersecurity Providing in Information and Telecommunication Systems vol. 3421 (2023) 278–283.
18. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148.
19. A. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.
20. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

РОЗДІЛ 25
РЕЄСТРАЦІЯ ПОДІЙ В СИСТЕМІ І АУДИТ



25.1. Реєстрація подій

25.2. Протоколювання й аудит

25.3. Функціональні компоненти й архітектура аудиту

25.1. РЕЄСТРАЦІЯ ПОДІЙ

Управління доступом і реєстрація подій в системі є важливими складовими стратегії безпеки будь-якої інформаційної системи, забезпечуючи контроль над тим, хто має доступ до ресурсів, і відстежуючи всі значущі дії, що відбуваються в системі. Управління доступом відповідає за забезпечення того, щоб лише авторизовані користувачі могли взаємодіяти з системними ресурсами, а реєстрація подій дозволяє фіксувати всі операції, що допомагають у моніторингу та аудиті безпеки.

Процес управління доступом складається з кількох важливих етапів. Перший етап — це ідентифікація користувача, під час якої визначається особа того, хто намагається отримати доступ до ресурсу. Ідентифікація зазвичай здійснюється за допомогою логіна або іншого унікального ідентифікатора. Другий етап — це аутентифікація, яка підтверджує ідентичність користувача, часто через паролі, біометричні дані або криптографічні ключі. Третій етап — авторизація, що визначає, які саме дії або ресурси будуть доступні користувачу після його аутентифікації. Крім того, важливим аспектом є аудит, який передбачає фіксацію всіх дій

користувача для подальшого аналізу. Цей процес дозволяє виявити порушення політик доступу та вчасно реагувати на потенційні загрози.

Реєстрація подій є невід'ємною частиною управління доступом, оскільки вона дозволяє зафіксувати всі важливі операції в системі. Це може включати як нормальні дії, так і спроби несанкціонованого доступу, зміни в налаштуваннях системи чи інші аномальні події. За допомогою реєстрації подій можна здійснювати моніторинг за діяльністю користувачів та виявляти підозрілі або несанкціоновані дії в системі. Збирання та збереження цих подій дозволяє проводити аудит, виявляти зловмисні атаки, аналізувати причини інцидентів безпеки та вживати відповідних заходів.

Зв'язок між управлінням доступом та реєстрацією подій є критичним для загальної безпеки системи. Ефективне управління доступом допомагає обмежити можливість несанкціонованого доступу, а реєстрація подій дозволяє вчасно виявити й проаналізувати порушення безпеки. Наприклад, коли користувач намагається отримати доступ до ресурсу, який йому не належить, система може зафіксувати таку спробу у журналі подій, що дозволить адміністраторам виявити порушення та вжити відповідних заходів. Завдяки такому моніторингу та запису подій можна створити ефективну систему попередження, що допоможе запобігти інцидентам безпеки.

Таким чином, взаємодія між управлінням доступом та реєстрацією подій є основою для забезпечення безпеки інформаційних систем, адже обидва компоненти працюють разом, щоб зберегти контроль над доступом до важливих ресурсів і своєчасно виявляти потенційні загрози.

Реєстрація подій і аудит є невід'ємною складовою частиною системи безпеки, що дозволяє забезпечити цілісність, конфіденційність і доступність даних. Ці процеси допомагають відслідковувати дії користувачів, а також виявляти та реагувати на потенційні загрози та порушення безпеки. Реєстрація подій передбачає збір, зберігання і аналіз інформації про всі важливі операції, що відбуваються в інформаційній системі. Це може включати спроби доступу до системи, використання ресурсів, зміни в конфігураціях або навіть виконання потенційно шкідливих програм. Для того, щоб ці події могли бути ефективно відслідковані, вони записуються в журнали подій, які містять таку інформацію, як дата і час дії, ідентифікатор користувача, тип дії і результат, що дозволяє провести докладний аналіз і виявити аномалії, що можуть свідчити про порушення безпеки.

Завдяки системі реєстрації подій адміністратор може здійснювати моніторинг системи, оперативно реагувати на спроби несанкціонованого

доступу або інші потенційно небезпечні дії. Аудит в свою чергу є важливою частиною процесу перевірки ефективності існуючих заходів безпеки. Аудитори перевіряють, чи відповідає система безпеки політикам організації, чи здійснюються необхідні заходи контролю доступу, чи є правильне шифрування даних та моніторинг подій. Аудит також передбачає оцінку ризиків та уразливостей у системі, що дає змогу виявити потенційні слабкі місця. Крім того, в ході аудиту проводиться перевірка журналів подій на наявність підозрілих або несанкціонованих дій, що дозволяє своєчасно реагувати на інциденти.

У результаті, ці два процеси — реєстрація подій і аудит — забезпечують не тільки виявлення порушень безпеки, але й допомагають організаціям відповідати вимогам нормативних актів, таких як GDPR або HIPAA. Вони є важливими для підтримки довіри клієнтів, партнерів і регулюючих органів, а також для забезпечення належної безпеки інформаційних систем. Здійснення регулярних аудитів і належна реєстрація подій дозволяють організаціям виявляти потенційні загрози на ранніх етапах, що допомагає запобігти серйозним інцидентам і мінімізувати можливі збитки. Тому ці практики є необхідними для ефективного управління інформаційною безпекою та гарантування захисту даних.

Реєстрація подій (протоколювання) – це збір і накопичення інформації про події в інформаційній системі.

Аудит – це аналіз накопиченої інформації, що проводиться в режимі реального часу, або періодично (наприклад, раз в день) з метою розслідування інцидентів безпеки ІКС.

Аудит є критично важливим інструментом для виявлення порушень безпеки, оскільки він дозволяє ретельно аналізувати дії, що відбуваються в системі, і фіксувати будь-які аномалії або підозрілі активності. Виявлення факту порушення за допомогою аудиту дає змогу оцінити характер впливу на систему, зокрема визначити, чи був здійснений несанкціонований доступ, чи є спроби маніпулювання даними або інші шкідливі дії. Також аудит допомагає з'ясувати, як далеко зайшло порушення: чи мова йде лише про спробу доступу або ж про фактичне витікання або модифікацію даних. Крім того, аудит надає цінну інформацію для подальшого розслідування інциденту. Використовуючи дані з журналів подій, адміністратор або аудитор може відтворити хронологію подій, з'ясувати точний шлях порушника в системі, а також визначити його дії на кожному етапі. Ця

інформація може бути вкрай важливою для встановлення особи порушника і розробки ефективних заходів для його затримання або блокування доступу. Окрім того, аудит пропонує шляхи для виправлення ситуації: від коригування уразливостей до удосконалення процедур доступу та моніторингу.

У результаті аудит не лише дозволяє своєчасно виявляти порушення, але й забезпечує можливість швидко реагувати на них, мінімізуючи потенційні наслідки для системи. Це також допомагає організації розробити стратегію для покращення безпеки, що дозволяє знижувати ризики в майбутньому.

Оперативний аудит з автоматичним реагуванням на виявлені нештатні ситуації (щонайменше – засоби оповіщення адміністратора, а іноді її засоби активної протидії зафіксованим порушенням) називається *активним*.

Однією з обов'язкових функцій аудиту є визначення користувачів, які причетні до зафіксованих подій у системі. Це дозволяє не лише виявити потенційні порушення безпеки, але й точно ідентифікувати осіб, що здійснюють підозрілі або несанкціоновані дії. Такий процес є надзвичайно важливим для розслідування інцидентів безпеки, оскільки дозволяє відновити хронологію подій, визначити їх причину та масштаб, а також сприяє виявленню уразливостей системи.

Підсистема аудиту забезпечує важливу властивість захищеної інформаційно-комунікаційної системи (ІКС) — **спостережність**. Спостережність означає здатність системи надавати чітке та прозоре відображення всіх дій, що відбуваються в її межах, і при цьому гарантувати можливість визначення конкретних користувачів, які здійснили ці дії. Це сприяє не лише моніторингу поточного стану безпеки, а й створює умови для ефективного виявлення та реагування на порушення, оскільки кожна дія залишається зафіксованою з точною інформацією про виконавця.

Таким чином, аудит є критично важливим елементом для досягнення повної спостережності в системі, що дає змогу забезпечити високий рівень безпеки, знизити ймовірність порушень та значно полегшити процес їх розслідування.

При протоколюванні в інтересах забезпечення безпеки інформації фіксуються не всі події, а тільки ті, що стосуються захисту інформації. Як приклади подій, що реєструються, можна навести вмикання та вимикання системи, вхід користувачів у систему та вихід із неї, невдалі спроби

аутентифікації, доступ суб'єктів до об'єктів, друк документів, зміну повноважень суб'єктів відносно об'єктів тощо. Більшість з цих подій пов'язані з діями суб'єктів системи до їх можливого доступу до конфіденційної інформації, а друк документів є одним із способів реалізації витоку інформації. Якщо документ не можна жодним способом скопіювати на носій, відправити по електронній пошті, зняти скріншот, то існує ще одна можливість його надрукувати.

Журнал реєстрації

Журнал реєстрації — це основний інструмент для фіксації подій та дій, що відбуваються в інформаційно-комунікаційній системі (ІКС). Він записує всі важливі операції, які можуть стосуватися безпеки, а також діяльності користувачів та адміністраторів системи. Цей журнал є необхідним компонентом системи аудиту, оскільки дозволяє відслідковувати події, пов'язані з доступом, змінами в системі, а також будь-які підозрілі дії.

Журнал реєстрації містить детальну інформацію про кожну подію, зокрема:

- **Час та дата** події.
- **Ідентифікатор користувача** або суб'єкта, що ініціював подію.
- **Тип події** (наприклад, вхід у систему, зміна налаштувань, спроба доступу до забороненого ресурсу тощо).
- **Результат події** (успішний або неуспішний).
- **Додаткові параметри**, які можуть включати дані про змінені об'єкти або ресурси.
- **IP-адреса** або інші дані, що дозволяють визначити місцезнаходження користувача чи джерело доступу.

Правильно організований журнал реєстрації має великий потенціал у виявленні аномалій та порушень, адже дозволяє не лише відслідковувати факти доступу, але й ідентифікувати зловмисні спроби, підозрілі дії або несанкціоновані зміни в системі.

Важливо, щоб журнали були надійно захищені від несанкціонованого доступу або модифікацій, адже їх змінювання може приховати сліди порушень. Для цього застосовуються різноманітні механізми шифрування та контролю доступу до журналів, а також політики зберігання та архівації даних, щоб забезпечити можливість їх подальшого аналізу у разі необхідності.

Для реєстрації подій створюється спеціальний файл (або група файлів), так званий журнал реєстрації, який є основним засобом фіксації всіх подій і дій в системі. Журнал реєстрації містить детальну інформацію

про події, що відбуваються в інформаційній або комп'ютерній системі, а саме про всі спроби доступу до ресурсів, зміну налаштувань, а також будь-які інші дії, які можуть мати значення для безпеки або функціонування системи.

Журнал реєстрації забезпечує можливість детального аналізу дій користувачів, адміністративних змін, а також непередбачуваних подій, таких як помилки чи несанкціоновані спроби доступу. Це дозволяє адміністраторам або іншим уповноваженим особам здійснювати моніторинг і виявляти потенційні загрози. Записи в журналі зазвичай містять інформацію про тип події, дату і час її виникнення, ідентифікацію користувача або процесу, який ініціював подію, а також деталі щодо результатів дії (наприклад, успішний або неуспішний доступ).

Дані з журналу реєстрації є важливими для проведення аудиту системи безпеки, а також для відновлення інформації після інцидентів. Журнали часто використовуються для розслідування порушень, зломів або інших проблем, що виникли в системі. Тому важливо, щоб журнал реєстрації був належним чином захищений від модифікацій, оскільки зміни в ньому можуть призвести до втрати важливої інформації про інциденти.

Залежно від вимог безпеки, журнали реєстрації можуть бути локальними або централізованими, де зберігаються записи з кількох систем або пристроїв. У деяких випадках може застосовуватися спеціальне шифрування для захисту журналів, що гарантує їхню цілісність і конфіденційність.

Записи журналу зазвичай містять інформацію про:

- ➔ дату і час події, що дозволяє в подальшому відновити хронологію подій;
- ➔ ідентифікатор суб'єкта, що ініціював подію, для того щоб в подальшому визначати, хто з суб'єктів відповідальний за ту чи іншу подію;
- ➔ тип події, а також її результат – успіх або невдача, тобто те, що дозволить визначити, здійснилося чи щось в системі чи ні, і якщо так, то що конкретно;
- ➔ джерело запиту, тобто, наприклад, який конкретний вузол мережі з'явився джерелом запиту;
- ➔ імена порушених об'єктів та опис змін, внесених до баз даних засобів захисту інформації.

Це, власне, те, що дозволяє визначати, які саме зміни були проведені внаслідок тієї чи іншої події в інформаційній системі, і таким чином

оцінити, чи несуть вони ту чи іншу загрозу для інформаційної системи, чи є вони частиною реалізації якогось шкідливого впливу.

Які події реєструвати? З яким ступенем деталізації?

Для ефективного управління безпекою інформаційно-комунікаційних систем важливо визначити, які події слід реєструвати в журналах та з яким ступенем деталізації це необхідно робити. Реєстрація подій є важливим аспектом моніторингу безпеки та забезпечення цілісності системи, оскільки вона дозволяє виявити потенційні порушення або аномалії в роботі системи. Всі важливі події, що відбуваються в системі, повинні бути зафіксовані для подальшого аналізу, розслідування та виявлення можливих загроз.

Одними з основних подій для реєстрації є авторизація та аутентифікація користувачів, оскільки ці події безпосередньо пов'язані з доступом до ресурсів системи. У цьому випадку слід реєструвати успішні й неуспішні спроби входу, а також інформацію про тип аутентифікації, джерело запиту (наприклад, IP-адресу) та причину неуспішного входу. Також важливо фіксувати події, пов'язані з доступом до чутливих ресурсів, таких як спроби читання, запису, зміни або видалення файлів. Це дозволяє відслідковувати дії користувачів і визначати, хто, коли і які операції виконував з важливими даними.

Іншим важливим аспектом є реєстрація адміністративних операцій, таких як зміна прав доступу, інсталяція нових програм або зміна конфігурації системи. Ці події можуть мати серйозні наслідки для безпеки, тому їх слід реєструвати з детальною інформацією про того, хто і які зміни вніс. Також слід фіксувати аномальні події та спроби атак, такі як спроби несанкціонованого доступу, DDoS-атаки, або спроби експлуатації уразливостей. Деталізація таких подій повинна включати тип атаки, джерело та дії, які були здійснені для запобігання або нейтралізації загрози.

Реєстрація подій також включає моніторинг виконання процесів та програм, що мають відношення до системи безпеки. Важливо відстежувати запуск, зупинку або помилки в процесах, оскільки це може вказувати на неполадки або спроби саботажу. Події, пов'язані з мережею, також повинні бути обов'язково зафіксовані, зокрема, коли користувачі підключаються до системи через різні протоколи або використовують підозрілі IP-адреси.

Ступінь деталізації записів залежить від критичності події та важливості її для системи. Наприклад, для подій, пов'язаних з безпекою або адміністративними змінами, слід використовувати високу деталізацію. Це може включати в себе додаткові параметри, як-то джерело запиту, тип дії, результат, а також метадані для більш точного відновлення хронології

подій. Для менш важливих подій, які не несуть безпосередньої загрози безпеці, можна застосовувати спрощене протоколювання, реєструючи тільки основні деталі, такі як час і тип події.

Важливо зазначити, що реєстрація подій повинна здійснюватися централізовано, що дозволить здійснювати моніторинг і аудит в реальному часі. Це допомагає не тільки своєчасно реагувати на порушення безпеки, але й надавати необхідні дані для подальшого розслідування інцидентів.

На подібні питання неможливо дати універсальні відповіді. Занадто велике або докладне протоколювання не тільки знижує продуктивність системи (що негативно позначається на доступності), а й ускладнює аудит, тобто не збільшує, а зменшує інформаційну безпеку.

Розумний підхід до протоколювання стосовно роботи операційних систем пропонується в *«Помаранчевої книзі»*, де виділені наступні події:

- ✱ вхід в систему (успішний чи ні);
- ✱ вихід із системи;
- ✱ звернення до віддаленої системи;
- ✱ операції з файлами (відкрити, закрити, перейменувати, видалити);
- ✱ зміна привілеїв чи інших атрибутів безпеки (режиму доступу, рівня благонадійності користувача і т. п.).

Ще одне важливе поняття, яке фігурує в *«Помаранчевої книзі»*, – вибіркове протоколювання як щодо користувачів (уважно стежити тільки за підозрілими), так і у відношенні подій.

Огляд груп подій і дій, які можуть бути виявлені і внесені до журналу

Огляд груп подій і дій, які можуть бути виявлені та внесені до журналу реєстрації, є важливою складовою безпеки інформаційних і комунікаційних систем (ІКС). Це дає змогу здійснювати моніторинг активностей, виявляти аномалії, визначати можливі загрози і забезпечувати належний контроль за станом системи. Події, які фіксуються в журналі реєстрації, поділяються на кілька основних груп, кожна з яких має специфічне значення для забезпечення безпеки.

Перша група подій включає події аутентифікації та авторизації користувачів. Вона охоплює реєстрацію всіх спроб входу до системи: успішних і неуспішних, а також часи доступу та виходу. Крім того, реєструються події, пов'язані зі зміною паролів, а також підключення з нових або підозрілих IP-адрес. Це дозволяє виявити потенційні загрози на ранніх етапах, наприклад, при несанкціонованих спробах доступу до системи.

Другу групу складають події доступу до ресурсів системи. Реєстрація цих подій дозволяє контролювати доступ до чутливих або критичних даних, таких як файли, бази даних або інші важливі ресурси. Сюди входить фіксація будь-яких дій, що стосуються змін або запису даних, таких як створення, редагування або видалення файлів. Важливою є також реєстрація доступу до адміністративних інтерфейсів, що надають користувачам можливість виконувати адміністративні дії.

Третя група подій стосується адміністративних дій, які виконують адміністратори або користувачі з високими правами доступу. Це включає реєстрацію змін у правах доступу, інсталяцію або видалення програмного забезпечення, а також зміни в конфігураціях системи, що можуть мати вплив на її безпеку. Події, пов'язані зі створенням або видаленням користувачів, також є важливими для моніторингу та аудиту, оскільки зміна складу користувачів може впливати на загальну безпеку організації.

Четверта група подій включає інциденти безпеки та аномалії, які можуть свідчити про порушення або загрози. Це можуть бути спроби несанкціонованого доступу, дії, що свідчать про можливий злом системи, або аномальні запити до системи. Виявлення таких подій є критично важливим для оперативного реагування на загрози та мінімізації потенційної шкоди.

П'ята група охоплює події моніторингу мережі, що дозволяють відслідковувати підключення до мережі, використання специфічних протоколів або виявлення підозрілих мережевих дій, таких як сканування портів чи завантаження шкідливих програм. Реєстрація таких подій дає змогу виявити вторгнення або зловмисну активність на рівні мережі.

Шоста група включає події, що стосуються фізичної безпеки. Це можуть бути спроби несанкціонованого доступу до серверних приміщень або підключення зовнішніх пристроїв зберігання даних, таких як USB-накопичувачі чи жорсткі диски. Ці події важливі для забезпечення фізичної безпеки системи та її елементів.

Сьома група включає події, пов'язані з процесами резервного копіювання та відновлення даних. Це можуть бути події створення резервних копій або їх відновлення з резервних носіїв, що також можуть вплинути на цілісність і доступність даних. Реєстрація таких подій важлива для забезпечення надійності збереження даних та запобігання їх втраті.

Всі ці події реєструються в журналі для забезпечення моніторингу, аналізу та своєчасного реагування на інциденти безпеки. Вони є основою для розслідування порушень безпеки, виявлення загроз і для подальших

дій щодо забезпечення надійного захисту інформаційних ресурсів організації.

Нижче наведено огляд груп подій і дій, які можуть бути виявлені і внесені до журналу:

Події системного рівня:

- продуктивність системи;
- спроби реєстрації користувачів (успішні і невдалі);
- ідентифікатор користувача, що реєструється;
- дата і час кожної спроби реєстрації;
- блокування користувачів і терміналів;
- використання адміністративних утиліт;
- використання пристроїв;
- виконання функцій;
- запити на зміну конфігураційних файлів.

Події прикладного рівня:

- повідомлення про помилки;
- відкриття та закриття файлів;
- зміни файлів;
- порушення безпеки в рамках програми.

Події рівня користувача:

- спроби ідентифікації і аутентифікації;
- використання файлів, сервісів і ресурсів;
- виконання команд;
- порушення безпеки.

25.2. Протоколювання й аудит

Протоколювання – це процес збору та зберігання інформації про події, що відбуваються в інформаційних системах. Кожен сервіс може мати свій набір подій, які можна умовно поділити на зовнішні (викликані діями інших сервісів), внутрішні (викликані діями самого сервісу) та клієнтські (викликані діями користувачів і адміністраторів).

Аудит – це процес аналізу накопиченої інформації, який може проводитися оперативно в реальному часі або на регулярній основі (наприклад, раз на день). Якщо аудит здійснюється з автоматичним реагуванням на виявлені порушення, його називають активним.

Реалізація протоколювання та аудиту дозволяє вирішити кілька важливих завдань:

- Забезпечення підзвітності користувачів і адміністраторів.
- Можливість реконструкції послідовності подій.

- Виявлення спроб порушення інформаційної безпеки.
- Надання даних для виявлення та аналізу проблем у роботі системи.

Протоколювання вимагає обґрунтованих рішень щодо того, які саме події слід реєструвати і з яким ступенем деталізації. Надмірне або занадто детальне протоколювання може знизити продуктивність системи та ускладнити аудит, що, в свою чергу, погіршує інформаційну безпеку. Важливо знайти баланс між виконанням завдань і мінімізацією витрат ресурсів.

Один з розумних підходів до протоколювання подій в операційних системах пропонується в "Оранжевій книзі", де визначено такі події, які необхідно фіксувати:

- Успішний та неуспішний вхід у систему.
- Вихід із системи.
- Доступ до видалених систем.
- Операції з файлами (відкриття, закриття, перейменування, видалення).
- Зміна привілеїв чи інших атрибутів безпеки (наприклад, зміна рівня доступу або благонадійності користувача).

При протоколюванні подій рекомендується фіксувати такі дані:

- Дата та час події.
- Унікальний ідентифікатор користувача, який ініціював дію.
- Тип події.
- Результат дії (успіх чи невдача).
- Джерело запиту (наприклад, ім'я терміналу).
- Імена порушених об'єктів (наприклад, відкриті або видалені файли).
- Опис змін, внесених до бази даних захисту (наприклад, зміна мітки безпеки об'єкта).

Вибіркове протоколювання, яке фокусується на підозрілих користувачах або подіях, є важливим для збереження ефективності системи. Протоколювання та аудит безпосередньо залежить від інших засобів безпеки, таких як ідентифікація та аутентифікація, а також управління доступом. Для забезпечення цілісності та конфіденційності реєстраційної інформації можуть застосовуватися криптографічні методи захисту.

Протоколювання та аудит мають на меті забезпечення підзвітності, що, зокрема, може діяти як стримувальний фактор для користувачів і адміністраторів. Якщо вони знають, що їхні дії реєструються, ймовірно, вони утримаються від здійснення несанкціонованих операцій. Також,

протоколювання дозволяє здійснювати розслідування порушень безпеки, а також виявляти некоректні зміни (за наявності даних до та після змін).

Реконструкція послідовності подій допомагає визначити слабкі місця в захисті сервісів, знайти винуватців вторгнень, оцінити збитки та відновити нормальну роботу системи. Активний аудит дає змогу виявляти порушення в режимі реального часу, що є важливим для швидкої реакції на загрози.

Протоколювання та аудит також дозволяють виявляти і усувати вузькі місця, які можуть погіршувати доступність системи, покращуючи таким чином її продуктивність.

У складних розподілених та різнорідних системах організація погодженого протоколювання та аудиту може бути складною. Деякі компоненти безпеки (наприклад, маршрутизатори) можуть не мати вбудованих засобів протоколювання, і в такому випадку необхідно використовувати інші сервіси для цієї мети. Важливо також синхронізувати події, що відбуваються в різних частинах системи, для забезпечення повної картини того, що відбувається в інформаційній інфраструктурі.

Реалізація протоколювання і аудиту

Реалізація протоколювання та аудиту в інформаційно-комунікаційних системах (ІКС) є важливою складовою для забезпечення належного рівня безпеки. Протоколювання передбачає запис важливих подій, що відбуваються в системі, таких як авторизація користувачів, доступ до ресурсів або зміни в конфігураціях. Для належної реалізації цієї функції важливо визначити, які події мають бути зафіксовані, забезпечити збір детальної інформації про ці події, захистити журнали від несанкціонованого доступу або змін і забезпечити їх архівацію для подальшого аналізу. Аудит, у свою чергу, передбачає перевірку зафіксованих подій для виявлення порушень безпеки, несанкціонованих дій або аномалій у роботі системи. Аудитори повинні постійно аналізувати ці події для виявлення потенційних інцидентів, проводити розслідування та складати звіти, що описують виявлені порушення та пропонують заходи для покращення безпеки. Оскільки аналіз журналів може бути складним і тривалим процесом, для автоматизації протоколювання і аудиту використовуються спеціалізовані інструменти, такі як системи моніторингу та виявлення вторгнень, а також рішення для централізованого збору журналів. Ці інструменти дозволяють не лише фіксувати події, але й оперативно виявляти порушення безпеки в

реальному часі. Важливим аспектом є також забезпечення безпеки самих журналів, їх захист від несанкціонованого доступу або змін, а також створення належних умов для зберігання та архівації даних. Завдяки ефективно реалізованому протоколюванню та аудиту організації можуть не тільки забезпечити прозорість роботи своїх ІКС, але й оперативно реагувати на порушення, виявляти потенційно небезпечні ситуації та запобігати майбутнім інцидентам.

Реалізація протоколювання і аудиту вирішує такі завдання:

- ➔ забезпечення підзвітності користувачів;
- ➔ забезпечення можливості реконструкції послідовності подій;
- ➔ виявлення спроб порушень інформаційної безпеки;
- ➔ надання інформації для виявлення і аналізу проблем.

Забезпечення підзвітності важлива, в першу чергу, як стримуючий засіб. Якщо користувачі знають, що всі їхні дії фіксуються, вони, можливо, утримаються від незаконних операцій. Очевидно, якщо є підстави підозрювати будь-якого користувача в нечесності, можна реєструвати всі його дії, аж до кожного натискання клавіші.

Реконструкція послідовності подій дозволяє виявити слабкості в захисті сервісів, знайти винуватця вторгнення, оцінити масштаби завданих збитків та повернутися до нормальної роботи.

Виявлення спроб порушень інформаційної безпеки – функція активного аудиту. При цьому забезпечується не тільки можливість розслідування випадків порушення режиму безпеки, а й відкат некоректних змін (якщо в протоколі присутні дані до і після модифікації). Тим самим захищається цілісність інформації.

Виявлення та аналіз проблем можуть допомогти поліпшити такий параметр безпеки, як доступність. Виявивши вузькі місця, можна спробувати переконфігурувати або переналаштувати систему, знову виміряти продуктивність і т.д.

Протоколювання вимагає для своєї реалізації здорового глузду.

Аудит інформаційної безпеки: сучасні аспекти

Аудит інформаційної безпеки є системним процесом, спрямованим на отримання об'єктивних якісних та кількісних оцінок поточного стану інформаційної безпеки автоматизованої системи відповідно до визначених критеріїв та показників безпеки. Це процес, який дозволяє оцінити рівень захищеності інформаційних ресурсів підприємства та забезпечити захист законних прав особистості й суспільства в інформаційній сфері.

Основною метою аудиту є оцінка поточного рівня безпеки функціонування інформаційної системи, прогнозування ризиків, управління їх впливом на бізнес-процеси, а також прийняття обґрунтованих рішень щодо захисту інформаційних активів, стратегічних планів розвитку, фінансових і маркетингових програм та корпоративних баз даних. Грамотно проведений аудит сприяє ефективному використанню коштів, інвестованих у систему безпеки.

В Україні аудит інформаційної безпеки регулюється стандартом ДСТУ ISO/IEC 27007:2018, який надає рекомендації щодо управління програмою аудиту системи управління інформаційною безпекою (СУІБ) та компетентності аудиторів. Крім цього, стандартизацію критеріїв активно підтримує міжнародна асоціація ISACA, яка розробила широко застосовуваний стандарт COBIT, що дозволяє адаптувати рекомендації під специфіку окремих підприємств.

Аудит охоплює низку напрямів, таких як атестація об'єктів інформатизації, контроль захищеності інформації, дослідження технічних засобів на наявність побічних електромагнітних випромінювань і наведень, а також проектування захищених систем і приміщень. Атестація включає перевірку автоматизованих систем, засобів зв'язку, приміщень для конфіденційних переговорів і технічних засобів, встановлених у виділених зонах. Контроль захищеності передбачає виявлення технічних каналів витоку інформації, перевірку ефективності засобів захисту та аналіз ризиків.

Види аудиту поділяються на зовнішній і внутрішній. Зовнішній аудит проводиться незалежними організаціями для оцінки ризиків, пов'язаних із зовнішніми атаками, включаючи сканування портів, пошук уразливостей, перевірку серверів і спроби проникнення. Спеціалізованою формою є етичне хакерство, коли експерти симулюють реальні атаки з метою перевірки систем захисту. Внутрішній аудит проводиться штатною командою підприємства для оцінки політики безпеки, контролю доступу до ресурсів і аналізу внутрішніх уразливостей.

Етапи проведення аудиту включають ініціацію процедури, збір інформації, аналіз даних, розробку рекомендацій і складання звіту. На етапі ініціації керівництво визначає межі аудиту, призначає відповідальну робочу групу та затверджує план дій. Збір інформації потребує ретельного аналізу організаційної структури, інтерв'ю з працівниками, вивчення компонентів інформаційної системи та використання спеціалізованих інструментів для тестування.

Основними завданнями аудиту є оцінка ризиків, інвентаризація ресурсів, визначення ефективності заходів захисту, аналіз мережевої

інфраструктури та навчання персоналу. Результатом є детальний звіт із рекомендаціями щодо покращення системи безпеки, усунення уразливостей і дотримання стандартів у сфері інформаційної безпеки.

Таким чином, аудит інформаційної безпеки забезпечує комплексну оцінку стану захищеності інформаційних систем підприємства, сприяє мінімізації ризиків та формуванню стратегічно обґрунтованих рішень у сфері кібербезпеки.

Аудит інформаційної безпеки (ІБ) є важливим інструментом для забезпечення надійного функціонування підприємств в умовах зростаючих кіберзагроз. Основою для проведення аудиту є Система менеджменту інформаційної безпеки (СМІБ, ISMS) – частина загальної системи управління, яка базується на оцінці ризиків з метою створення, впровадження, моніторингу та вдосконалення заходів захисту інформації. СМІБ включає організаційну структуру, політику, процеси, процедури, ресурси і діяльність з планування, що спрямовані на захист інформації.

Об'єктами аудиту можуть бути як інформаційно-телекомунікаційні системи (ІТС) підприємства в цілому, так і їхні окремі компоненти, що обробляють інформацію, яка потребує захисту. Аудит може бути кількох видів, зокрема: плановий і позаплановий внутрішній аудит, аудит для пошуку загроз та моделювання загроз. Окремим важливим елементом СМІБ є Система менеджменту інцидентів інформаційної безпеки (СМІІБ), яка дозволяє виявляти, обліковувати, аналізувати інциденти та забезпечувати оперативне реагування. Ефективність реалізації СМІІБ базується на стандартах, таких як ISO/IEC 27001:2013, ITU-T X-1051 та ISO/IEC 27035:2011.

Одним із ключових напрямків аудиту є активний аудит, спрямований на дослідження стану захищеності систем з позиції потенційного зловмисника. Цей підхід включає використання спеціалізованого програмного забезпечення та методів аналізу для оцінки мережевого захисту. Активний аудит може бути зовнішнім, коли моделюються дії зовнішнього зловмисника, або внутрішнім, спрямованим на оцінку ризиків, пов'язаних із внутрішніми загрозами. У рамках зовнішнього аудиту здійснюється сканування IP-адрес підприємства, аналіз сервісів, маршрутів трафіку та інших доступних даних. Внутрішній аудит передбачає імітацію дій внутрішнього порушника з використанням спеціалізованих інструментів.

Важливою складовою активного аудиту є стрес-тестування, яке дозволяє виявити критичні точки системи, визначити межі її навантаження та оцінити здатність протидіяти атакам на відмову в обслуговуванні. Результати активного аудиту включають перелік уразливостей, ступінь їх

критичності, методи усунення недоліків та рекомендації з модернізації системи захисту.

Іншим важливим видом аудиту є аудит відповідності стандартам, наприклад, ISO/IEC 27001. Він дозволяє оцінити поточний стан СМІБ підприємства, визначити рівень відповідності вимогам стандарту та внутрішнім політикам, а також розробити рекомендації з удосконалення системи захисту. За результатами такого аудиту формується звіт, який включає ступінь відповідності стандартам, список невідповідностей та рекомендації щодо покращення.

На етапі впровадження СМІБ важливу роль відіграє діагностичний аналіз, який допомагає оцінити існуючий рівень управління ІБ, визначити перелік робіт для приведення СМІБ у відповідність до стандарту та сформулювати чіткий план дій. Для цього можуть використовуватися опитувальники, такі як розроблений компанією Bridge Point, які дозволяють структурувати та автоматизувати процес діагностики.

Аудит є важливим інструментом для підприємств, які прагнуть своєчасно виявляти загрози, усувати уразливості та мінімізувати ризики, забезпечуючи захист інформації відповідно до сучасних стандартів і норм.

Активний аудит: основні концепції та сучасні підходи

Активний аудит є невід'ємною складовою системи інформаційної безпеки, що дозволяє оперативно виявляти підозрілу активність користувачів або компонентів інформаційної системи. Під підозрілою активністю розуміють такі дії, які є злочинними або нетиповими відповідно до визначеної політики безпеки. Завданням активного аудиту є виявлення цієї активності та надання засобів для автоматичного реагування на виявлені загрози.

Активність можна поділити на два основні типи:

1. **Атаки** — це дії, що порушують будь-яку осмислену політику безпеки і зазвичай мають руйнівний характер.
2. **Зловживання повноваженнями** — дії, що виконуються в межах наявних прав, але з порушенням встановлених правил і політики безпеки (наприклад, несанкціоноване використання прав адміністратора).

Методи активного аудиту включають **сигнатури атак** та **статистичний аналіз поведінки**:

- **Сигнатури атак** — це зафіксовані умови, при яких атака вважається дійсною, і на яку система реагує заздалегідь визначеним чином, наприклад, блокування терміналу після кількох невдалих спроб входу.

- **Статистичний аналіз** — виявляє нетипову поведінку, застосовуючи порогові значення або порівнюючи поточний профіль користувача з його довгостроковим профілем. Це дозволяє виявити нові типи атак, але може призвести до підвищеної кількості помилок другого роду, коли система неправомірно інтерпретує легітимну активність як загрозу.

Активний аудит також здатний забезпечити захист від атак на доступність, виявляючи аномалії та реагуючи на загрози, що можуть порушити нормальну роботу сервісів. Проте він має свої обмеження: хоча розпізнавання простих атак стало можливим, багато складних загроз, зокрема нових або розподілених атак, все ще важко виявити.

Сучасний підхід до активного аудиту полягає у використанні багаторівневих захистів, де активний аудит є одним із рубежів. Це дозволяє забезпечити гнучку та ефективну систему реагування на інциденти, враховуючи розвиток технологій, зокрема машинного навчання та штучного інтелекту для покращення виявлення нових загроз.

Засоби активного аудиту можуть бути розміщені на різних лініях оборони інформаційної системи, від точок підключення до зовнішніх мереж до внутрішніх корпоративних сервісів. Вони здатні виявляти підозрілу активність і зупиняти її, забезпечуючи комплексну безпеку інформаційної інфраструктури.

25.3. ФУНКЦІОНАЛЬНІ КОМПОНЕНТИ Й АРХІТЕКТУРА

АУДИТУ

Розширена архітектура засобів активного аудиту в сучасних інформаційних системах

Засоби активного аудиту виконують важливу роль в забезпеченні інформаційної безпеки, дозволяючи оперативно виявляти підозрілу активність у межах інформаційних систем. Ці системи складаються з різних функціональних компонентів, які працюють у єдиній архітектурі для виявлення атак, зловживань повноваженнями та інших нетипових поведінкових ознак.

Основні функціональні компоненти активного аудиту:

1. Компоненти генерації реєстраційної інформації

Ці компоненти перебувають на межі між засобами активного аудиту і контрольованими об'єктами. Вони фіксують всі критичні події, що можуть бути використані для подальшого аналізу підозрілої активності.

2. Компоненти зберігання згенерованої реєстраційної інформації

Зберігають інформацію в централізованих або розподілених сховищах, що необхідно для подальшого аналізу, зокрема для виявлення тривалих або складних атак.

3. Компоненти витягування реєстраційної інформації (сенсори)

Сенсори можуть бути мережевими чи хостовими. Мережеві сенсори встановлюються на мережевому обладнанні та контролюють трафік, тоді як хостові сенсори аналізують журнали операційних систем. Сучасні комутаційні технології стирають розмежування між цими типами сенсорів, оскільки мережеві сенсори часто вбудовуються в активне мережне обладнання, становлячи частину мережевої операційної системи.

4. Компоненти аналізу інформації, що надходить від сенсорів. До них належать різні типи аналізаторів:

- ✓ Пороговий аналізатор, який виявляє події, що перевищують встановлені пороги і можуть свідчити про підозрілу активність.
- ✓ Аналізатор порушень політики безпеки, який фіксує активність, що порушує встановлені правила безпеки.
- ✓ Експертна система для виявлення сигнатур атак, що допомагає виявляти типові та відомі атаки.
- ✓ Статистичний аналізатор, який виявляє нетипову поведінку, базуючись на аналізі довгострокових та короткострокових профілів користувачів.

5. Компоненти зберігання інформації для аналізу

Зберігають дані, які потрібні для виявлення атак, що розтягнуті у часі, та підтримують можливості для кореляції різних типів подій.

6. Компоненти прийняття рішень і реагування ("вирішувачі")

Визначають, як реагувати на виявлені загрози, зокрема можуть ініціювати автоматичне блокування підозрілих об'єктів або сповіщення адміністраторів про інциденти безпеки.

7. Інтерфейсні компоненти

Забезпечують взаємодію між різними елементами системи, а також між засобами активного аудиту та адміністраторами безпеки. Інтерфейсні компоненти можуть включати монітори, об'єднувальні аналізатори та сховища описів об'єктів.

Сучасні підходи та інтерфейси активного аудиту

Сучасні системи активного аудиту орієнтуються на архітектуру менеджер/агент, де основними агентами є сенсори, а функції аналізу та прийняття рішень виконують менеджери. Важливою складовою є створення довірених каналів між менеджерами та агентами, що забезпечує безпечний обмін інформацією.

Особливу увагу слід звернути на інтерфейсні компоненти. Вони забезпечують взаємодію між різними модулями системи активного аудиту, дозволяючи обробляти як внутрішні дані системи, так і зовнішні вхідні потоки. Це важливо для аналізу розподіленої активності, зокрема для виявлення складних або масштабних атак, що потребують координації між різними системами безпеки.

Удосконалення інтерфейсів дозволяє забезпечити розширюваність системи та інтеграцію з компонентами різних постачальників. Це, в свою чергу, підвищує універсальність і гнучкість системи, дозволяючи ефективно реагувати на нові типи загроз і атак.

Інтеграція з іншими системами безпеки та управління

Інтерфейсні компоненти також можуть сприяти інтеграції засобів активного аудиту з іншими системами управління безпекою, такими як системи виявлення вторгнень (IDS), системи управління подіями безпеки (SIEM) або навіть автоматизовані системи реагування на інциденти (SOAR). Це дозволяє створити комплексну систему безпеки, де різні компоненти можуть взаємодіяти та координувати свої дії для забезпечення більш високого рівня захисту.

Завдяки такій архітектурі, система активного аудиту може виконувати роль одного з ключових рубежів в багаторівневій обороні інформаційної інфраструктури, забезпечуючи своєчасне виявлення та реагування на нові, невідомі загрози, при цьому мінімізуючи ризики помилок та пропуску важливих подій.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 25

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.
2. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.
3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
5. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18.
6. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 68–83.
7. Машталяр, Я., Козачок, В., Бржезьська, З., Богданов, О., Оксанич, І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 156–167.
8. V. Dudykevych, et al., Detecting Deepfake Modifications of Biometric Images using Neural Networks, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 391–397.
9. Костюк Ю.В., Кравченко Д.В. Методи захисту даних на підприємствах соціальної сфери. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1033-1047.
10. Костюк Ю.В., Войткевич А.А. Дослідження технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1017-1032.
11. S. Shevchenko, et al., Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 333–342.
12. Костюк Ю.В., Шапран В.О. Технології виявлення аномальних подій та сигнатур в реальному часі. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1069-1084.
13. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.

14. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.
15. V. Shapoval, et al., Automation of Data Management Processes in Cloud Storage, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 410–418.
16. V. Buhas, et al., Cybersecurity Role in AI-Powered Digital Marketing, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 (2024) 1–11.
17. D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II-2, vol. 3188 (2021) 135–148.
18. S. Zybin, et al., Approach of the Attack Analysis to Reduce Omissions in the Risk Management, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 318–328.

КОНТРОЛЬНІ ПИТАННЯ

1. Розкрийте поняття логічного управління доступом.
2. Які завдання вирішуються при логічному управлінні доступом?
3. Дайте характеристику дискреційній моделі розмежування доступом.
4. Дайте характеристику мандатній моделі розмежування доступом.
5. Дайте характеристику рольовій моделі розмежування доступом.
6. Для чого проводиться реєстрація подій в ІКС?
7. Що таке управління доступом в інформаційних системах та які його основні принципи?
8. Які існують моделі управління доступом? Як вони відрізняються одна від одної?
9. Які переваги та недоліки має дискреційна модель розмежування доступу?
10. Як мандатна модель розмежування доступу забезпечує безпеку в організаціях з високим рівнем секретності?
11. Що таке рольова модель розмежування доступу і як вона працює в організації?

12. Яким чином рольове управління доступом підвищує ефективність адміністрування в великих підприємствах?
13. Що таке аудит подій в системі та яку роль він відіграє в забезпеченні безпеки?
14. Які події повинні бути зафіксовані в журналі реєстрації?
15. Як визначити рівень деталізації для реєстрації подій в системі?
16. Які типи подій є критичними для безпеки інформаційних систем?
17. Які функції повинні бути присутні в системі аудиту для забезпечення прозорості?
18. Як можна використовувати журнал реєстрації для виявлення потенційних загроз?
19. Які дані обов'язково повинні бути зафіксовані в записях журналу реєстрації?
20. Як система аудиту допомагає у виявленні несанкціонованого доступу до інформаційних ресурсів?
21. Яким чином забезпечується цілісність даних у журналі реєстрації?
22. Як взаємодіє система аудиту з іншими системами безпеки, такими як виявлення вторгнень або контроль доступу?
23. Які основні компоненти складають процес реєстрації подій в системі?
24. Як рольова модель управління доступом впливає на ефективність контролю доступу до системи?
25. Як організувати управління доступом в складних підприємствах із багаторівневою структурою?
26. Яким чином автоматизація реєстрації подій допомагає в забезпеченні оперативності реагування на інциденти безпеки?
27. Де знайти журнали реєстрацій подій в системі?
28. Назвіть основні події, що реєструються в системі в інтересах забезпечення безпеки.

ТЕМА 7. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

РОЗДІЛ 26 СТВОРЕННЯ ТА ОЦІНКА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ



- 26.1. Сутність та задачі комплексної системи захисту інформації**
- 26.2. Суб'єкти та об'єкти захисту КСЗІ**
- 26.3. Основні вимоги, завдання та принципи організації КСЗІ**
- 26.4. Концепція створення захищених КСЗІ**
- 26.5. Етапи створення комплексної системи захисту інформації**
- 26.6. Моделювання КСЗІ**
- 26.7. Вибір показників ефективності і критеріїв оптимальності КСЗІ**
- 26.8. Підходи до оцінки ефективності КСЗІ**
- 26.9. Концептуальні підходи до проектування систем захисту**

" Комплексні системи захисту інформації — це не лише про технології, але й про процеси та людей. Захист інформації вимагає цілісного підходу, що включає не тільки технічні рішення, але й правильне управління, навчання персоналу та постійний моніторинг."

Кевін Мітник, експерт з кібербезпеки

Комплексні системи захисту інформації - сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації.

До складу комплексних систем захисту інформації включаються технічні засоби, призначені для побудови систем охоронної і пожежної сигналізації, систем управління протипожежною автоматикою, телевізійного спостереження, контролю і управління доступом, і що володіють технічною, інформаційною, експлуатаційною сумісністю і зв'язаних єдиною програмою, що управляє (системою збору і обробки інформації).

Будь-яка комплексна система захисту інформації (КСЗІ) є складною системою. Основні підсистеми КСЗІ:

- ❖ Система контролю управління доступом;
- ❖ Система відеоспостереження;
- ❖ Система збору та обробки інформації;
- ❖ Система протидії економічному шпигунству;
- ❖ Система пожежної сигналізації;
- ❖ Система автоматичного пожежогасіння.

26.1. СУТНІСТЬ ТА ЗАДАЧІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Комплексна система захисту інформації (КСЗІ) — це сукупність організаційних, програмних, технічних та криптографічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації.

Основна мета КСЗІ — створення безпечного інформаційного середовища для підприємств або установ, де обробляється інформація, яка потребує захисту.

Основні підходи до створення комплексної системи захисту інформації

У сучасному цифровому середовищі захист інформації вже давно не обмежується лише питаннями безпеки даних, що обробляються комп'ютерами. З розвитком інформаційно-інтелектуальних систем, хмарних обчислень та інтернету речей, інформація стала поширеною по багатьом технологічним платформам та мережам, що значно ускладнює забезпечення її захисту.

На підприємствах інформація є одним із ключових активів, що потребує комплексного підходу до захисту. Об'єкт інформатизації включає

не лише персональні комп'ютери, а й сервери, мобільні пристрої, мережеві компоненти, бази даних та хмарні платформи. Інформаційна безпека охоплює всі рівні системи – від фізичного захисту приміщень до програмних і технічних заходів.

Сучасне підприємство являє собою складну інформаційно-інтелектуальну систему з багатьма взаємозалежними компонентами. Вони об'єднані для виконання стратегічних і оперативних завдань, які постійно змінюються під впливом внутрішніх і зовнішніх факторів.

Основні характеристики сучасного підприємства включають:

- складна організаційна структура;
- багатофункціональність операцій;
- висока технічна оснащеність;
- розгалужені коопераційні зв'язки;
- необхідність розширеного доступу до інформації;
- зростаюче використання цифрових технологій обробки даних;
- автоматизація значної частини процесів обробки інформації;
- прийняття важливих рішень на основі автоматизованої обробки інформації;
- висока концентрація інформаційних ресурсів;
- велике територіальне розподілення компонентів інформаційних систем;
- зберігання великих обсягів інформації на цифрових носіях;
- інтеграція різноманітної інформації в єдині бази даних;
- одночасний доступ до інформаційних ресурсів багатьох користувачів;
- інтенсивний обмін інформацією між компонентами систем.

Сучасні підходи до захисту інформації на підприємствах включають як організаційні, так і технологічні заходи, які враховують стрімкий розвиток технологій та загрози кіберпростору. Це охоплює використання багаторівневих моделей захисту, технологій шифрування, систем багатфакторної аутентифікації та засобів моніторингу кіберзагроз.

Індустрія обробки інформації створює умови для підвищення продуктивності праці, але одночасно породжує численні виклики щодо безпеки даних. Головним завданням сучасних підприємств є забезпечення надійного захисту інформації, що обробляється та циркулює в їхніх системах.

Основні підходи до створення комплексної системи захисту інформації включають:

❖ **Організаційно-правовий підхід:**

- ✓ Визначення політики інформаційної безпеки підприємства.

- ✓ Розробка нормативних документів, регламентів і процедур захисту інформації.
- ✓ Проведення навчання персоналу щодо правил безпеки.
- ✓ Регулярний контроль дотримання встановлених заходів захисту.
- ❖ **Технічний підхід:**
 - ✓ Впровадження систем контролю доступу до інформаційних ресурсів.
 - ✓ Захист мережевої інфраструктури за допомогою міжмережевих екранів (firewalls) та систем виявлення вторгнень (IDS/IPS).
 - ✓ Використання засобів криптографії для захисту даних.
 - ✓ Впровадження систем резервного копіювання та відновлення даних.
- ❖ **Програмний підхід:**
 - ✓ Використання антивірусного та антишпигунського програмного забезпечення.
 - ✓ Захист від шкідливого програмного забезпечення та експлойтів.
 - ✓ Регулярне оновлення програмного забезпечення для усунення вразливостей.
- ❖ **Фізичний підхід:**
 - ✓ Захист серверних кімнат та інших критичних об'єктів фізичними засобами (замки, сигналізація, відеоспостереження).
 - ✓ Контроль доступу до приміщень підприємства.
 - ✓ Захист технічних засобів від електромагнітного випромінювання.
- ❖ **Адміністративний підхід:**
 - ✓ Призначення відповідальних осіб за забезпечення інформаційної безпеки.
 - ✓ Проведення аудитів інформаційної безпеки та оцінка ризиків.
 - ✓ Аналіз інцидентів безпеки та коригування заходів захисту.
- ❖ **Проактивний підхід:**
 - ✓ Постійний моніторинг інформаційних систем для виявлення аномальної активності.
 - ✓ Оперативне реагування на кіберзагрози та вторгнення.
 - ✓ Використання засобів машинного навчання та штучного інтелекту для прогнозування загроз.
- ❖ **Комплексний підхід:**
 - ✓ Інтеграція всіх перелічених заходів у єдину систему.
 - ✓ Створення багаторівневого захисту інформації.
 - ✓ Безперервне вдосконалення системи захисту відповідно до нових загроз і вимог.

Поняття комплексної системи захисту інформації

Основні складові комплексної системи захисту інформації:

1. **Організаційні заходи** — політики, регламенти, нормативні документи, які визначають вимоги до захисту інформації та порядок реалізації заходів безпеки.
2. **Технічні засоби** — програмне та апаратне забезпечення, призначене для захисту даних, наприклад, системи шифрування, антивірусні програми, брандмауери, засоби контролю доступу.
3. **Процедурні заходи** — інструкції та алгоритми, що визначають порядок обробки, зберігання та передачі інформації, а також алгоритми реагування на інциденти безпеки.
4. **Фізичні заходи** — заходи щодо фізичного захисту інформації та обладнання (охорона, контроль доступу до приміщень, системи відеоспостереження).
5. **Механізми аудиту та моніторингу** — системи для спостереження за станом безпеки, виявлення порушень і реагування на інциденти.

Комплексна система повинна бути гнучкою та адаптивною до нових загроз, забезпечуючи баланс між рівнем захисту та зручністю користування інформаційними системами.

Захист інформації в Україні продовжує розвиватися відповідно до сучасних загроз та викликів інформаційної безпеки. Сформовано значний практичний і теоретичний досвід, який активно використовується для вдосконалення систем захисту на підприємствах. Нині вже нікого не переконує думка, що достатньо впровадити лише кілька організаційних заходів або технічних рішень для забезпечення безпеки інформаційних ресурсів.

Основним напрямом сучасного підходу до захисту інформації є створення комплексної системи, яка забезпечує безперервний процес захисту на всіх етапах життєвого циклу інформаційно-інтелектуальних систем, з використанням усіх наявних засобів захисту. При цьому засоби, методи та заходи об'єднуються в єдиний цілісний механізм, спрямований на захист не лише від зловмисників, але й від некваліфікованих користувачів та позаштатних ситуацій технічного характеру.

Сучасні проблеми реалізації систем захисту полягають у наступному:

- забезпечення надійного захисту інформації в системі, включаючи запобігання випадковому та навмисному доступу сторонніх осіб, чітке розмежування доступу до ресурсів системи для користувачів, адміністрації та обслуговуючого персоналу;
- забезпечення зручності користувачів, мінімізуючи негативний вплив систем захисту на їхню продуктивність та ефективність роботи.

Реалізація бажаного рівня захисту інформації потребує комплексного підходу, який включає науково-технічні, організаційні та технологічні заходи, а також застосування спеціалізованих засобів захисту.

На основі сучасних досліджень і практичного досвіду сформовано системно-концептуальний підхід до захисту інформації. підхід базується на інтеграції різноманітних методів і технологій для забезпечення комплексного захисту на всіх етапах життєвого циклу інформації. Важливим елементом є визначення та класифікація інформаційних активів, що потребують захисту, а також аналіз потенційних загроз і вразливостей. Системно-концептуальний підхід включає застосування багаторівневих заходів захисту, від фізичної безпеки до технологічних і програмних рішень. Крім того, великий акцент робиться на постійному моніторингу і адаптації системи до нових кіберзагроз. Важливою складовою є розробка та впровадження політик безпеки, що регулюють доступ до інформації та її обробку. Цей підхід також передбачає використання передових технологій, таких як штучний інтелект і машинне навчання, для вдосконалення процесів виявлення та реагування на загрози. Завдяки системному підходу до захисту забезпечується не лише високий рівень безпеки, але й гнучкість у адаптації до змінних умов кіберпростору.

Включає такі принципи:

1. Системність

- цільова — захист інформації розглядається як ключовий компонент якості інформаційних процесів;
- просторова — забезпечення захисту на всіх рівнях підприємства;
- тимчасова — безперервність робіт із захисту інформації відповідно до планів;
- організаційна — єдність організації всіх робіт із захисту інформації та управління ними.

2. Концептуальність - розробка єдиної концепції, яка містить науково обґрунтовані положення та рішення для оптимальної організації та забезпечення надійності захисту інформації.

Комплексний підхід до побудови систем захисту інформації передбачає:

▲ **Вивчення об'єкта** - аналіз структури інформаційних ресурсів та їх обробки;

▲ **Оцінювання загроз** - визначення потенційних загроз безпеці;

▲ **Аналіз засобів захисту** - вибір оптимальних технічних та програмних рішень;

▲ **Економічна доцільність** - оцінка витрат та їх обґрунтованість;

▲ **Аналіз системи** - вивчення властивостей системи та її можливостей для підвищення ефективності;

▲ **Співвідношення внутрішніх і зовнішніх чинників** - визначення взаємодії із зовнішнім середовищем;

▲ **Формулювання цілей і функцій** - чітке визначення мети та функцій системи захисту;

▲ **Критерії ефективності** - розробка критеріїв для оцінки якості функціонування системи.

Важливим аспектом сучасного захисту інформації є врахування взаємодії інформаційних систем із зовнішнім середовищем та їх інтеграція з іншими об'єктами. Це дозволяє забезпечити комплексний захист інформації на підприємствах.

Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури та участь людини в технологічних процесах обробки інформації, ефективний захист інформації можливий лише шляхом створення комплексної системи захисту на основі сучасного підходу та врахування актуальних стандартів і вимог до інформаційної безпеки.

Призначення комплексної системи захисту інформації

Головна мета створення системи захисту інформації (СЗІ) полягає в забезпеченні надійності захисту інформаційних ресурсів шляхом ефективного поєднання методів, засобів та процедур, які забезпечують її конфіденційність, цілісність та доступність. Система захисту інформації є організованою сукупністю об'єктів, суб'єктів, методів і засобів захисту, а також заходів, які здійснюються для мінімізації ризиків інформаційної безпеки.

Ключовим аспектом є те, що компоненти СЗІ не лише є частинами загальної системи, а й одночасно організовують її функціонування, здійснюючи заходи захисту. Система повинна бути побудована таким чином, щоб усі складові працювали в єдиному, узгодженому процесі, забезпечуючи комплексний захист. Важливою умовою є інтеграція всіх компонентів системи в єдину технологічно і логічно зв'язану структуру, де кожен елемент, виконуючи свою функцію, також забезпечує ефективність роботи інших елементів.

Надійність захисту інформації прямо залежить від системності підходу. У разі неузгодженості між окремими складовими системи ризик «проколів» у технології захисту значно збільшується.

Одним з основних аспектів створення комплексної системи є інтеграція локальних систем захисту в єдину структуру, де кожна з них має функціонувати в рамках загальної системи. Локальні системи захисту можуть включати різні види захисту, такі як правовий, організаційний, інженерно-технічний, і повинні взаємодіяти для досягнення загальних цілей.

Іншою важливою складовою комплексного підходу є забезпечення повноти всіх елементів системи захисту. Це включає не лише технологічні засоби і методи захисту, а й облік всіх факторів, які можуть вплинути на ефективність захисту: уразливості інформаційних об'єктів, потенційні загрози, засоби зберігання і передачі інформації, а також відповідні кадрові ресурси. Тільки через аналіз всіх цих чинників можна забезпечити необхідний рівень захисту.

Крім того, комплексний підхід передбачає забезпечення безпеки всіх елементів інформаційної інфраструктури, незалежно від їх місцезнаходження чи умов функціонування. Це включає захист усіх носіїв інформації на всіх етапах їхнього оброблення, зберігання та передачі. При цьому, важливим є і диференційований підхід до захисту, залежно від типу та рівня конфіденційності інформації, видів уразливості та каналів несанкціонованого доступу.

Отже, комплексний підхід до захисту інформації забезпечує:

- інтеграцію локальних систем захисту;
- забезпечення повноти всіх складових системи;
- всебічний захист інформації на всіх етапах її обробки та передачі.

Таким чином, комплексна система захисту інформації — це система, яка забезпечує повноту і всебічність захисту всієї захищуваної інформації, охоплюючи всі об'єкти, процеси та фактори, що можуть впливати на її безпеку.

26.2. СУБ'ЄКТИ ТА ОБ'ЄКТИ ЗАХИСТУ КСЗІ

Суб'єкти та об'єкти захисту комплексної системи захисту інформації (КСЗІ) — це ключові елементи, що визначають структуру та механізми функціонування системи безпеки інформації.

Суб'єкти захисту

Суб'єкти захисту — це фізичні або юридичні особи, а також програмно-апаратні комплекси, які здійснюють або взаємодіють з процесами захисту інформації в межах КСЗІ. Суб'єкти можуть бути розподілені на кілька категорій:

- **Користувачі** — фізичні особи або групи осіб, які мають доступ до інформаційних систем і можуть взаємодіяти з інформацією в межах своїх повноважень. Користувачі включають адміністративний персонал, технічних спеціалістів, кінцевих користувачів тощо.
- **Адміністратори системи** — особи, що відповідають за налаштування, управління та контроль за роботою системи захисту. Вони мають доступ до налаштувань систем безпеки та повинні бути обізнані з принципами захисту.
- **Інформаційні системи та програмні комплекси** — системи, що обробляють, зберігають, передають і захищають інформацію. Вони є основними суб'єктами у визначенні механізмів захисту, таких як шифрування, автентифікація і контроль доступу.
- **Кадрові ресурси безпеки** — співробітники, які здійснюють постійний моніторинг, аудит і реагування на інциденти безпеки. Це можуть бути спеціалісти з кібербезпеки, аудитори, розробники політик безпеки.
- **Зовнішні користувачі та партнери** — організації або фізичні особи, які мають доступ до інформаційних систем, наприклад, постачальники послуг, зовнішні консультанти, клієнти тощо.

До процесу створення комплексної системи захисту інформації (КСЗІ) також залучаються спеціалісти з інформаційної безпеки, які займаються проведенням аналізу ризиків, розробкою політик безпеки та впровадженням засобів захисту. Важливу роль у створенні КСЗІ відіграють розробники програмного забезпечення, які відповідають за інтеграцію технологічних рішень і забезпечення їх безпеки. Крім того, у разі необхідності, можуть бути залучені незалежні аудитори, які здійснюють перевірку відповідності системи захисту міжнародним стандартам безпеки. Також проводяться тренінги та навчання для співробітників організації з метою підвищення рівня обізнаності та відповідальності за безпеку інформації. Усі ці елементи повинні взаємодіяти у єдиній системі, забезпечуючи цілісність, конфіденційність та доступність захищеної інформації. До процесу створення комплексної системи захисту інформації (КСЗІ) залучаються наступні сторони:

❖ **Замовник** — організація, для якої здійснюється побудова КСЗІ. Це підприємство або інша організація, що має потребу в захисті своїх інформаційних ресурсів та забезпеченні їх безпеки.

❖ **Виконавець** — організація або компанія, яка здійснює розробку, впровадження та налаштування КСЗІ. Виконавець відповідає за технічне виконання проекту та забезпечення всіх необхідних заходів для належного захисту інформації.

❖ Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ) — орган державного контролю, який забезпечує відповідність КСЗІ вимогам законодавства та нормативних актів у галузі інформаційної безпеки. ДССЗІ здійснює нагляд за дотриманням стандартів і вимог безпеки в рамках розробки та експлуатації КСЗІ.

❖ Організатор експертизи — організація або установи, що проводять державну експертизу КСЗІ для оцінки відповідності системи захисту інформації державним стандартам і вимогам безпеки. Це може бути національна інституція, яка перевіряє, чи відповідає система захисту інформації стандартам та вимогам для її впровадження.

❖ Підрядник — організація або спеціалізована компанія, залучена для виконання конкретних робіт або надання послуг у процесі створення КСЗІ, таких як впровадження окремих компонентів системи захисту, аудит або інші спеціалізовані заходи. Підрядник може бути залучений за необхідністю для виконання окремих частин проекту.

Кожен з учасників процесу відіграє важливу роль у забезпеченні ефективної та безпечної реалізації комплексної системи захисту інформації, що має на меті не тільки технічне забезпечення, але й дотримання законодавчих та нормативних вимог в галузі інформаційної безпеки.

Об'єкти захисту

Захист інформації повинен бути системним, що містить у собі різні взаємопов'язані компоненти. Найважливішим з цих компонентів є об'єкти захисту, оскільки від їх складу залежать і методи, і засоби захисту, а також склад захисних заходів.

Інформація є предметом захисту, але захищати її як таку неможливо, оскільки вона не існує сама по собі, а фіксується (відображається) у певних матеріальних об'єктах або пам'яті людей, які виступають в ролі її носіїв і складають основний, базовий об'єкт захисту.

Для запису як секретної, так і несекретної інформації використовуються одні й ті ж носії. Як правило, носії інформаційно-захищеної обробки (ІзОД) охороняються власником цієї інформації. Носії захищеної інформації можна класифікувати за такими категоріями, як документи, вироби (предмети), речовини та матеріали, електромагнітні, теплові, радіаційні та інші випромінювання, акустичні та інші поля тощо.

Особливим носієм інформації є людина, мозок якої являє виключно складну систему, що зберігає і переробляє інформацію, яка надходить із зовнішнього світу. Властивість мозку відображати і пізнавати зовнішній світ, накопичувати в пам'яті великі обсяги інформації ставлять людину на

особливе місце як носія інформації. Людина має здатність генерувати нову інформацію. І як носій інформації має як позитивні, так і негативні риси.

Позитивні риси включають те, що без згоди суб'єкта-носія захищувана інформація з його пам'яті, як правило, не може бути вилучена. Людина може оцінювати важливість наявної в неї інформації та відповідно до цього ставитися до неї. Вона може ранжувати і споживачів захищеної інформації, знаючи, кому і яку інформацію вона може довірити.

Негативні риси полягають у тому, що людина може помилятися щодо істинності споживача захищеної інформації або навмисно не зберігати довірену йому інформацію (зрада чи просто її поширення).

Серед найбільш поширених видів носіїв конфіденційної інформації можна виділити наступні:

- **Паперові носії** - інформація фіксується рукописним, машинописним, електронним, типографським та іншими способами у вигляді тексту, креслень, схем, формул.

- **Магнітні носії** - аудіокасети для магнітофонів і диктофонів, відеокасети для відеоманітофонів, жорсткі диски, дискети та магнітні стрічки для ЕОМ. Інформація фіксується через магнітне накопичення, а відтворення здійснюється за допомогою магнітного пристрою.

- **Магнітооптичні та оптичні носії** - лазерні диски, компакт-диски. Запис даних здійснюється лазерним променем, а їх відтворення — за допомогою того ж променя.

- **Продукція (вироби)** - технічні рішення, що одночасно є носіями захищеної інформації, де інформація відображається у вигляді технологічних процесів і рішень.

- **Технологічні процеси** - включають технологію виробництва продукції та застосовувані компоненти (обладнання, матеріали, сировина тощо), в яких інформація відображається в вигляді технічних процесів і рішень.

- **Фізичні поля** - електромагнітні, теплові, акустичні поля, у яких інформація фіксується шляхом зміни інтенсивності чи кількісних характеристик.

Носії ІзОД, як об'єкти захисту, повинні захищатися від несанкціонованого доступу, втрати та витоку інформації. Для цього необхідно створювати багаторівневу систему захисту, де кожен рівень буде обмежувати доступ до носіїв.

Захист носіїв інформації залежить від їх видів і полягає в створенні рубежів захисту, що повинні забезпечувати фізичну охорону, захист від візуального спостереження, проникнення сторонніх осіб, а також забезпечення доступу лише уповноваженим особам.

Об'єкти захисту — це елементи, які потребують захисту від різних загроз. Об'єкти можуть бути матеріальними або нематеріальними і мають відношення до всіх аспектів інформаційної безпеки. Основні об'єкти захисту включають:

- **Інформація** — основний об'єкт захисту, що включає дані, які мають конфіденційність, цілісність і доступність. Це можуть бути як персональні, так і комерційні або державні дані, що зберігаються, передаються або обробляються в інформаційних системах.
- **Інформаційні системи** — апаратно-програмні комплекси, що виконують обробку, зберігання та передачу інформації. Це можуть бути сервери, бази даних, робочі станції, мережеві пристрої тощо.
- **Мережі передачі даних** — канали і мережеві структури, через які передається інформація. Вони потребують захисту від несанкціонованого доступу, витоку даних або інших атак.
- **Програмне забезпечення** — програми, які здійснюють обробку та захист інформації, включаючи операційні системи, додатки, антивірусні програми, системи моніторингу та управління безпекою.
- **Кадрові ресурси** — персонал, який безпосередньо відповідає за забезпечення безпеки інформаційних систем, адже від їхнього навчання, кваліфікації та дотримання стандартів залежить ефективність системи захисту.
- **Фізичні об'єкти** — обладнання, приміщення, носії інформації (наприклад, жорсткі диски, сервери, флеш-накопичувачі), які потрібно захищати від фізичного доступу або знищення.
- **Канали доступу** — засоби, через які здійснюється доступ до інформації, як то мережі, інтерфейси, пристрої доступу (наприклад, USB-порти, бездротові мережі Wi-Fi). Це канали, через які можуть бути здійснені атаки або витоки даних.
- **Процеси обробки інформації** — всі етапи роботи з інформацією, від її збору, зберігання, обробки до передачі та використання. Захист кожного етапу життєвого циклу інформації є необхідним для забезпечення загального рівня безпеки.

Взаємодія суб'єктів і об'єктів захисту

Система захисту інформації працює лише в разі ефективної взаємодії між суб'єктами і об'єктами захисту. Наприклад, адміни системи (суб'єкти) налаштовують програмне забезпечення та апаратні засоби (об'єкти) для захисту інформації, створюючи політики доступу, моніторинг і реагування на загрози. Важливим аспектом цієї взаємодії є навчання персоналу, який має розуміти та дотримуватися процедур безпеки. Спільно з технічними засобами, такі заходи дозволяють вчасно виявляти й нейтралізувати

загрози, забезпечуючи безпеку інформації. Кожен об'єкт захисту, будь то фізичний чи віртуальний, має бути належно інтегрований в систему для ефективного виконання своїх функцій. Це включає постійний моніторинг і оновлення систем захисту в разі виникнення нових загроз. Адміністратори системи також взаємодіють із розробниками програмного забезпечення для вдосконалення засобів захисту. Таким чином, всі компоненти системи захисту взаємодіють для забезпечення комплексного рівня безпеки на кожному етапі обробки інформації.

26.3. Основні вимоги, завдання та принципи організації КСЗІ

Комплексна система захисту інформації (КСЗІ) повинна забезпечувати конфіденційність, цілісність і доступність інформації на всіх етапах її обробки та зберігання, забезпечуючи захист від несанкціонованого доступу, змін або пошкодження даних. Основною вимогою є здатність системи забезпечити безпеку без значного погіршення характеристик функціонування автоматизованих систем (АС), зокрема не порушуючи їх продуктивність. Система захисту має бути економічно доцільною, з огляду на витрати на її впровадження та обслуговування, що включає як прямі витрати на апаратне і програмне забезпечення, так і витрати на підготовку персоналу та навчання.

Захист інформації має бути забезпечений на всіх етапах життєвого циклу АС, починаючи з проектування та розробки і завершуючи обслуговуванням і регламентними роботами, що включає технічну підтримку, оновлення систем і проведення заходів із забезпечення безпеки. Важливо, щоб система була гнучкою та масштабованою, забезпечуючи можливість її вдосконалення відповідно до змін у технологічних умовах або загрозах. Відповідно до цього, система захисту повинна передбачати можливості для розвитку і адаптації до нових технологій та вимог безпеки, щоб не втратити ефективність на етапах експлуатації.

Особливою вимогою є інтеграція системи захисту з іншими інформаційними системами, що дозволяє забезпечити комплексний підхід до безпеки. Це включає можливість розмежування доступу до інформаційних об'єктів, а також застосування механізмів активного та пасивного захисту, таких як використання помилкових даних для відволікання зломисників. При цьому важливо, щоб система дозволяла вести аудит, моніторинг та розслідування випадків порушення безпеки, що забезпечує можливість своєчасного реагування на інциденти.

Крім того, система повинна бути простій у використанні, не викликати психологічної протидії з боку користувачів, а також бути зручною і доступною для технічного обслуговування, що дозволяє знизити ймовірність спроб обійти систему. Водночас, система захисту не повинна погіршувати екологічну ситуацію або мати негативний вплив на інші технічні системи в організації. Останнім важливим аспектом є відповідність системи встановленим стандартам і нормативам безпеки, таким як ISO/IEC 27001, що гарантує її ефективність і здатність адаптуватися до сучасних викликів безпеки.

Основні вимоги до комплексної системи захисту інформації

- Система захисту інформації повинна забезпечувати безперешкодну роботу автоматизованої системи (АС), виконуючи основні функції без істотного погіршення її характеристик або ефективності.
- Вона повинна бути економічно ефективною, оскільки вартість системи захисту є частиною загальних витрат на впровадження та експлуатацію АС.
- Захист інформації в АС має бути забезпечений на всіх етапах її життєвого циклу, включаючи всі технологічні режими обробки, а також під час виконання регламентних та ремонтних робіт.
- У систему захисту інформації повинні бути вбудовані можливості для її вдосконалення та адаптації до змінюваних умов експлуатації і розвитку конфігурації АС.
- КСЗІ (Комплексна система захисту інформації) повинна забезпечувати ефективне розмежування доступу до інформаційно захищених об'єктів даних (ІзОД) із застосуванням механізмів відволікання порушника на помилкову інформацію, що забезпечує як активний, так і пасивний захист.
- У разі взаємодії захищеної АС з іншими, незахищеними системами, система захисту повинна гарантувати дотримання політик розмежування доступу, що відповідають встановленим стандартам і вимогам.
- Система захисту повинна забезпечувати можливість обліку, моніторингу та розслідування випадків порушення безпеки інформації в АС, надаючи інструменти для ретельного аналізу та реагування.
- Впровадження системи захисту не повинно спричиняти негативного впливу на екологічну ситуацію, бути складним у використанні для

кінцевих користувачів або викликати психологічний опір та бажання уникати її використання.

Цей підхід дозволяє забезпечити ефективний рівень безпеки в сучасних умовах, враховуючи актуальні технічні, економічні та психологічні фактори.

Завдання комплексної системи захисту інформації

Комплексна система захисту інформації повинна вирішувати низку важливих завдань, спрямованих на забезпечення безпеки інформаційних ресурсів. Одним із ключових завдань є забезпечення конфіденційності, що полягає в захисті інформації від несанкціонованого доступу через застосування механізмів автентифікації та контролю доступу для користувачів і систем. Не менш важливим є завдання забезпечення цілісності даних, що включає захист від їх змін або пошкоджень унаслідок атак, помилок або несанкціонованих дій. Для цього необхідно застосовувати методи перевірки цілісності та виявлення змін у даних. Водночас важливо забезпечити доступність інформації, гарантуючи її наявність для авторизованих користувачів у будь-який час, а також забезпечити відновлення даних після технічних збоїв чи атак.

Крім того, необхідно ефективно управляти ризиками, що включає ідентифікацію, оцінку та управління потенційними загрозами для інформаційних ресурсів, зокрема пов'язаними з людським фактором, технічними несправностями та кіберзагрозами. Для цього необхідно впровадити постійний моніторинг системи та реєстрацію подій, що дозволяє здійснювати аудит та реагувати на інциденти. У рамках захисту від зовнішніх і внутрішніх загроз система повинна включати засоби протидії атакам з боку зловмисників, а також запобігання зловживанням з боку внутрішніх користувачів, які мають доступ до критичних даних.

Інтеграція з іншими системами безпеки є важливим завданням, оскільки вона забезпечує сумісність КСЗІ з існуючими системами безпеки на підприємстві, такими як системи виявлення вторгнень, антивірусні програми та фізичні засоби захисту. Не менш важливим є навчання та підвищення кваліфікації персоналу, адже регулярне навчання користувачів і адміністрації сприяє підвищенню обізнаності про ризики та методи захисту. Для забезпечення безперервної роботи системи слід також розробити та впровадити плани відновлення після інцидентів, що включають відновлення інформаційних ресурсів та функціональності системи. Завершальним завданням є забезпечення відповідності стандартам і нормативам у сфері інформаційної безпеки, що дозволяє дотримуватися вимог національних і міжнародних стандартів щодо захисту, конфіденційності та відповідності законодавству.

Перелік основних завдань, які повинна вирішувати комплексна система захисту інформації (КСЗІ), включає:

1. **Управління доступом користувачів** до ресурсів автоматизованих систем (АС) для захисту від неправомірного, випадкового або навмисного втручання в роботу системи. Це також включає забезпечення захисту від несанкціонованого доступу до інформаційних, програмних та апаратних ресурсів, як з боку сторонніх осіб, так і з боку персоналу організації та авторизованих користувачів, якщо їхні дії перевищують надані повноваження.

2. **Захист даних, що передаються по каналах зв'язку**, через застосування криптографічних методів і засобів автентифікації, щоб уникнути несанкціонованого доступу, прослуховування або модифікації переданої інформації.

3. **Реєстрація, збір, зберігання, обробка та видача відомостей** про всі події, що відбуваються в системі і можуть впливати на її безпеку. Це включає ведення журналів аудиту та забезпечення їхньої цілісності для подальшого аналізу.

4. **Контроль роботи користувачів** системи з боку адміністрації, що передбачає моніторинг дій користувачів у реальному часі. Система повинна оперативно сповіщати адміністратора безпеки про спроби несанкціонованого доступу до ресурсів АС, щоб забезпечити швидке реагування на інциденти.

5. **Контроль і підтримка цілісності критичних ресурсів** системи захисту та середовища виконання прикладних програм. Це забезпечує захист від змін, які можуть бути здійснені зловмисниками або з метою помилок в роботі програмного забезпечення.

6. **Забезпечення замкнутого середовища перевіреного програмного забезпечення** для захисту від безконтрольного впровадження в систему небезпечних програм (наприклад, зловмисних кодів, шкідливих закладок або небезпечних помилок). Це також включає захист від розповсюдження комп'ютерних вірусів та інших шкідливих програм, що можуть поставити під загрозу безпеку системи.

7. **Управління засобами системи захисту**, що включає ефективне управління всіма компонентами системи захисту (апаратними засобами, програмним забезпеченням, криптографічними засобами тощо). Це дозволяє підтримувати високий рівень безпеки, а також забезпечує оперативне оновлення та вдосконалення засобів захисту відповідно до змінюваних умов експлуатації і загроз.

Ці завдання складають основу для реалізації ефективної та надійної системи захисту, здатної мінімізувати ризики і забезпечити безпеку інформаційних ресурсів організації.

Основні принципи організації КСЗІ

Захист інформації в автоматизованих системах (АС) повинен ґрунтуватися на ряді основних принципів, які забезпечують ефективну і стійку безпеку інформаційних ресурсів. Важливими є принципи системності, комплексності, безперервності захисту, розумної достатності, гнучкості управління і застосування, відкритості алгоритмів і механізмів захисту, а також простоти застосування захисних заходів.

Принцип системності полягає в необхідності врахування всіх взаємозв'язків і змінних елементів системи захисту інформації, а також можливих загроз та шляхів проникнення в інформаційні ресурси. У розробці системи захисту важливо враховувати не тільки відомі загрози, а й потенційно нові способи атак, що можуть виникнути з часом. Це дозволяє створювати систему, здатну протистояти не лише сучасним загрозам, а й майбутнім викликам.

Принцип комплексності передбачає використання широкого спектра заходів і засобів захисту в єдиній системі. Для цього важливо застосовувати різноманітні методи захисту на всіх етапах і рівнях системи: від фізичних заходів до програмних рішень. При цьому система захисту повинна бути побудована таким чином, щоб перекривати всі потенційні канали для реалізації загроз і не мати слабких місць на стиках компонентів.

Принцип безперервності захисту означає, що захист інформації має бути постійним процесом, який починається на етапі проектування системи і триває на всіх етапах її життєвого циклу. Постійна організаційна та технічна підтримка засобів захисту, своєчасне оновлення і контроль доступу дозволяють мінімізувати ризики. Важливо, щоб у разі збоїв або порушень роботи засобів захисту, зловмисники не могли скористатися перервами для реалізації своїх атак.

Принцип розумної достатності ґрунтується на тому, що повний захист від усіх можливих загроз є неможливим. Тому важливо встановити таку глибину захисту, яка буде забезпечувати прийнятний рівень безпеки з урахуванням витрат на захист і потенційних ризиків. Це дозволяє знайти баланс між ефективністю захисту та економічною доцільністю.

Принцип гнучкості дозволяє адаптувати систему захисту до змін у зовнішніх умовах і вимогах, зберігаючи можливість варіації рівня захисту. Цей принцип важливий, коли система вже працює і потребує оновлення або налаштування без порушення її нормальної роботи. Зміни в умовах

експлуатації можуть вимагати адаптації або модернізації засобів захисту, і гнучкість дозволяє уникнути необхідності повної заміни системи.

Принцип відкритості алгоритмів і механізмів захисту передбачає, що захист не повинен залежати від секретності алгоритмів чи структурних елементів системи. Однак це не означає, що система захисту повинна бути загальнодоступною. Принцип відкритості забезпечує прозорість алгоритмів, але не дозволяє зловмисникам використовувати цю інформацію для подолання захисту.

Принцип простоти застосування засобів захисту полягає в тому, що механізми захисту повинні бути зручними та інтуїтивно зрозумілими для користувачів. Засоби захисту не повинні створювати додаткових складнощів у використанні, таких як введення численних паролів чи виконання складних операцій, що може відволікати користувачів від їх основних завдань.

Принцип адаптивності – система повинна мати здатність адаптуватися до нових загроз, змінюваних умов експлуатації та технологічних новинок. КСЗІ повинна забезпечувати можливість оновлення та модифікації своїх компонентів без значного порушення її роботи.

Принцип надійності – компоненти КСЗІ повинні бути спроектовані та впроваджені таким чином, щоб забезпечити максимальний рівень стійкості до спроб злому чи несанкціонованого доступу. Для цього важливо використовувати надійні алгоритми шифрування, багаторівневу аутентифікацію, засоби детектування вторгнень.

Принцип прозорості – система захисту повинна забезпечувати аудит і контроль доступу до інформації, що дозволяє своєчасно виявляти порушення або спроби вторгнення. Усі дії користувачів і адміністраторів повинні бути зафіксовані для подальшого аналізу та виявлення можливих інцидентів.

Принцип простоти і зручності – для забезпечення ефективного функціонування КСЗІ важливо, щоб її механізми були зрозумілими і зручними для користувачів та адміністраторів. Вони не повинні створювати додаткових складнощів у роботі, щоб не знижувати продуктивність користувачів.

Принцип відповідності нормативним вимогам – система захисту повинна відповідати національним та міжнародним стандартам і нормативам в галузі інформаційної безпеки, що гарантує її правомірність та відповідність вимогам законодавства.

Таким чином, для забезпечення високої ефективності захисту інформації в АС важливо дотримуватись цих основних принципів, що

дозволяє створити систему, яка не лише забезпечує належний рівень безпеки, але й зберігає зручність і ефективність у її застосуванні.

26.4. КОНЦЕПЦІЯ СТВОРЕННЯ ЗАХИЩЕНИХ КСЗІ

При розробці та реалізації комплексної системи захисту інформації (СЗІ) в комп'ютерних системах необхідно дотримуватися методологічних принципів, що охоплюють всі етапи її життєвого циклу: дослідження, проектування, виробництво, експлуатацію та розвиток. Враховуючи складність таких систем, побудова СЗІ повинна базуватися на основних принципах створення складних систем з урахуванням специфіки вирішуваних завдань. Це забезпечить максимальну ефективність і знижує ризик виникнення уразливостей. Одним із ключових принципів є паралельна розробка комп'ютерної системи (КС) та СЗІ. Це означає, що захисні механізми повинні проектуватися та впроваджуватися на етапі розробки самої КС, що дозволяє забезпечити узгодженість між компонентами системи та системою захисту. Тільки в такому випадку можна досягти необхідного рівня захисту, враховуючи взаємний вплив блоків і пристроїв КС та захисних механізмів, що дозволяє створити системи з гнучким і високоякісним захистом.

Системний підхід є основним концептуальним принципом побудови СЗІ. В основі цього підходу лежить комплексний аналіз усіх можливих загроз безпеці інформації, зокрема фізичних, технічних та організаційних ризиків. На основі цього аналізу створюються ефективні механізми захисту, які повинні бути застосовані на всіх етапах життєвого циклу системи: від розробки до експлуатації. Принцип системності також передбачає інтегровану взаємодію всіх компонентів СЗІ, що дозволяє створювати багаторівневу структуру захисту, що перекриває один рівень захисту іншим. Такий підхід значно підвищує ефективність системи, оскільки зломисник повинен пройти через кілька рівнів захисту для того, щоб отримати доступ до конфіденційної інформації. Таким чином, чим більше рівнів захисту, тим складніше зламати систему.

Централізоване управління захистом інформації є важливим елементом для забезпечення єдиної політики безпеки на всіх рівнях підприємства або організації. Завдяки централізованому підходу можна організувати консистентний контроль за всіма компонентами СЗІ та своєчасно реагувати на можливі загрози. У випадку розподілених комп'ютерних систем управління захистом інформації може здійснюватися за ієрархічним принципом, коли на кожному рівні є відповідальні особи, які забезпечують функціонування та захист інформаційних ресурсів.

Блокова архітектура є ще одним важливим принципом, що дозволяє застосовувати стандартизовані модулі для розробки, тестування та верифікації пристроїв, зменшуючи складність і вартість обслуговування системи. Завдяки цьому можна легко інтегрувати нові блоки захисту в систему, покращуючи її здатність протистояти новим загрозам.

Блоки захисту, включаючи програмні, апаратні чи криптографічні компоненти, повинні бути взаємопов'язані між собою в певний спосіб, що дозволяє ефективно забезпечувати безпеку на всіх рівнях. Вони мають бути оптимально скомпоновані, щоб не лише забезпечувати високий рівень захисту, а й не знижувати продуктивність системи. Крім того, блокова архітектура дає можливість легко модернізувати систему в разі появи нових загроз або необхідності підвищення рівня безпеки. Застосування стандартних вхідних і вихідних інтерфейсів дозволяє забезпечити високий рівень взаємодії між різними блоками системи та забезпечує гнучкість при оновленні СЗІ.

Розвиток системи захисту інформації є важливим аспектом, оскільки інформаційні технології постійно змінюються, а також з'являються нові загрози, що потребують впровадження додаткових засобів захисту. Тому СЗІ повинна бути спроектована таким чином, щоб вона могла адаптуватися до змін, підтримувати нові технології і відповідаючи на нові виклики. Для цього на етапі розробки має бути передбачено достатньо ресурсів, що дозволяють без проблем розширювати можливості системи в майбутньому. Ресурси системи можуть бути витрачені для інтеграції нових користувачів або додаткових технологічних компонентів, що забезпечує постійну актуальність і здатність до масштабування.

Не менш важливим є принцип дружності системи до користувачів і обслуговуючого персоналу. Комплексна система захисту повинна бути максимально автоматизованою та зручними у використанні. Це дозволяє зменшити ймовірність помилок з боку персоналу, а також покращити взаємодію з системою без створення зайвих труднощів. Важливо, щоб система не створювала обмежень для виконання користувачами своїх функціональних обов'язків, а натомість забезпечувала їм необхідний рівень доступу до інформації в рамках встановлених правил безпеки.

Система повинна мати механізми, які дозволяють знімати захист з несправних пристроїв для відновлення їх працездатності, що дозволяє забезпечити безперервність процесів. Це також включає функції моніторингу і реагування на можливі порушення в роботі системи, що дозволяє своєчасно виявляти і усувати проблеми, не порушуючи основних функцій системи. Таким чином, комплексна система захисту інформації повинна бути високоякісною, гнучкою і адаптивною до змінюваних умов,

забезпечуючи надійний захист інформаційних ресурсів у сучасному цифровому середовищі.

26.5. ЕТАПИ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Система захисту інформації повинна розроблятися паралельно з створенням комп'ютерної системи (КС). Це дозволяє інтегрувати засоби захисту на всіх етапах життєвого циклу КС і забезпечити ефективну взаємодію між компонентами захисту та самою системою. Для побудови такої системи можуть бути використані як існуючі, так і спеціально розроблені засоби захисту, залежно від специфіки КС, умов її експлуатації та вимог до захисту інформації. В процесі створення комплексної системи захисту, зазвичай, включають наступні етапи:

- Розробка технічного завдання (ТЗ).
- Ескізне проектування.
- Технічне проектування.
- Робоче проектування.
- Виробництво дослідного зразка.

Один із важливих етапів розробки — це створення технічного завдання, яке визначає основні технічні вимоги до системи захисту інформації (КСЗІ). Саме на цьому етапі вирішуються ключові питання, пов'язані з вибором підходів та технологій захисту, а також узгоджуються взаємні зобов'язання між замовником і виконавцем.

Процес розробки, що завершується складанням технічного завдання, називається науково-дослідною розробкою, а наступні етапи — дослідно-конструкторською розробкою. Для цього використовуються системи автоматизації проектування, які дозволяють ефективно виконувати алгоритми проектування. Однак важливим є саме науково-дослідний етап, що визначає напрямок розвитку системи.

Метою науково-дослідного проектування є розробка технічного завдання, яке містить вимоги до характеристик і функцій КСЗІ, а також визначення параметрів, таких як швидкодія, продуктивність, надійність апаратних і програмних засобів. Програми захисту характеризуються вимогами до оперативної та зовнішньої пам'яті, програмного середовища, сумісності з операційними системами та іншими засобами. Основний зміст цього етапу — визначення функцій та режимів роботи засобів захисту, їх взаємодії з іншими компонентами системи.

Науково-дослідна розробка починається з аналізу загроз безпеці інформації, характеристик КС, що захищається, та оцінки важливості й конфіденційності інформації. Першим кроком є оцінка інформації, що обробляється в системі. Якщо інформація не є конфіденційною, то створення КСЗІ не буде доцільним. У разі, коли втрата цілісності і конфіденційності не має значних наслідків, можна обмежитися стандартними засобами захисту.

Аналіз інформації на цьому етапі дозволяє виявити потоки конфіденційної інформації та визначити елементи КС, що її обробляють і зберігають. Також важливим є визначення вимог до захисту інформації, що включають встановлення рівнів доступу та правил розмежування доступу.

Інформація для побудови КСЗІ також отримується через аналіз архітектури системи. Враховуються як внутрішні, так і зовнішні умови, які визначають взаємодію системи захисту з комп'ютерною системою та зовнішнім середовищем. Внутрішні умови залежать від архітектури КС, типу її компонентів, продуктивності та надійності елементів, а також можливих загроз, таких як відмови технічних засобів або помилки програмного забезпечення.

Зовнішні умови включають взаємодію з іншими системами та можливі випадкові або навмисні загрози, які можуть виникнути через зовнішні чинники. Аналіз загроз безпеці є критично важливим етапом побудови КСЗІ. Це включає створення моделі загроз безпеці, яка визначає всі можливі загрози для інформації в системі, їх ймовірність та серйозність. Моделювання загроз може бути здійснене через два підходи: модель висококваліфікованого зловмисника або модель, що враховує різні рівні кваліфікації зловмисників.

Моделювання зловмисників зазвичай включає три класи:

- Висококваліфікований зловмисник-професіонал.
- Кваліфікований зловмисник-непрофесіонал.
- Некваліфікований зловмисник.

Підхід до моделювання залежить від специфіки КС, її вимог до захисту і рівня можливих загроз. З іншого боку, для випадкових загроз також розробляються моделі, що ґрунтуються на статистичних даних і дозволяють прогнозувати виникнення таких загроз.

Моделі зловмисників та випадкових загроз формують основу для побудови КСЗІ, дозволяючи визначити необхідні заходи для забезпечення безпеки інформації та формулювати вимоги до захисту, враховуючи всі внутрішні і зовнішні умови. Ці моделі враховують різноманітні типи атак і вразливостей, зокрема, як зовнішні, так і внутрішні загрози, що може включати як людський фактор, так і технічні проблеми. Моделювання

зловмисників дає змогу передбачити різні сценарії атак і оцінити ймовірність їх здійснення. Це дозволяє створювати ефективні стратегії для захисту інформаційних систем на основі розуміння потенційних вразливостей і поведінки зловмисників. Одним із важливих аспектів є визначення рівня ризику, що залежить від характеру атакуючих, а також технічного й організаційного контексту. Врахування цих загроз дозволяє правильно сформулювати вимоги до технічних і організаційних заходів безпеки, сприяючи ефективному розподілу ресурсів для захисту інформації.

Загрози можуть бути класифіковані за різними параметрами, включаючи тип зловмисників (внутрішній, зовнішній, конкурент), їхню мету (викрадення даних, саботаж, шантаж) та використання технологій (фізичні, кібератаки, соціальна інженерія). Моделі випадкових загроз також мають важливе значення, оскільки вони допомагають визначити ймовірність несанкціонованого доступу через непередбачені обставини, такі як поломка обладнання чи помилки в програмному забезпеченні. Врахування моделей загроз є критичним для проектування адекватних заходів безпеки, що дозволяють ефективно реагувати на різноманітні атаки та забезпечити довгострокову надійність системи. Це забезпечує створення системи захисту, яка здатна передбачити й усунути більшість потенційних загроз на ранніх етапах.

26.6. Моделювання КСЗІ

Оцінка ефективності функціонування комплексних систем захисту інформації (КСЗІ) є складним науково-технічним завданням, яке включає етапи розробки, експлуатації та модернізації системи для вже існуючих об'єктів. Одним з основних підходів до проектування складних систем є синтез, після якого слідує аналіз для оцінки ефективності. Це дозволяє вибрати оптимальну систему шляхом моделювання. Моделювання КСЗІ полягає в створенні моделі системи, яка з певною точністю відображає реальні процеси, що відбуваються в захищеному середовищі.

Існують два основних типи моделей для оцінки систем: аналітичні та імітаційні. Аналітичні моделі описують функціонування системи через математичні або логічні співвідношення, використовуючи потужні методи математичної статистики, теорії ймовірностей та інші математичні інструменти. Імітаційне моделювання включає створення аналогів реальних систем, де відображаються зміни характеристик відповідно до математичних і логічних залежностей. Моделі можна розділити на

детерміновані та стохастичні, причому останні є більш актуальними для моделювання систем захисту, оскільки багато факторів, що впливають на безпеку, є випадковими.

Задача моделювання КСЗІ ускладнюється через кілька важливих аспектів:

- ✓ Складність формального представлення процесів через людський фактор.
- ✓ Різноманіття архітектурних рішень, що обумовлено різними структурами підсистем.
- ✓ Велика кількість взаємозв'язаних елементів та підсистем.
- ✓ Неоднозначність і випадковість процесів, що впливають на функціонування системи.
- ✓ Множинність критеріїв ефективності та складність визначення інтегрованих ознак системи.

Для подолання цих складнощів використовуються спеціальні методи моделювання, зокрема:

- Неформальні методи моделювання, засновані на теорії систем та структуризації процесів.
- Декомпозиція завдання на менші, що дозволяє легше оцінювати окремі аспекти ефективності.
- Макромодельовання, яке спрощує задачу через фокусування на основних характеристиках системи для попередніх оцінок.

Спеціальні методи неформального моделювання

Ці методи ґрунтуються на застосуванні неформальної теорії систем, що включає:

- * Структуризацію архітектури і процесів функціонування складних систем.
- * Неформальні методи оцінювання та пошуку оптимальних рішень.

Прикладом структурованих процесів може бути конвеєрне виробництво, де всі елементи і технологічні операції строго регламентовані та стандартизовані. Цей підхід активно застосовується в процесах розробки технічних засобів для КСЗІ, де на основі принципів структурного програмування формуються умови для розробки моделей систем. Важливими вимогами є повнота відображення елементів, адаптивність і простота організації.

Для оцінки складних характеристик, таких як ймовірність реалізації загроз, часто використовуються неформальні методи, зокрема експертні оцінки, коли залучаються фахівці для визначення характеристик системи.

Ці методи дозволяють отримати важливі дані про ефективність захисту, використовуючи знання та досвід експертів.

Декомпозиція завдання з оцінки ефективності функціонування КСЗІ

Зважаючи на складність і нечіткість початкових даних, ефективну оцінку складних систем за допомогою єдиного методу моделювання практично неможливо провести. Тому застосовується метод декомпозиції, що полягає в поділі загального завдання на окремі частини для аналізу. Наприклад, оцінка ефективності методу шифрування може бути розділена на менші завдання, що стосуються перебору ключів або методу шифрування. Але при цьому важливо враховувати взаємозв'язки між завданнями, як у випадку захисту інформації від електромагнітних випромінювань і резервування важливих блоків. Для цього використовуються підходи до моделювання, які дозволяють поділити систему на рівні або функціональні частини, що дає змогу більш точно оцінити кожен аспект її роботи. Така декомпозиція дозволяє створювати ефективні стратегії для вирішення окремих частин завдання, одночасно зберігаючи узгодженість всієї системи. Наприклад, при оцінці системи кібербезпеки важливо розглядати окремо захист від шкідливих програм, а також механізми аутентифікації та доступу. Крім того, вивчення кожного елемента системи за допомогою декомпозиції дозволяє виявити потенційні вразливості, які не були б помічені в загальній оцінці. Це також дозволяє оптимізувати роботу системи безпеки, зменшуючи кількість ресурсів, необхідних для її ефективного функціонування. Важливою перевагою цього підходу є можливість оцінити ймовірність атак на різні компоненти системи окремо, що дозволяє визначити пріоритети у впровадженні захисту.

Врахування зв'язків між підсистемами також допомагає у забезпеченні їх сумісності й ефективності. Зокрема, інтеграція різних технологій захисту може вимагати спеціальних заходів для забезпечення їх взаємодії та запобігання потенційним уразливостям у взаємодії між компонентами системи.

Макромодельовання

Для отримання попередніх оцінок ефективності системи застосовується макромодельовання. Це підхід, при якому на високому рівні враховуються лише основні характеристики системи, що дозволяє спростити задачу для отримання орієнтовних результатів. Макромодельовання є корисним на етапах попереднього аналізу, коли потрібно оцінити потенційну ефективність без глибоких детальних

розрахунків. Цей метод дозволяє швидко оцінити загальний стан безпеки або ефективність захисних заходів, враховуючи основні фактори, як, наприклад, рівень ризиків, обсяги інформації та характер загроз. Макромодельовання також дозволяє побудувати загальну картину можливих проблем у системі, яка буде уточнена на наступних етапах розробки. Однак варто зазначити, що такі попередні оцінки не завжди можуть забезпечити точність, оскільки не враховуються деталі реалізації конкретних технічних засобів захисту. Для досягнення точнішого розуміння потенційної ефективності, потрібно перейти до більш детальних моделей, зокрема до мікромоделювання, яке враховує індивідуальні характеристики компонентів системи. Макромодельовання має перевагу в швидкості, проте його обмеження полягають у недостатньому рівні деталізації. Таким чином, цей підхід застосовується в тих випадках, коли необхідно прийняти рішення на основі попередніх оцінок, зокрема, при виборі стратегій для подальшого проектування системи. На основі отриманих результатів макромодельовання можна вирішити, які напрямки потребують подальшого поглибленого аналізу та які фактори слід врахувати для уточнення проектних рішень.

Таким чином, для успішної оцінки ефективності КСЗІ необхідне використання комбінованих підходів, включаючи теоретичні методи, експертні оцінки, модельовання та декомпозицію задач, що дозволяє отримати обґрунтовані й детальні результати.

26.7. ВИБІР ПОКАЗНИКІВ ЕФЕКТИВНОСТІ І КРИТЕРІЇВ ОПТИМАЛЬНОСТІ КСЗІ

Ефективність інформаційних систем оцінюється за допомогою показників ефективності, які часто замінюють терміном "показник якості". Показники якості, в свою чергу, характеризують ступінь вдосконалення або функціональності певного товару, пристрою чи технології. У випадку складних людино-машинних систем, що включають, наприклад, інформаційну безпеку або кіберзахист, зазвичай використовують термін "показник ефективності функціонування", який визначає, наскільки система відповідає своїм призначеним цілям.

Прикладом показника ефективності може бути криптостійкість шифру, що вимірюється часом або ресурсами, необхідними для його зламу. Для шифру DES, наприклад, цей показник залежить від довжини ключа, тоді як для інших методів шифрування, таких як методи заміни чи

перестановки, криптостійкість визначається іншими характеристиками, наприклад, кількістю алфавітів заміни або розмірністю таблиць.

Для оцінки ефективності системи захисту інформації або порівняння різних систем використовують критерії ефективності. Критерій ефективності базується на порівнянні показників за допомогою певних підходів, які дозволяють встановити перевагу однієї системи над іншою.

Методи оцінки ефективності можуть включати:

Методи ранжування показників

Це підхід, при якому показники ефективності системи порівнюються по черзі в порядку їх значущості. Одним із прикладів є лексикографічний метод, який ефективний, коли різниця між показниками за важливістю є значною. Спочатку системи порівнюються за найважливішим показником. Якщо показники рівні, порівнюються другорядні характеристики, і так до отримання переваги.

Метод послідовних поступок

Застосовується в ситуаціях, коли є декілька важливих, але не однакових показників ефективності. Порівняння систем проводиться по черзі за кожним показником.

Метод Парето

Це метод, що використовує кілька показників для оцінки системи. Рішення в рамках методу Парето будуються в багатовимірному просторі, і область парето-оптимальних рішень визначає ті варіанти, які не можуть бути покращені без погіршення інших показників. У цій області розташовані рішення, для яких подальше покращення одного з показників веде до зниження інших.

Сучасні методи оцінки ефективності часто включають також алгоритми на основі машинного навчання та штучного інтелекту, що дозволяють автоматизувати процес порівняння та прийняття рішень в реальному часі. Ці підходи використовуються для постійного моніторингу та оптимізації роботи складних інформаційних систем, особливо в умовах високих ризиків та загроз у кіберпросторі.

26.8. Підходи до оцінки ефективності КСЗІ

Ефективність системи захисту інформації (КСЗІ) оцінюється як на етапі її розробки, так і в процесі експлуатації. Оцінка ефективності може здійснюватися за різними підходами в залежності від використовуваних показників і методів їх отримання. Зазвичай виділяють три основних підходи до оцінки ефективності КСЗІ:

1. Класичний підхід

Класичний підхід до оцінки ефективності базується на використанні критеріїв, що формуються за допомогою показників ефективності. Ці показники можуть бути отримані шляхом моделювання або обчислюватися на основі характеристик реальної КСЗІ. Такий підхід застосовується на етапах розробки та модернізації системи захисту інформації. Однак класичні методи мають певні обмеження: висока невизначеність початкових даних, складність формалізації процесів функціонування та відсутність універсальних методик для розрахунку показників і вибору оптимальних критеріїв створюють труднощі в їх застосуванні.

2. Офіційний підхід

Офіційний підхід до визначення ефективності КСЗІ має важливе практичне значення. Державна політика безпеки інформаційних технологій, зокрема у сфері КСЗІ, повинна спиратися на нормативні акти та стандарти, що регулюють вимоги до захисту інформації різних категорій конфіденційності та важливості. Вимоги можуть включати перелік механізмів захисту інформації, що мають бути наявні в системі для досягнення певного класу захисту. Критерієм ефективності є рівень цього класу захисту, визначений стандартами та нормативами.

Основною перевагою офіційного підходу є його простота, адже застосовуються чітко визначені стандарти безпеки. Однак є і недоліки: цей підхід не дає змоги оцінити ефективність конкретних механізмів захисту, а лише констатує їх наявність або відсутність. Водночас у деяких документах можуть бути визначені достатньо докладні вимоги до цих механізмів.

Зокрема, в США використовується стандарт TCSEC (Department of Defence Trusted Computer System Evaluation Criteria), відомий як Оранжева книга, яка оцінює комп'ютерні системи за чотирма групами безпеки: А, В, С, D. Кожна з груп включає класи, що визначають рівень захисту:

- **А (Гарантований захист)** – забезпечує високий рівень безпеки, методи захисту можуть бути перевірені формальними методами (A1).

- **В (Повний захист)** – має кілька класів (B1, B2, B3), що забезпечують різні рівні захисту залежно від складності механізмів.

- **С (Вибірчий захист)** – включає класи C1 і C2, які забезпечують мінімальний захист через контроль доступу.

- **D (Мінімальна безпека)** – для систем з базовим рівнем захисту.

Подібні стандарти також існують в інших країнах. Наприклад, в Європі країни, як Франція, Німеччина, Нідерланди та Великобританія, у 1991 році прийняли узгоджені «Європейські критерії», які поділяються на

шість класів безпеки (від E0 до E5), що характеризують різні рівні захисту інформації, зокрема дискреційний та мандатний захист, а також верифікацію. Ці класи допомагають визначити рівень надійності та ефективності систем захисту, залежно від складності та чутливості оброблюваної інформації.

В Україні також розроблені та впроваджуються національні стандарти в галузі інформаційної безпеки, зокрема, методики та класифікації для захисту інформаційних систем. Зокрема, стандарт ISO/IEC 27001, який є міжнародно визнаним стандартом для систем управління інформаційною безпекою, також активно використовують в Україні. Він сприяє впровадженню систем захисту на основі ризик-орієнтованого підходу, що дозволяє підприємствам та організаціям адекватно реагувати на сучасні загрози безпеці. Також важливим є розвиток стандарту ISO/IEC 27032 для кібербезпеки, що забезпечує зростаючий попит на захист цифрових ресурсів у всьому світі. Дослідження загроз та заходи захисту на основі цих стандартів дозволяють країнам узгоджено реагувати на глобальні виклики інформаційної безпеки. Стандарти та норми для забезпечення кібербезпеки мають важливе значення для адаптації до новітніх загроз та виявлення вразливостей в інформаційних системах. Впровадження подібних стандартів на національному рівні дозволяє країнам не лише посилити свої кіберзахисти, а й підвищити рівень безпеки критичної інфраструктури.

3. Експериментальний підхід

Цей підхід полягає в оцінці ефективності системи шляхом проведення реальних експериментів або тестувань. Експериментальний підхід дозволяє на практиці перевірити, наскільки система захисту відповідає вимогам безпеки та функціональності в реальних умовах. Це може включати тестування на проникнення, виявлення уразливостей або оцінку реакції системи на різні загрози та атаки.

Сучасні методи оцінки ефективності КСЗІ також включають використання автоматизованих інструментів для моніторингу безпеки, що дозволяє здійснювати постійний аналіз і корекцію системи в процесі її експлуатації, а також застосування методів машинного навчання для прогнозування можливих загроз і оцінки ефективності механізмів захисту в реальному часі. Таким чином, сучасні підходи до оцінки ефективності КСЗІ інтегрують як традиційні методи, так і новітні технології для досягнення комплексного і динамічного підходу до забезпечення безпеки інформаційних систем.

26.9. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ

Концептуальні підходи до проектування систем захисту інформації (КСЗІ) — це основні методології, за допомогою яких розробляються і реалізуються стратегії захисту інформаційних систем. Вони визначають загальні принципи і методи організації захисту в залежності від потреб і умов конкретної організації. Кожен підхід має свої особливості, що дозволяє адаптувати систему захисту до різних типів організаційних структур і технологічних середовищ. Підхід «від продукту» спрямований на інтеграцію вже існуючих рішень і продуктів без значних змін в архітектурі, що дозволяє швидко впроваджувати системи захисту. Однак цей підхід може бути обмежений у гнучкості і адаптивності до специфічних потреб організації. Підхід «від рішень» орієнтований на вибір окремих технологій, що комбінуються для вирішення конкретних загроз, проте може потребувати додаткових зусиль для інтеграції і сумісності компонентів. Найбільш комплексним є підхід «від потреб організації», при якому проектування системи базується на глибокому аналізі конкретних ризиків і потреб бізнесу. Це дозволяє створити індивідуальну стратегію захисту, яка відповідає вимогам організації на кожному етапі розвитку. Однак такий підхід вимагає значних ресурсів і висококваліфікованих фахівців. Вибір концептуального підходу залежить від масштабів організації, наявних ресурсів та вимог до безпеки. Можна виділити три основні концептуальні підходи до проектування систем захисту інформації (КСЗІ):

1. Підхід "від продукту"

Підхід зазвичай застосовується компаніями-виробниками систем захисту інформації, у яких є власні проектні групи. В таких компаніях інтеграція технологій почала розвиватися, коли замовники почали вимагати не просто продукт, а комплексне рішення, що включає проектування. Основна ідея цього підходу полягає в тому, щоб продукт, створений компанією, був центральним компонентом системи захисту, незалежно від конкретних задач. Однак цей підхід може бути проблемним в умовах агресивного маркетингу, коли продукт позиціонується як "панацея" від усіх загроз безпеки. Водночас, для замовників, які мають достатній рівень кваліфікації, цей підхід може забезпечити високоякісні проекти. Але для цього необхідна наявність фахівців, які можуть оцінити всі аспекти захисту, або залучення зовнішніх консалтингових компаній.

2. Підхід "від рішень"

У цьому випадку компанія-постачальник не обмежується одним продуктом, а пропонує комплексні рішення, що складаються з різних технологій захисту, таких як міжмережеві екрани, VPN, криптографічний захист і активний аудит. Такий підхід орієнтований на комбінування різних технологій для створення системи, яка може захистити від кількох видів загроз. Однак це може призвести до того, що вибір технологій базуватиметься не на потребах замовника, а на наявних засобах захисту, що може бути не оптимальним, особливо в організаціях з традиційними системами документообігу. Технології, такі як VPN чи електронні замки, можуть не мати сенсу, якщо інформація передається через звичайну електронну пошту або зберігається в незахищених папках.

3. Підхід "від потреб організації"

Підхід є найскладнішим і рідше застосовується на нашому ринку. У ньому система безпеки розробляється на основі ретельного аналізу потреб організації. Перш ніж запропонувати рішення, системний інтегратор проводить всебічне обстеження організації на трьох рівнях: рівень бізнес-процесів (для визначення документальних потоків і рівнів конфіденційності інформації), інфраструктурний рівень (для виявлення вразливих місць серверного парку та мережевого обладнання) і рівень додатків (для виявлення помилок у програмному забезпеченні та налаштуваннях систем захисту). На основі цього аналізу формується концептуальне рішення, яке включає організаційні, процедурні та технічні заходи захисту. Важливо, що система інформаційної безпеки повинна бути підтримуючою системою для всієї інформаційної системи організації, не домінувати над іншими її компонентами та бути адекватною до бізнес-завдань.

Таким чином, кожен з цих підходів має свої переваги і недоліки, і правильний вибір підходу залежить від конкретних умов та потреб організації. Важливо, щоб система захисту була розумно достатньою для забезпечення необхідного рівня безпеки, не заважаючи нормальній діяльності організації та її співробітників.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 26

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.

2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. Про основні засади забезпечення кібербезпеки України: Закон України // Відомості Верховної Ради України. 2017. № 45. Ст. 403.

3. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

4. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.

5. Костюк Ю.В., Гейдар Гейдаров. Роль токенів та сесійного керування в системах інформаційної безпеки для протидії міжсайтовим атакам. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1216-1231.

6. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.

7. Костюк Ю.В., Андрій Голинський. Стратегії інтегрованого захисту бездротових сенсорних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1232-1247.

8. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроектні рішення щодо побудови системи авторизації на основі концепції zero trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242.

9. G. Otto, et al., Parametric Model of a Laser with External Distributed Feedback in the System of Remote Measurement of Nanovibrations, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3421 (2023) 284–292.

10. P. Anakhov, et al., Hybrid Study of the Geophysical Situation in the Depressed Zone of Hydroelectric Power Plants Reservoir, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 269-274.

11. S. Abramov, A. Bessalov, V. Sokolov, Properties of Isogeny Graph of Non-Cyclic Edwards Curves, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 234–239.

12. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.
13. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158
14. Костюк Ю.В., Рзаєва С.Л. Стратегічні рішення SOC для забезпечення інформаційної безпеки в умовах сучасних кіберзагроз (2024) Сучасні вектори розвитку України: забезпечення сталості та безпеки. Збірник матеріалів II Міжнародної науково-практичної конференції (м. Київ, 28 жовтня 2024 року). Чернігів: ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2024, с.
15. R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, vol. 3800 (2024) 97–105.
16. L. Kriuchkova, V. Sokolov, P. Skladannyi, Determining the Zone of Successful Interaction in RFID Technologies, in IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (2024) 168–171.
17. S. Kulibaba, et al., Linked System of Data Organization and Management, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 117–126.

КОНТРОЛЬНІ ПИТАННЯ

1. Які основні принципи лежать в основі концепції створення захищених КСЗІ?
2. Які етапи включає процес розробки захищеної КСЗІ?
3. Яким чином визначається вимога до рівня захисту в концепції КСЗІ?
4. Які стандарти і нормативні акти слід враховувати при розробці КСЗІ?
5. Як концепція створення захищених КСЗІ взаємодіє з загальною політикою безпеки підприємства?
6. Надайте визначення комплексної система захисту інформації.
7. Опишіть концепцію створення захищених КС.
8. Які є етапи створення комплексної системи захисту інформації ?
9. В чому полягає науково-дослідна розробка КСЗІ ?

10. Що таке моделювання КСЗІ ?
11. Як проходить вибір показників ефективності і критеріїв оптимальності КСЗІ.
12. Опишіть підходи до оцінки ефективності КСЗІ
13. Які типи загроз повинні бути враховані на етапі створення КСЗІ?
14. Які критерії визначають вибір архітектури для КСЗІ?
15. Які основні етапи включає процес створення комплексної системи захисту інформації?
16. Як на кожному етапі створення КСЗІ здійснюється верифікація та тестування системи?
17. Чим відрізняються етапи проектування та реалізації КСЗІ?
18. Як визначити необхідність оновлення системи захисту інформації на різних етапах її розвитку?
19. Яким чином проводиться інтеграція захищених елементів в існуючі інформаційні системи?
20. Які методи моделювання використовуються для оцінки ефективності КСЗІ?
21. Як моделювання допомагає виявити потенційні уразливості в системах захисту інформації?
22. Яким чином проводиться симуляція атак на КСЗІ в рамках моделювання?
23. Які програмні засоби можна використовувати для моделювання КСЗІ?
24. Як визначити основні показники ефективності КСЗІ?
25. Які фактори впливають на вибір критеріїв оптимальності для КСЗІ?
26. Яким чином оцінюється криптостійкість системи захисту інформації як один з показників ефективності?
27. Які підходи до оцінки ефективності КСЗІ є найбільш ефективними на етапі експлуатації системи?

ТЕМА 8. ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ ІКС ПІСЛЯ РЕАЛІЗАЦІЇ ЗАГРОЗ, ЗДІЙСНЕННЯ КІБЕРАТАК, ЗБОЇВ

РОЗДІЛ 27 ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ ІКС



27.1. Організаційно-технічні заходи відновлення функціонування ІКС

27.2. Журнал аудиту подій

27.3. Політики резервного копіювання

"Безпека — це процес, а не продукт. Ключовим є здатність до відновлення після порушення, а не лише його запобігання."

Брюс Шнайєр, криптограф та експерт з кібербезпеки

27.1. ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ЗАХОДИ ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ ІКС

Організаційно-технічні заходи відновлення функціонування інформаційно-комунікаційних систем (ІКС) є невід'ємною частиною процесу забезпечення безперервності діяльності організації та збереження цілісності її даних у разі виникнення надзвичайних ситуацій, таких як технічні збої, кібератаки, природні катастрофи чи людські помилки. Задля ефективного відновлення ІКС після інцидентів необхідно впровадити комплекс заходів, які включають як технічні рішення, так і організаційні

процедури. Можливість повної втрати даних за відсутності програми післяаварійного відновлення ставить під загрозу діяльність організацій, які не мають коштів для відновлення працездатності після катастрофічних подій. У багатьох компаніях планування надзвичайних заходів фокусується вже насамперед на ІТ. Програма збереження безперервності бізнес-операцій та післяаварійного відновлення може стати одним із найцінніших вкладів відділу ІТ у успішну діяльність організації.

1. Оцінка ризиків і планування відновлення

Оцінка ризиків є першим і найважливішим кроком у створенні політики відновлення функціонування ІКС. Вона передбачає виявлення й аналіз потенційних загроз, які можуть вплинути на роботу системи: технічні збої, кіберзагрози, природні катастрофи чи людські помилки. Оцінка включає визначення ймовірності виникнення таких загроз та їх можливого впливу на ІКС. На основі отриманих результатів формується план відновлення, який включає в себе пріоритети відновлення критичних систем і даних, а також чітке визначення обов'язків та відповідальності для членів команди реагування. План відновлення повинен також включати часові рамки, необхідні для відновлення кожної функції та технічного компонента системи, що допомагає уникнути непотрібних затримок.

2. Технічні засоби для відновлення

Технічні засоби відновлення функціонування ІКС є ключовими елементами плану. Серед найбільш ефективних технічних рішень — це резервне копіювання даних. Регулярне створення резервних копій забезпечує можливість швидкого відновлення критичних даних після збоїв. Важливо, щоб резервні копії зберігались в безпечному місці, де вони не піддаються ризику одночасної втрати з основними даними, наприклад, в хмарних сервісах або на віддалених серверах. Також для підвищення стійкості ІКС важливо застосовувати кластеризацію та віртуалізацію. Ці технології дозволяють створити розподілені системи, де навантаження автоматично перерозподіляється між серверами, що знижує ймовірність збоїв і зменшує час відновлення. Окрім цього, впровадження систем резервування енергопостачання забезпечує безперебійну роботу серверів під час перебоїв з електроживленням, що критично важливо для систем, які працюють 24/7.

3. Організаційні заходи

Організаційні заходи відіграють важливу роль у відновленні функціонування ІКС, оскільки саме вони визначають, як швидко та ефективно буде реагувати команда на інцидент. Основним елементом є створення команди реагування на інциденти, яка повинна включати

спеціалістів з різних напрямків — системних адміністраторів, розробників, фахівців з кібербезпеки, а також керівників підприємства. Команда має бути готовою до швидкого реагування, що передбачає чітко визначені процедури взаємодії та організаційні заходи для розв'язання кожної конкретної ситуації. Окрім того, важливим аспектом є тренування персоналу, яке включає регулярні навчання і симуляції реальних інцидентів. Це дає змогу співробітникам швидко приймати правильні рішення в умовах стресу і не допускати затримок при відновленні ІКС. Заняття повинні охоплювати як технічні аспекти відновлення, так і організаційні процедури, що включають комунікацію та управління процесами.

4. Тестування та перевірка процесів відновлення

Перевірка ефективності плану відновлення є важливим етапом для забезпечення готовності системи до непередбачених ситуацій. Регулярне тестування плану відновлення дозволяє виявити можливі слабкі місця в процесах відновлення, що може суттєво знизити час простою системи під час реальних інцидентів. Тестування має бути всеохопним і включати перевірку кожної частини плану: від процедур відновлення даних до злагодженості роботи команди. Одним з важливих етапів є перевірка відновлення після інцидентів, що дозволяє не лише переконатися в правильності всіх налаштувань, а й забезпечити актуальність та працездатність резервних копій даних.

5. Документування і звітність

Після кожного інциденту в ІКС важливо вести документування всіх інцидентів і дій, пов'язаних з відновленням. Це допомагає проаналізувати, які етапи відновлення були виконані правильно, а які потребують удосконалення. Документування дозволяє створювати детальні звіти про інцидент, що включають причини збоїв, час простою та ефективність реагування команди. Важливо також зберігати цю інформацію для подальшого аналізу та навчання персоналу. Аналіз і звітність допомагають не лише оцінити ефективність відновлення, а й розробити кроки для мінімізації подібних інцидентів у майбутньому. Така ретельна документація дозволяє створити основу для вдосконалення плану відновлення і підвищення його ефективності.

6. Забезпечення безпеки під час відновлення

Безпека інформації під час процесу відновлення є надзвичайно важливим аспектом. Для цього необхідно забезпечити контроль доступу до відновлених даних. Важливо, щоб лише авторизовані користувачі мали доступ до відновленої інформації, адже інцидент може бути пов'язаний з

кіберзагрозами або несанкціонованим доступом. Відновлення даних повинно відбуватись через захищені канали зв'язку, що дозволяє уникнути перехоплення або модифікації важливої інформації. Крім того, шифрування резервних копій та передавання даних допомагає забезпечити конфіденційність і цілісність інформації навіть під час її переміщення чи відновлення.

7. Оновлення і вдосконалення політики відновлення

Завершальним етапом є оновлення і вдосконалення політики відновлення на основі аналізу результатів відновлення після інцидентів. Кожен випадок відновлення повинен бути ретельно проаналізований для виявлення недоліків у плані та внесення необхідних змін. Після кожного тестування або реального інциденту важливо оновлювати методи і інструменти відновлення з урахуванням нових загроз і технологічних змін. Також потрібно адаптувати політику відновлення до нових типів атак, таких як кіберзлочини або пандемії, які можуть суттєво змінити умови для відновлення ІКС.

Таким чином, комплексне впровадження організаційно-технічних заходів відновлення функціонування ІКС є важливою складовою стратегії управління ризиками та безпеки інформаційних систем підприємства.

ШІСТЬ ЕТАПІВ ПЛАНУВАННЯ ДІЙ У АВАРІЙНИХ СИТУАЦІЯХ

У термінології планування дій у аварійних ситуаціях фігурують два загальні поняття: *планування збереження безперервності бізнесу (Business Continuity Planning, BCP)* та *планування післяаварійного відновлення (Disaster Recovery Planning, DRP)*. Ці поняття, які часто використовуються як рівноцінні, представляють різні концепції. BCP традиційно передбачає планування заходів, що забезпечують збереження ділової активності організації у надзвичайних ситуаціях. Сфера відповідальності DRP, за суттю, є підмножиною BCP і стосується відновлення інформації та працездатності систем у разі аварії. Наприклад, вихід з ладу жорсткого диска на сервері бази даних потенційно загрожує цілісності бізнесу, але не є результатом катастрофічних подій. Розрив водопровідної труби з затопленням серверного приміщення і зануренням сервера бази даних у воду становить загрозу цілісності бізнесу, що розглядається в рамках плану післяаварійного відновлення (DRP). Планування заходів BCP і DRP – справа непроста, і у великих організаціях цим часто займаються спеціальні групи. Однак навіть без детального аналізу ступенів ризику та вирішення інших складних питань у рамках BCP та DRP у великих компаніях можна створити програму збереження

цілісності бізнесу та післяаварійного відновлення, якщо дотримуватись наведених нижче етапів.

Етап 1. *Визначення критично важливих ділових операцій*

Перший крок планування рамках BCP і DRP – визначення критично важливих ділових операцій, тобто. дій, які мають виконуватися у повсякденному режимі задля збереження працездатності організації. Наприклад, центр прийому заявок клієнтів на виконання технічного обслуговування повинен зберігати здатність приймати та фіксувати заявки. Юридична фірма повинна мати доступ до інформації про клієнтів, надсилати та приймати електронну пошту, користуватися інтерактивними довідниками з права, а також відповідати на телефонні дзвінки. На даному етапі планування необхідно співпрацювати з головними відповідальними особами організації у визначенні видів діяльності, важливих для збереження її працездатності. У центрі планування заходів у межах BCP знаходиться збереження ділової активності організації з допомогою відновлення цих видів діяльності.

Етап 2. *Упорядкування схеми інфраструктури інформаційних систем, які забезпечують виконання критично важливих ділових операцій.*

Від визначення критично важливих ділових операцій переходимо до визначення інформаційних систем, що забезпечують їхнє виконання. Зокрема, в центрі прийому заявок клієнтів на проведення технічного обслуговування можливість перегляду зареєстрованих та фіксації нових заявок залежить від працездатності серверів бази даних, де зберігаються ці записи, та програм, що забезпечують доступ до цих серверів. Крім того, має також функціонувати певна частина центральної мережної інфраструктури, щоб ці критично важливі ділові операції могли виконуватись. Наведені вище інформаційні системи необхідно підтримувати у працездатному стані за рахунок оперативного післяаварійного відновлення.

Етап 3. *Моделі загроз у вигляді передбачуваних та ймовірних подій*

Моделі загроз, що базуються на передбачуваних та ймовірних подіях, є важливим інструментом для визначення потенційних ризиків, які можуть загрожувати цілісності бізнесу. Більшість катастрофічних подій, що можуть призвести до серйозних порушень у роботі організації, можна передбачити з певним ступенем ймовірності. Це можуть бути як природні

катастрофи, такі як землетруси чи повені, так і технічні збої, зокрема відмова апаратних засобів або перебої в енергопостачанні. Наприклад, якщо компанія має важливу інфраструктуру у районі, схильному до штормів, необхідно врахувати ймовірність таких подій, адже вони можуть призвести до серйозних наслідків, як для фізичної інфраструктури, так і для інформаційних систем. Подібні ситуації можуть також виникнути внаслідок відмови технічних засобів. Наприклад, в компанії, що активно використовує сучасні технології, завжди існує ймовірність поломки обладнання, такого як сервери, накопичувачі даних чи мережеві компоненти, що може призвести до зупинки бізнес-процесів або втрати даних. У разі поломки таких систем, як база даних або сервери, може стати неможливим забезпечення безперервного функціонування важливих бізнес-процесів. Для зниження таких ризиків важливо здійснювати моніторинг критично важливих систем і забезпечувати їх резервування. Одним із способів моделювання ймовірних загроз є визначення критичних систем, що забезпечують працездатність бізнесу, і прогнозування можливих сценаріїв порушення їх функціонування. Наприклад, якщо система обробки заявок клієнтів залежить від доступу до бази даних, то ймовірним сценарієм є порушення працездатності цієї системи через відмову апаратних засобів або перебої у постачанні енергії. Можливими попередніми подіями в таких випадках можуть бути неполадки в харчуванні або збої в апаратному забезпеченні. Водночас природні катастрофи, як шторм або повінь, можуть знищити або пошкодити важливі компоненти інфраструктури, що призведе до тривалих перерв у роботі бізнесу. Моделювання загроз дозволяє чітко визначити ймовірні події, що передують кожній загрозі, і розробити стратегії для зменшення негативних наслідків. Важливо вчасно визначити, які інциденти можуть найбільше вплинути на функціонування бізнесу, та розробити системи для зменшення ймовірності їхнього виникнення. Наприклад, для запобігання пошкодженню або зупинці інформаційних систем варто застосовувати технології резервування, впроваджувати регулярне оновлення програмного забезпечення та налаштовувати системи безпеки для швидкого виявлення і усунення технічних проблем до того, як вони призведуть до серйозних наслідків.

Етап 4: Розробка планів та процедур збереження цілісності бізнесу

Після визначення критично важливих бізнес-операцій, інформаційних систем, що їх підтримують, та можливих загроз для їхньої безперебійної

роботи, необхідно розробити превентивні заходи для збереження цілісності бізнесу з використанням актуальних моделей загроз.

У сучасній практиці виділяються чотири основні категорії превентивних заходів:

- Відмовостійкість та швидке відновлення
- Резервне копіювання
- "Холодні" запасні ресурси
- "Гарячі" запасні ресурси

Детальний розгляд категорій превентивних заходів

Відмовостійкість та швидке відновлення

Ця категорія передбачає використання сучасних технологій, які забезпечують стійкість до відмов апаратного чи програмного забезпечення. Серед найкращих практик — використання кластеризованих серверних систем, SSD-накопичувачів з резервуванням, хмарних сервісів для дублювання даних, а також генераторних і акумуляторних систем живлення для забезпечення безперервності роботи.

Резервне копіювання

Резервне копіювання залишається ключовим елементом захисту інформації. Актуальними підходами є використання хмарних сервісів з автоматичним створенням резервних копій та інкрементальні копії для збереження ефективного використання дискового простору. Регулярна перевірка відновлюваності даних є обов'язковою.

"Холодні" запасні ресурси

"Холодні" ресурси — це обладнання та інфраструктура, які не працюють постійно, але готові до швидкого розгортання у разі потреби. Наприклад, сервери з попередньо встановленим програмним забезпеченням, які можна підключити та швидко активувати. Також "холодні" приміщення можуть мати базову інфраструктуру для відновлення робочих процесів. Такий підхід є економічно вигідним для підприємств малого та середнього бізнесу.

"Гарячі" запасні ресурси

"Гарячі" ресурси — це повністю функціонуючі дублюючі системи, готові до негайного використання. Вони синхронізуються в режимі реального часу з основною інфраструктурою. Прикладом є хмарні резервні платформи або центр обробки даних з автоматичним перемиканням на дублюючі сервери. Такий підхід забезпечує мінімальні простой, але є дорогим і підходить для критичних секторів, таких як фінансові установи чи служби безпеки.

Запровадження ефективних планів та процедур збереження цілісності бізнесу дозволяє підприємствам оперативно реагувати на кризові ситуації,

зберігаючи критичні функції та мінімізуючи втрати. Використання передових технологій та перевірених практик значно підвищує стійкість бізнесу до загроз.

Етап 5. Розробка планів та процедур післяаварійного відновлення

Не всі катастрофи або інциденти можна передбачити чи оцінити ймовірність їхнього виникнення. Як приклад непередбачуваної катастрофи можна згадати атаки на Всесвітній торговий центр 11 вересня 2001 року. Такі надзвичайні ситуації, а також інші серйозні катастрофи, які можуть призвести до повної втрати даних і працездатності основних систем, вимагають розробки чітких і ефективних планів та процедур для післяаварійного відновлення (Disaster Recovery Plan, DRP). Розробка таких планів є критично важливою для кожної організації, оскільки післяаварійне відновлення відноситься до стресових ситуацій, і вкрай важливо мати під рукою добре документовані, перевірені та регулярно тестовані процедури. Це дозволяє мінімізувати час, необхідний для відновлення функціонування бізнесу після інциденту. Для впевненості у працездатності збережених даних необхідно регулярно тестувати процедури відновлення, зокрема через імітаційні вправи, які дозволяють перевірити їхню ефективність у реальних умовах. Збереження резервних копій та процедур відновлення в безпечному місці поза основною системою є важливою частиною плану DRP. Одним з найбільш надійних і доступних варіантів для позасистемного зберігання резервних копій та планів є використання депозитарних осередків або банківських сейфів, що гарантують високий рівень фізичної безпеки для збереження критичних даних. Це дозволяє забезпечити доступ до необхідної інформації навіть у разі серйозних інцидентів або фізичного пошкодження основних серверів. Таким чином, регулярне оновлення планів післяаварійного відновлення, перевірка їхньої працездатності через тестування та забезпечення надійного позасистемного зберігання резервних копій є важливими елементами стратегій, що дозволяють забезпечити безперервність бізнес-процесів навіть після серйозних катастроф.

Етап 6. Перевірка працездатності планів збереження цілісності бізнесу та випробування засобів післяаварійного відновлення

Сучасні реалії кіберзагроз і природних катастроф підкреслюють критичну важливість регулярного тестування планів забезпечення безперервності бізнесу (BCP) та післяаварійного відновлення (DRP). Перевірка працездатності таких планів дозволяє виявити потенційні слабкі

місця та забезпечити їх актуальність відповідно до змін у бізнес-середовищі та ІТ-інфраструктурі. Одним із ключових підходів є проведення планових і спонтанних перевірок стратегій. Це може включати регулярну імітацію відмов кластерних вузлів або хмарної інфраструктури для перевірки їх стійкості. Важливим елементом є тестове відновлення систем із використанням резервних копій як на "холодних", так і на "гарячих" серверах, щоб переконатися у готовності систем до відновлення критично важливих функцій. Окрему увагу слід приділити кіберсимуляціям — моделюванню кібератак із перевіркою стійкості інформаційних систем та можливості швидкого відновлення операцій. Це дозволяє не лише оцінити ефективність захисту, а й підготувати персонал до реагування на реальні інциденти. Не менш важливим є тестування процесів відновлення даних із резервних копій, що зберігаються у хмарних сховищах або захищених фізичних сховищах. Використання сучасних хмарних платформ, таких як AWS, Azure чи Google Cloud, забезпечує автоматизацію процесів резервного копіювання, криптографічний захист та глобальну доступність даних. Регулярне тестування гарантує ефективність планів BCP і DRP, знижує ризики втрати даних та дозволяє підприємству оперативно реагувати на кризи. Важливим є також навчання персоналу, яке включає проведення кібернавчань із застосуванням симуляторів, що сприяє підвищенню загальної готовності підприємства до надзвичайних ситуацій.

Шість етапів захисту від катастрофи

Виконуючи перелічені етапи, можна допомогти підприємству створити програму BCP та DRP, яка забезпечить захист від наслідків природних, механічних та обумовлених людським фактором катастроф. Коли стільниковий телефон дзвонить о другій годині ночі, найменше хочеться гарячково винаходити шляхи відновлення даних, що знаходяться на сервері та стрічках і пробули під водою протягом 30 годин, або, що ще гірше, після фізичного руйнування інформаційного центру внаслідок катастрофи.

27.2. Журнал аудиту подій

Журнал аудиту подій є важливим елементом системи безпеки інформаційно-комунікаційних систем (ІКС) підприємства. Його основна мета — забезпечити фіксацію, збереження та аналіз подій, які відбуваються в системі, що дозволяє моніторити активність користувачів та систем, виявляти потенційні загрози та оперативно реагувати на

інциденти. Журнал не лише дозволяє фіксувати події, але й дає можливість для подальшого аналізу та вдосконалення заходів безпеки. Перш за все, журнал аудиту слугує для реєстрації всіх значущих подій, таких як входи користувачів, зміни в налаштуваннях безпеки, запуск важливих процесів та інші дії, які можуть вплинути на безпеку ІКС. Це дозволяє організаціям мати повну картину того, що відбувається в їх системі в будь-який час.

Основною функцією журналу аудиту є моніторинг та виявлення аномалій. Через регулярний збір та аналіз даних журналу можна виявляти несанкціоновані дії, спроби несанкціонованого доступу або інші підозрілі зміни в налаштуваннях системи. Такі аномалії можуть вказувати на можливі загрози або інциденти, що потребують негайного втручання. Журнал також важливий для аналізу та звітності, оскільки на основі зібраних даних можна створювати звіти, що використовуються для оцінки стану безпеки системи або для проведення аудиту. Звітність може включати детальну інформацію про час події, користувача, який її ініціював, тип дії та результат.

Журнал аудиту має особливе значення в контексті виявлення та документування інцидентів безпеки. У разі виявлення кіберінциденту, журнал є основним джерелом для розслідування та визначення причин події. Це важливо не лише для вжиття заходів щодо усунення наслідків інциденту, але й для розробки стратегії запобігання подібним подіям у майбутньому. Також важливо, що для багатьох підприємств, зокрема в фінансовому секторі або в сфері охорони здоров'я, ведення журналу аудиту є вимогою законодавства, що допомагає забезпечити відповідність нормативним стандартам безпеки та дозволяє зберігати необхідну документацію для перевірок та аудиту.

Журнал аудиту складається з кількох основних компонентів, таких як часова позначка, яка вказує точний час події і дозволяє оцінити хронологію подій; ідентифікація користувача, що дозволяє відстежити, який користувач або система ініціював подію; тип події, що визначає, яка саме дія була виконана, наприклад, вхід в систему або зміна налаштувань; результат події, що показує, чи була дія успішною чи неуспішною; деталі події, що містять додаткову інформацію про суть події, її параметри або обсяг доступу до даних; IP-адреса та геолокація, що вказують на місце та спосіб доступу до системи, що може допомогти у виявленні несанкціонованої активності.

Крім того, ведення журналу аудиту потребує дотримання ключових принципів, таких як невід'ємність даних, що забезпечує їх захист від модифікації чи видалення. Важливим є також забезпечення персоналізованого підходу до записів, де кожен користувач має свій

власний запис у журналі, що дозволяє точно відслідковувати його активність. Регулярне збереження журналу та зберігання його в безпечному місці є необхідним для забезпечення довготривалої доступності даних і можливості подальшого аналізу. Також журнал аудиту повинен бути доступний лише уповноваженим особам для забезпечення конфіденційності та безпеки інформації, а рівні доступу повинні чітко визначати, хто має право на перегляд чи зміни даних.

Таким чином, журнал аудиту подій є необхідним інструментом для забезпечення безпеки інформаційно-комунікаційних систем підприємства. Він не лише допомагає відслідковувати події в системі, виявляти аномалії та загрози, але й сприяє своєчасному реагуванню на інциденти та покращенню загальної стратегії безпеки.

Обробка інцидентів інформаційної безпеки: сучасні підходи та рекомендації

Для ефективного реагування на інциденти інформаційної безпеки (ІБ) важливо збирати, зберігати та аналізувати великі обсяги даних про події безпеки. Це дозволяє не лише оперативно відслідковувати загрози, але й детально розслідувати їх причини. Однак надмірний обсяг даних може створювати інформаційний шум і перевантажувати команду безпеки, що робить важливим налаштування систем моніторингу так, щоб вони фокусувалися на найважливіших подіях. Замість традиційних підходів корпорація Microsoft рекомендує використовувати хмарні рішення, зокрема Microsoft Sentinel. Це сучасна платформа типу SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation, and Response), яка дозволяє централізовано збирати та аналізувати події безпеки з різних джерел, включаючи хмарні сервіси й локальні ресурси. Microsoft Sentinel підтримує можливості машинного навчання для автоматизованого виявлення загроз та їх нейтралізації, що допомагає швидше реагувати на інциденти та мінімізувати вплив загроз на інфраструктуру. Для локальної інфраструктури компанія також пропонує інструменти Microsoft Security Compliance Toolkit, які містять рекомендовані налаштування аудиту та політики безпеки для серверів, робочих станцій і доменних контролерів. Окрім цього, для більш детального налаштування безпеки на платформах Windows корисні документи CIS Microsoft Windows Server Benchmark та CIS Microsoft Windows Desktop Benchmark, які надають кращі практики налаштування політик безпеки для різних версій Windows. Сучасним підходом є використання розширених політик аудиту (Advanced Audit Policy

Configuration), доступних у Windows починаючи з версій Server 2008 і Vista. Ці політики дозволяють налаштовувати події аудиту більш детально порівняно з класичними параметрами. Після активації розширених політик класичні параметри аудиту стають неефективними, якщо це не змінено через групові політики (Audit: Force audit policy subcategory settings). Тому важливо інтегрувати сучасні SIEM-рішення з локальними політиками аудиту та регулярно тестувати засоби безпеки, що дозволяє підвищити ефективність обробки інцидентів і своєчасно виявляти загрози.

Актуальні політики аудиту Windows для інформаційної безпеки

Ефективна політика аудиту Windows є важливим елементом системи інформаційної безпеки підприємства. Вона дозволяє своєчасно виявляти та реагувати на потенційно небезпечні події, запобігаючи загрозам і підтримуючи захищеність інформаційних ресурсів. Першим кроком у формуванні такої політики є контроль подій, пов'язаних з очищенням журналу безпеки. Подія з EventID=1102 виникає після очищення цього журналу й може свідчити про спроби приховати сліди шкідливої активності. Постійний моніторинг цієї події допоможе оперативно виявляти підозрілу поведінку. Не менш важливим є контроль NTLM-аутентифікації. У розділі «Конфігурація комп'ютера – Конфігурація Windows – Параметри безпеки – Локальні політики – Параметри безпеки» необхідно активувати політику «Мережева безпека: обмеження NTLM: вихідний трафік NTLM до віддалених серверів» у режимі «Аудит всього». Це дозволить фіксувати події з EventID=8001 у журналі Microsoft-Windows-NTLM/Operational, які надають інформацію про автоматичну аутентифікацію на веб-ресурсах із використанням облікових записів користувача. Щоб зменшити ризики передачі NTLM-хешів шкідливим ресурсам, важливо створити список дозволених веб-ресурсів (allow list), які легітимно можуть запитувати облікові дані користувача. Після цього політику слід перевести в режим блокування, що запобігатиме доступу до облікових записів зловмисних ресурсів, наприклад, через фішингові листи.

Також важливо використовувати гнучкі можливості підсистеми журналювання Windows. Вона дозволяє налаштовувати аудит не лише для системних подій, а й для окремих папок і гілок реєстру. Це дає змогу зосередитися на критично важливих об'єктах ІТ-інфраструктури та фіксувати всі дії з ними. Для сучасних операційних систем Windows рекомендується використовувати розширені політики аудиту (Advanced Audit Policy Configuration). Ці політики надають значно ширші можливості налаштування порівняно з класичними параметрами й забезпечують

детальний контроль подій. Додатково до локальних засобів моніторингу слід розглянути можливість використання Microsoft Defender for Endpoint, який автоматизує збір даних про події, здійснює їх кореляцію та реагує на загрози у хмарному середовищі. Інтеграція з SIEM-рішеннями, такими як Microsoft Sentinel, дозволяє централізовано аналізувати події безпеки та оперативно реагувати на інциденти за допомогою штучного інтелекту.

Таким чином, впровадження актуальних налаштувань політик аудиту Windows дозволить підприємствам забезпечити надійний контроль інформаційних активів і своєчасне реагування на інциденти інформаційної безпеки.

Утиліта Sysmon

Утиліта Sysmon з пакета Microsoft Windows Sysinternals є потужним інструментом для розширеного моніторингу та аудиту операційної системи, що значно перевершує стандартні можливості журналювання в Windows. Вона дає змогу детально відслідковувати важливі системні події, такі як створення файлів, ключів реєстру, процесів і потоків, завантаження драйверів та бібліотек, мережеві підключення, WMI-події та іменовані канали. Завдяки таким можливостям Sysmon є важливим інструментом для забезпечення інформаційної безпеки, оскільки він дозволяє оперативно виявляти потенційні загрози, які можуть бути приховані за звичайними системними процесами.

Однією з особливих переваг Sysmon є можливість відображення батьківського процесу та командного рядка, що дає змогу визначити джерело виконання процесу та його параметри, що можуть бути корисними для виявлення шкідливих дій. Крім того, утиліта дозволяє відображати геш-суми при створенні процесів або завантаженні драйверів та бібліотек, що є критичним для виявлення компрометацій і підозрілих змін у системі. Це дає змогу зібрати важливу інформацію для подальшого аналізу загроз, оскільки шкідливі програми часто модифікують або додають файли з невідомими або непідписаними кодами. Завдяки цій функції Sysmon може автоматично порівнювати отримані геш-суми з індикаторами компрометації (IoCs), що надходять з CyberThreat Intelligence фідів, що дозволяє миттєво виявляти відомі загрози.

Інтеграція з додатком QVTI для IBM QRadar дозволяє автоматизувати перевірку запусканих файлів через сервіс VirusTotal, що забезпечує ще одну лінію захисту від потенційно шкідливих програм. Ця функція автоматизує процес виявлення зловмисного ПЗ, що знижує ризики пропуску загроз. Для налаштування моніторингу в Sysmon можна використовувати XML-конфігурації, які дають можливість чітко вказати об'єкти для контролю та налаштувати параметри роботи утиліти під

конкретні вимоги. Завдяки таким конфігураціям Sysmon можна адаптувати до специфічних умов роботи підприємства або дослідницької лабораторії, що робить утиліту надзвичайно гнучким інструментом.

Таким чином, використання Sysmon дозволяє значно розширити можливості моніторингу та безпеки в операційних системах, надаючи детальну інформацію про активність в системі та дозволяючи ефективно виявляти та реагувати на потенційні загрози.

27.3. Політики резервного копіювання

Політики резервного копіювання — це комплекс визначених правил, процедур та стратегій, що регламентують процес створення, зберігання та відновлення резервних копій даних з метою забезпечення їх безпеки, доступності та відновлюваності у разі виникнення непередбачених ситуацій, таких як втрата або пошкодження інформації. Політики резервного копіювання є невід’ємною частиною управління інформаційною безпекою та дозволяють мінімізувати ризики для організації через забезпечення цілісності даних.

Основні елементи політики резервного копіювання включають:

1. Типи резервних копій:

- ✓ **Повні резервні копії** (Full backups) - зберігаються всі дані, що є на системі. Це дозволяє мати вичерпну копію, але займає найбільше місця та часу на створення.
- ✓ **Інкрементні копії** (Incremental backups) - копіюються лише ті дані, що змінились після останнього бекапу (повного або інкрементного). Це економить місце та час, але відновлення може бути довшим.
- ✓ **Диференціальні копії** (Differential backups) - копіюються всі зміни з моменту останнього повного бекапу. Вони займають більше місця, ніж інкрементні, але швидше відновлюються.

2. Частота резервного копіювання

Залежно від важливості даних та вимог до безперервності бізнесу, резервне копіювання може здійснюватися щодня, щотижня, після кожної важливої зміни або по запиті. Для критичних даних рекомендується часто здійснювати інкрементні копії.

3. Місце зберігання резервних копій

Зберігання копій може здійснюватися на різних носіях:

- ✓ **Локальні сервери** - на тих самих серверах, де працюють основні дані, але це не забезпечує повної безпеки в разі фізичних пошкоджень або атак.
- ✓ **Хмарні сховища** - зберігання резервних копій на віддалених серверах або у хмарних провайдерів (Amazon Web Services, Google Cloud, Microsoft Azure), що дозволяє зберігати дані у різних географічних локаціях.
- ✓ **Віддалені дата-центри** - зберігання копій в іншому дата-центрі для мінімізації ризиків від фізичних або природних катастроф.

4. Безпека резервних копій

Для забезпечення захисту копій даних важливо впровадити:

- ✓ **Шифрування** даних як під час створення, так і при їх зберіганні, щоб уникнути несанкціонованого доступу.
- ✓ **Контроль доступу** до резервних копій, щоб тільки уповноважені особи мали можливість отримати доступ до критичних даних.

5. Тестування та перевірка відновлення

Регулярне тестування процесу відновлення даних із резервних копій для перевірки їх цілісності та працездатності. Це дозволяє переконатися, що у разі збою можна швидко відновити функціонування системи.

6. Тривалість зберігання копій

Визначення політики щодо того, як довго будуть зберігатися резервні копії, а також коли і як будуть видалятися старі версії. Це важливо для оптимізації витрат на зберігання даних.

7. Процедури відновлення даних

Чітко визначені кроки для відновлення даних у разі катастрофи або втрати інформації. Процедури відновлення повинні бути максимально автоматизованими, щоб зменшити час простою та помилки.

8. Автоматизація процесів

Застосування програмного забезпечення для автоматичного створення резервних копій відповідно до встановленого графіку, що знижує людський фактор і забезпечує регулярність копіювання.

Загалом, політика резервного копіювання є важливим елементом для забезпечення безперервності операцій бізнесу, захисту від кібератак, а також для виконання нормативних вимог щодо зберігання та обробки даних, таких як GDPR. Вона допомагає організаціям ефективно зберігати критичні дані, запобігати їх втраті та забезпечувати швидке відновлення в разі надзвичайних ситуацій.

Політика резервного копіювання даних

Політики резервного копіювання даних — це набір правил і процедур, що визначають, як і коли здійснюється створення, зберігання та відновлення резервних копій даних у разі їх втрати, пошкодження або збоїв у системах. Метою таких політик є забезпечення цілісності, доступності та відновлюваності важливих даних, що дозволяє підприємствам або організаціям мінімізувати ризики втрати інформації та забезпечити безперервність бізнес-процесів.

Актуальна політика резервного копіювання даних є невід'ємною складовою інформаційної безпеки будь-якого підприємства. Резервне копіювання, або бекап, передбачає створення копій файлів і даних, що зберігаються на пристроях, жорстких дисках чи в хмарі, з метою збереження їх цілісності на випадок втрати або пошкодження інформації. Сучасні методи резервного копіювання можна поділити на кілька типів, зокрема повне та диференціальне. Повне копіювання передбачає створення повної копії всіх важливих даних, тоді як диференціальне копіювання зберігає лише змінені файли після першого повного копіювання. Обидва методи мають свої переваги, зокрема диференціальне копіювання є більш ефективним щодо часу і ресурсів, оскільки здійснюється лише для оновлених даних.

Втрати даних можуть відбутися з кількох причин, серед яких виділяються: помилки користувача, збій системи, вірусні атаки, зокрема шифрувальники, хакерські атаки або вихід з ладу обладнання. Важливою особливістю сучасних кіберзагроз є віруси-шифрувальники, які можуть блокувати доступ до інформації на всіх комп'ютерах і серверах підприємства, вимагаючи викуп за розшифрування даних. Це робить регулярне резервне копіювання важливим елементом захисту від таких інцидентів.

Періодичність виконання резервного копіювання повинна відповідати частоті змін даних на підприємстві. Наприклад, якщо оновлення документів відбуваються щодня, бекап слід виконувати щодня наприкінці робочого дня. В інших випадках, наприклад, якщо зміни відбуваються раз на тиждень, резервне копіювання можна виконувати щотижня. Окрім того, резервне копіювання необхідно виконувати перед значними змінами, такими як перевстановлення операційної системи або оновлення програмного забезпечення. Для зручності можна налаштувати спеціальні програми для автоматичного створення резервних копій, що значно полегшить процес.

Вибір програмного забезпечення для резервного копіювання залежить від кількох факторів, зокрема від можливості налаштування графіку

копіювання, управління розміщенням даних і копіями, а також від зручності користування програмою. Важливо, щоб програма підтримувала резервне копіювання на кілька носіїв і дозволяла здійснювати вибіркове копіювання змінених файлів після первісного копіювання. Програма повинна бути простою для користувачів, щоб забезпечити швидке освоєння співробітниками.

Для зберігання резервних копій даних можна використовувати різні фізичні носії, такі як SSD і HDD диски, USB-накопичувачі, оптичні диски (CD, DVD, Blu-ray) або мережеві сховища NAS. Кожен з цих носіїв має свої переваги та недоліки. SSD і HDD диски відрізняються високою надійністю, проте вимагають обережного поводження, оскільки можуть вийти з ладу при механічних пошкодженнях. USB-накопичувачі є компактними і доступними за ціною, але мають обмежений обсяг пам'яті і можуть мати обмежену кількість записів. Оптичні диски є бюджетним варіантом, але мають обмежений обсяг пам'яті і короткий термін служби. Мережеві сховища NAS забезпечують централізоване резервне копіювання для всіх комп'ютерів і серверів в організації, забезпечуючи надійний і ефективний спосіб зберігання даних, хоча вони є досить дорогими.

Хмарні сервіси для створення та зберігання резервних копій, такі як iCloud чи Google Drive, є популярними завдяки зручності і доступності. Більшість сервісів пропонують гнучкі умови для вибору обсягу сховища і часто надають певну кількість безкоштовного місця. Однак, використання хмарних сервісів має свої недоліки: це може включати проблеми з безпекою, оскільки передача корпоративних даних на чужі сервери може призвести до їх компрометації. Крім того, постачальники хмарних послуг не несуть відповідальності за збій у їхніх системах або за видалення даних.

Важливими об'єктами для резервного копіювання є робочі документи, бухгалтерські звіти, бази даних, файли налаштувань програм і контакти. Всі ці дані повинні бути регулярно копіювані на резервні носії, щоб уникнути їх втрати. Рекомендується робити кілька копій даних і зберігати їх на різних носіях та в різних місцях.

Процес створення резервної копії включає кілька етапів: підключення зовнішнього накопичувача або хмарного сховища, безпосередньо копіювання даних, перевірка їх цілісності і закриття процесу. Важливо також використовувати програми-архіватори, щоб зменшити обсяг даних, що зберігаються. Резервне копіювання є необхідною частиною стратегії інформаційної безпеки, що дозволяє зберегти важливі дані і уникнути значних втрат при непередбачених ситуаціях.

Політика резервного копіювання сайту

Політика резервного копіювання сайту є критично важливим елементом забезпечення безпеки та стабільної роботи веб-ресурсу. Резервні копії сайту створюються для того, щоб у разі втрати або пошкодження основних файлів, можна було оперативно відновити сайт у попередньому вигляді. Ситуацій, коли резервне копіювання є необхідним, може бути кілька. По-перше, це випадки, коли через несвоєчасну оплату послуг хостингу доступ до сайту блокується, а файли зберігаються лише деякий час. Наприклад, деякі провайдери можуть зберігати файли до 95 днів після закінчення терміну оплати, що дає час для поновлення доступу, якщо є резервна копія. По-друге, сайти, створені за допомогою відкритих систем управління контентом, таких як WordPress або Joomla, можуть стати об'єктом зловмисних атак через вразливості відкритого коду. У таких випадках резервне копіювання допомагає відновити сайт до попереднього стану, але це не вирішує проблеми з безпекою, оскільки уразливості треба усувати. Третя ситуація — помилкове видалення файлів. Людські помилки трапляються досить часто, і випадкове видалення важливих файлів без резервної копії може призвести до втрати даних, які буде неможливо відновити. Четвертий випадок — зникнення розробника або системного адміністратора, з яким ви працювали. Це особливо актуально для тих, хто замовляє послуги через фриланс-платформи, де розробник може припинити відповідати на запити. Якщо резервна копія є, відновити сайт можна без додаткових проблем. П'ятий випадок — переїзд на новий хостинг. Якщо поточний провайдер вас не влаштовує, важливо створити резервну копію сайту та переконатися, що вона містить всі необхідні файли та бази даних перед перенесенням на новий сервер.

Щоб мати можливість відновити сайт у будь-який час, важливо не тільки створювати резервні копії, а й правильно вибирати місце їх зберігання. Стандартні хостинг-провайдери зазвичай пропонують автоматичне резервне копіювання, виконуючи його на регулярній основі, наприклад, щодня або щотижня. Ці копії зберігаються в панелі керування хостингом, а старі копії замінюються новими через механізм ротації. Однак це не завжди є достатнім, особливо якщо мова йде про важливі дані, тому варто самостійно створювати резервні копії, особливо перед внесенням великих змін або оновлень на сайті. Крім того, резервні копії повинні зберігатися в безпечному місці. Ідеальним варіантом є зберігання копій на іншому сервері, що знаходиться в іншому дата-центрі. Це дозволяє мінімізувати ризики втрати даних у разі пошкодження основного сервера. У випадку використання віртуальних або виділених серверів, резервне копіювання зазвичай є відповідальністю розробників або системних адміністраторів, оскільки вони мають доступ до налаштувань і

файлів сервера. Власники сайтів повинні самостійно налаштувати систему резервного копіювання, використовуючи скрипти або спеціалізоване програмне забезпечення.

Щоб забезпечити максимальну безпеку та доступність даних, необхідно перевірити, чи налаштована функція автоматичного створення резервних копій на вашому хостингу або сервері, дізнатися, де зберігаються ці копії, і регулярно зберігати копії на альтернативних носіях або в хмарних сховищах. Рекомендується створювати резервні копії з певною періодичністю залежно від того, як часто відбуваються зміни на сайті. Відновлення сайту за допомогою резервної копії дозволяє швидко повернути систему до працездатного стану після будь-яких несправностей, що мінімізує час простою та втрату даних.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 27

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.
2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
3. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроектні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242.
4. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233.
5. S. Shevchenko, et al., Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 333–342.
6. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 99–120.

7. Машталяр, Я., Козачок, В., Бржезьська, З., Богданов, О., Оксанич, І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 156–167.
8. Y. Dreis, et al., Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection, in: Cyber Security and Data Protection, vol. 3800 (2024) 1–11.
9. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18.
10. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(24), 185–195.
11. O. Koppiika, P. Skladannyi, Use of Service-Oriented Information Technology to Solve Problems of Sustainable Environmental Management. Information Technology and Mathematical Modeling for Environmental Safety 3021 (2021) 66–75.
12. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.
13. Жданова, Ю., Шевченко, С., Спасітелєва, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.
14. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 374–391.
15. V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.
16. R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, vol. 3800 (2024) 97–105.
17. L. Kriuchkova, V. Sokolov, P. Skladannyi, Determining the Zone of Successful Interaction in RFID Technologies, in IEEE 29th International

Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (2024) 168–171.

18. D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II-2, vol. 3188 (2021) 135–148.

19. G. Otto, et al., Parametric Model of a Laser with External Distributed Feedback in the System of Remote Measurement of Nanovibrations, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3421 (2023) 284–292.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке журнал аудиту подій і яка його роль в інформаційно-комунікаційних системах?
2. Які типи подій повинні фіксуватися в журналі аудиту?
3. Як забезпечується захист журналу аудиту від модифікації або видалення?
4. Які основні принципи ведення журналу аудиту подій?
5. Які дані повинні бути включені до кожної події в журналі аудиту?
6. Як часто повинні оновлюватися записи в журналі аудиту?
7. Яким чином журнал аудиту допомагає у виявленні кіберзагроз?
8. Як можна аналізувати дані журналу аудиту для виявлення аномалій в системі?
9. Які вимоги до журналу аудиту існують з боку законодавства та нормативних актів?
10. Як організувати зберігання та архівування журналів аудиту для довготривалого доступу?
11. Як здійснюється моніторинг подій в інформаційно-комунікаційних системах підприємства?
12. Як проводиться аналіз журналу аудиту для виявлення спроб несанкціонованого доступу?
13. Які інструменти використовуються для автоматизації збору та аналізу журналів аудиту?
14. Які організаційно-технічні заходи є необхідними для забезпечення відновлення функціонування ІКС після інциденту?
15. Як забезпечити безперервність функціонування інформаційно-комунікаційних систем в умовах виникнення інцидентів безпеки?

16. Які етапи включають в себе заходи відновлення після кіберінцидентів?
17. Яким чином тестування планів відновлення допомагає забезпечити стійкість ІКС до атак?
18. Які типи резервних копій існують і які їх переваги та недоліки?
19. Як організувати політику резервного копіювання в інформаційно-комунікаційних системах?
20. Як вибирати місце для зберігання резервних копій даних?
21. Як часто повинні створюватися резервні копії даних і чому це важливо?
22. Як забезпечити відновлення даних з резервних копій при втраті або пошкодженні основних даних?
23. Які типи резервних копій найкраще підходять для забезпечення надійного відновлення даних в умовах атаки?
24. Яким чином резервне копіювання може допомогти при переїзді з одного хостингу на інший?
25. Які заходи необхідно вжити для забезпечення безпеки резервних копій та їх захисту від несанкціонованого доступу?

**ТЕМА 9. СУЧАСНІ ТА ПЕРСПЕКТИВНІ ТЕХНОЛОГІЇ
ЗАХИСТУ ІНФОРМАЦІЇ**

РОЗДІЛ 28
СУЧАСНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІКС



- 28.1. Технології виявлення та блокування кібератак на кінцевих пристроях (EDR, UBA, UEBA)**
- 28.2. Технології протидії витокам інформації (DLP)**
- 28.3. Технології механізму безпечного виконання програм (Sandbox)**
- 28.4. Стек ELK як система централізованого зберігання журналів**

"Інформаційна безпека в цифрову епоху — це не лише технології, а й культура свідомого захисту даних. Час, коли ми могли розраховувати на безпеку за рахунок ізоляції системи, давно минув. Сучасний підхід вимагає постійного моніторингу, гнучких стратегій захисту і готовності до нових викликів."

Брюс Шнайер, криптограф та експерт з кібербезпеки

Сучасні технології забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах (ІТС) включають широкий спектр методів і засобів, що сприяють захисту від різноманітних кіберзагроз і атак.

28.1. ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ КІБЕРАТАК НА КІНЦЕВИХ ПРИСТРОЯХ (EDR, UBA, UEBA)

Забезпечення безпеки кінцевих пристроїв є важливим завданням для підприємств, оскільки саме вони найчастіше стають ціллю для кіберзлочинців. Сучасні технології, такі як **Endpoint Detection and Response (EDR)**, **User Behavioral Analytics (UBA)** і **User and Entity Behavioral Analytics (UEBA)**, забезпечують ефективне виявлення, аналіз та блокування загроз у реальному часі.

Endpoint Threat Detection and Response (EDR) та User and Entity Behavioral Analytics (UEBA) є сучасними інструментами інформаційної безпеки, які забезпечують ефективне виявлення, розслідування та реагування на кіберзагрози в корпоративних інфраструктурах. Ці технології використовують методи машинного навчання, поведінкового аналізу та інтеграцію з потоками Threat Intelligence для забезпечення комплексного захисту кінцевих точок і аналізу поведінки користувачів та ІТ-сутностей.

Endpoint Threat Detection and Response (EDR)

За визначенням Gartner, EDR є інструментом, що дозволяє детектувати та розслідувати підозрілі активності на кінцевих точках, включаючи робочі станції, сервери та інші пристрої в мережі. Основна архітектура EDR передбачає встановлення агентів на кінцевих точках, які відстежують системні події, мережеву активність, зміни у файлах та реєстрах. Ці дані аналізуються локально або передаються на сервер чи в хмару для подальшого оброблення.

EDR забезпечує моніторинг у реальному часі, дозволяючи отримувати повну видимість активності кінцевих точок через єдину консоль управління. Завдяки цьому фахівці інформаційної безпеки можуть швидко виявляти загрози, пріоритезувати інциденти, проводити розслідування та застосовувати інструменти реагування, такі як ізоляція заражених пристроїв, блокування шкідливих доменів, зупинка шкідливих процесів та відновлення робочих станцій до початкового стану.



Рис. 28.1. Основні функціональні блоки EDR

Джерело: [2-10]

Для виявлення загроз EDR використовує:

- ✱ ІоС-сканування;
- ✱ поведінковий аналіз;
- ✱ ретроспективний аналіз;
- ✱ пісочниці;
- ✱ антивірусний захист;
- ✱ кореляцію подій.

Ці механізми дозволяють своєчасно фіксувати та блокувати складні атаки на ранніх стадіях.

User and Entity Behavioral Analytics (UEBA)

UEBA додає ще один рівень безпеки, орієнтований на аналіз поведінки користувачів та ІТ-сутностей. Ця технологія використовує великі обсяги даних для побудови моделей нормальної поведінки та виявлення аномалій, які можуть свідчити про інциденти безпеки. Джерелами даних для UEBA є журнали серверів, мережевих компонентів, систем аутентифікації, SIEM, DLP та навіть комунікації у поштових сервісах і месенджерах.

UEBA вирішує кілька важливих завдань:

- ➔ Збір та аналіз даних у реальному часі із застосуванням методів машинного навчання.
- ➔ Виявлення складних атак, які залишаються непоміченими традиційними засобами захисту.
- ➔ Пріоритизація інцидентів для оперативного реагування.

➔ Надання розширеної інформації про аномальні активності, включаючи всі об'єкти, залучені до інциденту.

Ці можливості дозволяють швидко ідентифікувати компрометацію облікових записів, інсайдерські загрози, неправильне використання доступу співробітниками тощо.

Інтеграція EDR та UEBA

Поєднання можливостей EDR та UEBA створює потужний інструмент для комплексного забезпечення безпеки. EDR надає глибокий рівень деталізації подій на кінцевих точках і дозволяє оперативно реагувати на загрози, тоді як UEBA додає аналіз поведінкових аномалій, що забезпечує виявлення інсайдерських атак та нетипових активностей.

UEBA є розвитком UBA, оскільки охоплює не лише аналіз поведінки користувачів, а й IT-сутностей, таких як сервери, кінцеві пристрої та мережеві вузли. Використовуючи машинне навчання, UEBA створює моделі поведінки для пристроїв і систем, виявляючи складні атаки, які не можуть бути виявлені традиційними засобами. Завдяки консолідації інцидентів за критичністю UEBA забезпечує пріоритизацію загроз і спрощує реагування на них.

Інтеграція технологій EDR, UBA та UEBA дозволяє створити багаторівневий захист, що включає виявлення складних загроз, швидке блокування шкідливих активностей і зниження ризиків для бізнесу. Такі рішення, як CrowdStrike Falcon, Microsoft Defender for Endpoint, Exabeam і Splunk UBA, пропонують комплексні функції моніторингу, аналізу та реагування, інтегруючись із сучасними системами безпеки.

Подальший розвиток цих технологій передбачає використання штучного інтелекту для автоматизації процесів, інтеграцію з архітектурою Zero Trust, підтримку IoT-пристроїв та хмарних сервісів, а також удосконалення механізмів прогнозування загроз. У сучасних умовах застосування EDR, UBA та UEBA є необхідним для підприємств, що прагнуть забезпечити високий рівень безпеки кінцевих пристроїв і мережевої інфраструктури.

Сучасні платформи, такі як Microsoft Defender for Endpoint, CrowdStrike Falcon, Splunk UBA та Exabeam, вже пропонують інтегровані рішення, які охоплюють функціонал обох технологій. Це дозволяє:

- ✓ покращити видимість загроз у реальному часі;
- ✓ забезпечити ефективне управління інцидентами;
- ✓ створювати звіти для аналізу та вдосконалення системи безпеки.

Переваги та перспективи

EDR і UEBA є ключовими компонентами сучасної стратегії кібербезпеки. Їх впровадження дозволяє не лише оперативно реагувати на загрози, а й проактивно запобігати потенційним атакам. Інтеграція цих рішень із іншими системами, такими як SIEM, DLP або EPP, робить їх незамінними для підприємств, які прагнуть досягти високого рівня інформаційної безпеки та захисту своїх даних.

28.2. ТЕХНОЛОГІЇ ПРОТИДІЇ ВИТОКАМ ІНФОРМАЦІЇ (DLP)

Системи захисту від витоків конфіденційної інформації (Data Leak Prevention, DLP) є ключовим інструментом для забезпечення інформаційної безпеки підприємств. Вони призначені для моніторингу і блокування передачі конфіденційних даних через електронну пошту, месенджери, IP-телефонію, а також на зовнішні носії, веб-ресурси та мережеві сховища. Основна мета таких систем – запобігання витоку інформації, що може статися як через помилку, так і навмисно.

Втрати конфіденційної інформації можуть спричинити серйозні негативні наслідки для підприємства: втрату довіри клієнтів і партнерів, погіршення репутації, зниження конкурентоспроможності та навіть фінансові збитки. Ситуацію ускладнює доступ співробітників до веб-пошти, соціальних мереж і месенджерів, що збільшує ризик витоків даних. Водночас спроби повного блокування таких ресурсів можуть викликати зворотний ефект, коли співробітники шукають обхідні шляхи, що підвищує рівень загроз.

DLP-системи аналізують потоки даних, які перетинають периметр корпоративної мережі, і забезпечують блокування передачі інформації, яка класифікована як конфіденційна. Наприклад, якщо система виявляє, що співробітник намагається передати чутливі дані за межі компанії, вона може автоматично заблокувати цей процес.

Ключовими функціями DLP-систем є зберігання копій даних, що передаються засобами електронної пошти, месенджерів та IP-телефонії, а також контроль файлів, які копіюються на зовнішні носії або завантажуються на веб-ресурси. Це дозволяє проводити розслідування інцидентів інформаційної безпеки.

Системи також забезпечують блокування витоків конфіденційної інформації як за межі організації, так і у внутрішній мережі. Крім того, вони можуть виявляти несанкціоновані копії конфіденційної інформації на робочих станціях або загальнодоступних ресурсах компанії, що значно підвищує рівень контролю.

Сучасні DLP-рішення використовують передові технології, зокрема контентний аналіз, цифрові відбитки та алгоритми пошуку ідентифікаторів. Це дозволяє їм ефективно працювати навіть у складних умовах, де інформація може передаватися різними каналами.

Окрім запобігання витокам інформації, DLP-системи часто застосовуються для контролю дій співробітників. Вони дозволяють відстежувати активність працівників, перевіряти їх присутність на робочому місці, аналізувати лояльність і благонадійність.

Ефективність впровадження DLP-систем залежить від інтеграції з іншими засобами безпеки, чіткого налаштування політик доступу до даних та навчання співробітників основам інформаційної безпеки. В сучасних умовах ці системи стали важливою складовою комплексного підходу до захисту конфіденційної інформації, допомагаючи підприємствам запобігати інцидентам і зберігати свою репутацію на високому рівні.

Архітектура DLP систем

Архітектура систем захисту від витоків конфіденційної інформації (DLP) включає кілька ключових компонентів, що забезпечують ефективний моніторинг, контроль і захист інформації від несанкціонованого витоку. Загалом, архітектура DLP-системи може бути розділена на кілька основних рівнів і складових частин, кожна з яких виконує свою функцію для забезпечення комплексної безпеки даних.

Архітектура DLP-системи

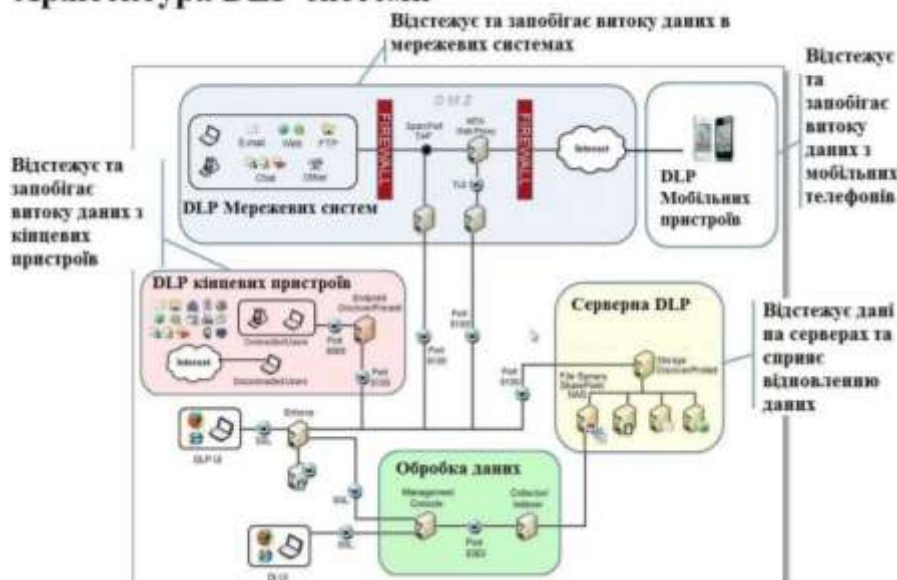


Рис. 28.2. Архітектура DLP систем

Джерело: [2-10]

Першим компонентом є засоби збору даних, до яких належать агентські програми, що встановлюються на кінцевих пристроях користувачів, таких як комп'ютери або мобільні пристрої, для відстеження операцій з файлами та даними на локальному рівні. Також на цьому рівні працюють шлюзи та проксі-сервери, які здійснюють моніторинг і контроль передачі даних між внутрішніми системами компанії і зовнішніми мережами, такими як Інтернет чи зовнішні сховища даних.

Другим компонентом є аналіз і фільтрація даних, де здійснюється перевірка інформації на предмет наявності чутливих даних за допомогою різних технологій, таких як пошук ключових слів, шаблонів або цифрових відбитків. Алгоритми ідентифікації чутливої інформації дозволяють визначити, наприклад, фінансові звіти чи персональні дані, що передаються або зберігаються у межах організації.

Третім важливим елементом архітектури є розробка політик захисту, що регулюють доступ до конфіденційної інформації та визначають правила для її передачі чи зберігання. Політики доступу визначають, які користувачі мають право доступу до конкретних типів даних, а політики блокування забороняють передачу або збереження конфіденційної інформації через небезпечні канали, такі як електронна пошта або зовнішні носії.

Четвертим компонентом є моніторинг і звітність, що дозволяють здійснювати постійний контроль за діями користувачів і створювати звіти для подальшого аналізу інцидентів безпеки. Система генерує сповіщення про спроби витоку даних і надає адміністратору можливість своєчасно реагувати на події.

П'ятий компонент архітектури — це управління інцидентами, яке включає механізми виявлення і реагування на інциденти безпеки, зокрема автоматичне блокування витоку інформації або сповіщення адміністратора для подальшого розслідування. Централізоване управління є шостим компонентом, яке дозволяє адмініструвати політики доступу і блокування, а також управляти агентами на кінцевих пристроях через єдину платформу.

Нарешті, важливою складовою DLP-системи є її інтеграція з іншими системами безпеки, такими як SIEM (система управління інцидентами та подіями безпеки) та IAM (система управління доступом), що дозволяє централізовано моніторити і корелювати події безпеки, а також автоматично застосовувати політики доступу до конфіденційної інформації. Така архітектура забезпечує багатофункціональність і гнучкість DLP-системи, дозволяючи ефективно запобігати витокам конфіденційної інформації в організаціях різного масштабу.

Шлюзові DLP-системи

Шлюзові DLP-системи (Data Loss Prevention Systems) — це технології, які забезпечують моніторинг і контроль інформаційних потоків на рівні шлюзів мережі для запобігання витокам чутливої або конфіденційної інформації. Вони виконують фільтрацію даних, що проходять через різні канали зв'язку (наприклад, електронну пошту, веб-трафік, FTP-з'єднання) і допомагають виявляти спроби несанкціонованого передачі або копіювання даних, які можуть призвести до порушення конфіденційності або безпеки. Основні характеристики шлюзових DLP-систем включають моніторинг і фільтрацію трафіку, що дозволяє відслідковувати всі вхідні та вихідні дані на рівні мережі, включаючи електронну пошту, веб-трафік, файли, що передаються через FTP, та інші канали зв'язку. Вони можуть застосовувати фільтри для виявлення і блокування передачі конфіденційної інформації. Далі, ці системи здатні ідентифікувати чутливу інформацію, таку як фінансові дані, особисті ідентифікаційні дані (РІІ), паролі, корпоративні секрети, медичні записи та інші чутливі дані, використовуючи бази даних шаблонів або технології машинного навчання для точного визначення цих даних.

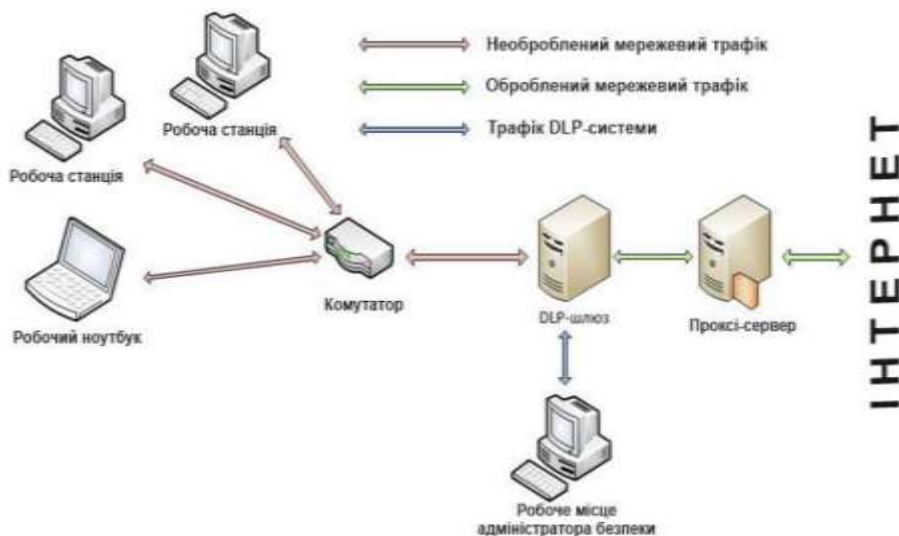


Рис. 28.3. Шлюзова DLP-системи, що працює в режимі блокування
Джерело: [2]

Крім того, шлюзові DLP-системи дозволяють налаштовувати політики доступу і контроль передачі, що включає блокування певних типів файлів, перевірку наявності чутливої інформації в переданих даних та повідомлення адміністратора, якщо виявлено порушення. Вони також можуть інтегруватися з іншими інструментами безпеки, такими як системи управління інцидентами безпеки (SIEM), для швидкого реагування на

інциденти і повідомлення про потенційні загрози. Також шлюзові DLP-системи здатні працювати з різними протоколами і форматами передачі даних, такими як HTTP/HTTPS, SMTP, FTP, POP3, IMAP та інші, що дозволяє комплексно захищати організацію на різних рівнях комунікацій.

Після виявлення спроби витоку інформації ці системи можуть створювати детальні звіти і аналізи, що допомагають зрозуміти, як і чому було порушено безпеку, що дозволяє коригувати політики безпеки для запобігання подібним інцидентам у майбутньому. Завдяки шлюзовим DLP-системам компанії можуть ефективно контролювати витік важливої інформації через відкриті канали зв'язку, знижуючи ризики шахрайства, витоку корпоративних секретів і порушення законодавства, що регулює обробку та захист даних.

Ці системи призначені для контролю трафіку, що проходить через традиційні інтернет-протоколи, такі як HTTP, FTP, POP3, SMTP тощо. Основна перевага шлюзових DLP-систем полягає в тому, що вони можуть здійснювати контроль за передачею даних через мережу, блокуючи потенційно небезпечні або конфіденційні повідомлення.



Рис. 28.4. Шлюзова DLP-системи, що працює в режимі моніторингу
Джерело: [2]

Однак цей тип системи має обмежену область застосування, оскільки він не здатний здійснювати моніторинг дій на кінцевих точках корпоративної мережі, тобто на локальних комп'ютерах і пристроях користувачів. Через це шлюзові системи не можуть контролювати всю діяльність, що відбувається на кінцевих точках мережі.

Хостові DLP-системи

На відміну від шлюзових DLP-систем, хостові DLP-системи використовують спеціальні агенти, які встановлюються безпосередньо на кінцевих пристроях, таких як комп'ютери користувачів.

Ці агенти виконують дві основні функції: вони контролюють діяльність користувачів, обмежуючи їх доступ до конфіденційної інформації або забороняючи передачу даних на зовнішні носії, і вони реєструють всі дії користувачів, передаючи цю інформацію до централізованого сховища для подальшого аналізу. Таким чином, хостові DLP-системи дозволяють більш детально контролювати діяльність користувачів на кінцевих точках, зокрема на комп'ютерах, що підключені до локальної мережі, або пристроях, безпосередньо підключених до цих комп'ютерів.

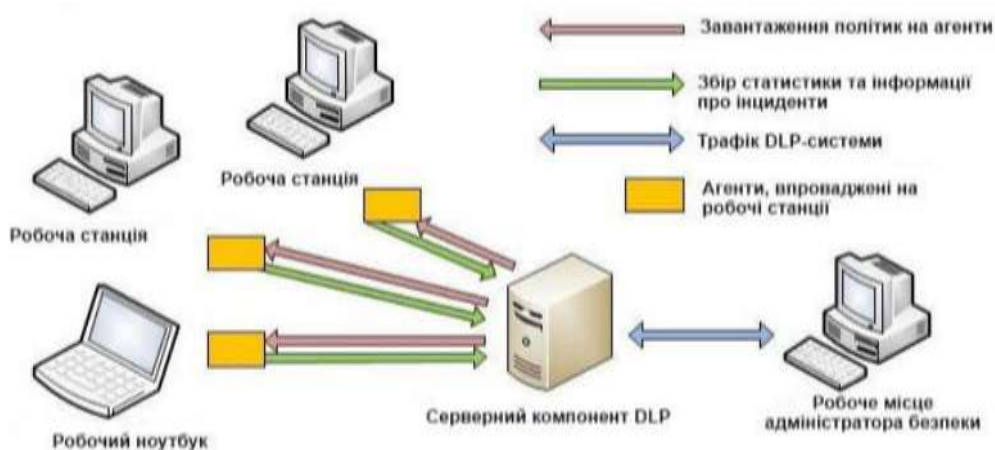


Рис. 28.5. Хостова DLP-система

Джерело: [2]

Проте сфера застосування таких систем обмежується лише тими пристроями, на яких встановлено агент, і вони не можуть моніторити трафік, що йде через мережу безпосередньо, як це роблять шлюзові системи.

28.3. ТЕХНОЛОГІЇ МЕХАНІЗМУ БЕЗПЕЧНОГО ВИКОНАННЯ ПРОГРАМ (SANDBOX)

Технології механізму безпечного виконання програм, або sandbox, полягають у створенні ізолюваного середовища для виконання програмного коду з метою обмеження його доступу до системних ресурсів

і мінімізації ризиків, пов'язаних з шкідливими або неперевіреними додатками. Це дозволяє запобігти небажаним змінам системи, пошкодженню даних або витоку конфіденційної інформації. Основними технологіями, що використовуються в механізмі sandbox, є віртуалізація, контейнеризація, ізоляція на рівні файлових систем, політики контролю доступу, поведінкова ізоляція, а також застосування моніторингу і машинного навчання.

Віртуалізація є однією з основних технологій sandbox, що дозволяє створювати віртуальні машини, які мають власне середовище і ресурси, ізольовані від основної операційної системи. Це дозволяє обмежити програму лише віртуальними ресурсами, запобігаючи її прямому доступу до фізичних ресурсів хоста. Іншим варіантом ізоляції є контейнеризація, яка дозволяє запускати програми в окремих контейнерах, що використовують одне ядро операційної системи, але забезпечують ізоляцію на рівні процесів і ресурсів. Завдяки меншому накладному ресурсу, ніж у віртуалізації, контейнери, такі як Docker, дозволяють ефективно ізолювати додатки, що знижує ризики, пов'язані з їх запуском.

Ізоляція на основі файлових систем є ще одним важливим аспектом sandbox, де програма отримує доступ лише до певних копій файлів або реєстрів, але не до реальних даних операційної системи. Це забезпечує додатковий рівень захисту, оскільки навіть у випадку атаки програма не може завдати шкоди важливим файлам і системним налаштуванням. Для контролю доступу до ресурсів використовуються політики обмеження, які визначають, що конкретна програма може робити в межах пісочниці. Ці політики можуть застосовуватися до файлів, мережі та інших ресурсів, дозволяючи запускати лише ті операції, які були явно дозволені.

Один із найефективніших підходів до ізоляції програм в sandbox полягає у використанні технологій на основі поведінки, де програма обмежується в доступі до системних ресурсів і дозволяється взаємодіяти з ними лише відповідно до попередньо заданих правил. Для реалізації цього підходу застосовуються різні методи моніторингу виконання програм, наприклад, за допомогою аналітики системних викликів, мережевого трафіку, зміни пам'яті тощо. Програми, які виконуються в пісочниці, можуть бути повністю ізольовані від основної операційної системи, а всі їх дії фіксуються і аналізуються для виявлення потенційних загроз.

Важливою частиною цього процесу є також застосування технологій машинного навчання, які дозволяють на основі аналізу великих обсягів даних створювати моделі для виявлення підозрілих або аномальних дій. Застосування алгоритмів машинного навчання дозволяє швидше і точніше

виявляти нові загрози, навіть якщо вони раніше не були зафіксовані, і своєчасно реагувати на потенційні ризики.

Таким чином, використання пісочниць для безпечного виконання програм дає змогу створити ефективні механізми захисту від шкідливих програм і атак, обмежуючи їх здатність шкодити основній системі. Віртуалізація, контейнеризація, ізоляція, моніторинг і поведінкова ізоляція разом складають комплексний підхід до забезпечення безпеки в інформаційних системах, що дозволяє мінімізувати ризики від шкідливого коду і запобігти можливим загрозам.

Пісочниця (англ. *Sandbox*) — це механізм для безпечного виконання програм, за допомогою якого здійснюється ізоляція підозрілого або непротестованого коду в контрольованому середовищі. Основним призначенням пісочниці є забезпечення захисту системи від потенційно небезпечних програм, таких як віруси, шкідливі скрипти чи інші програми з ненадійних джерел. Пісочниці дозволяють запускати і досліджувати код, не порушуючи безпеку основної операційної системи, завдяки обмеженому доступу до системних ресурсів, таких як файлові системи, мережі та апаратні пристрої.

Пісочниця зазвичай створюється як ізольоване середовище, яке має обмежений доступ до ресурсів комп'ютера (місце на жорсткому диску та в оперативній пам'яті) і функціонує в межах суворо контролюваного простору. Доступ до мережі та операційних ресурсів часто обмежується або емулюється, що дозволяє запобігти несанкціонованим модифікаціям або витоку даних. Вона є прикладом віртуалізації, оскільки ізолює виконуваний код від основної операційної системи, що дозволяє знизити ризики.

Однак, пісочниця не лише захищає від вірусів і шкідливого коду, але й забезпечує можливість безпечного виконання неперевіреного коду для його подальшого аналізу. Наприклад, пісочниці використовуються для тестування нових версій програмного забезпечення, а також для запуску програм, що можуть бути потенційно небезпечними або викликати великий навантаження на систему.

Види пісочниць:

1. Аплети, що виконуються у віртуальних машинах або інтерпретаторах

Це дозволяє запускати Java-код або інші типи програм з веб-сайтів без загрози для операційної системи. Віртуальні машини створюють ізольоване середовище, де програма може виконуватися без доступу до основних системних ресурсів.

2. Ізоляція на основі повної віртуалізації

Використання віртуальних машин (наприклад, VMware або VirtualBox) як захисного шару над основною операційною системою дозволяє створити високий рівень захисту від шкідливих програм, які можуть заражати систему через браузер або інші потенційно небезпечні програми.

3. Ізоляція на основі часткової віртуалізації файлової системи і реєстру

Цей підхід не потребує створення окремої віртуальної машини, але дозволяє дублювати об'єкти файлової системи та реєстру, так що всі зміни в пісочниці стосуються лише копій цих об'єктів, а реальні дані залишаються недоторканими. Такий підхід дозволяє знизити навантаження на систему і зменшити складність, але має обмеження у взаємодії між віртуальним і реальним середовищем.

4. Ізоляція на основі правил

У цьому випадку всі спроби змінити об'єкти файлової системи та реєстру розглядаються за допомогою набору внутрішніх правил, які визначають, які дії є допустимими, а які — заблокованими. Це дозволяє зберігати баланс між зручністю обміну даними та рівнем захисту від шкідливих програм.

Режими використання антивірусних пісочниць:

1. Режим постійного захисту.

У цьому режимі підозрілі процеси автоматично поміщаються в пісочницю при їх запуску. Це знижує ризики від атак, оскільки всі неперевірені програми виконуються в ізольованому середовищі.

2. Режим ручного захисту.

У цьому випадку користувач самостійно приймає рішення про те, чи запускати програму в пісочниці, що дає більше контролю, але вимагає обережності від користувача.

Онлайн-пісочниці:

Онлайн-пісочниці представляють собою системи, що працюють через інтернет і дозволяють користувачам завантажувати підозрілі файли для подальшого аналізу. Це зручний інструмент для дослідження шкідливого коду без необхідності встановлення спеціального програмного забезпечення. Один з популярних проєктів — Cuckoo Sandbox, що дозволяє перевіряти документи, скрипти та інші типи файлів, виконуючи їх у віртуальному середовищі та записуючи всі дії. Після виконання тесту система генерує звіт, що містить інформацію про дії, вчинені шкідливим кодом.

Офлайн-пісочниці:

Офлайн-пісочниці використовуються в умовах, коли доступ до інтернету обмежений або коли необхідно більш тонко налаштувати режим виконання файлу при аналізі. Наприклад, інструмент Cuckoo Sandbox може бути використаний для дослідження шкідливих програм в умовах офлайн, де можна настроїти віртуальну машину для більш точного контролю над тестованим кодом, а також для збереження всіх змін у файловій системі.

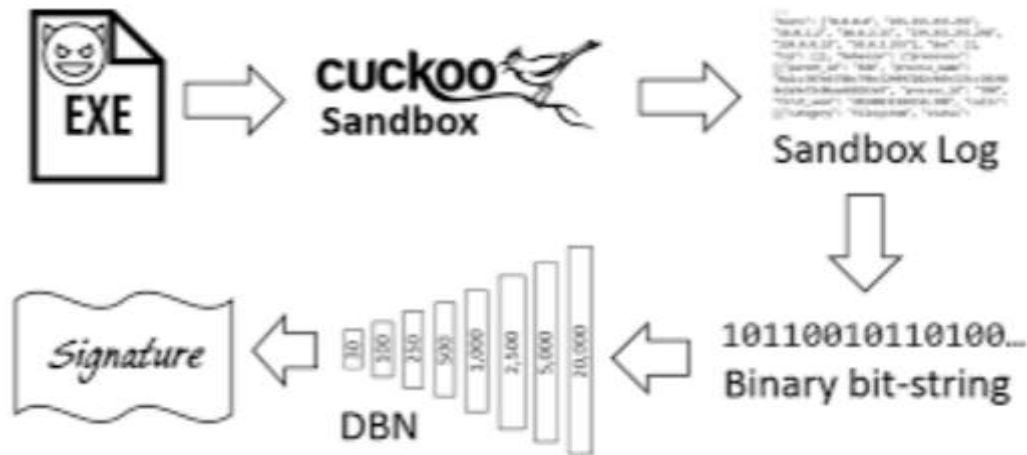


Рис. 28.6. Порядок аналізу файлів за допомогою Cuckoo Sandbox
Джерело: [2]

Cuckoo Sandbox є однією з найбільш відомих пісочниць, яка автоматизує процес дослідження шкідливого програмного забезпечення (ПЗ). Вона дозволяє аналізувати підозрілі файли, запускаючи їх у ізольованому середовищі, що імітує реальну операційну систему. Cuckoo може відслідковувати поведінку шкідливого ПЗ, включаючи зміну файлів, мережеву активність, спроби доступу до реєстру та інші дії, що можуть бути потенційно небезпечними. Після завершення аналізу пісочниця генерує звіт, що містить детальну інформацію про виявлену активність, допомагаючи дослідникам і аналітикам виявляти нові загрози та розробляти методи їх нейтралізації. Cuckoo Sandbox підтримує широкий спектр операційних систем, таких як Windows, Linux та macOS, що робить її універсальним інструментом для аналізу шкідливого ПЗ на різних платформах.

Вона забезпечує такі можливості:

- Моніторинг викликів функцій win32 API.
- Дамп мережевої активності.
- Аналіз пам'яті.
- Створення скріншотів під час виконання.

- Докладні звіти у форматах JSON, HTML та інших.

Пісочниці продовжують залишатися важливим інструментом для забезпечення безпеки при роботі з потенційно небезпечним кодом, дозволяючи безпечно досліджувати та аналізувати шкідливі програми без ризику для основної операційної системи.

28.4. Стек ELK як система централізованого зберігання журналів

Стек ELK (Elasticsearch, Logstash, Kibana) є потужним набором інструментів, що використовуються для централізованого збору, обробки, зберігання та візуалізації журналів подій і логів. Цей стек широко застосовується в різноманітних галузях для моніторингу й аналізу великих обсягів даних, які генеруються різними системами, додатками та серверами. Кожен із компонентів стека ELK виконує специфічні завдання, що забезпечують ефективність і швидкість роботи з логами в реальному часі.

Основним компонентом стека є Elasticsearch, розподілена пошукова і аналітична система, що використовує Apache Lucene для індексації і зберігання даних. Цей компонент відповідає за збереження всіх даних, що надходять від інших частин стека, і забезпечує швидкий пошук і аналіз даних, навіть при великих обсягах інформації. Завдяки індексації Elasticsearch може миттєво обробляти запити, виконуючи складні операції на збережених логах і даних.

Другий важливий компонент — Logstash, який є інструментом для збору, обробки і транспортування даних. Він отримує логи з різних джерел (сервери, додатки, бази даних, мережеві пристрої) і обробляє їх перед тим, як передати в Elasticsearch. Logstash має потужну систему плагінів для інтеграції з різними джерелами, а також фільтри для очищення і форматування даних, що дозволяє привести їх до єдиного стандарту, що відповідає вимогам подальшої обробки.

Крім цього, Kibana є важливою частиною стека, що надає інтерфейс для візуалізації даних, збережених в Elasticsearch. Завдяки Kibana користувачі можуть створювати інтерактивні дашборди, графіки, таблиці і інші візуальні елементи для аналізу і моніторингу даних. Це дозволяє отримати зрозумілу і зручну інформацію для прийняття рішень або швидкої реакції на потенційні проблеми в інфраструктурі. Kibana також підтримує функціонал для налаштування сповіщень і автоматичних алертів, що дає змогу оперативно реагувати на аномалії або критичні події.

Основний принцип роботи стека ELK полягає в тому, що Logstash збирає і обробляє логи з різних джерел, потім передає їх в Elasticsearch для індексації та зберігання, а вже через Kibana користувачі можуть здійснювати пошук, візуалізацію та аналіз отриманих даних. Цей процес дозволяє створити ефективну систему моніторингу і аналізу в реальному часі, що дуже важливо для сучасних інфраструктур, особливо в аспекті безпеки.



Рис. 28.7. Узагальнена схема роботи стека ELK

Джерело: [2]

Однією з основних переваг стека ELK є масштабованість. Оскільки Elasticsearch використовує розподілену архітектуру, він здатен ефективно працювати навіть з величезними обсягами даних, що дозволяє масштабувати систему в залежності від росту вимог до зберігання та обробки даних. Це робить стек ELK ідеальним рішенням для організацій будь-якого розміру, що потребують централізованого збору і аналізу журналів.

Крім того, гнучкість Logstash, що дозволяє налаштовувати збір і обробку даних через численні плагіни, дає змогу інтегрувати систему з майже будь-яким джерелом даних, чи то мережеві пристрої, чи додатки, чи сервери. Водночас Kibana забезпечує простоту візуалізації даних, що дозволяє створювати кастомізовані дашборди, які відповідають потребам конкретного користувача або організації. Це робить ELK не тільки потужним інструментом для обробки даних, а й зручним для оперативного моніторингу й аналізу інформації.

Використання стека ELK має велике значення для систем безпеки. Завдяки своїм можливостям для централізованого збору і аналізу журналів безпеки ELK дозволяє виявляти потенційні загрози, аномальні дії або спроби атак на інфраструктуру в реальному часі. У поєднанні з можливістю налаштування сповіщень і алертів це забезпечує своєчасну реакцію на інциденти безпеки. Наприклад, можна моніторити журнали доступу до критичних систем, виявляючи несанкціоновані спроби доступу або аномальні дії користувачів, що можуть свідчити про можливі загрози.

Стек ELK також є важливим інструментом для аудиту безпеки. Можливість зберігати всі дані про доступ і взаємодію з системами дає змогу проводити детальний аналіз активності користувачів, що є необхідним для забезпечення відповідності стандартам безпеки та виявлення порушень політик доступу. Крім того, система дозволяє здійснювати моніторинг інфраструктури, виявляючи проблеми, збої чи інші неполадки, що можуть вплинути на безпеку і стабільність роботи організації.

Завдяки своїй відкритості та підтримці великої кількості плагінів, а також активній спільноті, яка розвиває систему, ELK пропонує високий рівень кастомізації та можливість адаптації під конкретні потреби користувачів. Його використання в системах безпеки, моніторингу та аналізу журналів подій є ефективним і масштабованим рішенням для будь-якої організації, що потребує надійного інструменту для збору, зберігання і візуалізації даних.

Таким чином, стек ELK є важливим і потужним інструментом для централізованого збору, обробки та аналізу журналів подій, що забезпечує високу масштабованість, гнучкість і зручність у візуалізації даних. Його застосування в області безпеки і моніторингу дозволяє організаціям ефективно відслідковувати активність в реальному часі, виявляти потенційні загрози та здійснювати аудит діяльності, що є ключовим елементом для забезпечення безпеки IT-інфраструктури.

Стек ELK, який складається з Logstash, Elasticsearch та Kibana, є потужним інструментом для централізованого збору, обробки, зберігання та візуалізації даних, зокрема логів подій. Його застосування в системах моніторингу та безпеки дозволяє забезпечити ефективний аналіз великих обсягів даних в реальному часі.

Logstash – це інструмент для збору та обробки даних. Він дозволяє ефективно отримувати логи з різних джерел, таких як додатки, сервіси та апаратне забезпечення, і передавати їх для подальшого зберігання та аналізу. Logstash приймає дані через вхідні канали, які можуть бути налаштовані на отримання інформації з різних джерел (наприклад, файли журналів, мережеві потоки). В обробці даних Logstash використовує фільтри, такі як grok для розбору неструктурованих даних, geoip для додавання географічної інформації, або mutate для зміни полів. Цей процес дозволяє структурувати дані і зберігати їх у зручному для пошуку і аналізу форматі. Вихідними каналами можуть бути різні системи зберігання, зокрема Elasticsearch, що забезпечує подальшу обробку і зберігання даних.

Elasticsearch – це розподілена пошукова система, яка відповідає за зберігання і швидкий пошук великих обсягів даних. Вона дозволяє здійснювати повнотекстовий пошук у реальному часі та виконувати складні запити для аналізу структурованих та неструктурованих даних. Elasticsearch використовує формат JSON для зберігання даних і забезпечує можливість масштабування, що дозволяє обробляти великі обсяги логів. Пошукові та аналітичні функції Elasticsearch є основою для реалізації інтерфейсів візуалізації і моніторингу через Kibana.

Kibana – це інструмент для візуалізації даних, збережених у Elasticsearch. Він надає користувачам зручний веб-інтерфейс для створення графіків, діаграм, карт та інших візуальних елементів, що дозволяють аналізувати дані. Kibana підтримує інтерактивні дашборди, які дозволяють швидко реагувати на події в реальному часі, забезпечуючи візуалізацію даних та створення сповіщень на основі налаштувань користувача.

Scirius Community Edition – це веб-додаток для управління набором правил Suricata, системи виявлення вторгнень (IDS). Scirius дозволяє користувачам централізовано керувати правилами, що використовуються для аналізу мережевого трафіку та виявлення потенційних загроз. Він інтегрується з Logstash і Elasticsearch, що дозволяє забезпечити централізоване зберігання та аналіз журналів безпеки.

Beats, зокрема Filebeat, Metricbeat, Winlogbeat, Packetbeat та інші, є легкими агентами для збору даних з різних джерел і передавання їх у Logstash або Elasticsearch. Beats дозволяють здійснювати попередню фільтрацію та відправку даних в реальному часі, зменшуючи навантаження на основні системи збору. Кожен з клієнтів Beats призначений для конкретного типу даних, таких як журнали, метрики, події Windows, мережева інформація тощо.

Приклад конфігурації Filebeat включає визначення шляхів до журналів та налаштування їх відправки до Logstash, де ці дані будуть оброблені та передані в Elasticsearch. Конфігурація Logstash визначає, як обробляти отримані дані, включаючи фільтрацію та перетворення перед зберіганням у Elasticsearch. Основний формат конфігураційних файлів Logstash складається з трьох частин: input (вхідні канали), filter (фільтрація і обробка даних) та output (вихідні канали, наприклад, Elasticsearch).

Завдяки такій архітектурі ELK Stack дозволяє ефективно організувати процес збору, зберігання та аналізу великих обсягів логів, що важливо для забезпечення безпеки і моніторингу інформаційних систем. Всі компоненти стека працюють разом, забезпечуючи централізований

моніторинг і швидке реагування на інциденти безпеки, що є важливим для сучасних ІТ-інфраструктур.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 28

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
4. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.
5. R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, vol. 3800 (2024) 97–105.
6. S. Zybin, et al., Approach of the Attack Analysis to Reduce Omissions in the Risk Management, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 318–328.
7. O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 29–43.
8. Y. Dreis, et al., Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection, in: Cyber Security and Data Protection, vol. 3800 (2024) 1–11.
9. D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II-2, vol. 3188 (2021) 135–148.
10. S. Kulibaba, et al., Linked System of Data Organization and Management, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 117–126.

11. S. Shevchenko, et al., Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 333–342.
12. V. Shapoval, et al., Automation of Data Management Processes in Cloud Storage, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 410–418.
13. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 117–124.
14. Y. Dreis, et al., Restricted Information Identification Model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.
15. L. Kriuchkova, et al., Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 261–268.
16. S. Kulibaba, Advanced Communication Model with the Voice Control and the Increased Security Level, CEUR Workshop, 3288 (2022) 64–72.
17. O. Bahatskyi, V. Bahatskyi, V. Sokolov, Smart Home Subsystem for Calculating the Quality of Public Utilities, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 168–173.
18. A. Zahynei, et al., Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 432–439.
19. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке EDR і як ця технологія допомагає виявляти та реагувати на кібератаки?

2. Як системи EDR визначають шкідливі програми на кінцевих пристроях?
3. Які типи атак можуть бути виявлені за допомогою технології UEBA?
4. Як UBA допомагає виявляти аномальну поведінку користувачів в організації?
5. Яким чином технологія UEBA інтегрується з іншими системами безпеки для кращого виявлення загроз?
6. Як технології EDR взаємодіють з SIEM-системами для централізованого моніторингу?
7. Які основні методи використовується для виявлення нульових уразливостей в EDR?
8. Як UEBA аналізує поведінку користувачів для виявлення інсайдерських загроз?
9. Яка роль машинного навчання в системах EDR та UEBA?
10. Як технології EDR можуть блокувати спроби експлуатації уразливостей на кінцевих пристроях?
11. Як EDR-системи реагують на інциденти безпеки в реальному часі?
12. Яким чином системи EDR і UEBA можуть покращити виявлення складних, багатофазових атак?
13. Як технології UEBA використовують дані про поведінку користувачів для прогнозування можливих загроз?
14. Які переваги має використання UEBA для виявлення внутрішніх загроз порівняно з традиційними методами?
15. Як EDR допомагає забезпечити безпеку мобільних пристроїв?
16. Які функції має інтерфейс користувача в системах EDR?
17. Як система EDR виявляє та реагує на фішинг-атаки на кінцевих пристроях?
18. Яким чином EDR може блокувати атаки, що використовують техніки social engineering?
19. Як UEBA може виявляти порушення безпеки, спричинені зловживаннями привілеями?
20. Як ефективно налаштувати політики виявлення та блокування в системах EDR?
21. Як система UEBA може допомогти в управлінні доступом на основі поведінки?
22. Які технології аналізу використовуються для виявлення нульових атак в EDR?
23. Як інтеграція EDR з іншими засобами захисту, такими як антивіруси або фаєрволи, підвищує ефективність захисту?

24. Як UEBA може допомогти у виявленні порушень політик доступу в організації?
25. Які основні виклики при впровадженні EDR і UEBA в середовищах з великою кількістю кінцевих пристроїв?

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.
2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.
3. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. Про основні засади забезпечення кібербезпеки України: Закон України // Відомості Верховної Ради України. 2017. № 45. Ст. 403.
4. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.
5. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 229–252.
6. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.
7. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
8. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
9. Сагун А. В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. : для студентів спец. 125 - "Кібербезпека", 12 - "Інформаційні технології" всіх форм навчання / Андрій Вікторович Сагун, Олег Миколайович Кулініч, Владислав Володимирович Хайдуров. – Київ : НУБіП України, 2023.

10. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
11. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; За заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 С.
12. Довженко, Н., Мазур, Н., Костюк, Ю., & Рзаєва, С. (2024). Інтеграція ІОТ та штучного інтелекту в інтелектуальні транспортні системи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 430–444.
13. Костюк Ю., Шестак Я. Транспортний рівень моделі ISO/OSI в комп'ютерних мережах. Міжнародний науково-практичний журнал "Товари і ринки". 2021. № 4. С. 49-58.
14. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 374–391.
15. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. Information Technology, 4(6), 14-33.
16. Криворучко О. В., Костюк Ю. В., Самойленко Ю. О. Методологія тестування системи захисту інформаційної системи на проникнення // Проблеми кібербезпеки інформаційно-телекомунікаційних систем:Збірник матеріалів доповіді та тез; м. Київ, 15-16 квітня 2021 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: О.К. Закусило. (голова) та ін.–К.:ВПЦ"Київський університет", 2021.–190 с. (с. 137-138).
17. Довженко, Н., Мазур, Н., Костюк, Ю., & Рзаєва, С. (2024). Інтеграція ІОТ та штучного інтелекту в інтелектуальні транспортні системи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 430–444.
18. Kryvoruchko O., Kostiuk Y., Desiatko A. Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods// Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 140-149.
19. Самойленко Ю.О., Костюк Ю.В. Теорія інформаційної безпеки // Кібергігієна. Кібербезпека. Безпека держави : Матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – с. 16-17.

20. Костюк Ю.В., Рзаєва С.Л. Стратегічні рішення SOC для забезпечення інформаційної безпеки в умовах сучасних кіберзагроз (2024) Сучасні вектори розвитку України: забезпечення сталості та безпеки. Збірник матеріалів II Міжнародної науково-практичної конференції (м. Київ, 28 жовтня 2024 року). Чернігів: ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2024, с.
21. Криворучко О.В., Костюк Ю.М., Захаров Р.Г. Програми моніторингу мереж // VIII Міжнародна науково-практична конференція «Управління розвитком технологій», 26-27 березня 2021 р., Київ, Україна – с. 34-36.
22. Бурячок В. Л., Киричок Р. В., Складанний П. М. (2018) Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ. 320 с.
23. Жданова, Ю., Шевченко, С., Спасітелєва, С., & Сокульский, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.
24. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 390–400.
25. Костюк Ю.В., Самойленко Ю.О., Костюк І.В. Критерії оцінювання захищеності інформаційних систем та мереж // Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2021) : матеріали тез доповідей XI Міжнародної науково-практичної конференції (м. Чернігів, 26–27 травня 2021 р.): у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів: НУ «Чернігівська політехніка», 2021. – Т. 2. – с. 162.
26. Жданова, Ю., Шевченко, С., Спасітелєва, С., & Сокульский, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 330–343.
27. Костюк Ю.В., Самойленко Ю.О. Моніторинг інформаційної безпеки в інформаційно-комунікаційних системах та мережах // Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці: Матеріали II Міжнародної науково-практичної конференції (м. Київ, 7 грудня 2021 року). К.: ДУІТ, ХНУРЕ. 2021. с. 670.
28. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі

аналізу енергоспоживання та трафіку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 390–400.

29. Костюк Ю.В., Самойленко Ю.О. Кіберризики в системах управління безпекою на морському транспорті // International scientific conference «Maritime security of the Baltic-Black sea region: challenges and threats»: conference proceedings, December 23, 2021. Odessa: Izdevnieciba «Baltija Publishing», p.407.

30. Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 468–486.

31. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(24), 185–195.

32. Костюк Ю.В., Самойленко Ю.О. Моніторинг інформаційної безпеки в інформаційно-комунікаційних системах та мережах // Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці: Матеріали II Міжнародної науково-практичної конференції (м. Київ, 7 грудня 2021 року). К.: ДУІТ, ХНУРЕ. 2021. с. 670.

33. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273.

34. Крючкова, Л., & Ємельяненко, М. (2024). Захист web-ресурсу intranet від зовнішніх і внутрішніх загроз. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 318–327.

35. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 338–347.

36. Костюк Ю.В., Самойленко Ю.О. Проблеми захисту корпоративних інформаційно-телекомунікаційних мереж // Сучасні тенденції розвитку фінансових та інноваційно-інвестиційних процесів в Україні. Матеріали V Міжнародної науково-практичної конференції 25 лютого 2022 року : збірник наукових праць [Електронний ресурс]. – Вінниця: ВНТУ, 2022. – с. 781-783.

37. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного

інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18.

38. Костюк Ю.В., Самойленко Ю.О. Трансформація загроз економічній безпеці держави // Всеукраїнська науково-практична конференція за міжнародною участю «Сучасні тенденції та суперечності розвитку світової економіки та бізнесу»: збірник матеріалів конференції, м. Київ, 25 січня 2022 р. / ред. кол.: І. А.Семенець-Орлова (гол. ред.), І. І. Каліна (заст. гол. ред.), Ю. В. Мазур (упоряд. і відп. ред.) та ін. Київ: Міжрегіональна Академія управління персоналом, 2022. С. 239-241.

39. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 68–83.

40. Машталяр, Я., Козачок, В., Брже夫ська, З., Богданов, О., Оксанич, І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 156–167.

41. Марценюк, М., Козачок, В., Богданов, О., Іосіфов, Є., & Брже夫ська, З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 148–155.

42. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178.

43. Костюк Ю.В., Ковальова Л.І., Повна Н.І. Захист інформації у сегменті інформаційної системи на основі інтелектуальних технологій // Збірник тез VI Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2023. – с. 77-79.

44. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 99–120.

45. Костюк Ю.В., Самойленко Ю.О., Костюк І., Ковальова Л.І. Використання коригуючих кодів для інформаційного захисту комп'ютерних мереж // Тези доповідей дев'ятої міжнародної науково-практичної конференції «Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. // Відповідальна за випуск завідувач кафедри ІТ С.В. Цюцюра, – К.: КНУБА, 2022. – С. 69-70.

46. Спасітелева, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною

архітектурою. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 193–210.

47. Костюк Ю.В. Контроль інцидентів інформаційної безпеки в корпоративній телекомунікаційній мережі // Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці: Матеріали III Міжнародної науково-практичної конференції (м. Київ, 22 листопада 2022 року). К.: ДУІТ, ХНУРЕ. 2022.- с. 518-520.

48. Костюк Ю.В., Самойленко Ю.О., Костюк І.В. Особливості захисту конфіденційної інформації в професійному інформаційному середовищі // Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.). Івано-Франківськ: ІФНТУНГ, 2022. с. 59-63.

49. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції ZERO TRUST при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233.

50. Криворучко О.В., Костюк Ю.В. Інтелектуальне управління мережевою безпекою в інформаційно-телекомунікаційних системах // Міжнародна наукова конференція «Інтелектуальні Транспортні Системи: Екологія, Безпека, Якість, Комфорт». – К.: НТУ, 2022, Вип. 1 – с 86-87.

51. Костюк Ю.В., Самойленко Ю.О. Спеціалізовані моделі для проектування, розробки та реалізації інформаційних систем // Матеріали IX Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами», 25 листопада 2022 [Електронний ресурс]. – К: НУХТ, 2022. – с. 206-207.

52. Shevchenko, S., Zhdanova Y., & Spasiteleva, S. (2023). Математичні методи в кібербезпеці: теорія катастроф. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 165–175.

53. Костюк Ю.В., Самойленко Ю.О., Костюк І.В. Захист інформації в корпоративній інформаційній системі на основі інтелектуальних технологій // Інноваційні технології XXI століття: зб. наук. пр. / гол. ред. Л. Г. Білий. Хмельницький : Вид-во МАУП, 2022. Вип. 7. С. 85-93.

54. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроектні рішення щодо побудови системи авторизації на основі концепції ZERO TRUST. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242.

55. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158.
56. Yuliia Samoilenko, Yuliia Kostiuk. Cybersecurity of industrial control systems based on dial-up access // Захист інформації і безпека інформаційних систем: матеріали VIII Міжнар. наук.-техн. конф. – Львів: Видавництво Львівської політехніки, 2021. – с. 25-25.
57. Криворучко О. В., Костюк Ю. В., Самойленко Ю. О. Інформаційна безпека економічних систем // Глобалізаційні виклики розвитку національних економік : тези доповідей II Міжнар. наук.-практ. конф. (Київ, 19 жовтня 2021 р.) / відп. ред. А. А. Мазаракі. – Київ : Київ. нац. торг.-екон. ун-т, 2021. – с. 275-278 – Укр. та англ. мовами.
58. Костюк Ю. В., Левицький В. Ю. Система захисту передачі даних за допомогою інтернет-протоколів // Матеріали VIII Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами», 26 листопада 2021. [Електронний ресурс] – К: НУХТ, 2021 – с. 245-246.
59. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Порівняльний аналіз рішень для забезпечення контролю та управління привілейованим доступом в іт-середовищі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 98–112.
60. Костюк Ю.В. Стратегії захисту крайових пристроїв з використанням нейронних мереж Коско // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 26 квітня 2024 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2024. – с. 17-18.
61. Даник Ю. Г., Воробієнко П. П., Чернега В. М. (2019) Основи кібербезпеки та кібероборони: підручник. 2-ге вид., перероб. і доп. Одеса: ОНАЗ ім. О. С. Попова. 320 с.
62. Shevchenko, S., Zhdanova Y., Skladannyi, P., & Boiko, S. (2022). Інсайтери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 175–185.
63. Костюк Ю.В. Математичне моделювання захищених інформаційних систем // Інноваційний потенціал сучасної науки: зб. наук. праць IV Всеукраїнської наук.-практ. інтернет-конф., (18 травня 2023 року.

Кам'янець-Подільський). - Кам'янець-Подільський Заклад вищої освіти «Подільський державний університет», 2023. с. 171-174.

64. Костюк Ю.В. Математичне моделювання комп'ютерних мереж, керованих протоколами випадкового множинного доступу // Актуальні питання науки, освіти та технологій в умовах сучасних викликів: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 9 травня 2023 р.): у 2 ч. Кременчук: ЦФЕНД, 2023. Ч. 1. С. 57-58.

65. Костюк Ю.В., Войткевич А.А. Дослідження технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1017-1032.

66. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.

67. Костюк Ю.В. Виявлення загроз порушення інформаційної безпеки в мережах з динамічною топологією з використанням інтелектуальних методів // Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023) 26 травня <https://mmis.ipt.kpi.ua/2023/03/28/tacs-2023-announce/>

68. Костюк Ю.В., Шапран В.О. Технології виявлення аномальних подій та сигнатур в реальному часі. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1069-1084.

69. Костюк Ю. В Впровадження інтелектуальних систем у процес оцінки ризиків інформаційної безпеки в безпроводових мережах // Сьомі Геретівські читання: наукові статті, тези доповідей та інші матеріали Всеукраїнської науково-практичної конференції (м. Тернопіль, Україна, 22 вересня 2023 року). Науковий, методичний, інформаційний збірник Тернопільського обласного комунального інституту післядипломної педагогічної освіти / Редколегія: О. М. Петровський, В. С. Мисик, І. М. Вітенко, О. І. Когут, Ю. Ч. Шайнюк, Т. В. Магера, Ф. І. Полянський, Н. Б. Стрийвус, Г. І. Герасимчук. Тернопіль: ТОКІППО, 2023. С. 162-168.

70. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

71. Костюк Ю.В., Гейдар Гейдаров. Роль токенів та сесійного керування в системах інформаційної безпеки для протидії міжсайтовим атакам. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право»,

Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1216-1231.

72. Технології захисту інформації: підручник / М.М. Браїловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦП «Компринт», 2021. – 296 с.

73. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

74. Костюк Ю.В., Кравченко Д.В. Методи захисту даних на підприємствах соціальної сфери. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 4(32) 2024. с. 1033-1047.

75. Браїловський М.М. Аналіз кіберзахищеності інформаційних систем: монографія/ Браїловський М.М., Зибін С.В., Кобозева А.А., Хорошко В.О., Хохлачова Ю.Є. К.: ФОП Ямчинський О.В., 2021. – 360 с.

76. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

77. Лахно В. А., Васіліу Є. В., Гладких В. М., Домрачев В. М., Сивкова Н. М. (2020) Методи та засоби захисту інформації: навч. посіб. Київ: Компринт О. В. 444 с.

78. Костюк Ю.В., Андрій Голинський. Стратегії інтегрованого захисту бездротових сенсорних мереж. «Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 5(33) 2024. с. 1232-1247.

79. Костюк Ю.В., Єгор Константинов. «Вдосконалені методи безпеки в 4G мережах з метою забезпечення ефективного захисту від атак на передачу даних»(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 6(34) 2024.

80. Kryvoruchko O., Kostiuk Y., Desiatko A. Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods// Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 140-149. DOI: 10.18372/2225-5036.30.18615

81. Лахно В. А., Терещук А. М., Петренко Т. А. (2016) Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак. Захист інформації. Т. 18. № 2. С. 99–106.

82. Владислав Шапран, Юлія Костюк Виявлення аномальних подій та сигнатур у реальному часі. Інформаційні технології та кібербезпека в умовах воєнного часу [Електронний ресурс] : матеріали студ. наук.-практ. конф. (Київ, 18 квіт. 2024 р.) / відп. ред. К. В. Хорольська. – Київ : Держ. торг.-екон. ун-т, 2024. – с. 237-241.
83. Лахно В. А., Гусєв Б. С., Блозва А. І. Касаткін Д. Ю., Осипова Т. Ю. (2020) Кластеризація ознак мережевих атак в задачах аналізу захищеності інформації. Кібербезпека: освіта, наука, техніка. № 1(9). С. 45–58.
84. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
85. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
86. Гришук Р.В. Основи кібернетичної безпеки : Монографія / Ю.Г. Даник, Р.В. Гришук ; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2019. – 636 с.
87. Сунь-Цзи. (2014) Мистецтво війни: переклад Г. Латника. Київ: Арій. 128 с.
88. V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 23–32
89. V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.
90. I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27.
91. B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.
92. V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

93. V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.
94. M. TajDini, et al., Wireless Sensors for Brain Activity—A Survey, Electronics 9(12), iss. 2092 (2020) 1–26.
95. Костюк Ю.В., Владислав Марценюк. «Аналіз ефективності та розгляд сучасних тенденцій в застосуванні принципів двофакторної аутентифікації для забезпечення безпеки в веб-застосунках у сфері комерційних закладів охорони здоров'я»(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»): журнал. 2024. № 6(34) 2024.
96. F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021).
97. F. Kipchuk, et al., Investigation of Availability of Wireless Access Points based on Embedded Systems, in: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (2019).
98. A. Carlsson, et al., Sustainability Research of the Secure Wireless Communication System with Channel Reservation, in: 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020).
99. I. Bogachuk, V. Sokolov, V. Buriachok, Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers, in: 5th International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (2018) 581–585.
100. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.
101. A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 1–13.
102. P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 240–245.
103. P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in:

Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 169–176.

104. V. Zhebka, et al., Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3288 (2022) 149–155.

105. Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020).

106. Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25.

107. V. Sokolov, P. Skladannyi, A. Platonenko, Video Channel Suppression Method of Unmanned Aerial Vehicles, in: IEEE 41st International Conference on Electronics and Nanotechnology (2022) 473–477.

108. H. Hulak, et al. Formation of Requirements for the Electronic RecordBook in Guaranteed Information Systems of Distance Learning, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021, vol. 2923 (2021) 137–142.

109. M. TajDini, V. Sokolov, P. Skladannyi, Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 7–11.

110. M. TajDini, V. Sokolov, V. Buriachok, Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio, in: 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 287–296.

111. Yevseiev, Models of Socio-Cyber-Physical Systems Security: monograph, PC TECHNOLOGY CENTER (2023).

112. D. Shevchuk, et al., Designing Secured Services for Authentication, Authori-zation, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.

113. Z. Brzhevska, et al., Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 257–264.

114. R. Marusenko, V. Sokolov, V. Buriachok, Experimental Evaluation of Phishing Attack on High School Students, Advances in Computer Science for Engineering and Education III, vol. 1247 (2020) 668–680.

115. I. Iosifov, O. Iosifova, V. Sokolov, Sentence Segmentation from Unformatted Text using Language Modeling and Sequence Labeling Approaches, in: VII International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (2020) 335–337.
116. V. Buhas, et al., Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188, no. 2 (2021) 273–281.
117. M. Moshenchenko, et. al., Optimization Algorithms of Smart City Wireless Sensor Network Control, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 32–42.
118. D. Berestov, et al., Analysis of Features and prospects of Application of Dynamic Iterative Assessment of Information Security Risks, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 329–335.
119. B. Zhurakovskiy, et al., Secured Remote Update Protocol in IoT Data Exchange System, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 67–76.
120. V. Buriachok, et al., Implementation of Active Cybersecurity Education in Ukrainian Higher School, Information Technology for Education, Science, and Technics, vol. 178 (2023) 533–551.
121. P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 97–106.
122. Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 25–37.
123. R. Marusenko, V. Sokolov, P. Skladannyi, Social Engineering Penetration Testing in Higher Education Institutions, Advances in Computer Science for Engineering and Education VI, vol. 181 (2023) 1132–1147.
124. V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5.
125. O. Deineka, et al., Designing Data Classification and Secure Store Policy According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 398409.
126. V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165.

127. R. Marusenko, V. Sokolov, I. Bogachuk, Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation, *Advances in Artificial Systems for Logistics Engineering*, vol. 135 (2022) 583–594.
128. O. Romanovskyi, et al., Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition, *Advances in Computer Science for Engineering and Education IV*, vol. 83 (2021) 25–36.
129. R. Kyrychok, et al., Development of a Method for Checking Vulnerabilities of a Corporate Network using Bernstein Transformations, *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 9(115) (2022) 93–101.
130. O. Romanovskyi, et al., Prototyping Methodology of End-to-End Speech Analytics Software, in: *4th International Workshop on Modern Machine Learning Technologies and Data Science*, vol. 3312 (2022) 76–86.
131. S. Shevchenko, et al., Information Security Risk Management using Cognitive Modeling, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II*, vol. 3550 (2023) 297–305.
132. V. Zhebka, et al., Methodology for Predicting Failures in a Smart Home based on Machine Learning Methods, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 322–332.
133. V. Zhebka, et al., Methodology for Choosing a Consensus Algorithm for Blockchain Technology, in: *Workshop on Digital Economy Concepts and Technologies Workshop, DECaT*, vol. 3665 (2024) 106–113.
134. V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 449–457.
135. O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II*, vol. 3550 (2023) 29–43.
136. V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 290–300.
137. O. Mykhaylova, et al., Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 239–251.

138. M. Myrontsov, et al., Method for Determining Areas of Stable Solutions of Inverse Problems of Mathematical Physics by the Example of Well Electrometry, in: Workshop on Information Technology and Mathematical Modeling for Environmental Safety, vol. 3021 (2021) 115–126.
139. O. Kopiika, P. Skladannyi, Use of Service-Oriented Information Technology to Solve Problems of Sustainable Environmental Management. Information Technology and Mathematical Modeling for Environmental Safety 3021 (2021) 66–75.
140. I. Iosifov, et al., Natural Language Technology to Ensure the Safety of Speech Information, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 216–226.
141. B. Zhurakovskiy, et al., Modifications of the Correlation Method of Face Detection in Biometric Identification Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 55–63.
142. Z. B. Hu, V. Buriachok, V. Sokolov, Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm, Advances in Computer Science for Engineering and Education III, vol. 1247 (2020) 518–533.
143. V. Zhebka, et al., Stability Method of Connectivity Automated Calculation for Heterogeneous Telecommunication Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188 (2021) 282–287.
144. Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421. (2023) 266–271.
145. N. Dovzhenko, et al., Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes, in: Cybersecurity Providing in Information and Telecommunication Systems vol. 3421 (2023) 278–283.
146. S. Kulibaba, Advanced Communication Model with the Voice Control and the Increased Security Level, CEUR Workshop, 3288 (2022) 64–72.
147. Y. Dreis, et al., Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 277–289.
148. M. Astafieva, et al., Formation of High School Students' Resistance to Destructive Information Influences, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 87-96.

149. S. Shevchenko, et al., Conflict Analysis in the “Subject-to-Subject” Security System, *Cybersecurity Providing in Information and Telecommunication Systems* Vol. 3421 (2023) 56–66.
150. R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3288 (2022) 142–148.
151. L. Kriuchkova, et al., Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, in: *Cybersecurity Providing in Information and Telecommunication Systems II*, vol. 3550 (2023) 261–268.
152. V. Astapenia, V. Sokolov, P. Skladannyi, Problematic Issues of the Accelerating Lens Deployment, in: *IEEE 2nd Ukrainian Microwave Week* (2022) 337–341.
153. Y. Dreis, et al., Restricted Information Identification Model, in: *Cybersecurity Providing in Information and Telecommunication Systems* Vol. 3288 (2022) 89–95.
154. S. Buchyk, et al., Improvement of Steganographic Methods based on the Analysis of Image Color Models, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 2923 (2021) 117–124.
155. Y. Sovyn, et al., Minimization of Bitsliced Representation of 4×4 S-Boxes based on Ternary Logic Instruction, in *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3421 (2023) 12–24.
156. V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: *IEEE 5th International Conference on Advanced Information and Communication Technologies* (2023) 33–36.
157. V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: *IEEE 5th International Conference on Advanced Information and Communication Technologies* (2023) 1–4.
158. K. Tkachenko, et al., Ontological Approach in Modern Educational Processes, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 88–97.
159. V. Dudykevych, et al., Detecting Deepfake Modifications of Biometric Images using Neural Networks, in: *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS*, vol. 3654 (2024) 391–397.
160. V. Buhas, et al., Cybersecurity Role in AI-Powered Digital Marketing, in: *Workshop on Digital Economy Concepts and Technologies Workshop, DECaT*, vol. 3665 (2024) 1–11.

161. S. Shevchenko, et al., Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 333–342.
162. D. Virovets, et al., Soul Bound Token as Digital Twins in Peer-to-Peer Economic Systems, in: Digital Economy Concepts and Technologies, vol. 3665 (2024) 97–105.
163. S. Abramov, A. Bessalov, V. Sokolov, Properties of Isogeny Graph of Non-Cyclic Edwards Curves, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 234–239.
164. A. Ilyenko, et al., Practical Aspects of Using Fully Homomorphic Encryption Systems to Protect Cloud Computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 226–233.
165. Y. Dreis, et al., Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection, in: Cyber Security and Data Protection, vol. 3800 (2024) 1–11.
166. S. Kulibaba, et al., Linked System of Data Organization and Management, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 117–126.
167. Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.
168. G. Otto, et al., Parametric Model of a Laser with External Distributed Feedback in the System of Remote Measurement of Nanovibrations, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3421 (2023) 284–292.
169. D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II-2, vol. 3188 (2021) 135–148.
170. S. Zybin, et al., Approach of the Attack Analysis to Reduce Omissions in the Risk Management, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 318–328.
171. O. Trofymchuk, et al., On the Use of Gray Codes for Solving 0-1 Combinatorial Problems of Optimization and Decision-Making in Environmental and Economic Systems, in: Workshop on Information Technology and Mathematical Modeling for Environmental Safety, vol. 3021 (2021) 1–17.

172. P. Anakhov, et al., Hybrid Study of the Geophysical Situation in the Depressed Zone of Hydroelectric Power Plants Reservoir, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 269-274.

173. Костюк Ю.В., Степашкіна К.В. Моделювання інтелектуальних систем управління захистом інформації в інформаційно-телекомунікаційних системах // Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2023) : матеріали тез доповідей XIII Міжнародної науково-практичної конференції (м. Чернігів, 25–26 травня 2023 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2023. – Т. 2. – с. 252-253.

174. R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, vol. 3800 (2024) 97–105.

175. L. Kriuchkova, V. Sokolov, P. Skladannyi, Determining the Zone of Successful Interaction in RFID Technologies, in IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (2024) 168–171.

176. Savchuk, K., Rzaieva, S., Savchenko, T., Rzaiev, D. (2024). Data Protection Strategies and Technologies for Ensuring National Financial Security. In: Al Mubarak, M., Hamdan, A. (eds) Innovative and Intelligent Digital Technologies; Towards an Increased Efficiency. Studies in Systems, Decision and Control, vol 564. Springer, Cham.

177. Methods of Modeling Database System Security Rzaieva, S., Rzaiev, D., Kostyuk, Y., Hulak, H., Shcheblanin, O. CEUR Workshop Proceedings This link is disabled., (CPITS 2024), 2024, 3654, pp. 384–390.

178. Z. Hu, et al., Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range, DataCentric Business and Applications 48 (2020) 675–709.

179. H. Hulak, et al., Dynamic model of guarantee capacity and cyber security management in the critical automated systems, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2022) 102-111.

180. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

181. S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in:

Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.

182. A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

183. V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526.

184. V. Astapenya, et al., Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems, in: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021).

185. V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.

186. V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master's Program on Cybersecurity, Advances in Computer Science for Engineering and Education II, vol. 938 (2020) 610–624.

187. H. Shevchenko, et al., Information Security Risk Analysis SWOT, Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021) 309–317.

188. P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, J. Theor. Appl. Inf. Technol. 100(22) (2022) 6635–6644.

189. O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.

190. A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of NonSupersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

191. Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388.

192. M. TajDini, et al., Brainwave-based Authentication using Features Fusion, Comput. Secur. 129, no. 103198 (2023) 1–11.

193. D. Virovets, et al., Ways of Interaction of Autonomous Economic Agents in Decentralized Autonomous Organizations, in: Cybersecurity

Providing in Information and Telecommunication Systems, vol. 3421 (2023) 182–190.

194. Z. B. Hu, V. Buriachok, V. Sokolov, Implementation of Social Engineering Attack at Institution of Higher Education, in: 1th International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), vol. 2654 (2020) pp. 155–164.

195. A. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17.

Інтернет-джерела

1. Рекомендації CERT-UA щодо протидії APT (Advanced Persistent Threat). URL: <https://cert.gov.ua/recommendations/18>

2. Технологія VPN може загрожувати кібербезпеці. URL: <https://detector.media/infospace/article/126505/2017-05-31-tekhnologiya-vpnmozhe-zagrozhuvati-kiberbezpetsi-inau>

3. JP 3–12 Cyberspace Operations, 8 June 2018. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

4. DOD Dictionary of Military and Associated Terms. As of January 2019. URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>

5. Cybersecurity a generic reference curriculum (2016). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-162_curriculum.pdf

6. National Cyber Security Strategy Good Practice Guide (2016). URL: <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>

7. Castro D. (2018). Boosting the Cyberworkforce. URL: <http://www.govtech.com/data/Boosting-the-Cyberworkforce.html>

8. Cisco -Україна. URL: <https://www.cisco.com>

9. Про основні засади забезпечення кібербезпеки України: Закон України // Відомості Верховної Ради України. 2017. № 45. Ст. 403.

10. Закон України "Про інформацію".

11. Закон України "Про захист інформації в інформаційно-комунікаційних системах".

12. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT) "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги".

13. ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою".

14. ДСТУ ISO/IEC 27005:2022 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки".
15. ДСТУ ISO/IEC 27701:2022 "Розширення для управління конфіденційністю в системах управління інформаційною безпекою".
16. ДСТУ ISO/IEC 15408:2020 "Критерії оцінювання безпеки інформаційних технологій".
17. ДСТУ ISO/IEC 24762:2015 "Інформаційні технології. Методи захисту. Рекомендації з відновлення інформаційно-комунікаційних технологій після інцидентів".

Навчальне видання

КОСТЮК Юлія Володимирівна,
СКЛАДАННИЙ Павло Миколайович,
ГУЛАК Геннадій Миколайович,
БЕБЕШКО Богдан Тарасович,
ХОРОЛЬСЬКА Карина Вікторівна,
РЗАЄВА Світлана Леонідівна

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Підручник