Державний торговельно-економічний університет

В. І. Пашорін, Ю. В. Костюк

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Навчальний посібник

Київ 2023

УДК 004.056
П 22

Автори: В. І. Пашорін, канд. техн. наук, проф.,
Ю. В. Костюк, старш. викл.

Рецензенти: Н. В. Лукова-Чуйко, канд. фіз.-мат. наук, д-р техн. наук, доцент Київського національного університета ім. Тараса Шевченка, завідувач кафедри кібербезпеки та захисту інформації;
В. А. Лахно, д-р техн. наук, професор Національного університета біоресурсів і природокористування України, завідувач кафедри комп'ютерних систем і мереж;
В. П. Звєрєв, канд. техн. наук, ст. наук. співроб., професор кафедри інженерії програмного забезпечення та кібербезпеки, заступник керівника служби з питань інформаційної безпеки та кібербезпеки, керівник управління інформаційної безпеки Апарату РНБО України;
М. В. Сашньова, канд. техн. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету

Рекомендовано до друку вченою радою
Державного торговельно-економічного університету
(протокол № 3 від 30 вересня 2021 р.)

Пашорін В. І.

П 22 Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

ISBN 978-966-918-101-5
DOI: 10.31617/np.knute.2023-295

У навчальному посібнику розглянуто сучасні напрями забезпечення безпеки інформаційно-телекомунікаційних систем. Викладено технічні, криптографічні, програмні методи і засоби захисту інформації. Формулюються проблеми вразливості сучасних інформаційно-телекомунікаційних систем, розглядаються питання захисту інформації в розподілених інформаційних системах, організаційно-правове забезпечення захисту інформації. Розглянуті загальні питання технологій збереження даних в єдиному інформаційному просторі та впровадженню функцій протидій кіберзлочинності, здатності організовувати та підтримувати комплекс заходів щодо забезпечення безпеки інформаційної та кібербезпеки, з урахуванням їхньої юридичної та економічної обґрунтованості, технічної реалізації, запобігання можливих зовнішніх впливів, імовірних загроз, а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, застосування технологій захисту інформаційно-телекомунікаційних систем.

Призначено для студентів галузі знань 12 «Інформаційні технології», аспірантів, що вивчають методи захисту інформації та безпеки інформаційних систем.

УДК 004.056

ISBN 978-966-918-101-5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС	–	Інформаційна система
ІТ	–	Інформаційні технології
ІТС	–	Інформаційно-телекомунікаційна система
ЦОД	–	Центр обробки даних
ПЗ	–	Програмне забезпечення
IoT	–	Інтернет речей
IoE	–	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 ПЕМВН	–	Технічні засоби розвідки побічних електромагнітних 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
HTTP	–	Протокол передачі гіпертексту та інших типів даних
MAC	–	Унікальний ідентифікатор обладнання для комп’ютерних мереж

ВСТУП

Навчальний посібник містить основи теорії з дисципліни «Безпека інформаційних систем» для студентів галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека» спеціалізація «Безпека інформаційних та комунікаційних систем в економіці» та програмі дисципліни «Безпека інформаційних систем» денного, заочного та дистанційного навчання. Представлений матеріал відповідає вимогам робочої програми навчальної дисципліни «Безпека інформаційних систем» та навчальним планам і дозволяє охопити основні розділи даної дисципліни. Для кожної з частин визначені короткі теоретичні положення та контрольні запитання, що дозволяють оцінити знання студентів по кожному розділу дисципліни, що вивчається.

Посібник передбачає вивчення: законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; методів і засобів виявлення, управління та ідентифікації ризиків; методів і засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів і засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проєктування.

Корисний для студентів інших спеціальностей: «Комп'ютерна інженерія», «Інженерія програмного забезпечення», «Системний аналіз», а також аспірантів і здобувачів наукового ступеня кандидата технічних наук, які вивчають методи захисту інформації, заснованих на науково обґрунтованому аналізі ситуації та доступі до систем збору, зберігання й обробки інформації.

Метою посібника є надання необхідних теоретичних основ для засвоєння курсу майбутніми фахівцями з управління інформаційною безпекою та кібербезпеки й закріплення необхідних у подальшій роботі знань з основ інформаційної безпеки та отримати фахову компетентність щодо здатності відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів і походження, а також здатність впроваджувати та забезпечувати функціонування комплексних систем захисту (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів). Матеріал дисципліни пов'язаний зі спеціальними дисциплінами, що викладаються у закладах вищої освіти технічного профілю.

Забезпечення і підтримка інформаційної та кібербезпеки включають комплекс різнопланових заходів, що запобігають, відстежують і усувають несанкціонований доступ третіх осіб. Заходи інформаційної безпеки спрямовані також на захист від пошкоджень, спотворень, блокування або копіювання інформації. Принципово, щоб усі завдання вирішувалися одночасно – тільки тоді забезпечується повноцінний, надійний захист.

Для того, щоб національна безпека України могла відповідати рівню провідних економічних держав, необхідні як послідовні дії з боку держави, спрямовані на підвищення ефективності й розвиток системи взаємодії учасників ІКТ-галузі та забезпечення безпеки критично важливих об'єктів інформаційної та кіберінфраструктур, так і приділення підприємствами та організаціями нашої держави більшої уваги до питань власної інформаційної та кібербезпеки. Зважаючи на цей безперервний розвиток та постійну інформаційну боротьбу, що складає один з важливих елементів сучасної світової політики, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову кібербезпеки.

Розділ 1. КІБЕРПРОСТІР ТА КІБЕРБЕЗПЕКА: КЛЮЧОВІ ПИТАННЯ ТА ВИЗНАЧЕННЯ

ГЛАВА 1
Безпека інформаційних систем в умовах функціонування глобальних мереж

1.1. Актуальність безпеки інформаційно-телекомунікаційних систем (ІТС)
1.2. Класифікація та властивості інформації
1.3. Основні терміни і визначення безпеки ІТС

По-справжньому безпечною можна вважати лише систему, що:

1. *Виключена,*
2. *Замурована в бетонний корпус,*
3. *Замкнена в приміщенні зі свинцевими стінами,*
4. *Охороняється збройною вартою, але й у цьому випадку сумніви не залишають мене.*

Юджин Х. Спаффорд

Безпека інформаційних систем (ІС) та телекомунікаційних мереж залежить від обізнаності та навчання користувачів і застосування ними принципів кібербезпеки. Усвідомлення необхідності покращення стану кібербезпеки, а також усвідомлення того, що кібербезпека важлива для кожної країни в останні роки зростає.

1.1. Актуальність безпеки інформаційно-телекомунікаційних систем (ІТС)

Необхідною умовою ефективності функціонування і високої конкурентноздатності організацій, в тому числі і в торгово-економічній сфері, є впровадження електронного бізнесу, який використовує інформаційні технології для підвищення ефективності всіх сторін ділових відносин (продаж, маркетинг, платежі, фінансовий аналіз, пошук співробітників, підтримка клієнтів і партнерських відносин, послуги інтернет-банкінгу, електронна комерція, миттєве переведення коштів тощо). Одночасно з впровадженням електронного бізнесу виникають проблеми, пов’язані, по-перше, з необхідністю захисту інформації від неправомірного її використання (розкрадання, розголошення, зміни, руйнування), по-друге, з порушенням працездатності інформаційних ресурсів організації (тимчасова недоступність ресурсів, або блокування), коли навмисно або помилково порушуються процеси обробки і передачі інформації.

Неправомірна зміна, блокування, знищення, розкрадання або розголошення інформації, так само як і порушення працездатності інформаційних ресурсів організації, навмисно або помилково, коли порушуються процеси обробки і передачі інформації, завдають серйозної матеріальної та моральної шкоди суб’єктам інформаційної взаємодії. Інтереси цих суб’єктів полягають у тому, щоб певна частина інформації (конфіденційна комерційна і персональна інформація), була б постійно легкодоступна і в той же час надійно захищена від неправомірного її використання.

Дані проблеми покликана вирішити *СИСТЕМА БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ,* що захищає інформацію від несанкціонованого використання, а також інформаційні ресурси від впливів, спрямованих на порушення їх працездатності.

Чи поліпшується становище з безпекою електронного бізнесу? НІ.

Небезпека для сучасних інформаційних систем і комп'ютерних мереж, на жаль, не зменшується. Засоби злому інформаційних систем і маніпуляцій з електронною інформацією розвиваються так само швидко, як і всі високотехнологічні комп'ютерні галузі і тому цілий ряд причин.

По-перше, інформація стає особливим продуктом, вартість якого часто перевершує вартість інформаційної системи, в рамках якої він існує.

З переходом до ринкових відносин у сфері надання інформаційних послуг інформація здебільш розглядається як товар. Це породжує проблему володіння цим ресурсом, його знищення або зміни, виходячи з державних, комерційних, приватних та інших інтересів. Неправомірні використання, фальсифікація, знищення розголошення інформації завдають серйозної матеріальної шкоди власникам цієї інформації.

По-друге, змінилася інформаційне середовище. Ще 20...30 років тому, проблема безпеки інформаційних систем могла бути ефективно вирішена за допомогою організаційних заходів (режимний доступ до систем, охорона, сигналізація) завдяки територіальної концентрації інформаційних ресурсів і відсутності тісного зв'язку із зовнішнім світом. Загрози безпеці, виходили переважно від штатних співробітників.

Сучасне інформаційне середовище зовсім інше, сьогодні поширенні територіально розподілені системи і системи з віддаленим доступом до спільно використовуваних ресурсів.

Комп’ютери розміщуються в різних офісах організації і об’єднуються між собою за допомогою мереж, створюючи єдину ІТС.

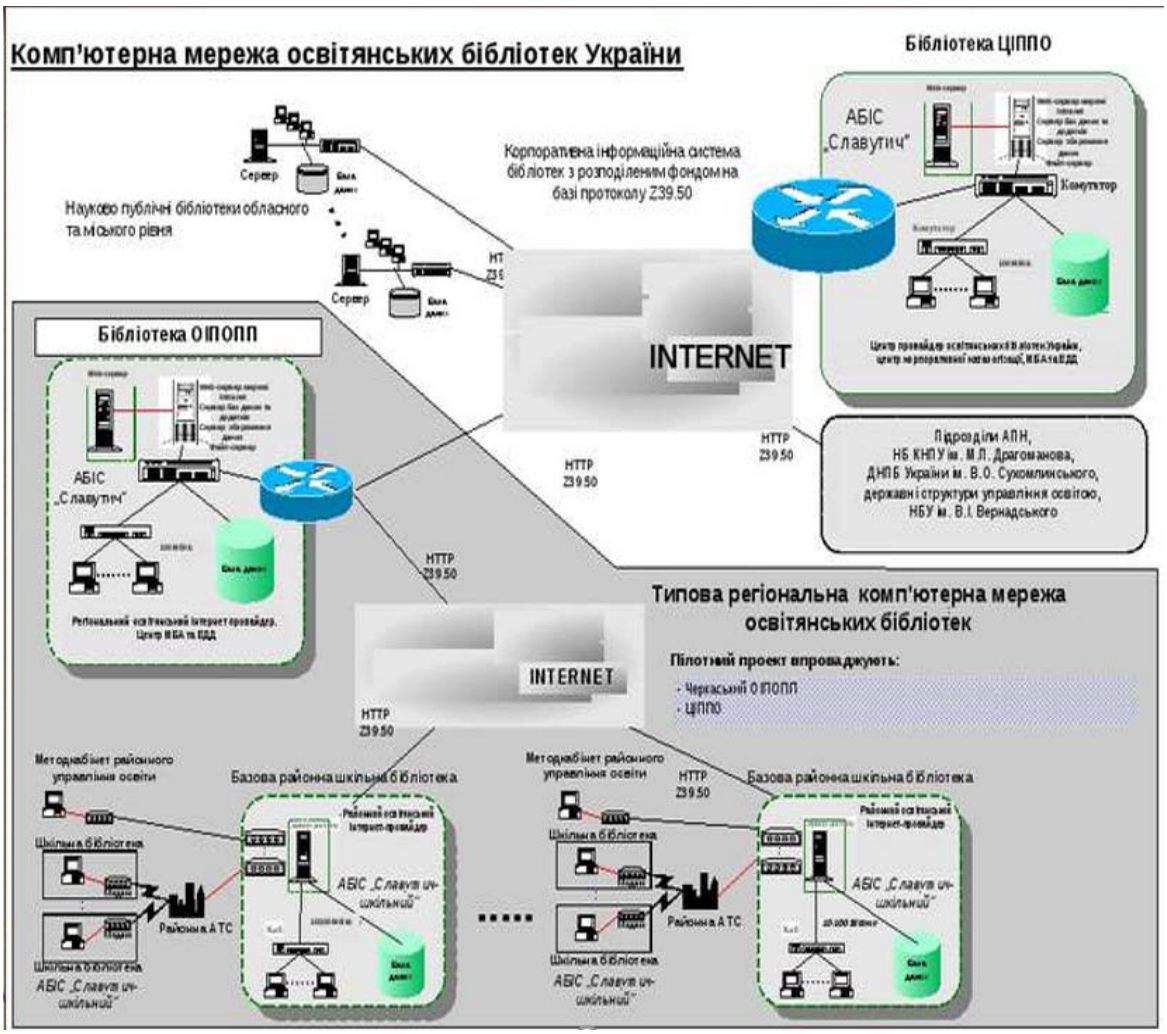


Рис. 1.1. Розподілена інформаційна система

Джерело: URL: http://www.medirent.com.ua/press-center/publications/information_systems_construction.html

Доступ до такої системи мають не тільки співробітники даної організації, а й зловмисник, який не має відношення до організації і може проникнути в систему віддалено й отримати інформацію, незважаючи на те, що знаходиться за тисячі кілометрів. Виникають нові можливі канали несанкціонованого доступу до інформації.

По-третє, зростають потужності сучасних ІТС при одночасному спрощенні їх експлуатації. Збільшується кількість джерел інформації та коло користувачів, які мають безпосередній доступ до інформаційних ресурсів, збільшуються обсяги інформаційних потоків даних, що обробляються і передаються каналами зв'язку.

По-четверте, розширилися сфери застосування ІТС (наприклад, тільки в торговельно-економічній сфері це впровадження систем, що виконують фінансові операції, обслуговують банківські та торговельні структури, обробляють комерційну таємницю організації тощо) і як наслідок, зростання кількості розподілених баз даних різного призначення. Відбувається перехід до автоматизованих систем управління та обробки інформації.

По-п'яте, все більшої популярності набуває використання для підтримки бізнесу «хмарного» середовища, що вимагає перегляду підходів до забезпечення безпеки ІТС.

«Хмарні» обчислення (Cloud computing) – це технологія розподіленої обробки даних, при якій спільно використовувані комп'ютерні ресурси, програмне забезпечення (ПЗ) і дані надаються користувачам за запитом як сервіс через Інтернет. «Хмарний» сервіс являє собою особливу клієнт-серверну технологію – використання клієнтом ресурсів (процесорний час, оперативна пам'ять, дисковий простір, мережеві канали, спеціалізовані контролери, програмне забезпечення). На перший погляд, вимоги до безпеки «хмарних» обчислень нічим не відрізняються від вимог до звичайних центрів обробки даних (ЦОД), але «хмарна» інфраструктура виявляється більш складною, має нові властивості і відповідно нові, невідомі досі вразливості. Перехід до «хмарного» середовища призводить до появи принципово нових загроз.

По-шосте. Зростання використання в бізнесі мобільних пристроїв та бездротових мереж, які можна вважати новими векторами атак, а також поява ефективних засобів технічної розвідки отримання інформації. Впровадження нових технологій

приносить і нові ризики безпеки, оскільки старі підходи до захисту не працюють. Наприклад, класичний метод пошуку вірусів на основі сигнатурного аналізу не має сенсу в сучасних мобільних операційних системах, оскільки це несумісне з моделлю поширення мобільних додатків і тому, що деякі типи вразливостей менш релевантні до мобільних додатків, ніж до десктопних і вебдодатків. Як виявилося, мобільну безпеку переважно зачіпає зберігання даних: додатки зберігають особисту інформацію, зображення, записи голосу, замітки, облікові дані, інформацію про бізнес, розташування тощо. Маючи номер телефона людини, можна отримати необмежений доступ до його особистого життя. Якщо врахувати, що мобільні пристрої легко губляться і викрадаються, а мобільні віруси зараз активно розвиваються, необхідність захисту даних стає ще більш очевидною.

По-сьоме **–** масове поширення інтернету речей (IoT). Пристрої інтернету речей ще не відповідають стандартам безпеки, що робить їх більш уразливими для атак. Зловмисники використовують їх для входу в мережу організації, а потім переходять до інших методів атак.

Рис. 1.2. Інтернет речей

Джерело: URL: http://www.telesphera.net/blog/internet-of-things.html

Цифровізація бізнесу (і формування Інтернету всього (IoE)) принесе нові приводи для занепокоєння. Кількість векторів атак неминуче збільшиться, що призведе до розширення робочого простору для зловмисників.

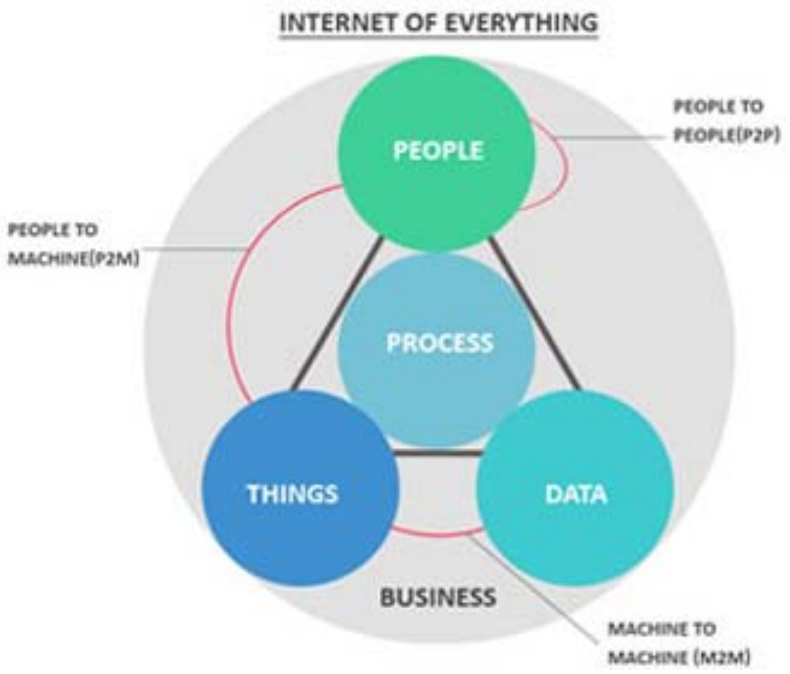


Рис. 1.3. Інтернет всього

Джерело: URL: https://www.netacad.com/ru/courses/iot/introduction-iot

Кожна нова технологія приносить нові ризики безпеки, спроба встигнути за цими змінами і є один з основних викликів, які стоять перед індустрією безпеки. Сторона захисту завжди на кілька кроків позаду. Спроба застосувати старий підхід: смартфони – це маленькі комп'ютери і мобільні додатки – звичайне ПЗ, а значить вимоги безпеки абсолютно такі – невиправдані. Наприклад, класичний метод пошуку вірусів на підставі сигнатурного аналізу не має сенсу в сучасних мобільних операційних системах, тому що це несумісне з моделлю поширення мобільних додатків і тому, що деякі типи вразливостей, такі як переповнення буфера і XSS, менш релевантні до мобільних додатків, ніж до десктопних і веб-додатків.

Не дивлячись на прийняття ряду заходів законодавчого характеру, комп'ютерна злочинність зростає. Недбале ставлення до безпеки інформаційних систем приводе до відповідних наслідків. Наприклад, зловмисники можуть пошкодити вебсайт компанії, розмістивши неправдиву інформацію, що призведе до руйнування репутації компанії, яка будувалась багато років, втрати довіри клієнтів і партнерів, втрати доходу і порушення бізнес-процесів. Це також може призвести до витоку конфіденційних документів, розкриття комерційних таємниць та викрадення інтелектуальної власності.

Рис. 1.4. Наслідки порушення безпеки ІТС

Джерело: URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

Тому в сучасних умовах відбуваються суттєві зміни в поглядах на безпеку ІТС. На великих підприємствах створюють спеціальні служби з чималим бюджетом, в завдання яких входить виявлення, локалізація і усунення загроз кібербезпеки підприємства. Вони використовують спеціальне дороге програмне і апаратне забезпечення, що потребує особливої підготовка персоналу для роботи з ним.

Рис. 1.5. Центральний офіс підрозділу кібербезпеки компанії

Джерело: URL: https://www.kas.de/documents/270026/4625039/UA+Ukraine+-+EU+-+NATO+cooperation+to+counter+hybrid+threats+in+cyber+sphere.pdf/c970b17f-d9db-aba3-7990-bb4441a3e041?version=1.0&t=1554283399244

У той же час на малих підприємствах, які мають досить скромний IT-бюджет проблеми кібербезпеки залишаються досить актуальними.

1.2. Класифікація та властивості інформації

Інформація становить певну цінність, незалежно від того, чи є вона власністю держави, всього суспільства або окремих організацій чи фізичних осіб. Тому вона потребує захисту від різних впливів, які можуть призвести до зниження її цінності, а відповідно і постає питання про безпеку інформації.

Однак не вся інформація має однакову цінність для компанії і було б неефективним витрачати однакові ресурси на захист різних типів інформації, що мають різний рівень цінності. Тому інформація повинна бути правильно класифікована відповідно до рівня збитку в разі її розголошення або недоступності. Результати класифікації інформації дозволять компанії визначити, які засоби захисту повинні застосовуватися для кожного класу, вирішити які завдання захисту інформації є найбільш пріоритетними.

Захист інформації коштує грошей, тому бажано витрачати ці кошти саме на ту інформацію, для якої це дійсно необхідно. Класифікація дозволяє забезпечити захист інформації найбільш ефективним (економічно) способом. Крім того класифікація інформації дозволяє показати необхідний для кожного типу інформації рівень захисту конфіденційності, цілісності та доступності.

Конфіденційність *(confidentiality)* – властивість інформації, яка полягає в тому, що інформація доступна тільки тим суб'єктам (користувачам, програмам, процесам), яким надано на те відповідні повноваження і захищена від несанкціонованого доступу.

Цілісність (integrity) – властивість інформації, що полягає в існуванні інформації в неспотвореному вигляді (незмінному по відношенню до деякого фіксованого її стану). Більш широкий термін – *достовірность* інформації, яка складається з *адекватності* (повноти і точності) і безпосередньо *цілісності* інформації, тобто її незмінності.

Доступність (availability) – означає, що повноважений суб'єкт може без особливих проблем отримати своєчасний доступ до інформації, або необхідного компонента системи з інформацією. Наприклад, коректно говорити про доступність ервера, сегмента мережі, служби електронної пошти тощо.

Рис. 1.6. Властивості інформації

Джерело: URL: https://svitppt.com.ua/informatika/ponyattya-informacii-ta-sposobi-ii-podannya.html

За режимом доступу до інформації її поділяють на ***відкриту інформацію*** і ***інформацію обмеженого доступу***.

Інформація з обмеженим доступом

У свою чергу інформація з обмеженим доступом поділяється на:

- *таємну;*
- *конфіденційну;*
- *службову.*

Конфіденційна інформація

До конфіденційної інформації відповідно до законодавства України відноситься наступна інформація:

- *службова таємниця* (лікарська, адвокатська, банківська, нотаріальна, таємниця страхування, таємниця суду і слідства, таємниця листування, телефонних переговорів, поштових відправлень, відомості про сутність винаходу, корисної моделі або промислового зразка до офіційної публікації (ноу-хау) і т.п.);

- *комерційна таємниця;*
- *персональні дані* (відомості про факти, події і обставини життя громадянина, що дозволяють ідентифікувати його особу).

Інші розподіли інформації

Деякі компанії використовують тільки два класи інформації, інші – більше.

Наприклад, комерційні організації часто використовують такі рівні:

- *конфіденційно (confidential);*
- *для внутрішнього використання (private);*
- *критична інформація (sensitive);*
- *відкрита інформація (public).*

Військові організації використовують інші рівні критичності:

- *цілком таємно (top secret);*
- *таємно (secret);*
- *конфіденційно (confidential);*
- *критична некласифікована інформація (sensitive but unclassified), некласифікована інформація (unclassified).*

Захист інформації

Як відкрита, а тим більше конфіденційна інформація потребують захисту.

Під **захистом інформації** розуміють **ДІЯЛЬНІСТЬ**, що дає змогу запобігти реалізації загроз порушення зазначених властивостей інформації або зменшити ймовірність їх реалізації, а також зменшити неприйнятні збитки від реалізованих загроз.

Зверніть увагу, що у визначенні перед іменником «збитки» стоїть прикметник «неприйнятні». Очевидно, застрахуватися від усіх видів збитків неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує розмір очікуваного збитку. Отже, з чимось доводиться миритися і захищатися слід тільки від того, з чим змиритися ніяк не можна. Поріг неприйнятності має матеріальне (грошове) вираження, а метою захисту інформації стає зменшення розмірів збитку до допустимих значень.

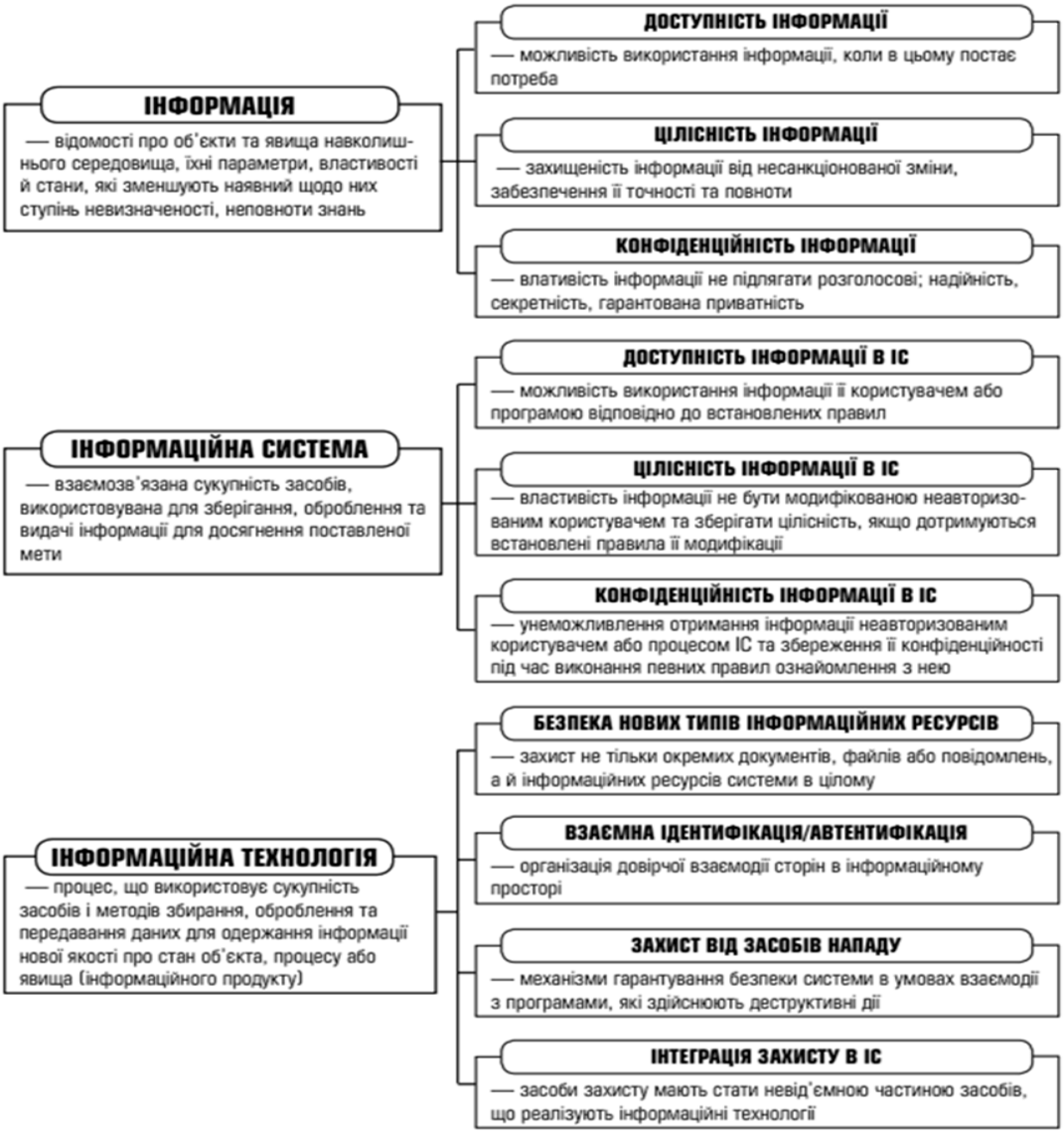


Рис. 1.7. Інформаційні системи та технології як об'єкти кібербезпеки

Джерело: URL: https://dut.edu.ua/uploads/p_303_79299367.pdf

1.3. Основні терміни і визначення безпеки ІТС

Ще кілька років тому терміни «безпека інформації» і «інформаційна безпека» були синонімічні і використовувались одночасно для визначення типових проблем.

На сьогодні під інформаційною безпекою розуміють захищеність суспільства й особистості від деструктивного інформаційного впливу (пропаганди, дезінформації, агресивної реклами, низькопробних видів мистецтва і т. п.), а також захищеність інформаційних прав і свобод людини.

Безпека інформації

Під **безпекою інформації** розуміють захищеність інформації від небажаного її розголошення (порушення конфіденційності), спотворення, або втрати (порушення цілісності), блокування інформації (порушення доступності), а також незаконного її тиражування (неправомірне використання).

Треба запам'ятати, що **безпека** – це *стан*, а **захист** – це *дія*.

Обробка інформації виконується за допомогою *інформаційних систем (ІС)*, тому при розгляді питань захисту інформації слід розглядати і необхідність забезпечення захисту і самих систем від несанкціонованого втручання в процес їх функціонування, а також від спроб розкрадання, незаконної модифікації і руйнування будь-яких компонентів цих систем.

При такому підході проблема захисту інформації є тільки частиною загальної проблеми забезпечення безпеки ІС, а поширений термін – «несанкціонований доступ до інформації» (НСД) було б правильніше трактувати як «несанкціоновані (неправомірні) дії», що порушують безпеку ІС.

Що ж таке безпека інформаційних систем (ІС)?

Часто говорять, що безпека – це відсутність небезпек. Проте це не зовсім правильно, оскільки повністю усунути всі можливі небезпеки не можна. Безпека – це захищеність від небезпек.

Безпека інформаційних систем – захищеність ІС від несанкціонованого втручання в нормальний процес її функціонування, а також від спроб розкрадання, незаконної модифікації або руйнування її компонентів (технічних засобів, ПЗ, даних). З об'єднанням комп'ютерів у мережі, які досягли глобального масштабу, виникли і набули поширення розподілені інформаційні системи.

Використання різноманітних телекомунікаційних мереж для об'єднання розподілених інформаційних систем призвели до нового поняття – інформаційно-телекомунікаційна система.

Інформаційно-телекомунікаційною системою (ІТС) називають складну систему, що виконує функції інформаційної системи, реалізуючи певну технологію (або сукупність технологій) оброблення інформації, та телекомунікаційної системи, що реалізує певну технологію (або сукупність технологій) передавання даних.

ІТС – це технологічна система, що поєднує інформаційну систему, мережеве обладнання та різноманітні мережі передачі інформації.

Треба зазичити, що загальноприйнятим терміном в Україні в галузі захисту інформації до поточного часу є «інформаційно-телекомунікаційні системи», саме він переважно використовується у законодавстві України щодо захисту інформації.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»: інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інші терміни, такі як «інформаційна і комунікаційна система», «інформаційно-комунікаційна система», «автоматизована система» використовують як синоніми ІТС.

Склад ІТС

ІТС складається:

1. Серверне обладнання.
2. Активне мережеве обладнання й обладнання зв'язку (комутатори, маршрутизатори, модеми, бездротові точки доступу, телефонія), а також пристрої захисту (міжмережеві екрани, системи виявлення та попередження вторгнень тощо).
3. Автоматизовані робочі місця співробітників (стаціонарні комп'ютери, ноутбуки, мобільні пристрої).
4. Середовище передачі даних (оптоволоконні лінії, кабелі бездротові канали передачі даних (Wi-Fi, Wi-Max, Bluetooth).

Безпека ІТС

Враховуючи, що безперебійну роботу ІТС забезпечує підтримуюча інфраструктура (системи електро-, водо- і теплопостачання, кондиціонери), яка вважається складовою частиною ІТС, то під ***безпекою ІТС*** **ми будемо розуміти** ***захищеність інформації, комп'ютерних систем, мереж і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку.***

Порушники можуть впливати на ІТС на будь-якому з перерахованих компонентів. Кожному з них притаманні характерні вразливості, а відтак – різні засоби захисту. Напрями, засоби, способи та методи забезпечення безпеки ІТС і є головним при вивчені цієї дисципліни.

ГЛАВА 2
Кібербезпека – складова частина безпеки ІТС

2.1. Кіберпростір і кібербезпека
2.2. Ключові питання кібербезпеки
2.3. Кіберзброя, кібертероризм і кібервійни

2.1. Кіберпростір і кібербезпека

В останні роки з’явися новий термін, щодо безпеки ІТС, а саме – кібербезпека. Поява такого терміна пов’язана з прийняттям нового явища в суспільстві, яке отримало назву – *кібернетичний простір*, або *кіберпростір*.

Відповідно до міжнародного стандарту ***кіберпростір*** – *це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж.*

Кіберпростір – це середовище, якого не існує в будь-якій фізичній формі. В сформованому ІТС кіберпросторі відбуваються процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, поданої у вигляді електронних комп'ютерних даних.

Законом України визначено, що **кіберпростір** – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Тобто в Україні кіберпростір розглядається як сфера діяльності складних соціотехнічних систем.

В кіберпросторі, як і в інших сферах, можливе вчинення заздалегідь спланованих деструктивних дій на кшталт проникнення в ІТС один одного, блокування або виведення з ладу найбільш вразливих елементів цих систем, дезорганізація автоматизованих систем управління транспортом і енергетикою, економікою й фінансовою системою тощо. Тому кіберпростір також потребує захисту від таких дій. А організація захисту базується на виконанні принципів кібербезпеки.

Згідно зі Словником DOD Dictionary of Military and Associated Terms. As of January 2019

Згідно зі Словником DOD Dictionary of Military and Associated Terms. As of January 2019 (URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs /dictionary.pdf), виданого в січні 2019 року ***кібербезпека*** *(безпека кіберпростору) – це дії, вжиті в захищеному кіберпросторі для запобігання несанкціонованому доступу, експлуатації або пошкодженню комп'ютерів, електронних систем зв'язку та інших інформаційних технологій, включаючи інформаційні технології платформи, а також інформацію, що міститься в ній, для забезпечення її доступності, цілісності, аутентифікації, конфіденційності і неспростовності.*

Згідно з українським законодавством

Українське ж законодавство комплекс цих заходів однозначно визначає як – технічний захист інформації (ТЗІ) (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» ***кібербезпека*** *– це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.* (Закон України № 2163-VIII від 5 жовтня 2017 року) URL: https://zakon.rada.gov.ua/laws/show/2163-19.

Тобто іноземні фахівці розглядають кібербезпеку як комплекс заходів та засобів захисту складних технічних систем, у той час як в Україні кібербезпека визначається як стан захищеності людини, громадянина, а також складних соціотехнічних систем. За останні три роки базова термінологія в сфері кібербезпеки в США змінилася на 25–30 %, що свідчить про гнучкість термінологічної системи.

Поєднуючи ці підходи до визначення кібербезпеки, можна сформулювати поняття кібербезпеки, як складової частини безпеки ІТС, таким чином.

> ***Кібербезпека*** – це стан захищеності кіберпростору в цілому або окремих об'єктів від ризику стороннього кібервпливу, за якого забезпечується своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і національним інтересам.

Як складова безпеки ІТС, *кібербезпека* – це перш за все безпека комп'ютерного та телекомунікаційного обладнання та його програмного забезпечення, цифрових даних і мереж, по яких ці дані передаються.

Виходячи с цього виникає питання визначення відношень між категоріями інформаційна безпека, комп'ютерна безпека, інтернет-безпека, та «кібербезпека». На жаль багатьма і сьогодні це сприймається як синонімічний ряд. Але ж в самих визначеннях наведених тут категорій продемонстровані суттєві розбіжності також і в сфері їх застосування.

Нагадаємо, що під *інформаційною безпекою* розуміють захищеність суспільства і особистості від деструктивного інформаційного впливу (пропаганди, дезінформації, агресивної реклами, низькопробних видів мистецтва і т.п.), а також захищеність інформаційних прав та свобод людини. Виходячи з цього визначення фахівець з інформаційної безпеки може мати іншу освіту, інший практичний досвід, інші напрями своєї діяльності. Більш того, фахівець з інформаційної безпеки може навіть не розумітися в інформаційних технологіях (ІТ) так, як фахівець з кібербезпеки.

Сертифікати спеціалістів із кібербезпеки

Навіть сертифікати спеціалістів з кібербезпеки відрізняються від сертифікатів фахівців з інформаційної безпеки:

- CEH (Certified Ethical Hacker);
- CISSP (Certified Information System Security Professional);
- CISA (Certified Information Systems Auditor);
- CCSP (Cisco Certified Security Professional);
- SSCP (Сертифікований спеціаліст з системної безпеки);
- OSCP (Offensive Security Certified Professional).

► **Certified Information Systems Security Professional (CISSP)** is an advanced security credential that demonstrates the technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage information security programs. This is the cybersecurity certificate most requested in advanced security roles.

► **Certified Information Systems Auditor (CISA)** demonstrates audit experience, skills, and knowledge, as well as the ability to assess vulnerabilities, report on compliance, and institute controls within an enterprise. This is the cybersecurity certificate most requested in cyber security auditor roles.

► **Certified Ethical Hacker (CEH)** is a theory based penetration testing and ethical hacking certification, requiring holders to understand attack methodologies and tools. Knowledge is assessed by answering multiple choice questions regarding various ethical hacking techniques and tools. This is the cybersecurity certificate most requested in junior penetration testing roles and general security roles.

► **Offensive Security Certified Professional (OSCP)** is a hands-on penetration testing and ethical hacking certification, requiring holders to successfully attack and penetrate various live machines in a safe lab environment. It is considered more technical than other ethical hacking certifications, and is one of the few certifications that require evidence of practical penetration testing skills. This is the cyber-security certificate most requested in penetration testing roles.

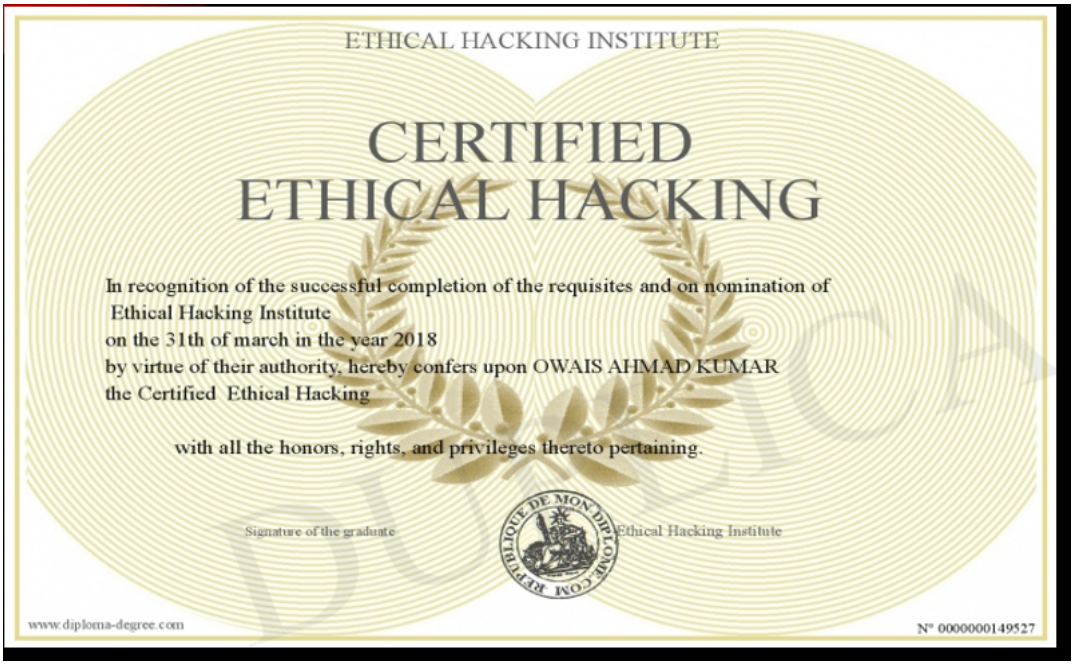


Рис. 2.1. Сертифікат етичного хакера

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Відповідність сертифіката і рівня підготовки фахівця з питань кібербезпеки наведено на рис. 2.2.

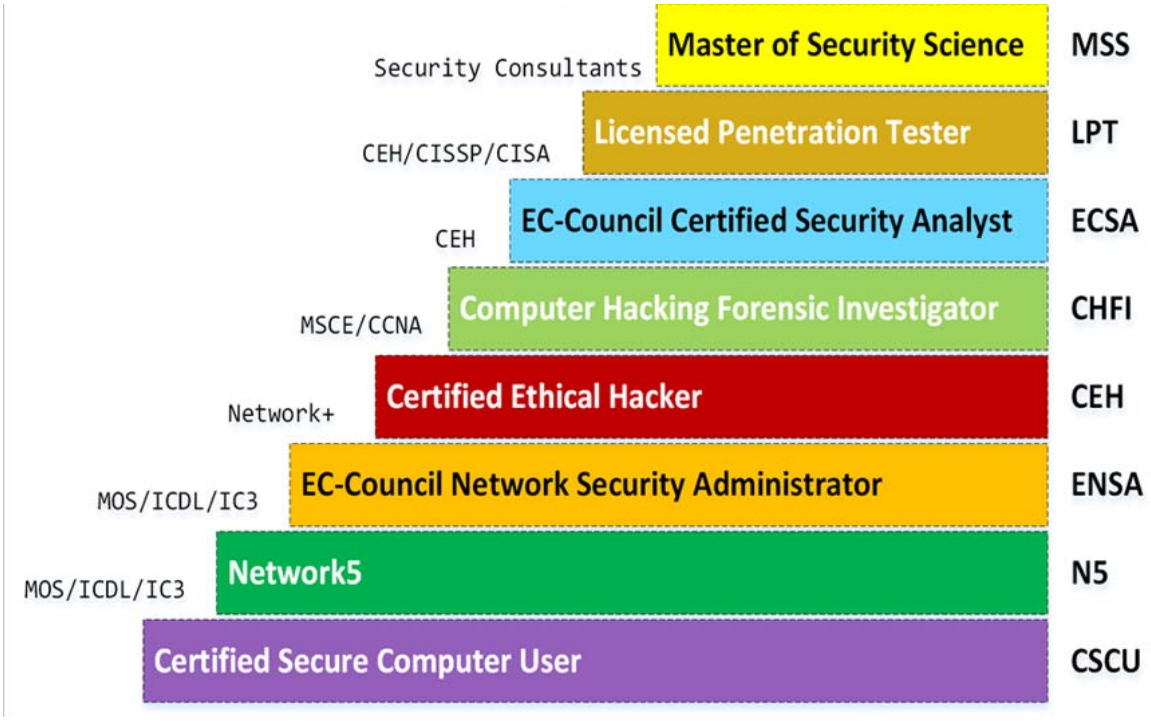


Рис. 2.2. Ступені майстерності фахівця з кібербезпеки

Джерело: URL: https://edu-cisco.org/courses/cybersecurity-essentials/

Повертаючись до питань визначень та термінології, слід зауважити, що термін *«комп'ютерна безпека»* також не є еквівалентом кібербезпеки, тому що комп'ютери – тільки одна з складових інформаційно-телекомунікаційних систем, і хоча інформація, яка зберігається, обробляється і передається за допомогою комп'ютерів, загалом безпека інформаційно-телекомунікаційних систем визначається всією сукупністю складових (комп'ютери, мережі і мережеве обладнання, підтримуюча інфраструктура, персонал тощо). З наведеного аналізу також зрозуміло, що і такий термін як «*інтернет-безпека»* є лише складовою частиною кібербезпеки.

Таким чином, необхідно чітко розуміти суттєві розбіжності в визначеннях кібербезпеки, використовувати правильні терміни і підтримувати тезаурус кібербезпеки.

2.2. Ключові питання кібербезпеки

Системна основа забезпечення безпеки ІТС зводиться в більшості випадків до відповіді на такі ключові питання:

- ▲ *Чи треба захищатися і що слід захищати?*
- ▲ *Від кого треба захищатися?*
- ▲ *Від чого треба захищатися?*
- ▲ *Як треба захищатися?*
- ▲ *Що забезпечить ефективність захисту?*
- ▲ *У що обійдеться розробка, впровадження, експлуатація та супровід систем захисту?*

Чи треба захищатися і що слід захищати?

Відповідь на це питання неоднозначна – багато що залежить від структури, області діяльності і цілей організації.

Для одних першочерговим завданням є запобігання витоку інформації до конкурентів (маркетингових планів, перспективних розробок, величини і розподілу прибутку та ін.). Інші можуть знехтувати конфіденційністю своєї інформації і зосередити свою увагу на її цілісності (наприклад, для організацій, що мають відкриті вебсервери).

Для провайдера Internet-послуг, оператора зв'язку або загальнодоступного довідкового сервера (google) на перше місце постає питання забезпечення максимальної доступності та безвідмовної роботи.

У режимних державних організаціях підхід такий – «нехай краще все зламається, ніж ворог дізнається хоч один секретний біт», а в навчальних закладах – «так нема у нас ніяких секретів, аби все працювало».

Розставити пріоритети і визначити необхідність і об'єкти захисту можна тільки в результаті аналізу діяльності організації.

Від кого треба захищатися?

В абсолютній більшості випадків відповіддю на це питання є фраза: «Як від кого – звичайно, від хакерів!». Дослідження показали, на думку більшості людей, що не займаються

кіберзахистом, основна небезпека виходить від зовнішніх зловмисників, які проникають в комп'ютерні системи банків і корпорацій, перехоплюють управління бізнес-процесами, «зламують» сайти, запускають «троянів» та ін.

Така небезпека існує і не можна її недооцінювати. У системах захисту обов'язково повинні бути відповідні модулі захисту від зовнішніх загроз подібного роду. Але ця небезпека часто перебільшена. Переважна більшість системних адміністраторів, тобто тих фахівців, які повсякденно підтримують нормальне функціонування системи, скажуть, що найбільша загроза виходить від легальних користувачів.

Інсайдерські загрози, що походять від діючих або звільнених співробітниками компанії почали випереджати загрози від шкідливих програм як за кількістю інцидентів, так і за обсягом завданої шкоди.

Потенційні можливості легального користувача в ІТС набагато більші, ніж у будь-якого зовнішнього порушника. Користувач має в системі певні повноваження. Він володіє інформацією про систему, а іншу інформацію може порівняно легко отримати (когось спитати, дещо підслухати, з кимось «неформально» поспілкуватися, десь підібрати якісь записи – йому це легше зробити, ніж будь-якій сторонній особі).

У публікаціях достатньо прикладів, коли співробітник компанії, вважаючи, що його на роботі не цінують, здійснює злочин, використовуючи ІТС компанії, що призводить до багатомільйонних збитків. Нерідкі випадки, коли після звільнення колишній співробітник компанії протягом довгого часу користується доступом у мережу корпорації. При звільненні цього співробітника ніхто із керівництва не подумав про необхідність скасування його пароля на доступ до даних і ресурсів, з якими він працював у рамках своїх службових обов'язків.

Однак найбільша небезпека може виходити не просто від звільнених або скривджених рядових співробітників, а від тих, хто наділений великими повноваженнями і має доступ до широкого спектра самої різної інформації. Зазвичай це спів-

робітники IT-відділів (аналітики, розробники, системні адміністратори), які знають паролі до всіх систем, що використовуються в організації. Їх кваліфікація, знання і досвід, які використовуються на шкоду, можуть призвести до дуже великих проблем. Крім того, таких зловмисників дуже важко виявити, оскільки вони володіють достатніми знаннями про систему захисту ІТС компанії, щоб обійти використовувані захисні механізми і при цьому залишитися «невидимими».

При побудові системи захисту необхідно захищатися не тільки і не стільки від зовнішніх зловмисників, скільки від зловмисників внутрішніх.

Від чого треба захищатися?

По-перше, це віруси і всілякі види непотрібної інформації, що розсилається абонентам електронної пошти (*Spam*).

Наступним поширеним типом небезпеки є ті дії, що спрямовані на виведення з ладу того чи іншого вузла мережі. Виведення з ладу вузла мережі на кілька годин може призвести до дуже серйозних наслідків. Наприклад, виведення з ладу сервера трансакційної системи банку призведе до неможливості здійснення платежів і, як наслідок, до великих прямих і непрямих фінансових і рейтингових втрат.

Ще одне істотне джерело загроз, яке з точки зору розміру шкоди може бути віднесене до одного з найбільш поширених – ненавмисні помилки користувачів ІТС, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. Статистика показує, що 65 % втрат наслідок ненавмисних помилок через комп'ютерну неграмотність і безвідповідальність співробітників і користувачів ІТС. Вочевидь, найрадикальніший спосіб боротьби з ненавмисними помилками – максимальна автоматизація інформаційних процесів, впровадження системи програмного та технічного «захисту від дурня» (*Fool Proof*), ефективне навчання персоналу і строгий процедурний контроль правильності їх дій.

Приклад системи контролю за витоком інформації: ***DLP – системи****, що призначені для моніторингу за інформацією, що пересилається і зберігається і здатні відстежувати кожен клік співробітника в офісі, такі системи призначені не для захисту від зловмисників, а саме від ненавмисних дій співробітників компанії.*

Як треба захищатися?

Сьогодні захист інформації – одне з головних завдань будь-якого бізнесу. Майже кожна компанія володіє торговими або промисловими секретами, приватними відомостями своїх співробітників, клієнтів і партнерів, а в деяких випадках інтелектуальною власністю та іншими цифровими активами. Щоб захистити всю цю інформацію найбільш простий спосіб – купити новітні рекламовані засоби захисту, встановити у себе в організації, не обтяжуючи себе обґрунтуванням їх корисності та ефективності. Якщо компанія багата, то вона може дозволити собі цей шлях.

Проте цей шлях не продуктивний, з точки зору затрат на захист і не ефективний з точки зору вирішення проблем захисту ІТС. Сучасний підхід передбачає побудову комплексної системи захисту ІТС в кілька етапів.

Перший етап – інформаційне обстеження підприємства. Саме на цьому етапі визначається, від чого, в першу чергу, необхідно захищатися. Спочатку будується так звана модель порушника, яка описує ймовірний вигляд зловмисника: його кваліфікацію, наявні кошти для реалізації тих чи інших атак, звичайний час дії і т.п. На цьому ж етапі виявляються і аналізуються вразливі місця і можливі шляхи реалізації загроз безпеки, оцінюється ймовірність атак і збиток від їх здійснення. За результатами етапу інформаційного обстеження виробляються рекомендації щодо усунення виявлених загроз, правильному вибору і застосування засобів захисту.

Наступним етапом побудови комплексної системи безпеки слугує придбання, встановлення та налаштування рекомендованих на попередньому етапі засобів і механізмів захисту.

У що обійдеться розробка, впровадження, експлуатація та супровід систем захисту?

При цьому необхідно враховувати, що придбання обладнання для захисту інформації зазвичай обходиться дорожче, ніж отримання обладнання такого ж рівня для несанкціонованого доступу. Це пов'язано з тим, що зловмисники використовують якийсь один спосіб несанкціонованого доступу, а забезпечувати захист треба від усіх можливих способів. Тому при організації захисту завжди визначається розумний компроміс між цінністю інформації та витратами на забезпечення її безпеки.

2.3. Кіберзброя, кібертероризм і кібервійни

За загальною думкою більшості фахівців з кібербезпеки, – настає час кібертероризму і кібервійни в кіберпросторі. Ілюстрацією цього є відомі приклади шкідливого програмного забезпечення – ***Stuxnet, Duqu, Flamer, Gauss***, які антивірусні компанії зараховують до кіберзброї.

Комп'ютерний хробак *Stuxnet*

Таблиця 2.1

Дослідження поширення Stuxnet (основними ураженими країнами в перші дні зараження були Іран, Індонезія та Індія)

Країна	Частка заражених комп'ютерів
Іран	*58,85 %*
Індонезія	*18,22 %*
Індія	*8,31 %*
Азербайджан	*2,57 %*
Сполучені Штати	*1,56 %*
Пакистан	*1,28 %*
Інші країни	*9,2 %*

Джерело: URL: https://sites.google.com/site/komputersvirus/home/5-hrobak-stuxnet

Комп'ютерний хробак ***Stuxnet*** був виявлений в промислових системах, керуючих автоматизованими виробничими процесами. Це перший відомий комп'ютерний хробак, який діє на рівні логічних контролерів і заражає не стільки програмне забезпечення, скільки апаратну основу системи, що значно ускладнює боротьбу з ним. ***Stuxnet*** завдав серйозної шкоди іранській ядерній програмі, вразивши 1368 з 5000 центрифуг на заводі зі збагачення урану в Натанзі, а також зірвав терміни запуску ядерної АЕС в Бушері. Замовник цієї атаки офіційно невідомий. Збиток, нанесений ядерним об'єктам Ірану, можна порівняти зі шкодою від атаки ізраїльських ВПС. ***Stuxnet*** визначив програми, які сигналізують співробітникам підприємства про стан центрифуг, і перекодував їх. Тепер працівники заводу вже не могли бачити, що відбувається з центрифугами насправді, – їм здавалося, що реактор працює ідеально. Одягнувши на операторів ці своєрідні «шори», вірус почав палити центрифуги: він то розганяв їх, то різко уповільнював, і обладнання виходило з ладу. Всього за десять місяців ***Stuxnet*** спалив таким чином від 1000 до 2000 центрифуг.

Stuxnet НЕ краде гроші, не шле спам і не краде конфіденційну інформацію. Цей код створений, щоб контролювати виробничі процеси, в буквальному сенсі керувати величезними виробничими потужностями. До певного часу ***Stuxnet*** ніяк себе не проявляє, але в заданий момент він може віддати команди, фізично виводять з ладу промислове обладнання.

Троян *Duqu*

Наступним інцидентом, який також можна класифікувати як епізод кібервійни, стало виявлення трояна ***Duqu***, метою якого було викрадення конфіденційної інформації з промислових об'єктів (кібершпіонаж). Таку дивну назву, *Duqu,* отримав завдяки розширенню створюваних ним файлів, – ***DQ***. Вперше це шкідливе ПЗ було виявлено в комп'ютерних системах європейських підприємств. Інформація, яку шукає

Duqu, стосується насамперед документів з описом IT-інфраструктури підприємства. Ймовірно, ці дані потрібні зловмисникам для здійснення подальших атак вже з метою встановлення контролю над різного типу промисловими системами. Як тільки хробак потрапляє в систему, відразу встановлюється кейлоггер, який записує всі дії користувача, а також відбувається пошук додаткової системної інформації. Хробак може копіювати список запущених у системі процесів, інформацію про аккаунт користувача, а також інформацію про домен. Робить він і скріншоти, записує мережеву інформацію, а також «досліджує» файли на всіх доступних дисках, включаючи знімні і мережеві. За даними компанії Symantec, хробак працює в системі 36 днів з моменту запуску, а потім самознищується.

Комп'ютерний вірус *Flame*

Таблиця 2.2

Список кодових імен для модулів вірусу у вихідному коді *Flame* і їх можливої мети

Flame	Модулі, які виконують функції атаки
Boost	*Модулі збору інформації*
Jimmy	*Атакуючий модуль*
Munch	*Модуль установки та поширення вірусу*
Snack	*Модуль місцевого поширення*
Spotter	*Модуль сканування*
Transport	*Модуль дублювання*
Euphoria	*Модуль збору даних*
Headache	*Модулі, які виконують функції атаки*

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Комп'ютерний вірус ***Flame*** складається з пакета модулів, який, будучи повністю розгорнутим, займає близько 20 МБ.

Основне завдання ***Flame –*** кібершпіонаж. Після свого впровадження в систему, ***Flame*** здатний проводити комплекс дій, наприклад перехоплення мережевого трафіку, зняття скріншотів, запис аудіорозмов, перехоплення клавіатури і т.п. Усі викрадені дані доступні для операторів через командні сервери. За командою з сервера ***Flame*** може повністю видалити сліди свого перебування на комп'ютері.

Кіберпростір став ще одним важливим аспектом війни, де країни можуть конфліктувати без зіткнення традиційних військ та техніки. Це дозволяє країнам з мінімальними військовими силами бути такими ж сильними, як і інші країни в кіберпросторі.

Кібервійна – це Інтернет-конфлікт, який передбачає проникнення у комп'ютерні системи та мережі інших країн. Нападники мають ресурси та спеціальні знання, щоб започатковувати масштабні інтернет-атаки проти інших країн, завдаючи збитків або порушуючи роботу сервісів, наприклад припинення роботи енергосистеми.

Основна мета *кібервійни* – отримати перевагу над супротивниками, незалежно від того, чи є вони державами або конкурентами. Кібервійна може дестабілізувати державу, зруйнувати торгівлю та впливати на довіру громадян у їхній уряд, навіть коли немає фізичного вторгнення в країну-жертву.

Свого часу глава АНБ, генерал Кіт Александер, виступаючи в Конгресі США, публічно заявив, що за останні кілька років загроза кібервійни зростає стрімкими темпами. Кіберпростір став новою зоною воєнних дій. «Точно так само, як сушу, море, повітряний та космічний простір, потрібно розглядати кіберпростір як сферу наших дій, яку ми будемо

захищати і на яку поширимо свою військову доктрину. Ось що спонукало нас створити об'єднане кіберкомандування в складі Стратегічного командування». Пентагон створив 40 груп (кілька тисяч цивільних осіб і військовослужбовців), які будуть займатися підготовкою можливих превентивних кібератак для захисту американських стратегічних інтересів.

На офіційному сайті Міністерства оборони США з'явилося повідомлення про заснування нової нагороди (***Distinguished Warfare Medal***). Цією медаллю нагороджуватимуть солдатів армії США, які беруть участь в кібервійні і проявили себе на службі. «Нова медаль є нашим визнанням видатних досягнень, які мали прямий вплив на хід подій, але не включають прояв мужності і не пов'язані з життєвим ризиком, які притаманні реальному бою. Поява нової нагороди говорить про зміни принципів військових дій», – пояснив міністр оборони США.

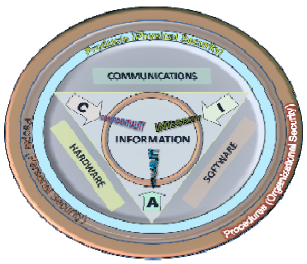
Для відстоювання своєї позиції і отримання цінної інформації організації та приватні особи все частіше вдаються до використання кіберзброї. Кіберпростір стає новою зоною конфліктів як між організаціями та окремими особами, так і між державами.

Контрольні запитання

1. Назвіть головні причини актуальності кібербезпеки.
2. Як класифікується інформація?
3. Які властивості інформації важливі з точку зору її безпеки?
4. У чому різниця між інформаційною безпекою і кібербезпекою?
5. Що таке безпека ІТС?
6. Назвіть основні ключові питання кібербезпеки.
7. Що відносять до кіберзброї?

Розділ 2. ВРАЗЛИВОСТІ ТА ЗАГРОЗИ ФУНКЦІОНУВАННЯ ІТС

ГЛАВА 3
ЗАГРОЗИ ІНФОРМАЦІЇ В ІТС



3.1. Загрози безпеки функціонування ІТС

Під час функціонування ІТС відбуваються різні події, що змінюють її стан.

Будь-яка непередбачена або небажана подія, яка може порушити діяльність ІТС називається *інцидентом безпеки системи.*

Прикладами інцидентів безпеки можуть бути:

- ❖ *втрата послуг, обладнання або пристроїв;*
- ❖ *системний збій або перевантаження;*

- *помилки користувачів;*
- *недотримання політик безпеки або рекомендацій;*
- *порушення фізичних заходів захисту;*
- *неконтрольовані зміни систем;*
- *збій програмного забезпечення і відмови технічних засобів;*
- *порушення правил доступу.*

Інциденти безпеки системи, викликані процесом або явищем, що можуть призвести до зміни функціонування як окремих програмних і апаратних засобів, так і ІТС в цілому, або призвести до нанесення іншої шкоди називають *ЗАГРОЗАМИ* безпеки для ІТС.

Безпека ІТС – це захищеність від можливого збитку, що наноситься системі.

Кінцевою метою забезпечення безпеки ІТС є її захист. Одним з найважливіших аспектів захисту ІТС є визначення, аналіз і класифікація можливих загроз безпеки. Мати уявлення про можливі загрози, а також про вразливі місця, які ці загрози зазвичай експлуатують, необхідно для того, щоб вибрати найбільш економічні засоби забезпечення безпеки. Перелік значущих загроз, оцінка ймовірностей їх реалізації, а також модель порушника слугує основою для формулювання вимог до системи захисту ІТС.

Загрозою безпеки ІТС називають потенційно можливу подію, викликану процесом або явищем, які за допомогою впливу на інформацію, її носії та процеси обробки можуть прямо або побічно призвести до зміни функціонування як окремих програмних і апаратних засобів, так і ІТС в цілому, або призвести до нанесення іншої шкоди.

До основних *загроз безпеки* інформації і безпечного функціонування ІТС відносяться:

- ❖ *витік конфіденційної інформації;*
- ❖ *несанкціоноване використання інформаційних ресурсів;*
- ❖ *помилкове використання інформаційних ресурсів;*
- ❖ *порушення інформаційного обслуговування;*
- ❖ *незаконне використання привілеїв.*

Витік конфіденційної інформації

Витік конфіденційної інформації – це безконтрольний вихід конфіденційної інформації за межі ІТС або кола осіб, яким вона була довірена.

Цей витік може бути наслідком:

- ❖ *розголошення конфіденційної інформації;*
- ❖ *розвідки;*
- ❖ *несанкціонованого доступу до інформації різними способами.*

Головні відмінності *розвідки* від *розголошення* полягають в тому, що інформацією, видобутої з допомогою розвідки, володіє обмежене коло осіб. Розвідка, як правило, ведеться з ворожими цілями, тоді як розголошення може таких цілей і не переслідувати. Розвідка завжди ведеться навмисно, а розголошення нерідко буває наслідком необачності особи–носія інформації.

Під несанкціонованим доступом (НСД) до інформації *розуміють дію, в результаті якої порушені правила розмежування доступу, і інформацією заволоділа особа, яка не має на те права.* Результатом НСД не обов'язково стає витік інформації. НСД може здійснюватися з метою активного впливу на інформацію, отримання незаконних привілеїв, задоволення амбіцій і т. п.

НСД може бути наслідком як умисних дій, так і ненавмисних (помилки в організації захисту інформації, недостатня кваліфікація персоналу і т. п.). Очевидно, що елементи НСД присутні і при веденні розвідки. У той же час розвідка може здійснюватися без несанкціонованого доступу до інформації та її носія (наприклад, шляхом збору відкритих відомостей).

Несанкціоноване використання інформаційних ресурсів

Несанкціоноване використання інформаційних ресурсів (несанкціонований доступ) – доступ до ІТС, що здійснюється з порушенням установлених правил.

Наслідком цих дій може бути:

- ***втрата інформації*** *– дія, внаслідок якої інформація в ІТС перестає існувати;*
- ***модифікація інформації*** *– навмисні дії, що призводять до змін інформації, яка має оброблятися або зберігатися в ІТС.*

Помилкове використання інформаційних ресурсів

Помилкове використання інформаційних ресурсів, будучи санкціонованим, також може призвести до руйнування, витоку або компрометації інформації. Дана загроза найчастіше і є наслідком помилок, наявних в ПЗ ІТС.

Порушення інформаційного обслуговування

Порушення інформаційного обслуговування – загроза, причиною якої може бути:

- ***блокування інформації*** *– дії, наслідком яких є припинення доступу до інформації (зловмисник не може сам скористатися інформацією, але має доступ до засобів її обробки і своїми (в тому числі несвідомими) діями перешкоджає законному власнику обробляти цю інформацію.*

Характерним прикладом є спамінг. Поштовий ящик власника виявляється забитий інформаційним сміттям, через якого той не може прийняти корисні повідомлення).

- ***порушення роботи ІТС*** *– дії або обставини, які призводять до спотворення процесу обробки інформації.*

Незаконне використання привілеїв

Більшість систем встановлюють певні набори привілеїв для виконання заданих функцій. Кожен користувач отримує свій набір привілеїв: звичайні користувачі – мінімальний, адміністратори – максимальний.

Несанкціоноване захоплення привілеїв, наприклад, за допомогою «маскараду», призводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або при наявності помилок в системі захисту, або через недбалість адміністратора при управлінні системою і призначення привілеїв.

3.2. Вразливості та вади захисту системи

З поняттям загрози безпеки тісно пов'язане поняття ***вразливості системи***.

Вразливість системи – нездатність системи протистояти певним впливам (випадковим або навмисним).

Причиною вразливості є відсутність або слабкість захисних заходів, недоліки в програмному забезпеченні, обладнанні або процедурі. Прикладом вразливих місць може бути слабка фізична безпека, яка дозволяє будь-кому увійти в серверну кімнату, відсутність управління паролями в системі, відкриті порти або запущена служба системи, що не використовуються в роботі, неоновлене ПЗ, в якому знайдені помилки.

Загальна кількість можливих вразливих місць в системі створює так звану *поверхню атак*.

Чим більше вразливих компонентів в системі, тим більше напрямів можливих впливів на систему, тим більша ***поверхня атак***.

Проміжок часу від моменту, коли з'являється можливість використовувати вразливе місце, і до моменту його ліквідації, називається *вікном небезпеки*, асоційованим з даними вразливим місцем.

Поки існує ***вікно небезпеки***, можливі успішні атаки на ІТС. Якщо мова йде про помилки в ПЗ, то вікно небезпеки «відкривається» з появою засобів використання помилки, а ліквідується – при накладенні латок, що її виправляють.

Класифікація вразливостей

У більш загальному вигляді вразливості можуть бути класифіковані по етапах життєвого циклу ІТС:

- *вразливості проєктування (проєктування);*
- *вразливості реалізації (реалізація);*
- *вразливості конфігурації (експлуатація).*

Вразливості проєктування

Вразливості проєктування найбільш серйозні – вони виявляються й усуваються з великими труднощами. В цьому випадку вразливість властива проєкту і, отже, навіть досконала реалізація алгоритму (що в принципі неможливо) не врятує від закладеної в ньому слабкості. Наприклад, вразливість стека протоколів TCP/IP. Недооцінка вимог з безпеки при створенні цього стека протоколів призвела до того, що не проходить і місяця, щоб не було оголошено про нову вразливість у протоколах стека TCP/IP. І усунути ці недоліки вже неможливо – існують тільки тимчасові або неповні заходи.

Вразливості реалізації

Вразливості реалізації полягають у появі помилки на етапі реалізації в програмному або апаратному забезпеченні коректного з точки зору безпеки проєкту або алгоритму. Яскравий приклад такої вразливості – ***«переповнення буфера»*** в багатьох реалізаціях програм, наприклад, *sendmail* або *Internet Explorer*. Виявляються і усуваються подібного роду вразливості відносно легко. Якщо немає вихідного коду програмного забезпечення, в якому знайдена вразливість, то її усунення полягає або в оновленні версії ПЗ, або в повній його заміні, або відмові від нього.

Вразливості конфігурації

Вразливості конфігурації полягають у помилках при конфігурації програмного або апаратного забезпечення. Ці

вразливості можуть бути також наслідком помилок, допущених в процесі експлуатації інформаційної системи, зокрема, до них можна віднести:

- *використання конфігурацій «за замовчуванням»* (облікові записи і паролі, встановлені за замовчуванням (Administrator, SYSADM), і т. д.)*;*
- *некоректно задані параметри захисних механізмів* (дозвіл «слабких» паролів або паролів довжиною менше 6 символів)*;*
- *невикористовувані мережеві сервіси, що доступні віддалено* (доступний сервіс Telnet).

▲ ***Common Vulnerabilities and Exposures.***

Проєкт CVE (http://cve.mitre.org), запущений в 1999 р, в даний час фактично став промисловим стандартом для позначення вразливостей. Запис про вразливість в каталозі CVE містить унікальний індекс, короткий опис вразливості і посилання на джерела, де можна отримати більш детальну інформацію. Позначення вразливості включає в себе префікс ~ cvE ~, рік виявлення і унікальний номер, наприклад CVE-2018-4250. Ця інформація про вразливість допомагає лише в загальних рисах зрозуміти, про що йде мова, а для отримання більш детальної інформації можна скористатися наведеними в цьому описі посиланнями.

 Деякі загрози не можна вважати наслідком якихось помилок або прорахунків, вони існують в силу самої природи сучасних ІТС. Наприклад, загроза відключення електрики існує в силу залежності апаратного забезпечення ІТС від якісного електроживлення. Загроза втрати інформації через збій в мережі електроживлення реалізується, якщо в ІТС не застосовуються джерела безперебійного живлення або засоби резервного електропостачання (це є вада захисту).

Вади захисту

Вади захисту – сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи.

Здебільшого під ***вадами захисту*** розуміють особливості побудови програмних (а іноді й апаратних) засобів захисту, що за певних обставин спричиняють їхню нездатність протистояти загрозам і виконувати свої функції. Тобто вади захисту є окремим випадком вразливості системи. Вади захисту можуть бути внесені в систему навмисно чи випадково.

Вади захисту, що вносять у систему ненавмисно, – це помилки, яких припускаються розробники програмного забезпечення під час його проєктування, реалізації, впровадження або супроводження.

Причинами появи таких вад захисту, окрім помилок самих програмістів, є використання фрагментів уже готового коду (стандартних бібліотек). Наприклад, найтиповіші помилки переповнення буфера, які надають зловмисникам можливість виконувати довільні команди на комп'ютері, як правило, виникають або внаслідок використання програмістами бібліотечних функцій з такою вадою, або через те, що ці функції викликаються іншими бібліотечними функціями, про що програмісти можуть не здогадуватися.

До вад захисту, що вносять у систему навмисно, належать програмні закладки – фрагменти коду, що виконує недокументовані функції, які здатні послабити захист системи.

Найчастіше програмісти за допомогою закладок створюють так звані люки, з метою спрощення процедур тестування і налагодження програми, а інколи і задля того, щоб у подальшому можна було скористатися ресурсами системи. Іноді вони вносять нешкідливі програмні закладки, які за виконання певних умов демонструють, наприклад, інформацію про розробників («Пасхальні яйця»). Але є й такі програмні закладки, які здійснюють шпигунську місію, приховано надсилаючи з системи конфіденційну інформацію.

3.3. Класифікація загроз безпеки

Носіями загроз безпеки є джерела загроз. Усі джерела загроз можна розділити на три групи:

- *обумовлені діями суб'єкта (антропогенні джерела загроз);*
- *обумовлені технічними засобами (техногенні джерела загроз);*
- *обумовлені природними джерелами (аварійні ситуації, стихійні лиха).*

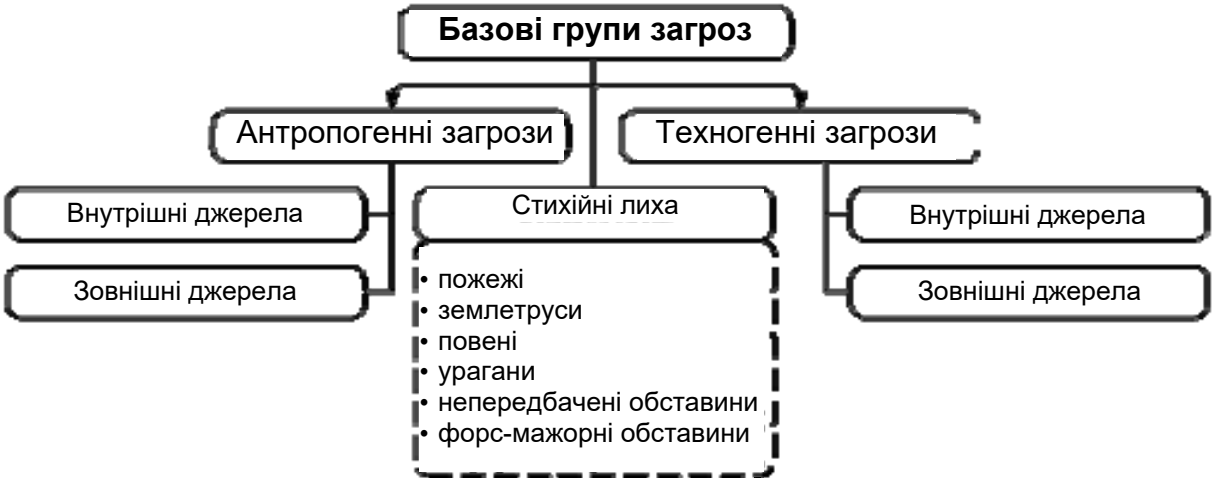


Рис. 3.1. Базові групи загроз

Джерело: URL: https://pidru4niki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi

Загрози можна класифікувати за кількома критеріями:

▲*за способом здійснення* (навмисні, випадкові, штучні, природні);

Рис. 3.2. Загрози за способом здійснення

Джерело: URL: https://sites.google.com/site/informacijnabezpeka15/zagrozi-informacijnij-bezpeci/klasifikacia-zagroz-informacijnij-bezpeci

▲*за розташуванням джерела загроз* (внутрішні, зовнішні);

▲*за складовими безпеки інформації, проти яких спрямовані загрози в першу чергу* (доступність, цілісність, конфіденційність);

▲*за компонентами інформаційних систем і технологій, на які загрози безпосередньо націлені* (дані, програмно-апаратні комплекси, мережі, інфраструктура).

Таблиця 3.1

Класифікація загроз за ознаками

Ознака класифікації	Причини, спрямованість, характеристики загроз
Природа виникнення	*Природні загрози (виникають через впливи на АС та її компоненти об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини)*

Продовження табл. 3.1

Ознака класифікації	Причини, спрямованість, характеристики загроз
Принцип несанкціонованого доступу (НСД)	*Фізичний доступ:* • *подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів;* • *розкрадання документів і носіїв інформації;* • *візуальне перехоплення інформації, виведеної на екрани моніторів і принтери;* • *підслуховування;* • *перехоплення електромагнітних випромінювань:* *Логічний доступ (доступ із використанням засобів комп'ютерної системи)*
Мета несанкціонованого доступу (НСД)	*Порушення конфіденційності (розкриття інформації).* *Порушення цілісності (повне або часткове знищення інформації, спотворення, фальсифікація, викривлення).* *Порушення доступності (наслідок – відмова в обслуговуванні)*
Причини появи вразливостей різних типів	*Недоліки політики безпеки.* *Помилки адміністративного керування.* *Недоліки алгоритмів захисту.* *Помилки реалізації алгоритмів захисту*
Характер впливу	*Активний (внесення змін в АС).* *Пасивний (спостереження)*
Режим несанкціонованого доступу (НСД)	*За постійної участі людини (в інтерактивному режимі) можливе застосування стандартного ПЗ.* *Без особистої участі людини (у пакетному режимі) найчастіше для цього застосовують спеціалізоване ПЗ*

Закінчення табл. 3.1

Ознака класифікації	Причини, спрямованість, характеристики загроз
Місцезнаходження джерела несанкціонованого доступу (НСД)	*Внутрішньосегментне (джерело знаходиться в локальній мережі). У цьому випадку, як правило, ініціатор атаки – санкціонований користувач.* *Міжсегментне:* • *несанкціоноване вторгнення з відкритої мережі в закриту;* • *порушення обмежень доступу з одного сегмента закритої мережі в інший*
Наявність зворотнього зв'язку	*Зі зворотним зв'язком (атакуючий отримує відповідь системи на його вплив).* *Без зворотного зв'язку (атакуючий не отримує відповіді)*
Рівень моделі взаємодії відкритих систем OSI (Open Systems Interconnection)	*Вплив може бути здійснено на таких рівнях: фізичному, канальному, мережевому, транспортному, сеансовому, представницькому, прикладному рівнях, тобто на всіх рівнях моделі OSI*

Джерело: URL: https://uadoc.zavantag.com/text/2674/index-1.html?page=10

Класифікація за способом здійснення

Загрози, спричинені людською діяльністю:

➔ ***штучні загрози;***

➔ ***ненавмисні (випадкові) –*** це більш небезпечні;

➔ ***навмисні.***

До ***ненавмисних (випадкових)*** загроз відносяться:

➢ ***помилки в проєктуванні ІТС і в розробці програмних засобів ІТС;***

- ***випадкові збої в роботі апаратних засобів ІТС та ліній зв'язку (збої роботи серверів, робочих станцій, мережевих карт, устаткування і електроживлення);***
- ***помилки користувачів ІТС;***
- ***вплив на апаратні засоби ІТС фізичних полів інших пристроїв.***

Ненавмисні помилки штатних користувачів (неправильно введені дані, помилки адміністрування або помилка в програмі, що викликала крах системи) є найчастішими й найнебезпечнішим.

Навмисні загрози розглянемо в подальшому більш детально.

Класифікація за складовими безпеки інформації

Загрози поділяються відповідно на :

- *загрози доступності;*
- *загрози цілісності;*
- *загрози конфіденційності.*

Загрози доступності

Загрози доступності класифікуємо по компонентах ІТС, на які націлені загрози:

▼ відмова користувачів:

- ✓ неможливість працювати із системою внаслідок відсутності відповідної підготовки (недолік загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією тощо);
- ✓ неможливість працювати із системою в наслідок відсутності технічної підтримки (неповнота документації, недолік довідкової інформації тощо).

▼ відмова інформаційної системи:

- ✓ некоректні дії користувачів або обслуговуючого персоналу;
- ✓ відмови компонентів програмного або апаратного забезпечення;
- ✓ руйнування даних або ушкодження апаратури.

▼ відмова підтримуючої інфраструктури:

- ✓ порушення роботи систем зв'язку;
- ✓ електроживлення;
- ✓ водо- і теплопостачання, кондиціювання).

Наприклад, короткочасні імпульси напруги призводять до вигоряння устаткування, вихід з ладу систем кондиціювання к зупинці роботи серверів, а прорив труб водо- чи теплопостачання к непередбаченим наслідкам, а не тільки доступності системи.

Загрози цілісності

Загрози порушення цілісності інформації, що зберігається в ІТС чи передається по каналу зв'язку, спрямовані на її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена навмисно зловмисником, а також у результаті об'єктивних впливів з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації – комп'ютерних мереж і систем телекомунікацій. Потенційно вразливі з точки зору порушення цілісності не тільки дані, а й програми, тому впровадження шкідливого ПЗ також є прикладом загроз цілісності.

Загрози конфіденційності

Загрози конфіденційності пов'язані з можливими каналами витоку інформації і несанкціонованим використанням ресурсів ІТС. Даний вид загроз пов'язаний з розголошення інформації, що є комерційною таємницею, за допомогою

відсилання її по електронній пошті, через Інтернет (чат, форум і т.д.), за допомогою засобів обміну миттєвими повідомленнями, шляхом копіювання інформації на переносні носії або роздрукування даних. Для виявлення факту розголошення конфіденційної інформації різні компанії пропонують перехоплення поштового, внутрішньомережевого (на рівні TCP/IP) і вебтрафіку (протоколи HTTP, FTP, IM і т.д.) з подальшим аналізом різними методами фільтрації, в тому числі за допомогою аналізу контенту.

Рис. 3.3. Ознаки загроз конфіденційності, цілісності та доступності інформації

Джерело: URL: http://mishchenkoanna2015.blogspot.com/2017/11/blog-post.html

Класифікація за компонентами ІТС

У загальному випадку система обробки і передачі інформації в ІТС складається з таких основних структурно-функціональних елементів:

- *робочих станцій* – окремих ЕОМ або терміналів мережі, на яких реалізуються автоматизовані робочі місця користувачів (абонентів, операторів);
- *серверів,* призначених для реалізації функцій зберігання, друку даних, обслуговування робочих станцій мережі та подібних дій;

- *мережевих пристроїв* (маршрутизаторів, комутаторів, шлюзів, центрів комутації пакетів, комунікаційних ЕОМ) – елементів, які забезпечують з'єднання декількох мереж передачі даних, або декількох сегментів однієї і тієї ж мережі, можливо мають різні протоколи взаємодії;
- *каналів зв'язку.*

Робочі станції є найбільш доступними компонентами мереж, саме з них можуть бути зроблені найбільш численні спроби скоєння несанкціонованих дій. З ***робочих станцій*** здійснюється управління процесами обробки інформації, запуск програм, введення і коригування даних. Саме на ***робочих станціях*** здійснюється введення імен і паролів користувачами. Тому ***робочі станції*** повинні бути надійно захищені від доступу сторонніх осіб і повинні містити засоби розмежування доступу до ресурсів з боку законних користувачів, що мають різні повноваження. Крім того, засоби захисту повинні запобігати порушенням конфігурації робочих станцій і режимів їх функціонування, викликані ненавмисним втручанням недосвідчених (неуважних) користувачів.

Особливого захисту потребують такі привабливі для зловмисників елементи мереж, як ***сервери*** *і* ***мережеві пристрої.*** Перші – як концентратори великих обсягів інформації, другі – як елементи, в яких здійснюється перетворення даних при узгодженні протоколів обміну в різних ділянках мережі. Сприятливими, для підвищення безпеки цих пристроїв, обставинами є наявність можливостей їх надійного захисту фізичними засобами і організаційними заходами. Тут головне скоротити до мінімуму число осіб з персоналу, що мають безпосередній доступ до них. Іншими словами, безпосередньо випадковий вплив персоналу і навмисні локальні дії зловмисників на виділені сервери і мережеве устаткування можна вважати практично неможливим.

У той же час все більше поширеними стають масовані загрози на ***сервери*** та ***робочі станції*** з використанням

засобів віддаленого доступу. Тут зловмисники використовують недоліки протоколів обміну і засобів розмежування віддаленого доступу до ресурсів.

Канали зв'язку також потребують захисту. З огляду на велику протяжність ліній зв'язку (через неконтрольовану або слабо контрольовану територію) практично завжди існує можливість підключення до них з пасивним прослуховуванням, або з втручанням в процес передачі даних.

3.4. Основні навмисні загрози

Навмисні загрози – це цілеспрямовані дії зловмисника.

Цей клас загроз динамічний, постійно оновлюється новими загрозами, як правило, зараз недостатньо вивчений.

До ***основних навмисних загроз*** слід віднести:

- *дезорганізація роботи ІТС;*
- *несанкціонований доступ до інформаційних ресурсів.*

Навмисна дезорганізація роботи ІТС

Шляхи *навмисної дезорганізації роботи* і виведення системи з ладу:

- *фізичне руйнування системи* (шляхом вибуху, підпалу тощо або вивід з ладу всіх або окремих найбільш важливих компонентів ІТС пристроїв, носіїв важливої системної інформації, осіб з числа персоналу і т. п.);
- *відключення або виведення з ладу інфраструктури*, що забезпечує функціонування ІТС (електроживлення, опалення, охолодження та вентиляції, ліній зв'язку і т. п.);

- *дезорганізація функціонування системи* (зміна режимів роботи пристроїв або програм, постановка потужних активних радіоперешкод на частотах роботи пристроїв системи і т. п.);
- *розкрадання носіїв інформації і цілих ПЕОМ.*

Несанкціонований доступ до інформаційних ресурсів

Способи *несанкціонованого доступу:*

- *впровадження агентів у число персоналу системи* (в тому числі, можливо, і в адміністративну групу, яка відповідала за безпеку);
- *вербування персоналу, що має певні повноваження* (схилення до співпраці, ініціативна співпраця, випитування):

1. ***Ініціативна співпраця*** проявляється в певних діях осіб з числа працюючих в організації, готових на будь-які протиправні дії. Відомо досить прикладів ініціативної співпраці з політичних, моральних або фінансових міркувань. Фінансові труднощі, політичні або наукові розбіжності, незадоволення начальством, або своїм статусом штовхають на співпрацю із злочинними угрупованнями та іноземними розвідками.

2. ***Схилення до співпраці*** – це, як правило, насильницька дія з боку зловмисників. Схилення або вербування може здійснюватися шляхом підкупу, залякування, шантажу. Дуже близько до схилення лежить і переманювання фахівців фірми конкурента на свою фірму з метою подальшого володіння його знаннями.

3. ***Вивідування, випитування*** – це прагнення під виглядом наївних питань отримати певні відомості. Випитувати інформацію можна і помилковими працевлаштуваннями, і створенням помилкових фірм, іншими діями.

- *застосування підслуховуючих пристроїв, дистанційна фото- і відеозйомка* (підслуховування, спостереження, фотографування);
- *перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і ліній зв'язку*. Сучасні технічні засоби дозволяють отримувати інформацію без підключення до комп'ютерної системи, перебуваючи на достатньому віддалені від об'єкта за рахунок випромінювання обладнання;
- *пасивне перехоплення даних*, переданих по каналах зв'язку;
- *несанкціоноване копіювання носіїв інформації*;
- *незаконне отримання паролів і інших реквізитів розмежування доступу* (шляхом підбору, шляхом імітації інтерфейсу системи і т. п.) з подальшим маскуванням під зареєстрованого користувача («маскарад»);
- *впровадження апаратних «спецвкладень», або програмних «закладок»,* що дозволяють долати систему захисту і здійснювати доступ до системних ресурсів;
- *незаконне підключення до ліній зв'язку* з метою прямої підміни законного користувача з подальшим введенням дезінформації та нав'язуванням неправдивих повідомлень.

Підробка – це модифікація листів, рахунків, бухгалтерських і фінансових документів, ключів, пропусків, паролів і т. п.

Знищення – знищуються і люди, і документи, і засоби обробки інформації, і продукція.

Рис. 3.4. Способи несанкціонованого доступу до інформації

Джерело: URL: https://studfile.net/preview/7435414/page:11/

Для досягнення поставленої мети зловмисник використовує не один, а деяку сукупність з перерахованих вище шляхів.

ГЛАВА 4
Мережеві загрози

4.1. Сучасні мережеві загрози: інтернет-шахрайство

До інтернет-шахрайства відносять:

- *фішинг;*
- *вішинг;*
- *фармінг;*
- *розсилка СПАМу;*
- *Fraud online services.*

Фішинг (phishing)

Фішинг – вид інтернет-шахрайства, мета якого змусити користувача виконати якусь дію, наприклад перейти по наданій адресі на сайт, завантажити програмне забезпечення, перевести гроші на певний рахунок і т. п., що може в подальшому нашкодити користувачу.

Шахраї спочатку через фішінг отримують від користувачів ідентифікаційні дані, паролі, номери кредитних карток, PIN-кодів і т.п., а потім використовують цю інформацію для своїх цілей. Фішинг використовує не технічні недоліки програмного забезпечення, а легковірність користувачів Інтернету. Сам термін ***«phishing»***, співзвучний з ***fishing*** (рибний лов), розшифровується як ***password harvesting fishing – вивудження пароля.***

На сьогоднішній день фішинг можна розділити на три види:

- *поштовий*;
- *онлайновий*;
- *цільовий*.

Поштовий фішинг. За допомогою спам-технології по електронній пошті розсилається лист, складений таким чином, щоб бути максимально схожим на справжній лист, наприклад, від обраного банку. При складанні листа використовуються логотипи банку, імена і прізвища реальних керівників банку. Лист попереджає про необхідність звірити реквізити банківського рахунку й про припинення банківських операцій доти, поки відповідні дані не будуть надані. В цьому листі, як правило, повідомляється про те, що через зміни програмного забезпечення в системі інтернет-банкінгу користувачеві необхідно підтвердити або змінити свої облікові дані ***(!!!!!!! ставтеся з особливою обережністю до повідомлень,***

у яких запитується особиста інформація, навіть якщо вони виглядають цілком правдоподібно) і пропонується перейти за наведеним посиланням на заздалегідь створений фальшивий сайт банку, щоб ввести свої конфіденційні дані.

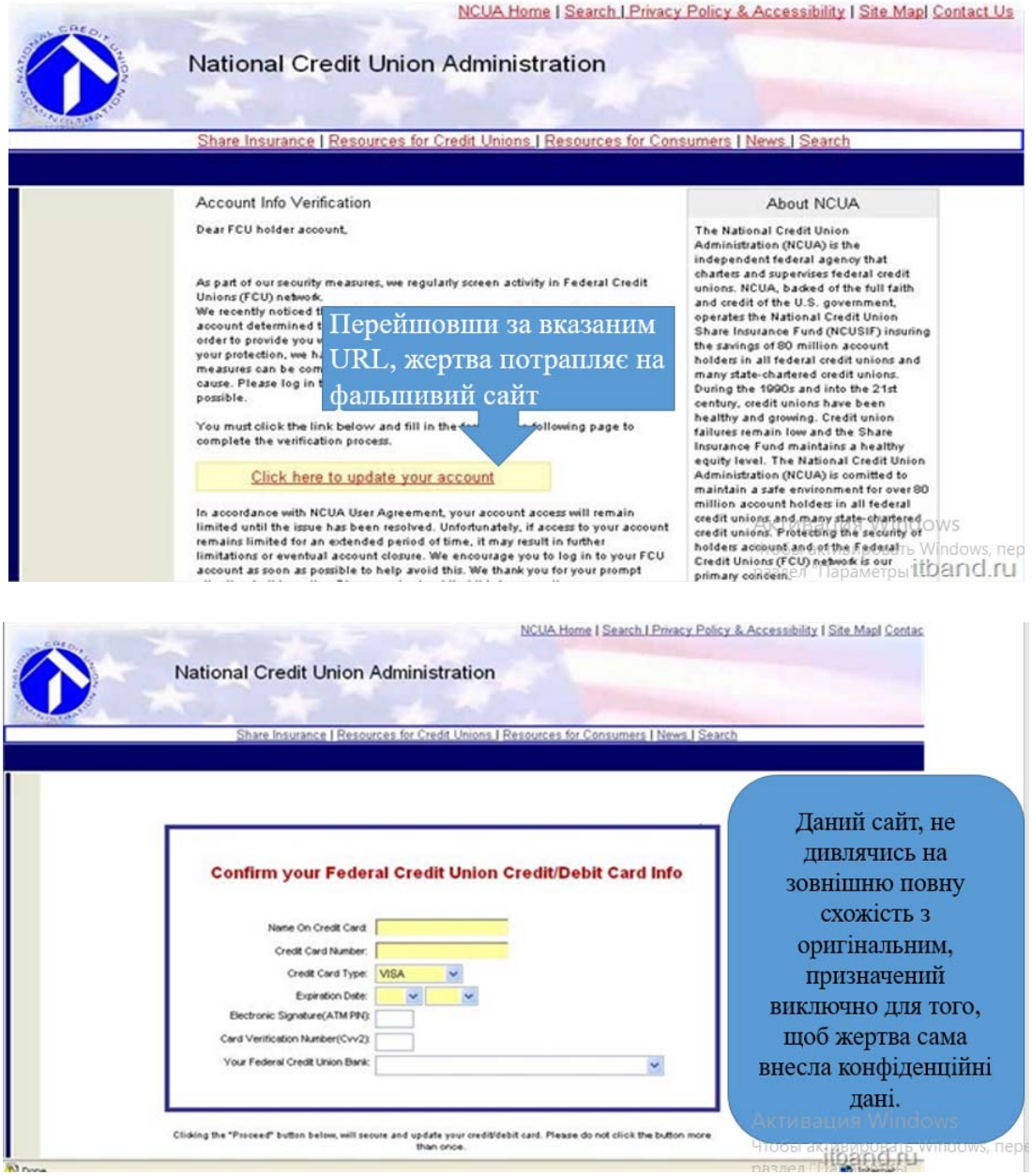


Рис. 4.1. Приклад листа від фінансової організації, який надсилається за допомогою спам-технології та схожий на справжній

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Головна мета такого листа – **змусити користувача НАТИСНУТИ НА ПОСИЛАННЯ**, що наведені в листі, тобто змусити користувача перейти на фальшивий сайт, а потім ввести свої конфіденційні дані.

Або, ще один популярний варіант. Жертва отримує повідомлення нібито з банку, в якому, наприклад, повідомляється про зробленою нею досить дорогу покупку. Далі йдеться про те, що при знятті коштів за цю покупку у банківської системи виникли якісь проблеми. Для вирішення ситуації клієнту пропонується терміново пройти за посиланням на сайт банку. Жертва, схвильована тим, що ніякої такої покупки вона не скоювала, поспішає прояснити ситуацію, клацає на запропонованому посиланню і бачить на екрані знайомий логотип свого банку й інтерактивну форму, яка запитує персональні дані клієнта, які і потрібні зловмисникові. Перейшовши за вказаним URL, жертва потрапляє на фальшивий сайт. Однак даний сайт, не дивлячись на зовнішню повну схожість з оригінальним, призначений виключно для того, щоб жертва сама внесла конфіденційні дані, а також розраховано на жадібність:

> «Today, a transfer has arrived in your account, the amount of which exceeds $ 1,000.
>
> In accordance with regulations and the agreement, you need to confirm its receipt. If you do not do this within three days, the money will be sent back.
>
> In order to confirm receipt of the transfer, open link at the end of this letter and enter the necessary information»

Не слід натискати на посилання у листі, або копіювати URL із повідомлень у вікно веб-браузера через буфер обміну, навіть якщо запропоноване посилання містить назву існуючої компанії. Замість цього введіть URL в поле адресу браузера для відвідування вебвузла. Зловмисники можуть використовувати для

підробки посилань маскування, це означає, що відображуване посилання здійснює перехід на підроблений вебвузол, а не на той, що нібито записаний у посиланні.

Перша техніка, яку використовують зловмисники, це субдомени і домени з помилками.

Наприклад, замість адреси **www.microsoft.com** можна підставити **www.micosoft.com** або **www.mircosoft.com.**

Наступний приклад техніки – це так звана **омографічна атака**.

Омограми – це слова з однаковим правописом, але з різними значеннями. Наприклад, вебадреса виглядає як справжня, тому що візуально не можна визначити, що «с» є символом кирилиці, а не «с» латиниці (www.microsoft.com). Або запис нулів замість букв «о» чи одиниць, замість літер «l».

Окрім посилань на підроблені сайти ознакою фішингового листа може бути:

- ▲*Відсутність особистого звернення.*
- ▲*Демонстраційні ввічливість і люб'язність.*
- ▲*Терміновий і (або) погрожувальний характер листа.*
- ▲*Запит особистої інформації в повідомленні електронної пошти.*
- ▲*Підозрілі вкладення.*

1. *Відсутність особистого звернення.*

Фішингові повідомлення електронної пошти не адресовані користувачеві особисто, у той час як справжні повідомлення від банку або компанії електронної комерції, клієнтом якої може бути користувач, звичайно, містять особисті дані.

2. Демонстраційні ввічливість і люб'язність.
Фішингові повідомлення електронної пошти відрізняються ввічливою й люб'язною формою. Як правило, це спонукає користувача відповісти на повідомлення, або клацнути включене в повідомлення посилання.

3. Терміновий і (або) погрожувальний характер листа.
У листі створюється видимість терміновості, щоб користувач відповідав негайно, не роздумуючи.

«Дорогий (2) клієнт! (1) Наш банк цінує Вашу довіру (2), і повідомляє про необхідність провести звірення даних про Ваш банківський рахунок через велику кількість неактивних користувачів. У випадку відмови Ваш обліковий запис буде вилучений. (3) Для звірення даних клацніть наведене нижче посилання»

4. Запит особистої інформації в повідомленні електронної пошти.
Як правило, фінансові установи та організації, що вже мають персональні дані клієнтів, ніколи їх не запитують в своїх листах. Ніколи не відповідайте на повідомлення електронної пошти, у яких запитуються ваші особисті відомості, навіть якщо вони виглядають цілком правдоподібно. Краще зателефонуєте в цю компанію за номером, що ви одержали від цієї компанії особисто, але не дзвоніть за номером, зазначеним у повідомленні електронної пошти.

5. Підозрілі вкладення.
У багатьох схемах фішингу користувача просять відкрити вкладення в повідомленні електронної пошти, що може заразити комп'ютер вірусом, або встановити шпигунське ПЗ.

Звертайте увагу і ПЕРЕВІРЯЙТЕ:
Метадані листа
Вкладення в листі
Посилання
Стилістику листа

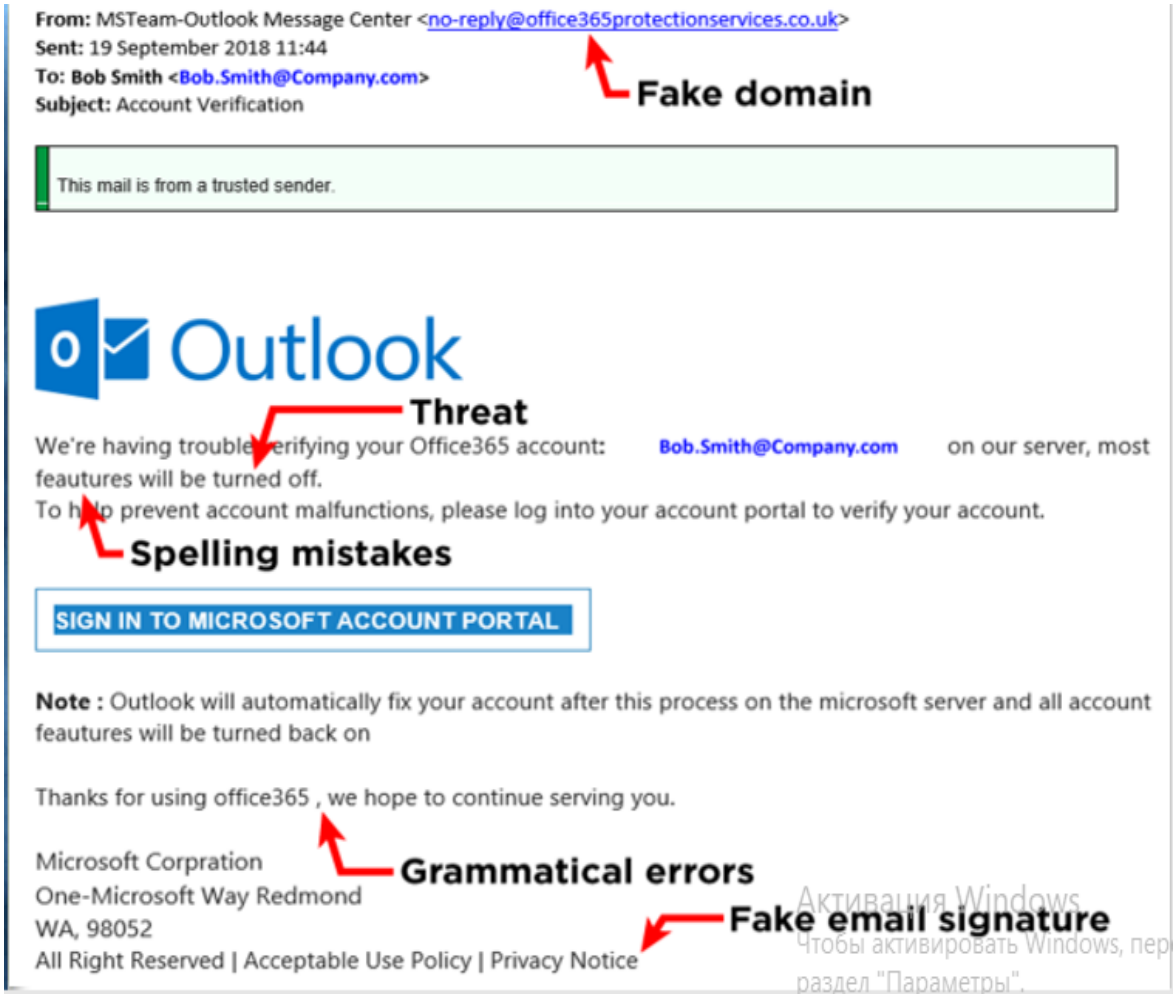


Рис. 4.2. Ознаки фішингового листа

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Онлайновий фішинг

Під ***онлайн фішингом*** мається на увазі, що зловмисники копіюють якісь сайти (найчастіше це Інтернет-магазини онлайнової торгівлі), використовуючи схожі доменні імена та аналогічний дизайн. Ну а далі все просто. Жертва, потрапляючи в такий магазин, вирішує придбати будь-який товар. Причому, число таких жертв досить велике, адже ціни в такому «неіснуючому» магазині будуть низькими, а всі підозри розсіюються через популярність копіюємого сайта. Купуючи товар, жертва реєструється і вводить номер та інші дані своєї кредитної картки.

Крім маніпуляцій з URL-адресами, існують приховані перенаправлення URL-адрес, які використовують ***вразливості*** до міжсайтового скриптінгу або міжсайтової підробки запиту. Можлива ситуація, коли отримують посилання на реальний сайт, але воно вже «отруєне» скриптом, щоб виконати будь-яку атаку, наприклад замість справжнього екрана авторизації підставити фейковий екран авторизації. Це і називається ***вразливістю до підробки міжсайтового запиту***. Якщо в вебсайті є вразливості, подібні XSS-вразливості, або відкриті перенаправлення, то фішингові атаки можуть бути ще небезпечнішими.

Цільовий фішинг

Цільовий фішинг (Spear Phishing), застосовують зловмисники для того, аби змусити користувача виконати якусь деструктивну дію на кшталт встановлення шкідливого ПЗ на сервері компанії. Із цією метою зловмисники надсилають певним працівникам компанії ретельно підготовлені цільові повідомлення, що мають переконати жертву відкрити шкідливе вкладення або перейти за посиланням на сайт, що містить експлойти для зламу програм на боці користувача.

Експлойт (exploit) – це комп'ютерні програми, які використовують вразливості в програмному забезпеченні для проведення атаки на комп'ютерну систему.

Метою може бути як захоплення контролю над системою, так і порушення її функціонування.

Вішинг

Вішинг (vishing) – вид шахрайства, що полягає в отриманні у користувача інформації під час телефонної розмови, названий так за аналогією з «фішингом».

Схеми обману ідентичні, тільки в цьому разі в повідомленні міститься прохання зателефонувати на певний міський номер. При цьому зачитується повідомлення, в якому потенційну жертву просять повідомити свої конфіденційні дані. Власників такого номера знайти не просто, оскільки з розвитком Інтернет-телефонії, дзвінок на міський номер може бути автоматично перенаправлений в будь-яку точку земної кулі на віртуальний номер.

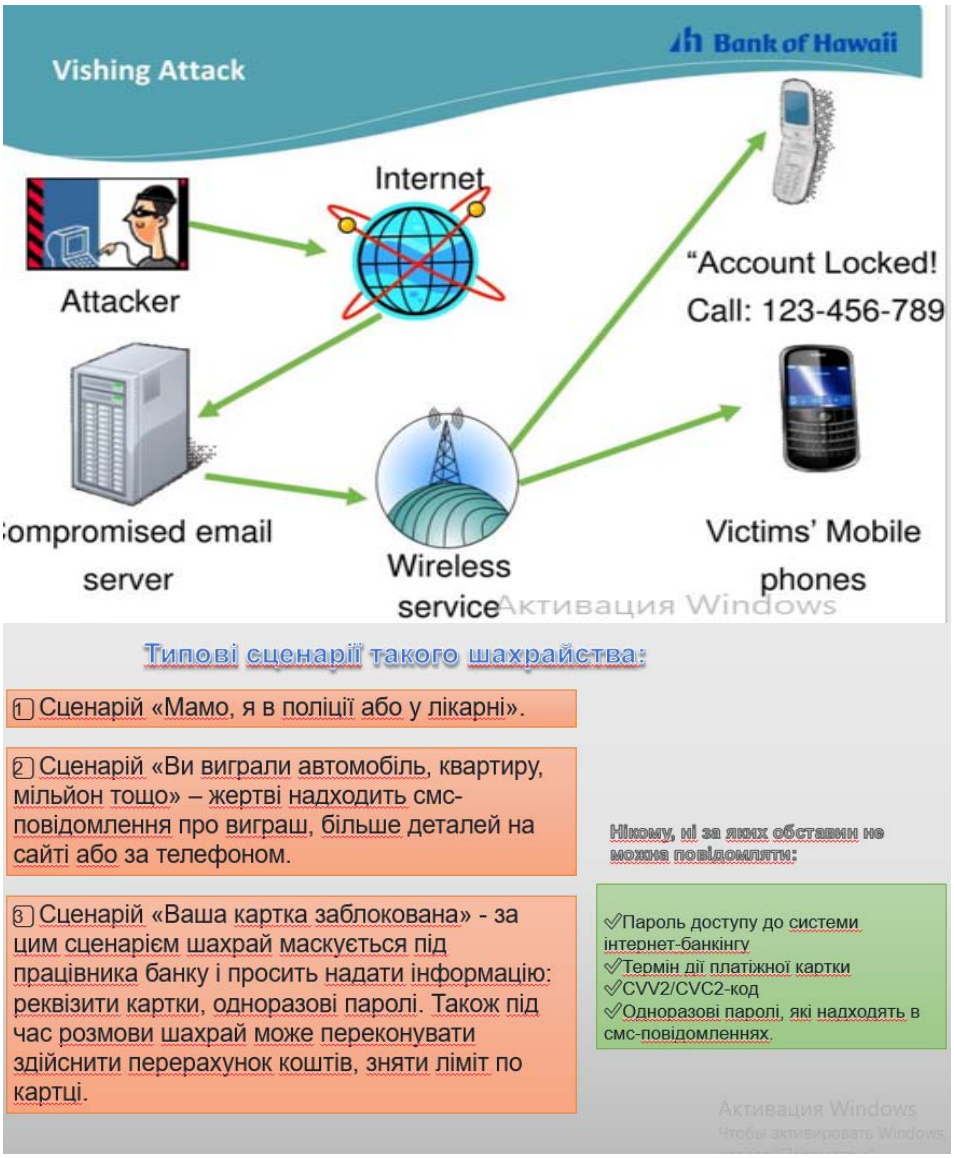


Рис. 4.3. Приклад вішингу

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

Фармінг

Фармінг (*Pharming*) – вид шахрайства, що ставить метою отримати персональні дані користувачів, але не через пошту, а прямо через офіційні вебсайти. Зловмисники замінюють на серверах DNS IP-адреси легітимних вебсайтів на підроблені, або спотворюють файл *hosts* на комп'ютері користувача, внаслідок чого користувачі перенаправляються на сайти шахраїв.

Цей вид шахрайства ще небезпечніший, оскільки помітити підробку практично неможливо, потенційна жертва навіть не повинна відкривати лист з некоректним посиланням. Фармінг – це просунутий варіант фішингу. Користувачу не пропонують перейти на фальшивий сайт за посиланням, тому що тепер липовий сайт замість справжнього відкривається сам. Результат: людина намагається зайти на сайт свого банку, але програма переадресує його на фальшиву копію сайта.

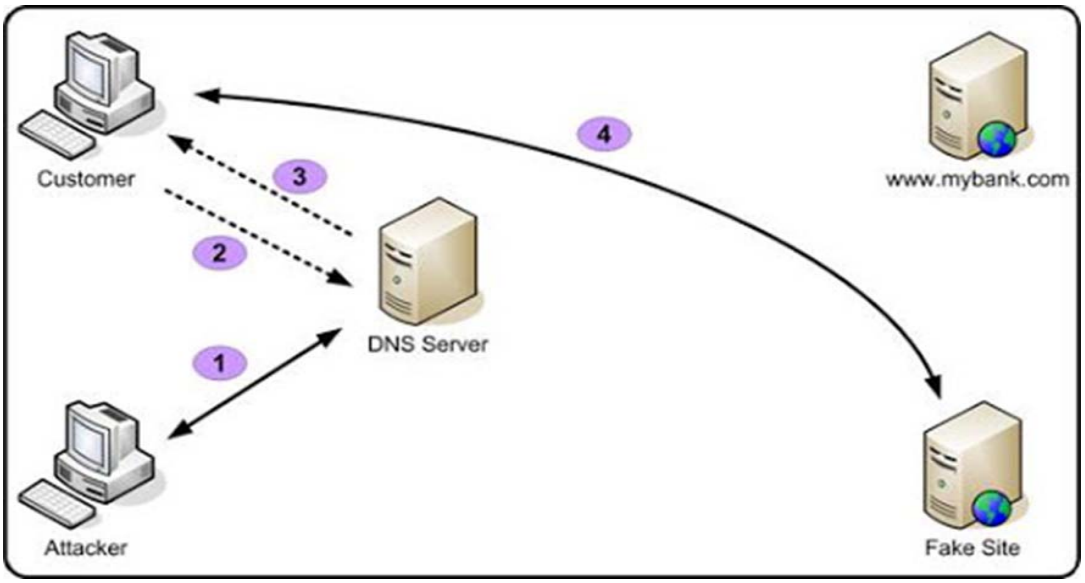


Рис. 4.4. Принцип роботи фармінгу

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

Розсилання СПАМ

У результаті цього шахрайства користувачі отримують на свої електронні поштові скриньки повідомлення, які ними не очікувались, та які містять інформацію рекламного або шахрайського характеру (реклама лікарського засобу та різноманітних послуг, прохання перейти за посиланнями тощо). Близько двох третин трафіку електронної пошти (65 %) припадає на спам. Спам може створювати загрозу доступності інформації, блокуючи поштові сервери, або використовуватися для розповсюдження шкідливого програмного забезпечення. Але, як показали дослідження, обробка СПАМу працівниками займає велику кількість робочого часу і загальні витрати на цю дію складають сотні мільйонів доларів.

Fraud online services

Fraud online services – це шахрайські сервіси, що тільки декларують, але не виконують свої функції.

Наприклад, фальшивий антивірус виводить повідомлення про виявлення шкідливих програм, пропонує виправити нібито виявлені помилки і вилікувати систему, але вже за гроші, хоча насправді – він нічого не знаходить і не лікує.

Рис. 4.5. Приклад шахрайського сервісу – Fraud online services

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

4.2. Сучасні мережеві загрози: крадіжка особистості

Тепер розглянемо загрози з фокусуванням на особистість

Всі відомості, що стосуються конкретної людини (ПІБ, адреса, телефон і т. п.) – це персональні дані. До персональних даних належать паспортні та біографічні дані, відомості про професію і освіту, адреса і телефон, відомості про склад сім'ї та багато іншого. Персональні дані охороняються законом з метою захисту прав на недоторканність приватного життя, особисту і сімейну таємницю.

Навіщо і кому можуть знадобитися ваші особисті дані?

Ними можуть скористатися рекламодавці (для збільшення числа розсилок). Особисті дані використовуються для отримання кредитів і крадіжок коштів з банків. Дані можуть бути вкрадені з хуліганських спонукань (наприклад оприлюднити листування). Дані можуть бути вкрадені для подальшого перепродажу.

Де знаходяться ваші дані?

Коли ви ділитесь своїми фотографіями в Інтернеті з друзями, чи знаєте, хто може одержати копії фотографій? Копії фотографій містяться на ваших власних пристроях. Ваші друзі можуть мати копії фотографій, завантажених на їхні пристрої. Якщо фотографії публікуються десь у мережі, як загальнодоступні, незнайомці також можуть мати їх копії. Вони можуть завантажувати ці фотографії або робити скріншоти з цих фотографій. Оскільки зображення були розміщені в мережі, вони також зберігаються на серверах, розташованих у різних частинах світу.

Тепер ці фотографії можна знайти не лише на ваших електронних пристроях. Персональна інформація кожного окремого споживача тепер зберігається на десятках, якщо не на сотнях серверів по всьому світу.

Більшість з нас просто не здогадується, наскільки легко інша людина може переглянути цю інформацію. Якщо знати, де шукати, ця інформація доступна абсолютно кожному. Ви напевно надавали свої дані навчальному закладу або іншій організації, тому існує ймовірність, що частина цієї інформації тепер в Інтернеті і будь-яка компанія, яка заробляє на зборі персональних даних людей, може її отримати. З цим фактом приходить очевидний результат: збільшення крадіжки особистих даних.

Крадіжка персональних даних – *це великий бізнес*. Американці значно частіше стають жертвами крадіжки особистих даних, ніж будь-хто ще.

У 2018 році в США було вкрадено понад 791 млн посвідчень. Франція значно відстала, – на другому місці, вкрадено 85 млн посвідчень особистості. (Джерело: Symantec)

43 % опитаних дорослих в США зізнаються, що роблять покупки онлайн через загальнодоступний Wi-Fi. (Джерело: Experian)

33 % опитаних дорослих в США зізнаються, що діляться своїми іменами і паролями з іншими. (Джерело: Experian).

Шахрайство з кредитними картками в даний час являє собою другий найбільш поширений тип крадіжки особистих даних в США – 33 % усіх активних повідомлень про шахрайство. (Джерело: FTC).

Рис. 4.6. Приклад шахрайства з кредитними картками

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

На особистому рівні найважливішим питанням є захист того, що ви найбільше цінуєте, а також досягнення достатнього рівня безпеки в ваших справах онлайн.

Крадіжка особистості (identity theft)

Однією із небезпечних загроз є крадіжка персональних даних, або *крадіжка особистості (Identity theft).*

> *Крадіжка особистості (identity theft)* – несанкціоноване заволодіння персональними даними іншою особою.

З розвитком послуг, що надаються через Інтернет, все більш популярними стають афери, коли одна людина видає себе за іншу, коли не потрібна її особиста присутність, а автентичність доводиться по телефону чи використовується інтерактивна система вебсайта. Зловмисник вирішує видати себе за іншого, щоб отримати доступ до ресурсів, користуватися послугами, наприклад, взяти кредит на чуже ім'я, розрахуватися за покупку чужою карткою, отримати іменне запрошення на закритий захід.

Подумайте зараз про свої аккаунти, файли, електронну пошту, відвідувані вами вебсайти та запитайте себе:

Що з цього я вважаю найбільш конфіденційним?
Що не можете дозволити собі втратити?
Що незамінне?
Що може заподіяти найбільшу шкоду?
Що може вдарити по вашій репутації?

1. **Що з цього найбільш конфіденційне?**
2. **Що ви не можете дозволити собі втратити?**
3. **Що незамінне?**
4. **Що може заподіяти найбільшої шкоди?**
5. **Що може вдарити по репутації?**

- фото
- дані платіжних карток
- дані банківських рахунків
- інформація по аккаунтах
- історія браузера
- інформація про паролі

Подумайте про речі, які викрадені, знищені або зашифровані, так що ви не можете більше їх використовувати, або вони розміщені в публічному доступі в Інтернеті, або коли вони потрапили до рук злочинців. За допомогою викраденої ідентичності вашої особи, можна також відкривати кредитні карткові рахунки та накопичувати борги на ваше ім'я. Доступ до особистих облікових даних також може відкрити доступ і до корпоративних даних та державних таємниць.

Соціальні мережі.

Через соціальні мережі можна дізнатися багато інформації про людину: вік, стать, місце роботи чи навчання, склад сім'ї, розмір доходу тощо. Ця інформація робить людину вразливою до будь-яких негативних дій зловмисника. Також така інформація може бути використана для дискредитації особи чи оформлення кредиту.

Фейкові роботодавці.

Коли особа подає заявку на роботу з вкладеним резюме, це може мати негативні наслідки як при прийомі на роботу,

так і для подальшого життя особи. Є несправжні компанії, котрі викладають на сайт пошуку роботи вакансії. Жертва відгукується на вакансію, надсилаючи резюме, і нічого не отримує взамін, адже навіть справжні компанії не можуть фізично відповісти на абсолютно всі заявки. Цим і користуються зловмисники, котрі збирають дані жертв і використовують у своїх корисливих цілях.

Отже, мотив для отримання доступу до облікового запису, крадіжки персональних даних, захоплення вашого комп'ютера – гроші. Кіберзлочинці можуть використовувати ваш комп'ютер в якості вебсервера, здійснювати незаконну діяльність з нього (атаки, підключати ваш комп'ютер до ботнет, шантажувати і т. п).

4.3. Загрози приватності при роботі в відкритих мережах

Популярність Інтернету негативно вплинула на приватність його користувачів. Потенційно всі дії користувача в Інтернеті – відвідані сайти, переглянуті сторінки, запити пошуку можуть бути зафіксовані і проаналізовані, тому що вебсервери ведуть журнали відвідувань своїх сайтів із запам'ятовуванням IP-адрес клієнтів і надають ці дані власникам сайтів у зручній формі. Багато сайтів потребують відповідної авторизації користувачів, яка полягає в надані сайту персональних даних користувача.

Ви можете переконатися, як багато відомостей про вас стає відомо при такій, здавалося б, нешкідливій процедурі як реєстрація на сайті, коли вас попросять повідомити ім'я, прізвище, стать, дату народження, адресу електронної пошти, країну і місто проживання, а при завершенні реєстрації ще й номер телефону. Ще більш важливі відомості повідомляються при пошуку роботи, при різних видах платіжних операцій, при зверненні на сайти держструктур і т. п. Звичайно,

в ряді випадків справжню інформацію надавати не обов'язково. Анонімність при використанні багатьох сервісів навіть вітається. Але дуже часто без надання достовірної інформації обійтися не можна, наприклад, при користуванні електронними держ-послугами, медичними системами і т. п. Політика безпеки цих ресурсів передбачає зберігання конфіденційної інформації та персональних даних користувача, але часто відбувається порушення через банальне недбальство або свідомі злочинні наміри. Витік персональних даних виявляють постійно, причому часто це «робота» навіть не зловмисників, а саме тих ресурсів, якими ми користуємося. Причиною витоків можуть бути недоліки програмного забезпечення, але часто самі власники сервісів збирають інформацію про користувачів у різних цілях.

Браузери користувачів також впливають на приватність, бо ведуть журнали відвідування сайтів і сторінок, а також відстежують місцезнаходження пристрою, на якому цей браузер запущений. Але цю функцію в браузері можна відключити, або сфальсифікувати дані про місцезнаходження.

Відкрийте Chrome і натисніть клавіші Ctrl + Shift + I, щоб відкрити вікно Інструменти розробника (Developer Tools).

Натисніть кнопку (три вертикальних точки) у верхньому правому куті панелі, що з'явилася, щоб відкрити меню (не основне меню браузера, а меню панелі з інструментами розробника!).

У меню, виберіть пункт More Tools → Sensors.

Перейдіть на відкриту вкладку Sensors і знайдіть список, що розкривається Geolocation.

Виконавши ці дії, можна вказати точну широту і довготу.

Можна взяти відому географічну точку або вибрати координати посеред океану.

У будь-якому випадку сайт не впізнає, де насправді знаходиться браузер.

Всі пристрої, з яких здійснюється вихід в Інтернет, мають певну IP-адресу, яка однозначно вказує на географічне місцезнаходження цього пристрою, або місцезнаходження інтернет-провайдера, який надає доступ в інтернет. Однак IP-адресу цього пристрою можна змінити на іншу, щоб виключити можливість правильного визначення місцезнаходження. Для цього можна, наприклад, використовувати проксі-сервери, які у всіх зверненнях з пристрою в мережу замінюють IP-адресу цього пристрою, на свою IP-адресу. Інший спосіб маскування IP-адреси пристрою полягає в використанні браузера ***Tor***. При використанні ***Tor,*** з'єднання між пристроєм, з якого виходять в інтернет, і цільовим сайтом здійснюється не безпосередньо, а через використання проміжних додаткових вузлів і кожні 30 секунд ланцюжок вузлів, що зв'язує пристрій з сайтом, змінюється. Крім доступу в звичайний Інтернет, ***Tor*** дає можливість відкривати сайти ***Даркнету.***

Загрозу приватності користувачам несуть також і файли ***куки***.

Куки (cookies) являють собою невеликий фрагмент текстових даних, яким обмінюються вебсервер і браузер.

Куки містять інформацію про поточний стан цього сеансу, автентифікаційні дані і персональні налаштування клієнта, а також унікальний для сервера номер сеансу. Протягом усього сеансу куки зберігаються на стороні браузера.

При встановленні з'єднання сервер генерує куки і передає їх браузеру. Веббраузер, отримавши текст куки від вебсервера, зберігає його у вигляді файла. Протягом усього сеансу користувача, а можливо, і при всіх повторних зверненнях

даного користувача до даного сайта, браузер передає куки серверу в тому ж вигляді, в якому він його отримав при останньому відвідуванні сервера.

Таким чином досягається ефект запам'ятовування стану сеансу, причому стан запам'ятовується на стороні клієнта. Вебсервер, зазвичай, застосовує куки користувача для зручності: наприклад, інтернет-магазини, зазвичай, зберігають в куки картку покупок користувача, в них також може зберігатися історія навігації користувача по сторінках сайта.

Куки бувають постійними – вони зберігаються в файловій системі ОС і мають тривалі терміни дії і тимчасові, браузер зберігає їх в оперативній пам'яті і видаляє після свого закриття.

Оскільки куки є текстові файли, то загрози безпеки для користувача вони не несуть (за винятком випадку, коли в них міститься аутентифікаційна інформація користувача).

Віруси та інші шкідливі коди за допомогою куків не поширюються, так що існуюча думка, що куки можуть заразити комп'ютер клієнта, не відповідає дійсності. У той же час куки можуть нашкодити приватності, особливо якщо в них міститься чутлива особиста інформація – дані платіжних карток, форми запитів з ім'ям і прізвищем, адресою і т.д.

Найпростішим способом захисту приватності є повна заборона на прийом куків від будь-яких сайтів. Однак при цьому можна втратити деякі зручності, засновані на використанні куків, наприклад тих чи інших додаткових послуг інтернет-магазину. Тому браузери залишають користувачу можливість вирішувати, від яких сайтів він забороняє приймати куки, а від яких дозволяє.

Порушення приватності в кіберпросторі може призвести до ряду наслідків: від легкого втручання в приватне життя до загрози самому життю. Рівень приватності і анонімності прямо пропорційний рівню безпеки: чим більше потрібно приватності, тим більше необхідно засобів безпеки.

Брюс Шнайер говорив: «Приватність полягає не в тому, щоб що-небудь заховати. Приватність полягає в тому, щоб мати можливість контролювати те, якими ми постаємо перед цим світом. Вона полягає в тому, щоб ви могли зберігати своє публічне обличчя і в той же час мали можливість приватно мислити і діяти. Приватність полягає в підтримці особистої гідності. Може бути, тобі і нема чого приховувати, але тобі є що захищати».

«То який сенс захоплювати мій комп'ютер чи мій аккаунт?»

Що ж, це хороше питання.

Потрібно зрозуміти наступне: в наш час атакує вже навіть не людська істота. Людина лише написала або навіть купила автоматичні програми, які полюють на вразливе програмне забезпечення без участі людини, а тому жертвами такого полювання може стати хто завгодно і де завгодно.

4.4. Соціальна інженерія

Соціальна інженерія – це метод несанкціонованого доступу до інформації шляхом психологічного впливу, маніпулювання та управління діями людини з метою змусити його виконати бажане.

Спеціалісти по кібербезпеці кажуть, що найслабкішою ланкою у безпеці є людина. Можна поставити надскладні паролі чи суперсучасне програмне забезпечення: антивіруси, фаєрволи, системи обмеження та розмежування прав доступу, однак людина, яка працює за комп'ютером – може всі ці системи відключити або обійти іншим способом і допомогти

зловмиснику потрапити у систему. Більшість заражень відбувається шляхом обману користувачів з використанням методів соціальної інженерії. Метод соціальної інженерії орієнтований не на технічну складову інформаційної системи, а на людину. Основне завдання цього методу – змусити користувача виконати дії, які необхідні зловмиснику для ураження ІТС. Наприклад, зловмисник може подзвонити уповноваженому працівнику з приводу негайної проблеми, вирішення якої вимагає негайного доступу до мережі. При цьому зловмисник розраховує на марнословство співробітника, залякує керівником або просто може скористатися жадібністю працівника.

«Емоційна буря»

Дуже часто зловмисники, атакуючи користувачів розраховують на емоційну реакцію. Найяскравішим прикладом соціальної інженерії є так звані ***«WOW-повідомлення»***. Це ***«гра»*** на природній цікавості та емоційності користувачів. Вони мають вигляд коротких повідомлень від друзів на пошту, у соцмережах, месенджерах, зміст яких має спонукати перейти за посиланням у тілі повідомлення. ***«ОГО! Подивись, яка прикольна річ. Я був у шоці!»*** – класичний приклад такого методу соціальної інженерії. Посилання можуть вести як на фішингові сайти, так і на автоматичне завантаження шкідливого ПЗ, яке також буде використано для крадіжки конфіденційної інформації з зараженого ПК.

Ще один з прикладів, рольова ситуація у Facebook. Від одного із друзів отримано повідомлення: ***«Вау, яке відео, ну ти і даєш! Як же тобі не соромно!»*** і в кінці йде посилання. Перша реакція: що ж там таке? Ви намагаєтесь запустити посилання, і тут Вам ще пропонується завантажити відео, відкриваючи його просто із цікавості Ви заражаєте комп’ютер. Але ж достатньо просто зупинитись і витримати паузу 10 секунд і подумати: У чому сенс повідомлення, яке це може бути відео? Хто мені це прислав, наскільки часто ми спілкуємось? Чому текст такий загальний? Нічого конкретного?

У крайньому випадку можна зв'язатись з відправником листа, можливо запитати в нього, що це таке, якщо він не відповідає – ще раз подумати, якщо є можливість – зателефонуйте йому. Але не поспішайте відкривати і тим паче закачувати і запускати на ПК те, що Вам пропонують. Намагання зловити користувача на емоційній реакції дуже легко нівелюється простою зупинкою і думкою про те, що не варто поспішати і просто подумати, що це і для чого.

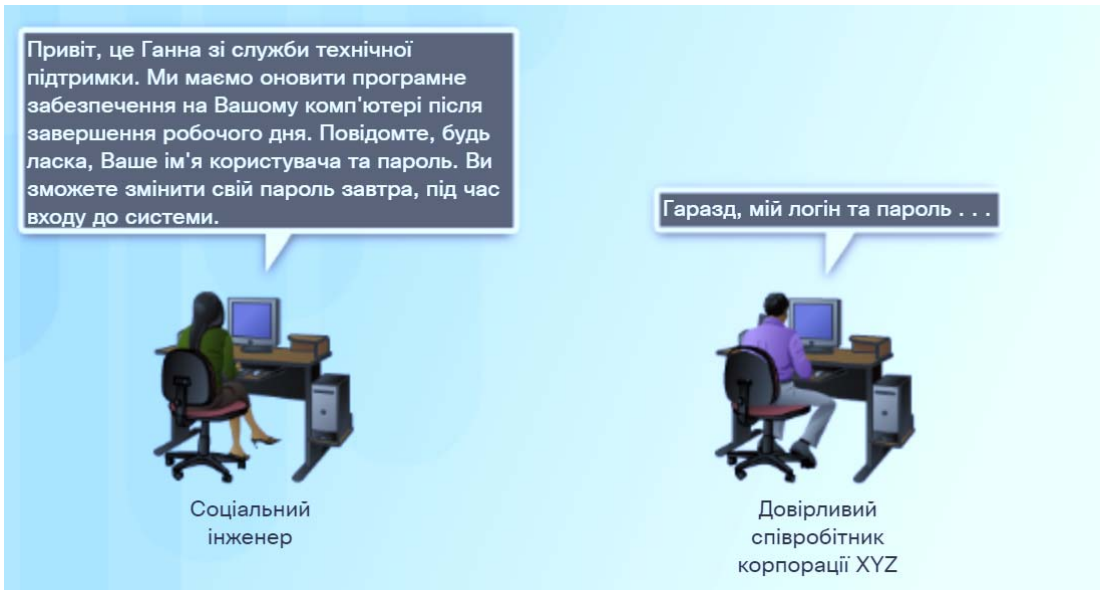


Рис. 4.7. Приклад соціальної інженерії

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Деякі види атак соціальної інженерії

Претекстінг (Pretexting) – атакуючий телефонує конкретній особі і обманом намагається отримати доступ до привілейованих даних. Наприклад, зловмисник вимагає надати персональні або фінансові дані для підтвердження особи одержувача. Однак такий вид інтернет-шахрайства вимагає дуже якісної підготовки та збору всієї необхідної попередньої інформації про особу.

Послуга за послугу (Quid pro quo) – вид атаки, коли злочинець запитує персональну інформацію в обмін на

щось, наприклад, безкоштовний подарунок. Вказаний вид інтернет-шахрайства базується на вмінні особи у телефонній розмові або електронною поштою увійти в довіру до жертви (зазвичай офісного працівника) та, представившись співпробітником служби технічної підтримки, запропонувати йому вирішення проблеми, в ході чого він і отримає всю необхідну конфіденційну інформацію.

Тактики соціальної інженерії

- ***повноваження;***
- ***залякування;***
- ***консенсус / соціальне підтвердження;***
- ***дефіцит;***
- ***терміновість;***
- ***близькі відносини/симпатія;***
- ***довіра.***

Повноваження – люди, як правило, виконують дії, коли інструкції надходять з «авторитетного джерела». Наприклад, співробітник відкриває заражений Pdf-файл, який виглядає як офіційна повістка.

Залякування – злочинці змушують жертву до відповідних дій. Наприклад, секретар керівника отримує дзвінок про те, що його керівник збирається представити важливу презентацію, але файли пошкоджені. У той же час зловмисник вимагає негайно надіслати йому ці файли.

Консенсус/соціальне підтвердження – люди швидше діятимуть, якщо вважатимуть, що інші зробили б так само. Наприклад, злочинці створюють вебсайти з фальшивими відгуками про безпечність продукту для його реклами.

Дефіцит – люди швидко діятимуть, якщо будуть думати, що кількість привабливих пропозицій обмежена. Наприклад, злочинці пропонують обмежену можливість певного продукту, що має примусити жертву швидко вчинити певні дії.

Терміновість – люди швидко діятимуть, якщо вважатимуть, що мають обмежену кількість часу для прийняття рішення. Наприклад, злочинці встановлюють крайній термін для прийняття рішення, мотивуючи жертву зниженою ціною.

Близькі відносини/Симпатія – злочинці будують приязні відносини з жертвою. Жертва охоче виконає прохання зловмисника, якщо відчуватиме до нього симпатію.

Довіра – злочинці створюють довірчі відносини з жертвою, цей підхід може вимагати більше часу. «Експерт з питань безпеки» пропонує жертві послуги та може підтвердити свою кваліфікацію. Допомагаючи жертві, зловмисник виявляє «серйозну помилку», яка потребує негайної уваги. За рахунок вирішення цієї проблеми, зловмисник отримує можливість досягнути своєї цілі.

«Серфінг через плече» і «Дайвінг у смітнику»

Кіберзлочинець спостерігає за жертвою або виконує «серфінг через плече», щоб отримати PIN-коди, коди доступу чи номери кредитних карток. Зловмисник може знаходитися максимально близько до своєї жертви, або використовувати біноклі чи системи відеоспостереження для підглядання. Це одна з причин, чому дані на екранах банкоматів видно лише під певним кутом. Такі запобіжні заходи безпеки ускладнюють підглядання для злочинців.

«Сміття однієї людини – скарб для іншої». Ця фраза особливо підходить для «дайвінгу у смітнику», який передбачає досліджен ня сміття жертви, щоб дізнатися, яку інформацію організація викидає. Рекомендовано обмежити доступ до контейнерів для сміття. Будь-яка конфіденційна інформація має бути належним чином утилізована шляхом подрібнення або використання пакетів для спалення, які зберігають секретні або конфіденційні документи для подальшого знищення вогнем.

«Дорожне яблуко»

Цей спосіб здійснення шахрайства ґрунтується на використанні фізичних носіїв інформації. Так, зловмисник може залишити їх у будь-яких публічних місцях (на підлозі ліфта або у вестибюлі, у паркінгу) із таким зображенням, підробленим під офіційний і підписом, покликаним викликати цікавість у жертви. Співробітник через незнання може підібрати носій і вставити його в комп'ютер, щоб задовольнити свою цікавість, або просто як «добрий самаритянин» віднесе в компанію.

Зворотна соціальна інженерія

Реалізація цього способу може бути здійснена лише у випадку, коли шахрай попередньо знайомий із жертвою та заслуговує на її довіру. У такому випадку жертва сама звертається до шахрая (наприклад, системного адміністратора), із проханням допомогти відновити втрачений файл (який заховав сам шахрай). При цьому їй повідомляється, що таку дію можна зробити якнайшвидше лише зайшовши у її обліковий запис. Таким чином, жертва за власним бажанням повідомляє всю інформацію шахраю. Зловмисник може застосувати такі техніки:

- **Диверсія** (створення оборотної неполадки на комп'ютері жертви);
- **Реклама** (зловмисник підсовує жертві оголошення: «Якщо виникли неполадки з комп'ютером, зателефонуйте за таким-то номером»).

Уособлення і розіграш

Уособлення (імперсоніфікація) – це спосіб видавати себе за когось іншого. Наприклад, нещодавня телефонна афера була спрямована на платників податків. Злочинець, який представлявся співробітником податкового управління, повідомляв жертвам, що вони мають заборгованість, яку жертви повинні сплатити негайно за допомогою банківського переказу.

Самозванець погрожував, що відмова від сплати призведе до арешту. Злочинці також використовують уособлення, щоб атакувати інших. Вони можуть підірвати довіру до публічних осіб за допомогою публікацій на вебсайтах або в соціальних мережах.

Містифікація або розіграш – це дія, призначена для обману. Містифікація в кіберсвіті може завдати стільки ж клопоту, як і в реальному. Мета розіграшу – викликати реакцію жертви. Це може бути незрозумілий страх і нелогічна поведінка. Користувачі самі розповсюджують обмани через електронну пошту та соціальні мережі.

В чому полягає небезпека соціальної інженерії?

Із пандемією коронавірусу у 2,5 раза збільшилась кількість атак на робітників, які працюють дистанційно. Досить часто кіберзлочинцям навіть не потрібно вдаватися до складних зломів захищених онлайн-платформ та сервісів – довірливі користувачі самі віддають доступ до власних коштів чи приватної інформації.

Люди, які знаються на соціальній інженерії, дуже небезпечні, бо володіють психологічними прийомами маніпуляції свідомістю. Тому серед головних методів протидії прийомам соціальної інженерії візьміть за золоте правило один незмінний принцип: перебуваючи в мережі, **НЕ ВІРТЕ НІКОМУ**. Мається на увазі незнайомі людей, які надсилають незрозумілі пропозиції, чи будь-якими іншими способами намагаються вивідати у вас конфіденційну інформацію.

Як уберегтися від атак зловмисника в мережі?

Існують доволі прості способи протидії фішингу, вішингу та смішингу:

1. *Ніколи не переходьте за підозрілими посиланнями. Якщо не впевнені, проігноруйте лінк, не потрібно по ньому переходити. Завжди звертайте увагу на назву сайтів, чи немає «битої» назви.*

2. *Ніколи не розпаковуйте незрозумілі файли з розширеннями.rar (та й будь-якими іншими архівними розширеннями),.***dll** *та.***exe** *(такі розширення мають файли, які запускають виконання якоїсь команди чи програми, під такі файли дуже часто маскується шкідливе ПЗ (віруси, трояни і хробаки. А цього добра в інтернеті вистачає). Одним словом, не відкривайте файли з будь-якими підозрілими розширеннями, щоб не запустити в свою систему небажаних гостей.*
3. *Пам'ятайте, що працівники банків ніколи не запитують конфіденційну інформацію по телефону, в месенджерах та за допомогою електронної пошти.*
4. *Якщо вам надійшло радісне повідомлення про те, що ви здобули перемогу в лотереї – ви можете поцікавитися у свого мобільного оператора, чи була така акція та уточнити її деталі.*

Як протистояти ризикам, які надходять з мережі

Немає різниці, чи ви працюєте віддалено, чи в офісі. Використовуйте робочий ноутбук лише для робочих завдань. Це суттєво знизить ризик крадіжки конфіденційної інформації.

▲ З'єднання повинне бути надійним. Уникайте користування публічними мережами, адже за сусіднім столом із ноутбуком і склянкою чаю може сидіти непримітна людина, яка в цей час займатиметься крадіжкою грошей чи персональних даних з відвідувачів закладу. Такі теж випадки траплялися, не потрібно думати, що вас це не зачепить. Така ситуація може трапитися з кожним.

▲ Доступ до корпоративних даних не повинні мати всі підряд, включаючи стажерів та новачків.

▲ Корпоративний захист даних означає не лише встановити надійний антивірус на головному сервері. Це також означає, що на роботі потрібно завести звичку використовувати цифрові ключі доступу та шифрування важливої корпоративної документації.

▲ В компанії час від часу повинні проводитися освітньо-практичні семінари щодо безпечного поводження в мережі. Співробітники повинні вміти протидіяти випадкам використання соціальної інженерії в злочинних цілях.

Уважність та ще раз уважність

Протидія соціальній інженерії схожа на внутрішню боротьбу з людською суттю. Є декілька правил, які допоможуть вам не попадатись на гачки шахраїв:

1. Звертайте увагу на написання адрес сайтів.
2. Якщо вам пропонують переглянути сайт/фото/відео, зазиваючи емоційними закликами – не переходьте одразу. Порахуйте до 10 та згадайте, що це можливо приклад соціальної інженерії.
3. Вводячи логін/пароль в аккаунтах на сайтах, звертайте увагу на незвичайні зміни зовнішнього вигляду сторінок. Якщо щось викликає підозру – краще перевірити оригінальність ресурсу ще раз.
4. Критично ставтесь до електронних листів, а особливо до посилань, за якими пропонують перейти незнайомі відправники повідомлень.

Ці чотири правила не є вичерпними, але тримаючи їх у пам'яті та використовуючи як фільтр під час користування Інтернет, ви зможете суттєво покращити свій інформаційний захист та стати менш вразливим до методів соціальної інженерії.

Контрольні запитання

1. Що відносять до інцидентів безпеки системи?
2. Дайте визначення загрози безпеки функціонування ІТС.
3. Назвіть основні загрози ІТС.
4. Що таке вразливість системи?
5. Як класифікуються загрози безпеки ІТС.
6. Що таке вади захисту?
7. Які загрози відносяться до навмисних?
8. Що таке фішінг?
9. Які головні ознаки фішингового листа?
10. Що таке крадіжка особистості і чим вона небезпечна?
11. Як захистити приватність при роботі в відкритих мережах?
12. Що таке соціальна інженерія?

Розділ 3. АТАКИ НА ІТС. ПОРУШНИКИ КІБЕРБЕЗПЕКИ

ГЛАВА 5
Атаки на інформаційні системи

5.1. Визначення атаки на ІТС
5.2. Фази атаки. Ланцюг кібервбивства
5.3. APT-атака

5.1. Визначення атаки на ІТС

Загроза – Атака – Проникнення – Компрометація

Потрібно розрізняти загрозу, яка робить потенційно можливим здійснення несприятливого впливу на ІТС, та атаку, яка є дією, тобто реалізацією загрози.

Атака – це навмисна спроба реалізації існуючої загрози ІТС, що виконується порушником.

Атака може бути безрезультатною, тому що спрацюють механізми захисту в системі, але якщо атака є успішною (здійснено подолання засобів захисту), то говорять про *проникнення* в ІТС.

Результатами проникнення можуть бути, наприклад: несанкціоноване розширення прав доступу в мережі або на конкретному вузлу:

- *спотворення інформації;*
- *розкриття інформації;*
- *несанкціоноване використання комп'ютера або мережевих сервісів без погіршення якості обслуговування інших користувачів;*
- *навмисне зниження продуктивності ІТС або блокування доступу до мережі, або комп'ютера.*

Наслідком успішної атаки є порушення безпеки системи, яке називають *компрометацією системи.*

Цікавим є визначення атаки в міжнародному стандарті по кібербезпеці **ISO/IEC 2700: 2014:**

«[Computer] Attack – attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset».

Атака [комп'ютерна] – спроба знищення, розкриття, зміни, блокування, крадіжки, отримання несанкціонованого доступу до активу або його несанкціонованого використання.

Розрізняють ***нетаргетовані*** та ***таргетовані (цільові)*** атаки.

Нетаргетовані атаки не мають конкретної жертви і націлені на довільні системи. До цього виду атак відносяться:

- *розповсюдження шкідливого ПЗ;*

➔ *розсилка СПАМу;*
➔ *створення ботнетів;*
➔ *скритий майнінг криптовалют та інше.*

Таргетовані атаки націлені на конкретні інформаційні системи і їх метою є крадіжка інформації, шпигунство, блокування роботи системи та інше.

5.2. Фази атаки. Ланцюг кібервбивства

Цільова атака, як правило, складається з 4 головних фаз, кожна з яких є сукупністю дій та прийомів:

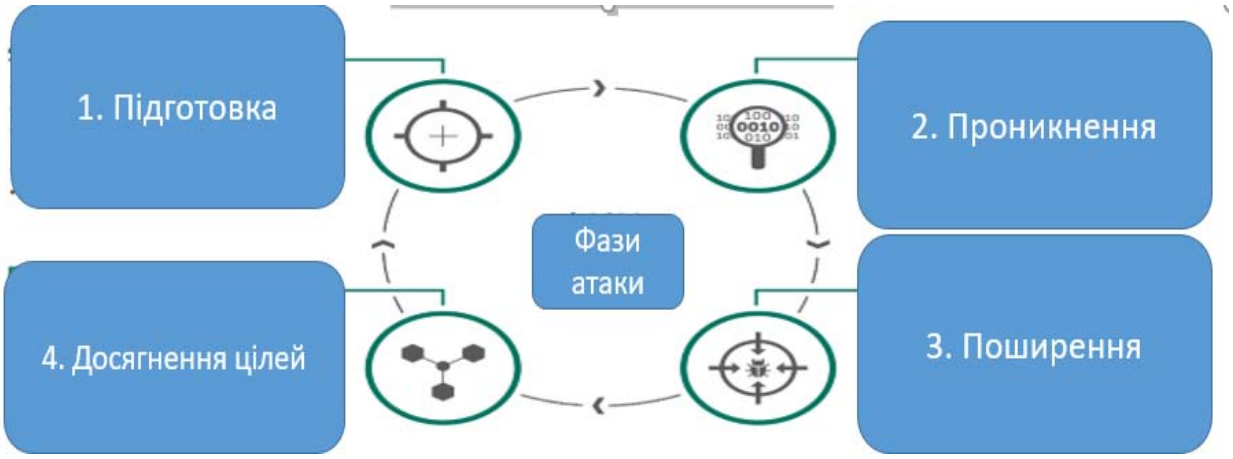


Рис. 5.1. Фази цільової атаки

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

1-а фаза атаки – *Підготовка*

Визначається жертва з подальшим збором детальної інформації про неї і виявляються «слабкі» місця в інформаційні системі. На цій фазі також аналізується зібрана інформація, розробляється стратегія по досягненню результату і створюється необхідний для атаки інструмент.

Збір інформації про жертву виконується:

a) по відкритих джерелах за технологію OSINT;

b) *використовуючи інсайдерів* (підкуп, шантаж, обман, довіра, рекрутінг);

c) використовуючи соціальну інженерію (телефонні дзвінка від імені співробітника, спілкування в соціальних мережах тощо).

За допомогою спеціального ПЗ виявляються:

a) мережева топологія жертви;

b) тип і версія операційної системи;

c) доступні мережеві сервіси (відкриті порти і т. п.).

Опираючись на зібрану інформацію, створюється стенд-полігон з ідентичними як у жертви версіями ПЗ, що дає можливість випробувати проникнення на моделі, відпрацювати техніку прихованого впровадження і обходу стандартних засобів захисту інформації.

Закінчується перша фаза атаки розробкою набору інструментів ***(Toolset)*** для атаки або його купівля. Тіньовий ринок пропонує досить широкий вибір різних інструментів, що значно скорочує час, за винятком унікальних випадків. Важливо визначитися між фінансовими витратами на купівлю вже готових інструментів на ринку та трудовитратами і часом для створення власних. Як правило, ***Toolset*** складається з трьох компонентів:

1. Модуль керуючого центру.

2. Інструменти проникнення.

3. Payload.

1. Модуль керуючого центру (*Command and Control Center, C&C, C2*) забезпечує взаємодію та передачу команд підконтрольним шкідливим модулям.

2. Інструменти проникнення:

- ***експлойт (Exploit)*** – шкідливий код, що використовує вразливості в ПЗ вузла-жертви для його первинного інфікування і ініціалізації доставки на нього модулів шкідливого ПЗ;

- ➔ ***валідатор*** – шкідливий код, здатний зібрати інформацію про вузол, що атакується і передати її C&C для подальшого прийняття рішення про розвиток атаки або повну її відміну на конкретній машині, вибравши відповідну команду:
  - ↗ ***завантаження –*** приступити до виконання цільової атаки;
  - ↗ ***самознищення –*** у випадках, коли комп'ютер і дані на ньому не представляють цінності для цільової атаки;
  - ↗ ***очікування*** – рішення відкладається, режим «сну».
- ▲ ***завантажувач (Downloader);***
- ▲ ***модуль доставки (Dropper)*** – шкідлива програма, завданням якої є доставка основної програми (*Payload*) для атаки на заражену машину жертви.

3. Payload – основний шкідливий модуль, який може складатися з декількох функціональних модулів, залежно від поставленої мети і завдання:

- ➔ ***клавіатурний шпигун;***
- ➔ ***модуль запису екрану;***
- ➔ ***модуль віддаленого доступу;***
- ➔ ***модуль поширення усередині інфраструктури;***
- ➔ ***модуль взаємодії з C&C;***
- ➔ ***модуль шифрування для захисту використовуваних технологій порушників і відповідно унеможливлення детектування атаки;***
- ➔ ***модуль очищення слідів активності та самознищення;***
- ➔ ***модуль пошуку інформації на диску.***

Для подолання стандартних засобів захисту в ІТС до складу ***Payload*** можуть входити модулі, що дозволяють обдурити або обійти захисні механізми.

Для цього використовується:

- заплутування коду на рівні алгоритму за допомогою спеціальних компіляторів, що ускладнює його аналізу антивірусом (обфускація коду);
- багаторівневе шифрування частини коду для приховання від детектуючих механізмів антивірусів;
- інжектування в чужі процеси, що дозволяє використовувати усі привілеї легітимного процесу у своїх цілях, не звертаючи на себе увагу встановлених засобів захисту. Цей метод дозволяє обійти різні системи контролю безпеки. Інжектування застосовується на рівні створення нового потоку у віртуальному просторі легітимного процесу;
- впровадження руткітів, які дозволяють маскувати свою присутність в системі (приховуючи процеси, файли на диску, ключі в реєстрі);
- обхід емулятора антивірусу завдяки динамічній заміні алгоритму коду, що не дозволяє йому визначити логіку виконання коду шкідливої програми;
- обхід «пісочниці» антивірусу, яка по специфічним ділянкам коду в аналізуємій програмі виявляє невідомі для антивірусу загрози. Обхід заснован на тимчасовій затримці виконання модулів ***Payload,*** оскільки час перевірки «пісочницею» обмежений.

2-а фаза атаки – *Проникнення*

Активна фаза цільової атаки, що використовує різну техніку для первинного інфікування жертви і проведення внутрішньої розвідки. Після закінчення розвідки і визначенні приналежності інфікованого хоста (сервер/робоча станція) по команді порушника через центр управління може завантажуватися додатковий шкідливий код. За сукупністю вживаної

техніки ця фаза є для порушників однієї з найскладніших у виконанні і реалізації. Після виконання автоматичних ухилень від виявлення і системних тестів на відповідність операційному середовищу *Payload* активує основні функціональні модулі, встановлюючи закрите шифроване з'єднання з командним центром і сигналізуючи про свій активний статус. На цій стадії порушники приступають до консольної роботи, використовуючи термінал підконтрольної машини. Їм дуже важливо швидко зорієнтуватися всередині, щоб зберегти свою присутність і закріпитися в мережі. Першочергове завдання – підняття рівня доступу до привілейованого.

3-я фаза атаки – *Поширення. Встановлення контролю та підвищення привілеїв*

Ця фаза включає декілька кроків.

Крок 1. *Закріплення всередині інфраструктури*, тобто реалізація комплексу заходів, спрямованих на організацію гарантованого доступу в інфраструктуру жертви. Справа у тім, що первинною точкою проникнення, як правило, буває комп'ютер співробітника з обмеженими правами і з фіксованим робочим часом, а це значить, що доступ порушників до ІТС буде обмеженим. З урахуванням зібраних даних про топологію мережі відбувається ручний відбір ключових робочих станцій і серверів. Вибрані машини порушники беруть під свій контроль і використовують під нові завдання.

Крок 2. *Поширення*. Значущим аспектом є наявність постійних активних точок входу, зазвичай для цього використовуються сервери з малим часом простою. На цьому кроці порушники вже мають адміністративні права і усі їх дії по відношенню до систем безпеки абсолютно легальні. Використовуючи стандартні засоби віддаленого доступу, вони вибирають найбільш зручні з точки зору їх завдань сервери і робочі станції.

Крок 3. *Оновлення*. Виконується, коли певна функція, що необхідна для поширення атаки, відсутня в арсеналі вже задіяного шкідливого модуля. Наприклад, такою функцією може бути запис звуку із мікрофону або ввімкнення камери. Можливість відновити модуль заздалегідь передбачена розробником атаки і може бути активована при необхідності.

4-а фаза атаки – *Досягнення цілей*

Фаза складається з декількох кроків.

Крок 1. *Виконання шкідливих дій*. На цьому етапі порушники вже можуть виконати будь-яку дію, спрямовану проти компанії, що атакується.

Перерахуємо основні типи дій:

➔ *розкрадання інформації*:

- у комерції – це цілий бізнес, заснований на конкуренції і великих грошах; у державних структурах – це шпигунство, рідше отримання інформації, що містить конфіденційні дані для наступного перепродажу;
- у фінансовому секторі – це інформація про платіжні і білінгові системи, рахунки великих клієнтів та інша фінансова інформація для проведення незаконних транзакцій, а саме розкрадання відбувається максимально непомітно для систем моніторингу компанії;

➔ *зміна даних* – наприклад у відомій атаці, від якої постраждали сотні фінансових організацій, кіберзлочинці, використовуючи контроль над платіжною системою, змінювали доступний кредит на балансі кредитної картки, тим самим дозволяли спільникам кілька разів знімати кошти з однієї і тієї ж картки. А у разі кіберпограбування *Carbanak* злочинці діяли від імені співробітників, використовуючи онлайн-банкинг для переказу коштів на підконтрольні кіберзлочинцям рахунки;

➔ *маніпуляції з бізнес-процесами і шантаж.* Наочний випадок стався з компанією *Sony Pictures*, інформаційна система якої була атакована. В результаті були викрадені

тисячі файлів і документів, фінансових даних, а також до кіберзлочинців у руки потрапили фільми, що готовились до прокату. У компанії розповіли, що більшість її комп'ютерів вийшли з ладу, а на екранах робочих станцій відображувалася фраза «ми оволоділи вашими секретами». Усі дані на жорстких дисках робочих комп'ютерів були стерті, кіберзлочинці погрожували опублікувати інформацію, якщо компанія не підкорятиметься їх вимогам;

➔ *знищення даних* – інший приклад розвитку цільової атаки. Близько 30 тис. персональних комп'ютерів, що належать найбільшій у світі нафтовидобувній компанії *Saudi Aramco*, було виведено з ладу. Кіберзлочинці переслідували дві цілі: перша – розкрадання закритої інформації, друга – повна зупинка бізнес-процесів компанії. У результаті атаки компанія була вимушена майже на місяць припинити свою операційну діяльність, відключивши філії від мережі Інтернет.

Крок 2. *Приховання слідів.* Упродовж усієї цільової атаки порушники прагнуть маскувати свою присутність під легітимний процес, в крайніх випадках, коли це неможливо, вони вручну очищають журнали подій. Як правило, велика частина активності протікає під адміністративним доступом, не викликаючи підозри.

Крок 3. *Збереження доступу*. На фінальному етапі атаки багато порушників прагнуть залишити усередині засіб, що дозволяє їм у разі потреби повернутися назад в інфраструктуру. Таким засобом зазвичай є керований завантажувач, здатний по команді завантажити шкідливий модуль.

Перші три фази атаки створюють так званий *«Ланцюг кібервбивства» (Cyber Kill Chain).*

Етап 1. Розвідка – збір інформації про ціль атаки.

Етап 2. Озброєння – нападник створює експлойт та готує засоби для відправки на ціль.

Етап 3. Доставка – нападник відправляє експлойт до цілі по електронній пошті або іншим способом.

Етап 4. Проникнення – запуск виконання експлойта.

Етап 5. Встановлення – нападник встановлює зловмисне ПЗ та чорний хід.

Етап 6. Керування та контроль – віддалене керування ціллю.

Етап 7. Поширення всередині мережі.

Етап 8. Дія – нападник здійснює шкідливі дії, такі як крадіжка інформації, або виконує додаткові атаки на інші пристрої в мережі, знову використовуючи етапи *Kill Chain*.

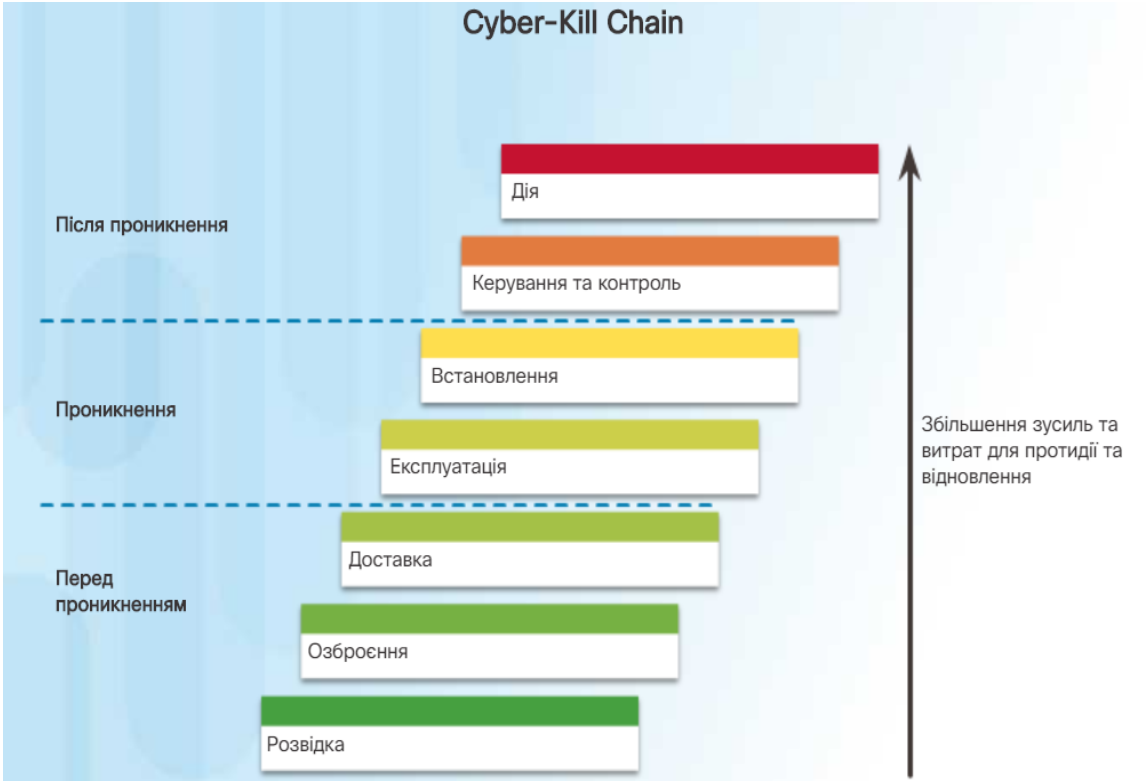


Рис. 5.2. Ланцюг кібервбивства

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

5.3. APT-атака

APT-атака – це також цільова, або таргетована атака, яка відрізняється довготривалістю і складністю виконання атаки, виконуються переважно на IT-інфраструктуру військових і державних об'єктів.

Як правило, їх проводять спецслужби інших країн або кібервійська. Метою APT-атак є отримання постійного несанкціонованого доступу до інформаційних систем. Журналісти розширили поняття APT-атак до багаторівневих атак, метою яких є мережа будь-якої організації. Також в медіа можна побачити, що APT – це група зловмисників або навіть країна, які беруть участь в тривалих кібератаках на організації або країни.

Термін *APT (Advanced Persistent Threat)* перекладають як ***«розвинена стійка загроза»*** або ***«складна постійна загроза»***, маючи на увазі багатоетапний сценарій атаки, використовувані в ній інструменти і тип виконавців атаки.

На рис. 5.3 надані технології, що використовуються при виконанні APT-атак.

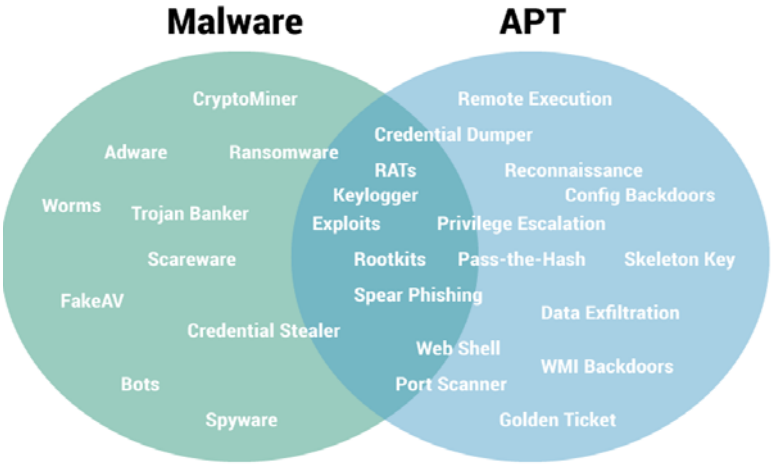


Рис. 5.3. Технології, що використовуються при виконанні APT-атак

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

Багато технологій вже відомо по попередньому матеріалу, тому надаємо коментар до нерозглянутих технологій.

Remote Execution – віддалене впровадження і виконання коду на вузлах інформаційної системи.

Credential Dumper – це дампер облікових записів, що дозволяє получати логіни і паролі у вигляді відкритого тексту (наприклад, програма ***Mimikatz***).

RATs – використання інструменту віддаленого адміністрування систем. Програма ***Skeleton Key*** дозволяє кіберзлочинцям обходити системи захисту, які реалізують однофакторну парольну аутентифікацію в корпоративних мережах тільки через контролер домену ***Active Directory***.

Data Exfiltration – цільова крадіжка даних.

Web Shell – оболонка, що зазвичай являє собою невеликий фрагмент шкідливого коду, написаний на типових мовах програмування веброзробки (***ASP, PHP, JSP***), який зловмисники впроваджують на вебсервери для забезпечення віддаленого доступу і виконання коду для функцій сервера. Вебоболонки дозволяють зловмисникам запускати команди на серверах для крадіжки даних або використовувати сервер як стартовий майданчик для інших дій, таких як крадіжка облікових даних, переміщення по внутрішній мережі, розгортання додаткових «корисних» навантажень.

Windows Management Instrumentation (WMI) бекдори

WMI – інфраструктура локального і віддаленного керування системою.

Може використовуватися:

- для отримання системної інформації;
- керування реєстром, файловою системою;

- виконання команд тощо. Інструментарій, що корисний для системних адміністраторів, не менш корисний і для зловмисників. Наприклад, може використовуватися для створення безфайлового бекдору на атакованому вузлі.

Це програми, що пишуться за допомогою *PowerShell* і мають дві особливості:

- ✓ відсутність файлів і відсутність процесу. Основний принцип полягає в тому, що код шифрується і зберігається у *WMI-об'єкті;*
- ✓ при дотриманні встановлених умов система автоматично запускає процес *PowerShell* для виконання бекдор-програми, а потім після виконання процес зникає.

Golden tickets – це технологія, що дозволяє зловмисникові мати повний і необмежений доступ до всього домену – всім комп'ютерам, файлам, папкам і, що найбільш важливо, самій системі контролю доступу, де управління доступом здійснюється за допомогою квитків *Kerberos,* що видаються користувачам службою розподілу ключів. Це дозволяє зловмисникові створювати квитки на їх видачу для всіх облікових записів в домені *Active Directory.*

Особливості APT-атак:

- ❖ *це завжди цілеспрямована атака.* Метою зазвичай виступає не конкретна людина або організація, а якийсь більш загальний сегмент (наприклад, фінансові установи) або однорідна група людей (постояльці готелю, вболівальники на стадіоні, пасажири круїзного лайнера);
- ❖ *це довгострокова атака.* Вона може тривати не один місяць до переможного кінця або втрати доцільності;

- *це добре фінансована атака.* Навіть банальний DDoS – витратна процедура, якщо відбувається тривалий час;
- *це багатостадійна атака.* В APT послідовно використовується кілька векторів і різних технік. Самі по собі вони можуть бути примітивні, цікаво саме їх поєднання. Наприклад, секретарці шлють фішингові листи, щоб скомпрометувати її корпоративний аккаунт і через неї (як від довіреної особи) відправити заражений документ на ноутбук шефа;
- *APT не зупиняють окремі інструменти безпеки (антивірус, файрвол, спам-фільтри, SIEM системи), і вона довго може залишатися непоміченою (в середньому до 200 діб).* Важливіше те, що аномальна поведінка мережі або окремих пристроїв зберігається, хоча при процедурних перевірках нічого підозрілого не буває;
- *в ході APT часто використовують просунуті техніки, що ефективно маскують їх компоненти від типових систем захисту (наприклад, reverse shell для обходу фаєрволу).*

ГЛАВА 6
Класифікація та приклади атак на ІТС

6.1. Таксономія та приклади кібератак
6.2. Мережеві атаки. Застосування бот-мереж
6.3. Сучасні типові атаки на ІТС

6.1. Таксономія та приклади кібератак

Атаки на інформаційні ресурси можна класифікувати за різними критеріями:

- *Класифікація за програмними цілями*
- *Класифікація за місцезнаходженням порушника*
- *Класифікація за механізмами реалізації атак*
- *Класифікація за зовнішніми проявами атаки*
- *Класифікація за використовуваними інструментальними засобами*
- *Класифікація за об'єктами атаки.*

За програмними цілями поділяють на:

- ❖ *порушення нормального функціонування об'єкта атаки (відмова в обслуговуванні);*
- ❖ *отримання контролю над об'єктом атаки (установка серверної частини системи віддаленого керування);*
- ❖ *отримання конфіденційної і критичної інформації (перехоплення мережевого трафіку і пошук у ньому інформації, що передається у відкритому вигляді);*
- ❖ *модифікація і фальсифікація даних (наприклад, зміна інформаційного наповнення вебсервера).*

За розміщенням атакуючого об'єкта відносно атакованого розрізняють локальні і віддалені атаки.

Під віддаленою атакою прийнято розуміти несанкціонований інформаційний вплив на ІТС, що здійснюється програмно по каналах зв'язку.

Об'єктом віддалених атак можуть бути:

- ⇨ *мережеве обладнання (маршрутизатори, комутатори, міжмережеві екрани);*
- ⇨ *кінцеві пристрої (сервери, робочі станції, принтери, IP-камери);*
- ⇨ *канали зв'язку (мережі, в тому числі і бездротові);*
- ⇨ *проміжні пристрої: ретранслятори, шлюзи, модеми;*
- ⇨ *підтримуюча інфраструктура ІТС;*
- ⇨ *програмне забезпечення;*
- ⇨ *персонал.*

За автоматизацією атаки розподіляються на:

- *мануальну;*
- *автоматизовану;*
- *автоматичну (вірусна).*

Мануальна атака (підглядання, збирання сміття, вилучення інформаційних носіїв, підміна положень вмикачів, режимів тощо) реалізується за прямою участю людини без використання будь-яких спеціальних засобів.

Автоматизована атака здійснюється за постійною участю оператора з використанням широкого спектра програмних і апаратних засобів.

Автоматична атака реалізується без участі людини і, як правило, з використанням спеціалізованих програмних засобів, функціонування яких базується на вірусних технологіях.

За характером впливу виділяють атаки:

- *активні;*
- *пасивні.*

У результаті ***активної*** атаки на ресурси ІТС здійснюється порушення функціональності та зміна конфігурації системи. До активних атак відносяться, наприклад, виведення з ладу комп'ютера або його операційної системи, спотворення відомостей в базах даних, руйнування програмного забезпечення комп'ютерів, порушення роботи ліній зв'язку і т. д. Активні атаки впливають на систему, змінюють її стан, а після свого завершення вони, як правило, залишають сліди. Наприклад, це може бути спотворення даних на сторінках вебсайта, додатки в системі будуть виконуватися неправильно, уповільнено або взагалі зависати, або в роботі системи з'являються незрозумілі сплески активності.

Пасивна атака спрямована переважно на несанкціоноване використання інформаційних ресурсів ІТС, не надаючи при цьому впливу на її функціонування. Пасивні атаки не порушують нормальну роботу системи: вони пов'язані зі збором інформації про систему, наприклад, вони можуть прослуховувати мережевий трафік або перехоплювати повідомлення, передані по лініям зв'язку. У багатьох випадках пасивні атаки не залишають слідів, тому їх дуже складно виявити, часто вони так і проходять непоміченими.

Основа для порівняння	Активна атака	Пасивна атака
ДІЯ	Намагається змінити системні ресурси або вплинути на їх роботу.	Намагається читати або використовувати інформацію з системи, але не впливає на системні ресурси.
МОДИФІКАЦІЯ ІНФОРМАЦІЇ	виникає	не відбувається
ШКОДА СИСТЕМІ	викликає пошкодження системи.	не завдає шкоди.
НА ЩО ВПЛИВАЄ	Цілісність і доступність	Конфіденційність
ОБІЗНАНІСТЬ	Суб'єкт (жертва) отримує інформацію про атаку.	Суб'єкт не знає про атаку.

Рис. 6.1. Порівняння активної та пасивної атак за дією

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

На практиці рідко зустрічається активна або пасивна атаки в чистому вигляді. Найчастіше атака включає підготовчий етап – етап збору інформації про цільову систему, а потім на основі зібраних даних здійснюється активне втручання в її роботу. До корисної для атакуючого інформації відносяться типи ОС і додатків, IP-адреси, номера відкритих портів, імена і паролі користувачів.

За використовуваним інструментальним засобом:

- *програмна;*
- *апаратна;*
- *нетипова.*

Програмна атака ґрунтується на використанні спеціальних програм, які завантажуються в комп'ютер-жертву.

Апаратна атака ґрунтується на різноманітних пристроях, які використовуються автономно, чи в поєднанні з іншою апаратурою для виконання відповідних функцій. Наприклад, в кімнаті для нарад може бути встановлений «жучок» для прослуховування конфіденційних розмов. Цей приклад є характерним для апаратної атаки.

Нетипова атака реалізується на підґрунті таких засобів, які не відносяться до апаратних або програмних, наприклад, фізичне руйнування компонентів системи, вплив на інфраструктуру тощо.

За механізмом впливу атаки можна поділити на:

1. Атаки на мережу

Атаки на мережу – отримання несанкціонованого доступу до внутрішньої мережі організації і переданих даним або порушення роботи мережі.

До цього типу атак відносяться:

- *Сканування портів* – здійснюється з метою виявлення доступних у мережі сервісів. У процесі сканування портів також зазвичай збираються банери – інформаційні повідомлення, що видаються службами у відповідь на встановлення з'єднання з метою з'ясування типу і версії програмного забезпечення.

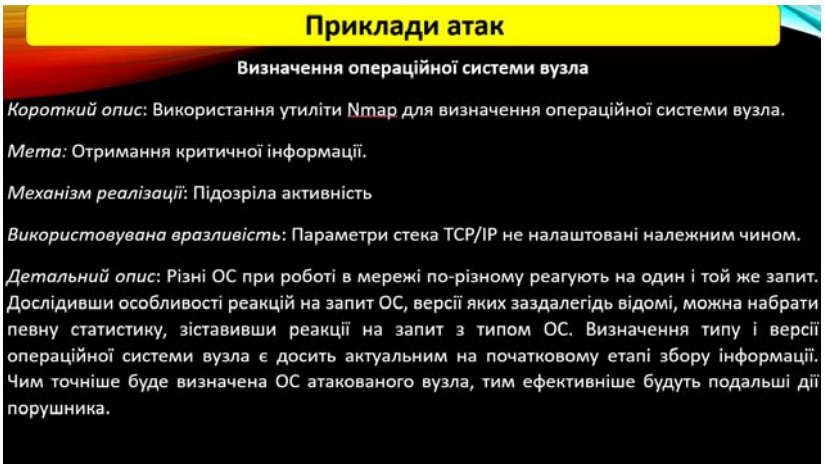


Рис. 6.2. Приклади атак визначення операційної системи вузла

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

✹ *Прослуховування мережі* – здійснюється з використанням програм-сніфферов на етапі збору даних про мережу і з метою крадіжки конфіденційної інформації. При цьому з боку порушника не проводиться жодних активних дій, а тому виявлення таких атак – складне завдання. У цьому випадку мета – побудувати карту мережі, зробити припущення про роль у мережі окремих вузлів, визначити встановлені на них операційні системи, перехоплення трафіку і подальший пошук у ньому конфіденційної інформації.

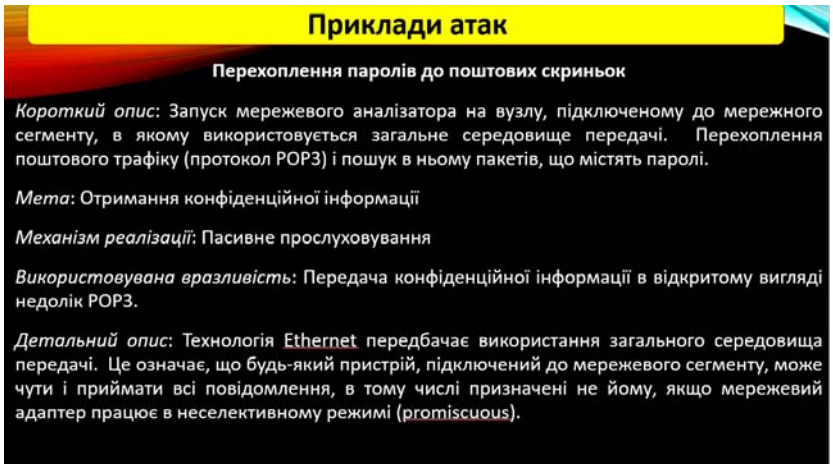


Рис. 6.3. Приклади атак перехоплення паролів до поштових скриньок

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

✹ *IP-спуфинг* – підміна адрес з метою отримати доступ до мережі від імені довіреної системи.

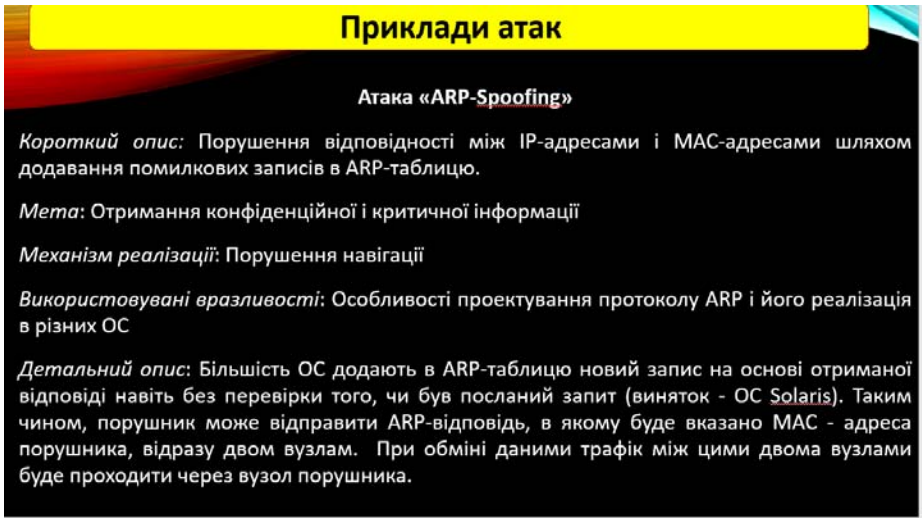


Рис. 6.4. Приклади атак «ARP-Spoofing»

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

✹ *Перехоплення з'єднання* – і подальша робота в ній від імені довіреної системи, яка з'єднання втрачає.

✹ *Повторна передача* – використання попередньо перехоплених у ході прослуховування даних для відправки в довірену мережу.

✹ *«Людина посередині».* Атака *«людина посередині» (Man-in-the-Middle – MITM)* – це форма кібератаки, при якій для перехоплення даних використовуються методи, що дозволяють впровадитися в існуюче підключення або процес зв'язку. Зловмисник може бути пасивним слухачем, що непомітно краде якісь відомості, або активним учасником, змінюючи зміст ваших повідомлень, або видаючи себе за людину або систему, з якими ви, на вашу думку, розмовляєте. Ця атака зазвичай використовується на ранніх етапах – під час розвідки, вторгнення і зараження. Зловмисники часто використовують атаки «людина посередині» для збору облікових даних і інформації про свої цілі.

✹ *«Відмова в обслуговуванні»* – блокування роботи мережевого сервісу за рахунок перевантаження його великою кількістю запитів або навмисним створенням ситуацій, що призводить до помилок програмного забезпечення. Такі атаки, як правило, реалізуються через безліч скомпрометованих систем.

Рис. 6.5. Приклади атак SynFlood

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

2. Атаки на програмне забезпечення

Атаки на програмне забезпечення – порушення роботи або несанкціоноване отримання контролю над операційною системою або прикладними програмами.

До цього типу атак відносяться:

✹ *Шкідливий код* – код, що заподіює шкоду комп'ютеру чи системі та виконує несанкціоновані дії. До цього виду засобів відносяться віруси, хробаки, троянські програми та ін. засоби. Наприклад, запуск серверної частини трояна, передача управління ворожої програмі шляхом переповнення стека,

виконання шкідливого мобільного коду, вбудованого в вебсторінку.

✹ *Атака на налаштування безпеки за замовчуванням* – використання вразливостей конфігурації за замовчуванням різних програмних засобів.

✹ *Зловживання привілеями* – використання наявних привілеїв для отримання доступу до конфіденційної інформації.

✹ *Використання помилок* в програмному забезпеченні – наприклад, переповнення буфера і некоректна обробка коду веббраузерами.

✹ *Атаки на паролі* – реалізуються у формі: вгадування і підбору за словником (dictionary attack), повного перебору (brute force). Атака може припускати доступ до бази ідентифікаційної інформації системи або реалізовувати підбор пароля зі спробою мережевого доступу до системи.

6.2. Мережеві атаки. Застосування бот-мереж

Мережеві атаки – дії, що спрямовані на отримання несанкціонованого доступу до ІТС, порушення штатного режиму її функціонування, порушення доступності її сервісів, порушення властивостей інформації і т. п. через комп'ютерні мережі.

Основні категорії мережевих атак:

✹ *Атака доступу;*

✹ *Атака модифікації;*

✹ *Атака на відмову в обслуговуванні;*

✹ *Атака на відмову від зобов'язань.*

Атака доступу

Атака доступу – це спроба отримання зловмисником інформації, для ознайомлення з якою у нього немає дозволу. Атака доступу спрямована на порушення конфіденційності інформації.

Підглядання (snooping) – атака, що передбачає віддалене таємне проникнення до системи з метою перегляду файлів або документів, щоб знайти потрібну зловмиснику інформацію.

Пасивне прослуховування мережі (sniffing) – атака, що перехоплює мережний трафік, призначений для інших вузлів, та здійснює його подальший аналіз. Якщо дані передаються по комп'ютерних мережах у незахищеному форматі (відкритим текстом), то зловмисник, який має доступ до каналу передачі даних, може перехопити конфіденційну інформацію (наприклад, імена користувачів і їх паролі).

Дана атака реалізується за допомогою спеціальних програм – ***сніферів (sniffer).***

Сніфер – це прикладна програма, яка використовує мережеву карту, що працює в нерозбірливому режимі ***(promiscuous mode),*** що дозволяє їй приймати всі пакети незалежно від того, кому вони адресовані (без перевірки MAC-адреси в заголовку прийнятого пакета).

Приклади програм: ***tcpdump, Wireshark, Microsoft Network Monitor, NetXRay, LanExplorer***. Сніфери можуть працювати в мережах на цілком законній підставі: вони використовуються для діагностики і аналізу трафіку, що дає змогу виявити паразитний, вірусний і закільцьований трафік; виявити в мережі шкідливе та несанкціоноване ПЗ (мережні сканери, флудери, троянські програми тощо).

Атака модифікації

Атака модифікації – спрямована на порушення цілісності інформації: *зміна даних, додавання даних, видалення даних.*

Перехоплення даних (hijacking). На відміну від прослуховування, перехоплення – це активна атака. Зловмисник перехоплює інформацію в процесі її передачі до місця призначення і використовує для своїх потреб.

Перехоплення сеансу (Session Hijacking) – з'єднання, встановлене законним користувачем, перемикається порушником на свій вузол, а серверу видається команда розірвати з'єднання з вузлом користувача.

Окрім цільових атак доступу на інформаційні ресурси існують і так звані рандомні атаки (хто попадеться на гачок невідомо).

Перехоплення браузера (browser hooking) – зловмисники розміщують на вебсайтах контент, який містить шкідливі скрипти (сценарії). Відкриваючи такий сайт рандомний користувач фактично запускає на своїй машині ці скрипти, що надає зловмисникові можливість контролю над браузером. Перехоплений у такий спосіб контроль над браузером користувача дозволяє зловмисникові використовувати його як відправну точку для подальших атак на інші системи, у тому числі внутрішні ресурси мережі й сервери компанії.

Атака на відмову в обслуговуванні (Denial-of-Service, DoS)

Атака на комп'ютерну систему, що має на меті зробити комп'ютерні ресурси недоступними для користувачів через перевищення припустимих меж функціонування мережі, операційної системи або додатка.

Жоден із серверів у мережі не здатен обробити дуже велику кількість звернень клієнтів, якщо ці звернення до нього приходять одночасно. Він починає спочатку гальмувати, а потім і зовсім стає недоступний, перестаючи відповідати на запити. Наприклад, реєстрація електронних кабінетів абітурієнта, на сайті МОН, який «завис» в перший день реєстрації. Відмова в обслуговуванні може наступити не тільки в результаті різкої флуктуації інтенсивності запитів, а й зловмисних дій, коли перевантаження створюється штучно, а саме: на сервер надсилається інтенсивний потік запитів, з метою зупинки його діяльность – це і є ***DoS***-атака. Ці атаки поділяються на ***локальні і віддалені.***

До локальних відносяться різні шкідливі програми, що відкривають по мільйону файлів або запускають якийсь циклічний алгоритм, який «з'їдає» пам'ять та процесорні ресурси. Таким чином, атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним.

Віддалені DoS-атаки поділяються на два види:

- віддалена експлуатація помилок в ПЗ з метою довести його до неробочого стану;
- Flood – посилка на адресу жертви величезної кількості пакетів. Метою флуду може бути канал зв'язку або ресурси машини.

Зловмисник може багаторазово посилити ефект від проведення такої атаки, якщо атака проводиться одночасно через безліч пристроїв на один і той же сервер і це вже розподілена атака на відмову в обслуговуванні ***DDoS (Distributed DoS)***. Для проведення потужної атаки зловмисник захоплює контроль над деякою кількістю комп'ютерів, організовує їх узгоджену роботу і направляє весь сумарний потік запитів з цих комп'ютерів на комп'ютер-жертву.

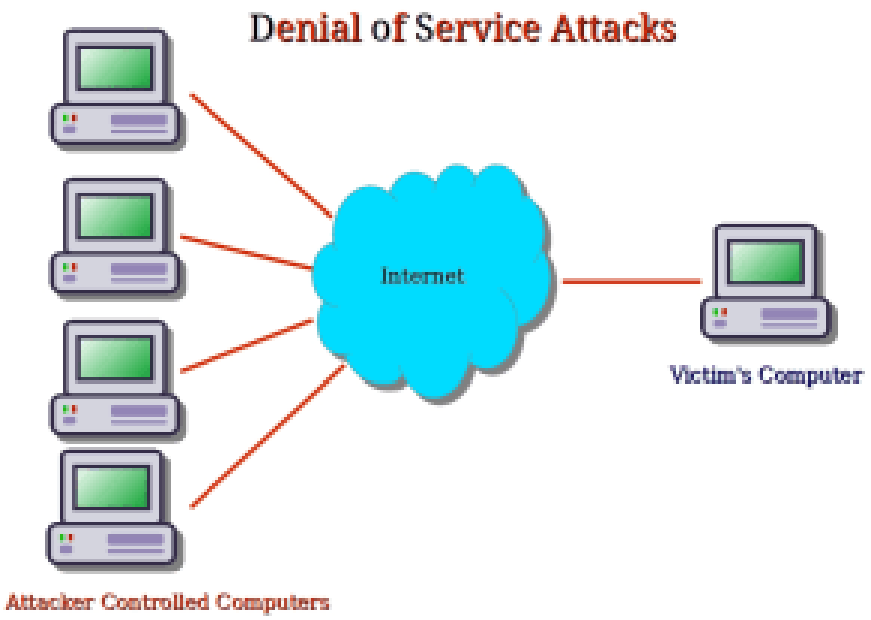


Рис. 6.6. Принцип DDoS-атаки

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

Атака *Smurf*

Принцип атаки полягає в посилці пакета ICMP ECHO REQUEST з адресою вузла, що атакується. Всі машини, отримавши запит, відповідають джерелу пакетом ICMP ECHO REPLY. Розмір відповідного потоку пакетів зростає в пропорційне кількості хостів число раз. У результаті вся мережа піддається відмови в обслуговуванні через перевантаження.

Принциповою відмінністю атаки є те, що вона не націлена на отримання доступу до мережі або на отримання з цієї мережі будь-якої інформації. Ця атака робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. По суті, ця атака позбавляє звичайних користувачів доступу до ресурсів мережі організації.

У цьому випадку вузли мережі над якими зловмисник здійснює свій контроль називаються ***зомбі-вузлами***, а вся мережа «зазомбованих», узгоджено працюючих вузлів – ***бот-мережею (botnet).***

Бот-мережа – це мережа комп'ютерів, заражених шкідливою програмою (*бот-програмою*), яка дозволяє кіберзлочинцям віддалено керувати зараженими машинами.

При цьому господар бот-мережі може централізовано управляти зараженими машинами – не має значення звідки: з іншого міста, країни або навіть з іншого континенту з одного сервера, так званого ***C2 сервера (C & C, Command and Control)*** з використанням технології ***Fast Flux.***

Ця технологія дозволяє кіберзлочинцям приховувати IP-адреси своїх серверів за допомогою маніпуляції параметрами DNS.

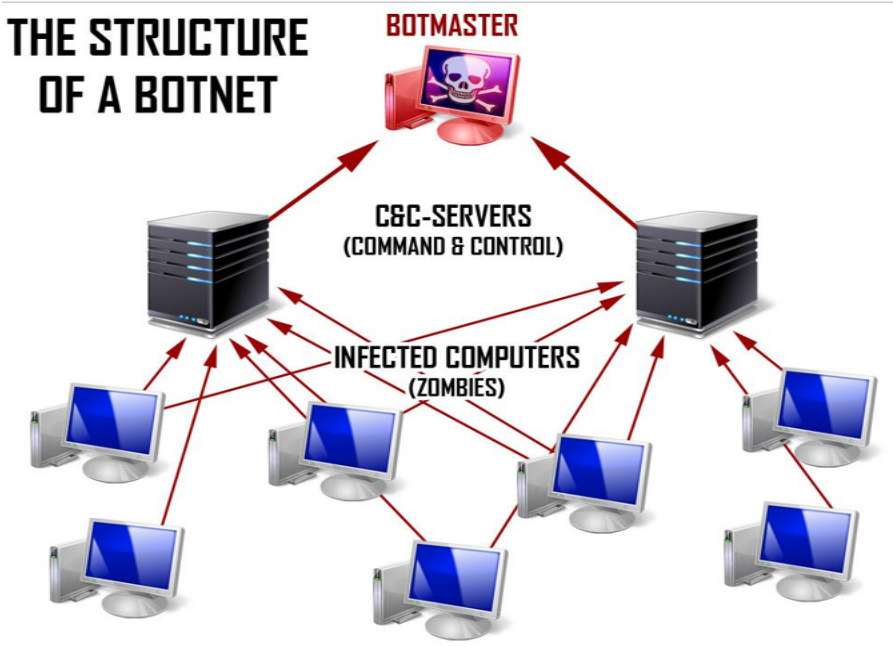


Рис. 6.7. Структура бот-мережі

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Бот-програма (бот) – це програма, яка виконує автоматичні (часто інтелектуальні) дії по командам віддаленого центру управління.

Зазвичай зловмисник заражає кодом бота кілька комп'ютерів, використовуючи відомі вразливості ОС і додатків, а потім вже код бота, подібно мережному хробаку, намагається заразити якомога більше машин.

Боти проникають у віддалені комп'ютери нелегально, так що користувач може не знати, що його комп'ютер заражений ботом. Сам бот не завдає особливої шкоди комп'ютеру, бо його цілі – інші комп'ютери десь у мережі. Саме тому заражені комп'ютери, що знаходяться під таємним контролем кіберзлочинців, називають ще ***зомбі-комп'ютерами***, а мережа, в яку вони входять, ***зомбі-мережею***.

Бот є програмним роботом, який може реагувати на ситуацію і отримані ззовні команди деякими діями – протоколюванням повідомлень, відправкою повідомлень, наприклад, підтриманням «розмови» з віддаленим співрозмовником або ж участю в ***DDoS-атаці*** на будь-який сайт або мережу. Бот може, наприклад, розпізнавати певний, заданий йому контекст в дискусії користувачів соціальних мереж Інтернету і стати її учасником, видаючи ті чи інші повідомлення. Бот зазвичай знаходиться в режимі спостереження, аналізуючи повідомлення і чекаючи команди з центру управління або виникнення заздалегідь певної ситуації. Є багато схожого у бота і механіко-електронного робота – обидва запрограмовані на сприйняття інформації з навколишнього світу, аналіз її на предмет виявлення певної ситуації і виконання заздалегідь запрограмованих дій.

Оскільки «господар» ботнету точно не знає, які саме машини виявилися зараженими кодом бота, для розпізнавання використовуються методи мережевого сканування, наприклад сканування портів, якщо код бота слухає певний порт TCP.

Застосування ботнетів. Ботнети можуть використовуватися зловмисниками для масованих атак: від розсилки спаму до підробки результатів пошукової системи та виконання масованих ***DDoS-атак***.

Розсилка спаму – це найбільш поширений і один з найпростіших варіантів експлуатації ботнетів. У результаті такої атаки користувачі отримують у значній кількості на свої електронні поштові скриньки повідомлення, які ними не очікувались та які містять інформацію рекламного та/або шахрайського характеру (реклама лікарського засобу та різноманітних послуг, прохання перейти за посиланнями тощо). Спам може створювати загрозу доступності інформації, блокуючи поштові сервери, або використовуватися для розповсюдження шкідливого програмного забезпечення.

Але, як показали дослідження, найбільша небезпека полягає в тому, що обробка СПАМу працівниками займає велику кількість робочого часу і загальні витрати на цю дію складають сотні мільйонів доларів.

За експертними оцінками, нині більше як 80 % спаму розсилається із зомбі-машин. Багатотисячні ботнети дозволяють спамерам здійснювати із заражених машин мільйонні розсилки впродовж короткого часу. Ще одна «перевага» ботнетів – можливість збору адрес електронної пошти на заражених машинах. Спам з ботнетів необов'язково розсилається власниками мережі. За певну плату спамери можуть взяти ботнет в оренду.

Анонімний доступ в мережу – зловмисники можуть звертатися до серверів у мережі, використовуючи зомбі-машини, і від імені заражених машин здійснювати кіберзлочини, наприклад зламувати вебсайти або переказувати вкрадені грошові кошти.

Крадіжка конфіденційних даних (ботнет-стіллери). Бот, яким заражені комп'ютери в зомбі-мережі, може запускати іншу шкідливу програму – ***стіллер.***

Стіллер – це шкідливе програмне забезпечення (троян), створене для крадіжки особистих даних (логіни, паролі, інформація про банківскі картки).

У такому разі інфікованими троянською програмою виявляться усі комп'ютери, що входять в цю *зомбі-мережу*, і зловмисники зможуть дістати паролі з усіх заражених машин. Вкрадені паролі перепродаються або використовуються, зокрема, для масового зараження вебсторінок (наприклад, паролі для усіх знайдених FTP-аккаунтів) з метою подальшого поширення шкідливої програми-бота і розширення зомбі-мережі.

Атака на відмову від зобов'язань

Атака спрямована проти можливості ідентифікації вхідної інформації за рахунок фальсифікації адреси відправника. Такий технічний прийом називається *спуфинг (spoofing),* коли зловмисник маскує себе за іншу особу, щоб дезорієнтувати пристрої в мережі або користувача з метою викликати довіру.

Спуфінг як технологія використовується і для *«замітання слідів»* при мережевих атаках.

Види спуфінгу:

- *IP-спуфінг* – має місце, коли зловмисник видає себе за законного користувача, за рахунок підміни свого реального IP-адреси на IP-адресу, що знаходиться для цієї організації в межах діапазону санкціонованих IP-адрес. Зловмисник може також використовувати спеціальні програми, що формують IP-пакети таким чином, щоб вони виглядали як вихідні з дозволених внутрішніх адрес корпоративної мережі (підміна IP-адреси відправника повідомлення іншою адресою);

- *ARP-spoofing* – підміна MAC-адрес;
- *e-mail-спуфинг* – підробка адреси відправника листів для маскування справжнього відправника;
- *Caller-ID-spoofing* – підміна номера абонента телефону в VoIP-мережах;
- *SMS-spoofing* – підміна номерів відправника SMS-повідомлення;
- *DNS-спуфинг (фарминг)* – зміна налаштувань сервера DNS, щоб переадресувати користувачів на шахрайські сайти, які маскуються під справжні.

6.3. Сучасні типові атаки на ІТС

Кібершантаж

Кібершантаж – атака, наслідками якої є блокування роботи комп'ютера, наприклад шляхом тотального шифрування файлів. За зупинку атаки зловмисники вимагають викуп.

Сьогодні багато компаній працюють тільки через Інтернет, і для них недоступність серверів означає повну зупинку бізнесу, що, природно, призводить до фінансових втрат. Щоб якнайшвидше повернути стабільність своїх серверів, такі компанії зазвичай готові виконати вимоги шантажистів. Саме на це і розраховують кіберзлочинці.

Виплата викупу не гарантує, що буде відновлений доступ до даних. Фактично, деякі люди або організації ніколи не отримували ключів для розшифровки після сплати викупу.

Деяким жертви, які оплатили вимогу повідомили, що знову стали мішенями. Після виплати необхідного викупу деяким жертвам було запропоновано заплатити більше, щоб отримати обіцяний ключ для розшифровки.

Рис. 6.8. Приклад дії атаки кібершантажу

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

Успіх атак вірусів-вимагачів на організації по всьому світу спонукає все більше нових зловмисників «вступити в гру».

Одним з таких нових гравців є група, яка використовує шифрувальник ***ProLock***. Він з'явився в березні 2020 р. Атаки шифрувальника ***ProLock,*** перш за все, націлені на фінансові та медичні організації, державні установи і сектор роздрібної торгівлі.

Розглянемо основні тактики, техніку і процедури (TTP), що використовуються операторами ***ProLock***. Для первинного доступу використовується троян ***QakBot***, що поширюється через фішингові листи. Фішинговий лист може містити прикріплений документ ***Microsoft Office*** або посилання на такий файл, що знаходиться в хмарному сховищі (***Microsoft OneDrive***).

Виконання

Після завантаження та відкриття зараженого документа користувачеві пропонується дозволити виконання макросів, у разі успіху здійснюється запуск ***PowerShell***, який дозволить завантажити і запустити корисне навантаження (а таким є ***ProLock)*** з командного сервера ***C2***. Важливо відзначити, що корисне навантаження витягується з файла ***BMP*** або ***JPG*** і завантажується в пам'ять за допомогою ***PowerShell.*** Це також можна ***розглядати як метод обходу захисту***.

Закріплення в системі

Для ***QakBot*** характерні різноманітні механізми закріплення. Найчастіше даний троян використовує розділ реєстру ***Run***.

Отримання облікових даних

QakBot володіє функціоналом кейлоггера. Крім цього, він може завантажувати і запускати додаткові скрипти для збору інформації.

Мережева розвідка

Після отримання доступу до привілейованих облікових записів оператори ***ProLock*** здійснюють мережеву розвідку, яка, зокрема, може включати в себе сканування портів і аналіз середовища ***Active Directory***.

Запуск

Запуск ***ProLock*** на хостах здійснюється за допомогою ***WMI (Windows Management Instrumentation).*** Даний інструмент також набуває все більшої популярності серед операторів програм-вимагачів.

Цільовий вплив

Далі ***ProLock*** шифрує і додає розширення ***.proLock, .pr0Lock*** або ***.proL0ck*** до кожного зашифрованого файла і поміщає файл [***HOW TO RECOVER FILES].TXT*** в кожну папку. Цей файл містить інструкції про те, як розшифрувати файли, включаючи посилання на сайт, де жертва повинна ввести унікальний ідентифікатор і отримати платіжну інформацію.

Рис. 6.9. Приклад дії програми-вимагача

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate

Платити чи не платити кіберзлочинцям при шантажі?

Якщо час на відновлення даних з резервних копій займає багато часу, а це може виявитися критичними для бізнесу, то слід заплатити. Однак є причини, які говорять про те, що це рішення може виявитися фатальним.

По-перше, немає ніякої гарантії, що після оплати кіберзлочинці перешлють ключ розшифрування, тому що це злочинці і у них відсутні звичні моральні принципи.

По-друге, зробивши платіж, організація продемонструє готовність платити і це може викликати нові атаки. Поки що універсального рецепта немає ***(2021, Colonial Pipeline, $ 2,3 млн).***

Кібершантаж стає сьогодні більш ризикованим, оскільки правоохоронні органи в усьому світі повели активну боротьбу з такими зловмисниками, та і компанії стали більш уважними до збереження своїх інформаційних ресурсів.

Зловмисники звернулися до менш ризикованих типів атак.

Кріптоджекінг (cryptojacking) – це впровадження в ПЗ комп'ютерів програми для майнінгу криптовалют за рахунок обчислювальних ресурсів інших людей без їх дозволу.

Майнінг – це процес виконання складних математичних обчислень, необхідних для ведення регістра блокчейна. Цей процес генерує монети, але вимагає значних обчислювальних ресурсів.

Деякі люди і організації інвестують в обладнання і електроенергію для законних операцій з видобутку монет. Однак інші шукають альтернативні джерела обчислювальної потужності і намагаються знайти свій шлях в корпоративні мережі для цього. Наприклад, зразок шкідливого програмного забезпечення, виявленого як троян: ***Win32/Coinminer,*** який майнить криптовалюту ***Monero.***

Оскільки мета кріптоджекінга – не крадіжка даних, а використання обладнання, то фізичні компоненти комп'ютера відчувають підвищене навантаження. У кращому випадку це призведе до уповільнення роботи, а в гіршому – до перегрівання процесора, раптового відключення системи і навіть пошкодження обладнання. В ідеалі користувач не підозрює про те, що обчислювальні потужності його пристрою йдуть на підтримку додаткового процесу.

Дефейс. Атака полягає у зміні змісту головної сторінки вебсайта, в результаті чого при його відвідуванні замість звичного контенту відображається щось інше (написи ***«Hacked By»,*** нецензурні або провокаційні фрази/малюнки тощо). Наприклад, як виглядала головна сторінка ФІТ після зламу.

Рис. 6.10. Приклад дії атаки дефейсу

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

Можна зробити ряд кроків, щоб пом'якшити наслідки атак або звести до мінімуму шанси атакуючих.

1. Оновлення ПО (патчінг). Головне завдання патчингу – це усунення вразливостей в ПЗ, але багато користувачів його ігнорують Оновлення ПЗ необхідно не тільки на робочих станціях, а й також на всіх мережевих вузлах і серверах. Класичний приклад того, у що вилилося зволікання з установкою патчів безпеки – поширення шифрувальника ***WannaCry.*** Він блокував роботу безліч організацій, незважаючи на те, що патч, що перешкоджає загрозам ***WannaCry***, був випущений за кілька місяців до появи цього шифрувальника.

2. Навчання персоналу. Мова йде про виконання правил кібергігієни, наприклад при роботі з електронною поштою. Основне правило: ні в якому разі не варто відкривати листи, отримані від невідомих відправників, і тим більше не потрібно натискати на посилання в таких листах. Варто остерігатися вкладень, оскільки це стандартний шлях до зараження шкідливим ПЗ.

3. Адміністрування доступу. Згідно з дослідженням близько третини атак здійснюється через підключення до віддаленого робочого столу ***(remote desktop protocol,***

RDP), шляхом злому аккаунтів користувачів і підбору паролів методом ***«грубої сили» (brute force).*** Зазвичай ці атаки проводяться зі залученням ботів, а оскільки багато хто не змінюють паролі, які були встановлені виробниками обладнання за замовчуванням, або ж вибирають комбінації, що легко вгадуються, атаки за допомогою ***«грубої сили»*** не втрачають актуальності.

Слід також уникати використання облікових записів з привілеями адміністратора. Більшість повсякденних завдань вирішується без прав «адміна» (це стосується і домашніх комп'ютерів).

4. Сегментація мережі. Щоб завдати максимальної шкоди, шкідливі програми поширюються на якомога більшу кількість комп'ютерів. Для запобігання поширенню потрібно провести сегментування мереж в організації, а також обмежити і додатково захистити облікові записи адміністраторів, які мають доступ до всієї інфраструктури.

5. Резервне копіювання. Важливим кроком захисту систем від атак є своєчасне резервне копіювання всієї критично важливої для бізнесу інформації.

6. Сканування і фільтрація пошти. Найпростіший спосіб убезпечити своїх співробітників від фішингових листів – зробити так, щоб вони ніколи не потрапили в їх поштову скриньку. Для цього потрібно застосовувати засоби сканування контенту і фільтрації пошти.

Нещодавно стали відомі деталі злому лабораторії реактивного руху ***NASA,*** яка робить космічні телескопи і марсоходи. Атакуючі використовували дешевий одноплатний комп'ютер на базі ***Raspberry Pi***, щоб потрапити у внутрішню мережу і отримати доступ до секретних даних місії на Марс та іншої інформації. Пізніше з'ясувалося, що у лабораторії було як мінімум три типи проблем кібербезпеки: з видимістю підключених пристроїв, сегментацією мереж і реагуванням на інциденти (в деяких випадках інциденти не обробляли по пів року).

ГЛАВА 7
Порушники безпеки

7.1. Порушники безпеки ІТС

Порушник – це особа, що зробила спробу виконання заборонених операцій (дій) помилково, по незнанню або усвідомлено зі злим умислом (з корисливих інтересів), або без такого (заради гри або самоствердження), навіть якщо вона є зареєстрований користувач системи.

Для порушників, які прагнуть завдати шкоди організації використовують термін «*зловмисник*», чим наголошують умисність здійсненого ним порушення, тоді як просто порушник може здійснювати порушення ненавмисно (наприклад, через необережність або недостатню обізнаність).

Порушник використовує для цього різні можливості, методи і засоби (агентурні методи отримання відомостей, технічні засоби перехоплення інформації без модифікації компонентів системи, штатні засоби та недоліки систем захисту, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм і т. п.).

Визначення переліку загроз і побудова моделі порушника є обов'язковим етапом проєктування системи захисту ІТС. Для кожної системи перелік імовірніших загроз безпеки, а також характеристика найбільш ймовірного порушника індивідуальні. Для досягнення своїх цілей порушник повинен докласти певних зусиль, витратити певні ресурси. Дослідивши причини порушень, можна вплинути на самі ці причини, або визначити вимоги до системи захисту від даного виду порушень чи злочинів. У кожному конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена модель порушника, яка повинна бути адекватна реальному порушнику для даної системи. Модель порушника відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії і т. п.

При розробці моделі порушника визначаються наступні припущення:

- *категорія осіб, до якої відноситься порушник;*
- *мотиви порушника;*
- *цілі порушника;*
- *кваліфікація і технічна оснащеність порушника;*
- *можливі дії порушника;*
- *час дії (постійно, в певні інтервали).*

Стосовно досліджуваної системі порушники можуть бути ***внутрішніми*** (з числа персоналу системи) або ***зовнішніми*** (сторонніми особами).

Внутрішнім порушником може бути особа з наступних категорій персоналу:

- *користувачі системи;*
- *персонал, що обслуговує технічні засоби (інженери, техніки);*
- *технічний персонал, що обслуговує будинки, (прибиральники, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення);*

- *співробітники служби безпеки;*
- *керівники різних рівнів посадової ієрархії.*

Співробітники підприємства забезпечують функціонування системи, її охорону і захист. У той же час вони, за певних обставин, можуть стати головним джерелом загрози для системи й інформації.

Сторонніми особами, які можуть бути порушниками, є:

- *клієнти;*
- *відвідувачі (запрошені з будь-якого приводу);*
- *представники організацій, що взаємодіють з питань забезпечення життєдіяльності організації (енерго-, водо-, теплопостачання);*
- *представники конкуруючих організацій, іноземних спецслужб, або особи, що діють за їх завданням;*
- *особи, що порушили пропускний режим;*
- *кримінальні структури.*

Зовнішній порушник може здійснювати НСД наступними способами:

▲ через автоматизовані робочі місця, підключені до мереж загального користування (наприклад, Інтернет);

▲ за допомогою програмного впливу на інформацію (програмні закладки, віруси та ін.);

▲ через елементи автоматизованої системи, які побували за межами контрольованої зони (наприклад, знімні носії інформації).

Злочинці мають свою мотивацію, їх зазвичай цікавлять цінні об’єкти (як віртуальні, так і фізичні). Доступ до об’єктів, наприклад, до портативних комп’ютерів – це ключовий момент при виявленні злочинців в якості загрози компанії.

Можна виділити кілька *основних мотивів вчинення порушень:*

- ➔ *безвідповідальність (некомпетентність, халатність, прагнення надати безкорисливу послугу приятелю з конкуруючої фірми);*
- ➔ *самоствердження, прагнення показати свою значимість;*
- ➔ *вандалізм;*
- ➔ *примус (прагнення убезпечити себе, рідних і близьких від загроз, шантажу, насильства);*
- ➔ *помста (прагнення завдати шкоди керівництву або колезі по роботі, а іноді державі);*
- ➔ *корисливий інтерес (прагнення отримати матеріальну вигоду, прагнення просунутися по службі тощо);*
- ➔ *ідейні міркування.*

Обставинами (передумовами), що сприяють появі цих причин, можуть бути:

- ✓ *важке матеріальне становище, фінансові труднощі;*
- ✓ *користолюбство, жадібність;*
- ✓ *схильність до розваг, пияцтва, наркотиків;*
- ✓ *заздрість, образа;*
- ✓ *невдоволення державним устроєм, політичне або наукове інакомислення;*
- ✓ *особисті зв'язки з представниками конкурента;*
- ✓ *невдоволення службовим становищем, кар'єризм;*
- ✓ *боягузтво, страх;*
- ✓ *марнославство, зарозумілість, завищена самооцінка, хвастощі.*

Цілі порушника:

- ***особиста авторизація, або авторизація інших осіб для одержання доступу до ресурсів ІТС з метою ознайомлення, модифікації, знищення, зміни режимів використання або загального функціонування системи;***
- ***проникнення на місця розміщення ресурсів ІТС шляхом подолання охорони або охоронної сигналізації;***
- ***одержання атрибутів доступу шляхом використання технічних засобів, крадіжок, купівлі, або іншим шляхом;***
- ***зміна режимів функціонування ІТС, її ресурсів та послуг системи;***
- ***установка програмних засобів копіювання інформації або модифікації системного програмного забезпечення з метою перевантаження систем і порушення, таким чином, доступності ресурсів ІТС.***

За рівнем знань порушників можна класифікувати наступним чином:

- ***знає функціональні особливості системи, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;***
- ***володіє високим рівнем знань і досвідом роботи з технічними засобами системи та їх обслуговування;***
- ***володіє високим рівнем знань в області програмування та обчислювальної техніки, проєктування і експлуатації автоматизованих інформаційних систем;***
- ***знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.***

За рівнем можливостей (використовуваним методам і засобам):

- *застосовує тільки агентурні методи отримання відомостей;*
- *застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);*
- *використовує тільки штатні засоби та недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії інформації, які можуть бути приховано пронесені через пости охорони;*
- *застосовує методи і засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).*

При розробці моделі порушника також розрізняють ***порушників за часом дії:***

- *в процесі функціонування системи;*
- *в період неактивності компонентів системи (в неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонту і т. п.).*

За місцем дії:

- *без доступу на контрольовану територію організації;*
- *з робочих місць кінцевих користувачів;*
- *з доступом в зону даних (серверів баз даних, архівів і т. п.);*
- *з доступом в зону управління засобами забезпечення безпеки АС.*

За характером дій порушників можна класифікувати на:

1. Випадкових порушників

Випадкові порушники – авторизовані користувачі, які порушили політику безпеки ненавмисно.

Завжди є ймовірність того, що хто-небудь відкриє фішинговий лист, або скопіює файл з конфіденційною інформацією на свій носій для роботи у відрядженні.

Причинами ненавмисного дестабілізуючого впливу на інформацію з боку людей можуть бути:

- *некваліфіковане виконання операцій;*
- *недбалість, безвідповідальність, недисциплінованість, несумлінне ставлення до виконуваної роботи;*
- *недбалість, необережність, неакуратність;*
- *фізичне нездужання (хвороби, перевтома, стрес, апатія).*

До обставин (передумов) появи цих причин можна віднести:

- *низький рівень професійної підготовки;*
- *зайву балакучість, звичку ділитися досвідом, давати поради;*
- *незацікавленість в роботі (вид роботи, її тимчасовий характер, зарплата), відсутність стимулів для її вдосконалення;*
- *розчарованість у своїх можливостях і здібностях;*
- *перезавантаженість роботою, терміновість її виконання, порушення режиму роботи;*
- *погане ставлення з боку адміністрації.*

2. Порушників-інсайдерів

Порушники-інсайдери – авторизовані користувачів, які порушили політику безпеки навмисно.

***3.* Локальних зловмисників,** які не є співробітниками і прагнуть перебороти засоби організаційного обмеження доступу та охоронної сигналізації і одержати можливість фізичного доступу до засобів обробки, зберігання і передачі інформації з метою виводу їх з ладу, крадіжки носіїв інформації та ін.;

4. Зловмисників, які використовують засоби віддаленого доступу до інформаційних ресурсів.

Зловмисники, яких слід брати до уваги:

- Службовці організації. Вони мають необхідний доступ і знання про системи в силу специфіки своєї роботи. Тут головне питання полягає в наявності мотивації.
- Колишні працівники. Вони також мають знання про системи. Залежно від процедур анулювання доступу, існуючих в організації, у них може зберегтися доступ до системи.
- Конкуренти завжди мають мотивацію для отримання конфіденційної інформації або для заподіяння шкоди залежно від умов конкуренції. Ці конкуруючі організації володіють деякими знаннями про компанії, оскільки діють в тій же області. При наявності відповідної уразливості вони можуть отримати необхідні відомості і здійснити доступ.
- Терористи також мають мотивацію для нанесення шкоди, їх дії зазвичай націлені на працездатність систем.
- Злочинці мають свою мотивацію, їх зазвичай цікавлять цінні об’єкти (як віртуальні, так і фізичні). Доступ об’єктів, наприклад, до портативних комп’ютерів – це ключовий момент при виявленні злочинців в якості загрози компанії.
- Компанії-постачальники послуг, клієнти, відвідувачі повинні розглядатися як можливе джерело загрози.

При побудові моделі потенційного порушника треба враховувати наступне:

1. Порушник може з'явитися в будь-який час і в будь-якому місці периметра системи.
2. Кваліфікація і обізнаність порушника може бути на рівні розробника даної системи.
3. Порушнику відома інформація про принципи роботи системи, включаючи секретну.
4. Для досягнення своїх цілей порушник вибирає найбільш слабку ланку в захисті.
5. Порушником може бути не тільки стороння особа, а й законний користувач системи.

На підставі даної моделі можуть бути сформульовані основні принципи побудови захисту ІС:

1. Необхідно побудувати навколо предмета захисту постійно діючий замкнутий контур захисту.
2. Властивості перепон, що становлять захист, повинні відповідати очікуваної кваліфікації та обізнаності порушника.
3. Для входу в систему законного користувача необхідна змінна секретна інформація, відома тільки йому.
4. Підсумкова міцність системи захисту визначається його слабкою ланкою.
6. Необхідно розмежовувати доступ користувачів до інформації відповідно до їх повноважень і виконуваними функціями.

7.2. Хакінг та етичний хакінг

Ключова ідея етічного хакінгу
«Знай ворога і знай себе і ти пройдеш сотню бійок без поразок».
Сунь Цзи
«Мистецтво війни»

Використання терміна ***«хакер»*** щодо порушників не є на наш погляд правильним рішенням. ***Хакер – не означає порушник***. Коли комп'ютери тільки з'явилися, слово «хакер»

було поважним. Його використовували для позначення комп'ютерних геніїв, здатних переписати частину ядра операційної системи, щоб вона стала краще працювати або «скинути» всіма забутий адміністраторський пароль.

Завдяки кіно, засобам масової інформації та художнім романам цей термін зараз набув негативного відтінку.

За своїм історичним походженням і до тепер термін «хакер» слід застосовувати до тих, хто добре розуміється на принципах роботи обчислювальних систем, особисто ПЗ і вміє виявляти вразливості систем.

Тобто *хакер* – це той, хто має високу кваліфікацію і знаходить вразливості системи.

Значна частина зловмисників не мають високої кваліфікації і вважати таких зловмисників хакерами некоректно. Для здійснення атаки їм достатньо знайти необхідний інструментарій та інструкції з його використання в Інтернеті, не розуміючи принципів його роботи. Деякі з них роблять це просто з цікавості, а інші намагаються продемонструвати свою майстерність і завдати шкоди. Вони можуть використовувати базові інструменти, але результати можуть бути руйнівними. За такими зловмисниками закріпилась назва – ***скрипт-кідді (Script Kiddies).***

Ось декілька визначень терміна ***«хакер»:***

1. Людина, що захоплюється дослідженням програмованих систем, вивченням питання підвищення їх можливостей.

2. Хто-небудь, хто програмує з ентузіазмом, або люблячий програмувати.

3. Експерт щодо певної комп'ютерній програми, або той хто часто працює з нею.

4. Експерт або ентузіаст будь-якого роду.

5. Той, хто любить інтелектуальні випробування, які полягають у творчому подоланні або обході обмежень.

6. Фахівець з комп'ютерної безпеки.

7. «Hacker. A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular». **RFC – 1983 Internet Users' Glossary**.

***Переклад**: Людина, якій подобається мати глибоке розуміння внутрішньої роботи системи, зокрема комп'ютерів і комп'ютерних мереж.*

DEF CON – найстаріший і один з найбільших зльотів хакерів. Конференція проводиться ОФІЦІЙНО, щороку, в Лас-Вегасі, а злочинці відкрито не збираються.
Я ХАКЕР!

Які бувають хакери?

1. ***Кібертерористи*** – хакери, які використовують свої навички в терористичних цілях (злом критичних систем, керуючих небезпечними виробництвами, deface для пропаганди ідей і цінностей тероризму та ін.).

Рис. 7.1. Хакер – кібертерорист

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

2. ***Кібервійська*** – хакери, які використовують свої навички в інтересах і під контролем держави. Вони фінансуються державою, здійснюють розвідку чи саботаж від імені свого уряду. Ці нападники, як правило, якісно підготовлені та добре фінансуються, а їх атаки зосереджені на корисних для їхнього уряду конкретних цілях.

Рис. 7.2. Хакери – кібервійська

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

3. ***Хактивісти*** – хакери, які використовують свої навички з метою просування політичних ідей, свободи слова, захисту прав людини та забезпечення свободи інформації.

Рис. 7.3. Хакери – хактивісти

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

4. ***Кіберзлочинці –*** хакери, метою яких є заподіяння шкоди.

Висококваліфіковані фахівці з IT, тобто хакери, дійсно можуть займатися зломом різноманітних систем не будучи порушниками та злочинцями. Це ланка професіоналів, що займаються зломом у рамках правового поля. Законним злом інформаційних систем може бути, коли зламують систему, що належить організації, з якою укладено письмову угоду про проведення аудиту або тестів на проникнення до системи. Це так званий ***«етичний хакінг»***.

Хакінг

Хакінг – дослідження комп'ютерних технологій і систем з метою глибокого і досконального розуміння їх устрою і принципів роботи, пошук недекларованих можливостей і функцій.

Рис. 7.4. Види хакінгу

Джерело: URL: https://www.netacad.com/courses/cybersecurity/network-security

Етичний хакінг – санкціонований власником системи процес пошуку вразливостей в безпеці цієї системи із застосуванням методів і технік професійного хакінгу, з метою підвищення захищеності даної системи.

Термін «етичний хакінг» є збірним і, як правило, має на увазі використання всіляких хакерських методик, тобто термін не означає якийсь один тип дослідження або діяльності по оцінці захищеності системи.

Тестування на проникнення – головний метод оцінки захищеності комп'ютерних систем або мереж засобами моделювання атаки зловмисника.

Тестування на проникнення – фактично тестовий злом системи. Результати тесту оформлюються у вигляді звіту.

Навіщо проводити тестування на проникнення?

1. Оцінка ефективності вжитих заходів безпеки для захисту від зовнішніх і внутрішніх загроз.
2. Оцінка стійкості систем (і) або додатка до найбільш поширених видів зовнішніх атак.
3. Внутрішня політика (тест на проникнення як інструмент впливу).

Крім тесту на проникнення є ще інші форми етичного хакінгу:

- ➔ аудит кібербезпеки;
- ➔ аналіз вразливостей;
- ➔ атестація інформаційної системи (це більше не форма аналізу захищеності, а форма оцінки відповідності).

Рис. 7.5. Складові етичного хакінгу

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

ЗВЕРНІТЬ УВАГУ! Ніяких чорних чи білих хакерів. Це журналістський штамп, розповсюджений в Україні.

У світі кібербезпеки є умовний поділ хакерів на групи. Професіоналів, що володіють глибокими знаннями в області ІТ і використовують їх для здійснення незаконної, шкідливої або деструктивної діяльності, займаються зломом ІТС, відносять до так званої групи ***«Black Hat»,*** а професіоналів, що займаються тестуванням систем на проникнення, тобто етичним хакінгом – до групи – «***White Hat».*** Існує ще одна група – ***«Gray Hat»,*** які зламують ІТС, але не використовують отриманий доступ або інформацію в будь-яких своїх цілях, а повідомляють про знайдену вразливість власнику ресурсу. Такі спеціалісти зазвичай тісно співпрацюють з компаніями-розробниками ПЗ і отримують за свої послуги гідну винагороду (наприклад ***Google,*** платить за надану інформацію про знайдені в їх продуктах вразливості і помилки).

Компанія *Huawei* також оголосила програму ***«bug bounty»*** (пошук вразливостей на *ОС Android* за винагороду), максимальна виплата в якій може досягати 200 тисяч євро. У *Huawei* пояснили, що хакеру, який претендує на максимальну суму, потрібно буде захопити пристрій під свій контроль таким чином, щоб жертві при цьому не довелося куди-небудь «клікати». При атаці з використанням серйозної вразливості допускається безпосередній контакт хакера з пристроєм.

Варто нагадати також, що *Apple* недавно підвищила максимальну винагороду за виявлення критичної вразливості в *iPhone* до 1 млн доларів. Компанія виплатить цю суму тому, хто зможе отримати віддалений доступ до ядра *iPhone* без будь-яких дій з боку користувача пристрою. Найбільша

виплата *Apple* за повідомлення про знайдену вразливість на сьогодні склала 200 тис. доларів. На щорічній конференції в Лас-Вегасі з безпеки в 2019 році американська корпорація заявила, що запрошує всіх бажаючих фахівців взяти участь у пошуку слабких місць в пристроях *Apple*, включаючи комп'ютери *Mac*. Розмір нагороди, які зможуть отримати хакери, буде залежати від серйозності виявлених вразливостей, які компанія згодом виправить, випустивши пакет оновлень для свого ПЗ.

6 квітня 2020 року дослідник Райан Пікрен опублікував звіти про те, що виявив сім вразливостей в браузері *Safari* і його движку ***Webkit,*** які дозволяли шкідливим вебсайтам віддалено включати камери *Mac, iPhone і iPad*. Пікрен повідомив про помилки компанію *Apple*. Вона виправила помилки і заплатила Пікрену 75 тис. доларів у рамках програми винагороди за знайдені вразливості.

У 2019 році *«ПриватБанк»* виплатив 512 тис. грн у вигляді винагороди хакерам його електронних сервісів, які допомогли усунути потенційні вразливості електронних систем. Премії отримали 127 хакерів, а з 2020 року *«ПриватБанк»* відкрив спеціальний сайт для мисливців за помилками, на якому вони можуть зареєструватися в програмі і отримувати гроші.

«Серед найпопулярніших банківських сервісів, таких як «Приват24» зараз знайти вразливості все складніше, але ми готові і далі платити реальні гроші за кожне підтверджене повідомлення!» – заявив керівник напряму кібербезпеки банку.

Контрольні запитання

1. Дайте визначення атаки на ІТС.
2. Як класифікуються атаки на ІТС?
3. Дайте характеристику основних фаз атаки.
4. Що таке ланцюг кібервбивства?
5. У чому полягають особливості APT-атак?
6. Що таке кібершантаж і як його запобігти?
7. Що таке кріптоджекінг і чому він небезпечний?
8. За якими признаками класифікуються кібератаки?
9. Що таке сніфінг?
10. Для чого використовують спуфінг?
11. Поясніть ідею DDoS-атак.
12. Що таке бот-мережа і для чого вона використовується?
13. Поясніть різницю між поняттями «порушник безпеки», «зловмисник», «хакер».
14. Як класифікуються порушники безпеки і хто такі внутрішні порушники?
15. Дайте визначення і назвіть складові етичного хакінгу.

Розділ 4. ТЕОРІЯ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ІТС

ГЛАВА 8
Технології та методи захисту ІТС

8.1. Сучасні технології захисту інформаційних ресурсів
8.2. Основні методи забезпечення безпеки ІТС
8.3. Комплексне обстеження ІТС (аудит безпеки ІТС)

8.1. Сучасні технології захисту інформаційних ресурсів

Під захистом інформаційних ресурсів розуміють діяльність, спрямовану на забезпечення безпеки ІТС у цілому, що дає змогу:

- унеможливити загрози;
- запобігти реалізації загроз;
- зменшити ймовірність завдання збитків від реалізації загроз.

Для того щоб забезпечити захист ресурсів ІТС і гарантувати економічно вигідне і безпечне використання цих ресурсів для електронного бізнесу повинні бути реалізовані ефективні *технології інформаційного захисту*. До них відносяться:

- *технології автентифікації для перевірки автентичності користувачів і об'єктів ІТС;*
- *технології аудиту і моніторингу;*
- *технології програмного захисту від шкідливого ПЗ, спаму та несанкціонованого доступу до ІТС;*
- *технології криптографічного захисту даних для забезпечення конфіденційності, цілісності та автентичності інформації;*
- *технології захисту корпоративних мереж і створення захищених каналів;*
- *технології виявлення і запобігання вторгнень в інформаційні системи;*
- *технології безпеки «хмарних» обчислень;*
- *розробка політики безпеки в організації і комплексний багаторівневий підхід до забезпечення захисту ІТС.*

Незважаючи на велику різноманітність по складу і напрямам використання ІТС, вони всі мають певні типові рівні, на яких вирішуються спільні для всіх систем завдання. Зазвичай розглядають чотири рівні.

1. Перший рівень – комунікаційне устаткування ІТС. Кабельні системи, бездротові точки доступу, повторювачі, мости, комутатори, маршрутизатори й модульні концентратори. Усі ці складові перетворилися з допоміжних компонентів ІТС на основні як за впливом на характеристики ІТС, так і за вартістю. Сьогодні комунікаційний пристрій може бути складним спеціалізованим комп'ютером, який потрібно конфігурувати, оптимізувати й адмініструвати.

2. Другий рівень – комп'ютерні системи, основа будь-якої ІТС, що створена стандартизованими комп'ютерними платформами (стаціонарні комп'ютери, ноутбуки, мобільні пристрої).

3. Третій рівень – операційні системи. Рівень операційних систем – відповідає за обслуговування апаратного та прикладного програмного забезпечення.

4. Четвертий рівень – прикладне програмне забезпечення (СУБД, офісні застосування, бухгалтерські програми, системи автоматизації колективної роботи, спеціально розроблені для кожної окремої ІТС програмні засоби, що реалізують специфічні для системи функції, і т. ін.). СУБД відповідає за зберігання та обробку даних. Іноді СУБД є центральним елементом ІТС (наприклад, облік товарів на складі), а іноді виконує допоміжні функції.

З точку зору захисту в ІТС виділяють три рівня:

Перший рівень – *програмно-апаратний.* Використовуються захисні засоби операційних систем, антивірусні пакети, засоби і пристрої локальної автентифікації користувача, засоби криптографічного захисту даних.

Другий рівень *– мережевий.* Захист ІТС на цьому рівні включає:

- *засоби мережевої автентифікації користувачів;*
- *засоби фізичного і програмного розмежування доступу до розподілених інформаційних ресурсів;*
- *засоби захисту домену локальної мережі;*
- *засоби проміжного доступу (Proxy Server) і міжмережеві екрани;*
- *засоби організації віртуальних локальних підмереж (Virtual Local Area Network – VLAN);*
- *засоби виявлення атаки і вразливостей в системі захисту мереж.*

Третій рівень *захисту ІТС – міжмережевий.* На третьому рівні захисту ІТС використовуються *VPN*-технології, технології електронного цифрового підпису та технології управління публічними ключами і сертифікатами криптографічного захисту (*Public Key Infrastructure – PKI*).

8.2. Основні методи забезпечення безпеки ІТС

Превентивні методи захисту інформації і систем її обробки можна поділити *на п'ять груп: правові, організаційні, інженерно-технічні, програмно-апаратні і криптографічні*.

1 група. Правові – законодавчі та морально-етичні методи захисту

Законодавчі. До цієї групи відносять чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, та регулюють інші питання використання ІТС. Законодавчі заходи захисту носять переважно попереджувальний, профілактичний характер і вимагають постійної роз'яснювальної роботи з користувачами і обслуговуючим персоналом ІТС, є стримуючим фактором для потенційних порушників.

Морально-етичні методи захисту – це норми поведінки персоналу, які не є обов'язковими, як вимоги нормативних актів, проте їх недотримання веде зазвичай до падіння авторитету або престижу людини, групи осіб або організації. Ці норми можуть бути неписані (наприклад чесність) або оформлені в якийсь статут правил.

2 група. Організаційні – організаційно-адміністративні та організаційно-економічні методи захисту

Організаційно-адміністративні заходи регламентують процеси функціонування ІТС, використання її ресурсів,

діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки.

Організаційно-адміністративні методи передбачають:

- ➔ *організацію спеціального документообігу;*
- ➔ *відведення спеціальних захищених приміщень і засобів захисту;*
- ➔ *використання зареєстрованих носіїв інформації.*

Організаційно-економічні методи охоплюють заходи зі стандартизації, методів і засобів інформації, сертифікації засобів ЕОТ згідно з вимогами кібернетичної безпеки, страхування інформаційних ризиків, ліцензування діяльності у сфері захисту інформації тощо.

3 група. Інженерно-технічні – технічні і фізичні засоби захисту

Технічні засоби – пристрої, що вбудовуються безпосередньо в обчислювальну техніку, або пристрої, які сполучаються з нею по стандартному інтерфейсу. Це різного роду механічні, електро- або електронно-механічні пристрої, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення функціювання компонентів ІТС, стихійних лих, саботажу, диверсій і т. ін.

Фізичні засоби включають різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту та здійснюють захист персоналу, матеріальних засобів і фінансів, інформації від протиправних дій. Приклади фізичних засобів: замки на дверях, грати на вікнах, засоби електронного охоронної сигналізації тощо.

4 група. Програмно-апаратні засоби захисту

Програмно-апаратні засоби захисту забезпечують ідентифікацію та автентифікацію користувачів, розмежування

доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІТС, захист від комп'ютерних вірусів, мережевих атак, проникнення до системи тощо.

Програмні засоби включають захисні інструменти операційних систем і прикладні програми, призначені для вирішення завдань безпеки.

Прикладом апаратних засобів, що спеціалізуються на інформаційному захисті, є джерела безперебійного живлення, генератори напруги, засоби контролю доступу в приміщення та ін.

5 група. Окремо виділяють ще засоби, що реалізують механізми криптографічного захисту інформації

Криптографічний захист (шифрування) – це перетворення інформації засноване на спеціальному алгоритмі, з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

До криптографічних засобів захисту відносяться: засоби шифрування, засоби імітозахисту – засоби, що реалізують можливості виявлення змін, імітації, фальсифікації або модифікації інформації, засоби електронного підпису.

Розглядаючи програмні засоби захисту, доцільно відмітити і стеганографічні методи захисту.

Стеганографія означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування.

Як правило, для захисту використовують всі перелічені види заходів. Систему таких заходів називають комплексною системою захисту інформації (КСЗІ). Створення КСЗІ є життєво необхідним для ІТС. У багатьох випадках обов'язковість створення КСЗІ визначається чинним законодавством.

Відеокамера і надійний замок в офісі, продумана процедура прийому співробітників на роботу, закон, що загрожує зловмиснику кримінальним переслідуванням, стандарт, що допомагає провести аналіз можливих збитків через дії порушника, – всі ці мало схожі між собою засоби однаково важливі для забезпечення безпеки.

КСЗІ має наступні рівні захисту

1. Рівень захисту від несанкціонованого доступу до ресурсів системи

На цьому рівні реалізовано такі механізми захисту:

- *ідентифікація;*
- *автентифікація;*
- *керування доступом;*
- *шифрування;*
- *контроль справжності інформації;*
- *знищення залишкових даних;*
- *захист від комп'ютерних вірусів.*

2. Рівень захисту від несанкціонованого використання ресурсів системи

На цьому рівні реалізовано:

- *контроль за виділенням ресурсів, квоти;*
- *контроль за складом програмних засобів ІТС;*
- *захист програм від копіювання, дослідження, модифікації та несанкціонованого запуску.*

3. Рівень захисту від некоректного використання ресурсів системи

На цьому рівні реалізовано такі механізми:

- *ізолювання ділянок оперативної пам'яті;*
- *підтримка цілісності та несуперечності даних;*
- *попередження користувача перед виконанням небезпечних дій.*

4. Рівень внесення інформаційної та функціональної надмірності

На цьому рівні здійснюються:

- ❖ *резервування інформації;*
- ❖ *тестування і самотестування системи в цілому та її елементів;*
- ❖ *відновлення і самовідновлення даних;*
- ❖ *дублювання компонентів.*

Сервіси рівня 1 і 2 захищають від несанкціонованих дій користувачів і програмних засобів, тобто здебільшого від реалізації навмисних загроз. Рівні 3 та 4 захищають від реалізації загроз, які були ненавмисно спричинені персоналом або виникли випадково.

8.3. Комплексне обстеження ІТС (аудит безпеки ІТС)

Ефективне управління питаннями забезпечення безпеки ІТС має принципове значення для існування будь-якого підприємства.

Для прийняття грамотних управлінських рішень в цій сфері і вироблення адекватних заходів, необхідно:

- ➔ *сформувати систему поглядів на проблему забезпечення безпеки ІТС та шляхи її вирішення з урахуванням сучасних тенденцій розвитку інформаційних технологій і методів і засобів захисту інформації;*
- ➔ *виробити єдину політику в галузі забезпечення безпеки ІТС;*
- ➔ *виявити загрози безпеки ІТС і оцінити можливі ризики;*
- ➔ *створити комплексну систему забезпечення захисту інформації (КСЗІ);*
- ➔ *скоординувати діяльність підрозділів по забезпеченню безпеки ІТС.*

При створенні будь-якої інформаційної системи на базі сучасних комп'ютерних технологій неминуче виникає питання про захищеність цієї системи від внутрішніх і зовнішніх загроз. Але перш ніж вирішити, як і від кого захищати інформацію, необхідно усвідомити реальний стан в області забезпечення безпеки ІТС на підприємстві та оцінити ступінь захищеності інформаційних активів. Для цього проводиться комплексне обстеження захищеності ІТС (або аудит безпеки), засноване на виявлених загрозах безпеки ІТС і наявних методах їх ліквідації, результати якого дозволяють:

- ➔ *оцінити необхідність і достатність вжитих заходів забезпечення безпеки ІТС;*
- ➔ *сформувати політику безпеки;*
- ➔ *правильно вибрати ступінь захищеності інформаційної системи;*
- ➔ *виробити вимоги до засобів та методів захисту;*
- ➔ *домогтися максимальної віддачі від інвестицій в створенні і обслуговуванні КСЗІ.*

Належний ефект при аудиті безпеки може дати тільки комплексний підхід до обстеження, коли відбувається перевірка достатності не тільки прийнятих програмно-апаратних та технічних заходів захисту, а й перевірка достатності інженерно-технічних, правових, економічних і організаційних заходів захисту (фізичного захисту, роботи з персоналом, регламентації його дій).

Комплексне обстеження дозволяє прийняти комплекс обґрунтованих управлінських рішень по забезпеченню необхідного рівня захищеності інформаційних активів підприємства.

Результатом аудиту можуть бути рекомендації щодо зміни інфраструктури систем, коли недоцільно або неможливо досягти необхідного рівня захищеності при існуючій інфраструктурі ІТС, хоча вона і є оптимальною для вирішення бізнес-завдань.

Таким чином, метою проведення робіт з комплексного обстеження захищеності ІТС є отримання об'єктивних даних про поточний стан забезпечення безпеки ІТС, що дозволяють

провести мінімізацію ймовірності заподіяння шкоди в результаті ймовірних атак, а також вироблення комплексу заходів, спрямованих на підвищення ступеня захищеності ІТС.

На різних етапах обстеження використовуються різні методи: технічні, аналітичні, експертні, розрахункові. При цьому, результати, отримані одними методами, можуть доповнюватися результатами, отриманими іншими методами.

Основними групами методів при обстеженні є:

- Експертно-аналітичні методи *передбачають перевірку відповідності обстежуваного об'єкта встановленим вимогам з безпеки на підставі експертної оцінки повноти і достатності поданих документів щодо забезпечення необхідних заходів захисту інформації, а також відповідності реальних умов експлуатації обладнання вимогам, що пред'являються по розміщенню, монтажу та експлуатації технічних і програмних засобів.*
- Експертно-інструментальні методи *передбачають проведення перевірки функцій або комплексу функцій захисту інформації за допомогою спеціального інструментарію і засобів моніторингу, а також шляхом пробного запуску засобів захисту інформації та спостереження реакції за їх виконанням.*
- Моделювання дій зловмисника *(«дружній злом» системи захисту інформації) застосовуються після аналізу результатів, отриманих в ході використання перших двох груп методів. Цим методом підтверджуються також реальні можливості потенційних зловмисників (як внутрішніх, легально допущених до роботи з тим або іншим рівнем привілеїв в ІТС, так і зовнішніх – у разі підключення ІТС до глобальних інформаційних мереж).*

Крім того, подібні методи можуть використовуватися для отримання додаткової інформації про об'єкт, яку не вдалося отримати іншими методами.

ГЛАВА 9
Теоретичні аспекти захисту ІТС


9.1. Моделі безпеки ІТС

Поняття безпеки ІТС може бути роз'яснено за допомогою так званих моделей безпеки.

Модель безпеки – абстрактний формалізований чи неформалізований опис політики безпеки. Модель безпеки використовують під час проєктування системи для визначення механізмів і алгоритмів захисту, а також під час аналізу захищеності системи для перевірки й доведення коректності та достатності реалізованих механізмів.

Суть моделей безпеки полягає в наступному: безліч всіх видів порушень безпеки поділяється на кілька базових груп таким чином, щоб будь-яке можливе порушення обов'язково можна було віднести принаймні до однієї з цих груп. Потім система оголошується безпечною, якщо вона здатна протистояти кожній з цих груп порушень. Найбільш популярні такі моделі безпеки:

- ***Тріада «Конфіденційність, Цілісність, Доступність» (КЦД)***
- ***Гексада Паркера***
- ***Модель S T R I D E***

а *б* *в*

Рис. 9.1. Моделі безпеки ІТС: а) Тріада «Конфіденційність, Цілісність, Доступність»; б) Гексада Паркера; в) Модель STRIDE

Джерело: URL: https://yztm.ru/lekc/l13/

Тріада «конфіденційність, цілісність, доступність» (КЦД)

Однією з перших моделей безпеки є модель, запропонована Зальцером і Шредером. Автори постулювали, що всі можливі порушення безпеки завжди можуть бути віднесені щонайменше до однієї з трьох груп: порушення конфіденційності, порушення цілісності або порушення доступності. Відповідно, інформаційна система знаходиться в стані безпеки, якщо вона захищена від порушень конфіденційності, цілісності і доступності.

Інформаційно-телекомунікаційні системи і середовище, в якому вони функціонують, зазнають змін, тому не дивно, що з'явилися нові типи порушень, які набагато складніше трактувати за допомогою тріади КЦД.

Розглянемо, наприклад, ситуацію, коли легальний клієнт банку надсилає електронною поштою запит на зняття з рахунку великої суми, а потім заявляє, що цей запит, який хоча і був посланий від його імені, він не відправляв.

Чи є це порушенням безпеки? Так.

Чи були при цьому порушені конфіденційність, доступність або цілісність? Ні.

Отже, список властивостей слід розширити, додавши до КЦД ще одну властивість – *«неспростовність»*.

Неспростовність (non-repudiation) – це такий стан системи, при якому забезпечується неможливість заперечення користувачем, що виконав будь-яку дію, факту їх виконання, зокрема щодо заперечення відправником інформації факту її відправлення та/або заперечення одержувачем інформації факту її отримання.

Дискусії про те, який набір властивостей ІТС, що характеризують її безпеку тривають, у результаті пропонуються все нові і нові моделі безпеки.

Гексада Паркера

Однією з альтернатив тріаді КЦД є так звана *гексада Паркера*, в якій визначено шість базових видів порушень, в число яких, крім порушень конфіденційності, доступності та цілісності, входять ще три види порушень: *автентичності, володіння і корисності.*

Автентичність (*authenticity)* – це стан системи, при якому користувач не може видати себе за іншого, а документ завжди має достовірну інформацію про його джерела. З цього визначення видно, що автентичність є аналогом неспростовності.

Модель STRIDE

Ще одним варіантом визначення безпеки є ***модель STRIDE*** (*абревіатура від англійських назв типів порушень безпеки, перерахованих нижче*). Згідно з цією моделлю ІТС знаходиться в безпеці, якщо вона захищена від таких типів порушень:

- ***підміни даних, зміни;***
- ***відмови від відповідальності;***
- ***розголошення відомостей;***
- ***відмови в обслуговуванні;***
- ***захоплення привілеїв***.

Модель STRIDE використовується компанією Microsoft при розробці безпечного програмного забезпечення.

Підміна *або «маскарад» (Spoofing)* – це використання чужих облікових даних для доступу до закритих активів, таке порушення, при якому користувач шляхом підміни, наприклад IP-адреси відправника, успішно видає себе за іншого.

Заміна *(Tampering)* – модифікація даних, порушення цілісності.

Відмова від відповідальності (Repudiation) являє собою негативну форму властивості неспростовності (non-repudiation).

Розголошення інформації *(Information disclosure)* – це порушення конфіденційності.

Відмова в обслуговуванні *(Denial of service)* стосується порушення доступності.

Захоплення привілеїв *(Elevation of privilege)* полягає в тому, що користувач несанкціонованим чином підвищує свої повноваження в системі (незаконне привласнення зловмисником прав адміністратора знімає практично всі захисні бар'єри на його шляху).

9.2. Особливості сучасних ІТС, з точки зору безпеки

Інформаційна система сучасної організації є досить складним утворенням, побудованим в багаторівневій архітектурі клієнт/сервер, яке користується численними зовнішніми сервісами і, в свою чергу, надає власні сервіси зовні. Навіть порівняно невеликі магазини, що забезпечують розрахунок з покупцями за пластиковими картками (і, звичайно, мають зовнішній вебсервер), залежать від своїх інформаційних систем і, зокрема, від захищеності всіх компонентів систем і комунікацій між ними.

Найбільш істотні аспекти сучасних ІТС

З точки зору безпеки найбільш істотними є наступні ***аспекти сучасних ІТС:***

- *корпоративна мережа має кілька територіально рознесених частин (оскільки організація розташовується на кількох виробничих майданчиках), зв'язки між якими знаходяться у веденні зовнішнього постачальника*

мережевих послуг, виходячи за межі зони, контрольованої організацією;

- *корпоративна мережа має кілька підключень до Internet;*
- *на кожній з виробничих майданчиків можуть знаходитися критично важливі сервери, в доступі до яких потребують співробітники, що працюють на інших майданчиках, мобільні користувачі і, можливо, співробітники інших організацій;*
- *для доступу користувачів можуть застосовуватися не тільки комп'ютери, а й пристрої, що використовують, зокрема, бездротовий зв'язок;*
- *протягом одного сеансу роботи користувачеві доводиться звертатися до кількох інформаційних сервісів, що спирається на різні апаратно-програмні платформи;*
- *до доступності інформаційних сервісів висуваються жорсткі вимоги, які зазвичай виражаються в необхідності цілодобового функціонування з максимальним часом простою порядку декількох хвилин;*
- *інформаційна система являє собою мережу з активними агентами, тобто в процесі роботи програмні компоненти, такі як аплети або сервлети, передаються з однієї машини на іншу і виконуються в цільовому середовищі, підтримуючи зв'язок з віддаленими компонентами;*
- *не всі користувальницькі системи контролюються мережевими або системними адміністраторами організації;*
- *програмне забезпечення, особливо отримане по мережі, не може вважатися надійним, у ньому можуть бути помилки, що створюють проблеми в захисті;*

- *конфігурація інформаційної системи постійно змінюється на рівнях адміністративних даних, програм і апаратури (змінюється склад користувачів, їхні привілеї та версії програм, з'являються нові сервіси, нова апаратура і т. п.).*

Слід враховувати ще принаймні два моменти.

По-перше, для кожного сервісу основні грані безпеки (доступність, цілісність, конфіденційність) трактуються по-своєму. Цілісність з точки зору системи управління базами даних і з точки зору поштового сервера – речі принципово різні. Безглуздо говорити про безпеку локальної або іншої мережі взагалі, якщо мережа включає в себе різнорідні компоненти. Слід аналізувати захищеність сервісів, що функціонують в мережі. Для різних сервісів і захист будують по-різному.

По-друге, основна загроза організацій як і раніше виходить не від зовнішніх зловмисників, а від власних співробітників.

9.3. Принципи побудови систем безпеки

З практичної точки зору найбільш важливими є наступні принципи безпеки:

- ➔ *безперервність захисту в просторі і часі;*
- ➔ *неможливість минати захисні засоби;*
- ➔ *дотримання визнаним стандартам, використання апробованих рішень;*
- ➔ *ієрархічна організація ІТС з невеликим числом сутностей на кожному рівні;*
- ➔ *посилення самої слабкої ланки;*
- ➔ *неможливість переходу в небезпечний стан;*

- ➔ *мінімізація привілеїв;*
- ➔ *поділ обов'язків;*
- ➔ *ешелонування оборони;*
- ➔ *розмаїтість захисних засобів;*
- ➔ *простота і керованість системи.*

Принцип безперервності захисту в просторі і часі

Принцип безперервності захисту передбачає, що захист інформації – це не разовий захід і навіть не певна сукупність проведених заходів та встановлених засобів захисту, а безперервний цілеспрямований процес, який передбачає прийняття відповідних заходів на всіх етапах життєвого циклу ІТС. Розробка системи захисту повинна здійснюватися паралельно з розробкою ІТС. Це дозволить врахувати вимоги безпеки при проєктуванні архітектури і, в кінцевому рахунку, створити більш ефективні захищені інформаційні системи.

Принцип неможливості минати захисні засоби

Якщо в зловмисника з'явиться така можливість минати захисні засоби, він, зрозуміло, так і зробить. Зазначені вище екрануючі сервіси повинні виключити подібну можливість.

Принцип дотримання визнаним стандартам, використання апробованих рішень

Слідування визнаним стандартам і використання апробованих рішень підвищує надійність ІТС і зменшує вірогідність попадання в тупикову ситуацію, коли забезпечення безпеки зажадає непомірно великих витрат і принципових модифікацій.

Ієрархічна організація ІТС з невеликим числом сутностей на кожному рівні

Ієрархічна організація ІТС з невеликим числом сутностей на кожному рівні необхідна з технологічних міркувань. При порушенні даного принципу система стане некерованою і, отже, забезпечити її безпеку буде неможливо.

Принцип посилення самої слабкої ланки

Надійність будь-якої оборони визначається найслабшою ланкою. Зловмисник не буде бороти проти сили, він віддасть перевагу легкій перемозі над слабістю.

(Часто самою слабкою ланкою виявляється не комп'ютер чи програма, а людина, і тоді проблема забезпечення кібербезпеки отримує нетехнічний характер).

Принцип неможливості переходу в небезпечний стан

Принцип неможливості переходу в небезпечний стан означає, що при будь-яких обставинах, у тому числі позаштатних, захисний засіб або цілком виконує свої функції, або цілком блокує доступ.

Принцип мінімізації привілеїв

Стосовно програмно-технічному рівню принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків. Цей принцип дозволяє зменшити шкоду від випадкових або навмисних некоректних дій користувачів і адміністраторів.

Принцип поділу обов'язків

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, щоб одна людина не могла порушити критично важливий для організації процес або створити пролом у захисті за замовленням зловмисників. Зокрема, дотримання даного принципу особливо важливо, щоб запобігти зловмисні чи некваліфіковані дії системного адміністратора.

Принцип ешелонування оборони

Принцип ешелонування оборони наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався.

За засобами фізичного захисту повинні впливати програмно-технічні засоби, за ідентифікацією й аутентифікації – керування доступом і, як останній рубіж, – протоколювання й аудит. Ешелонована оборона здатна, принаймні, затримати зловмисника, а завдяки наявності такого рубежу, як протоколювання й аудит, його дії не залишаться непоміченими.

Принцип розмаїтості захисних засобів

Принцип розмаїтості захисних засобів припускає створення різних за своїм характером оборонних рубежів, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками.

Принцип простоти і керованості системи

Дуже важливий принцип простоти і керованості інформаційної системи в цілому і захисних засобах особливо. Тільки для простого захисного засобу можна формально чи неформально довести його коректність. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснювати централізоване адміністрування.

9.4. Архітектурна безпека

Сервіси безпеки, якими б потужними вони не були, самі по собі не можуть гарантувати надійність програмно-технічного рівня захисту. Тільки перевірена архітектура здатна зробити ефективним об’єднання сервісів, забезпечити керованість інформаційної системи, її здатність розвиватися і протистояти новим загрозам при збереженні таких властивостей, як висока продуктивність, простота і зручність використання.

Теоретичною основою вирішення проблеми архітектурної безпеки є наступне фундаментальне твердження: *«Кожен процес, який діє від імені користувача,*

укладається всередині одного компонента і може здійснювати безпосередній доступ до об'єктів тільки в межах цього компонента. Кожен компонент містить свій монітор звернень, що відслідковує всі локальні спроби доступу, і всі монітори проводять в життя узгоджену політику безпеки. Комунікаційні канали, що зв'язують компоненти, зберігають конфіденційність і цілісність переданої інформації».

Три важливі принципи містяться в наведеному твердженні:

- *необхідність вироблення і проведення в життя єдиної політики безпеки;*
- *необхідність забезпечення конфіденційності і цілісності при мережевих взаємодіях;*
- *необхідність формування складових сервісів по змістовному принципом, щоб кожен отриманий таким чином компонент володів повним набором захисних засобів і з зовнішньої точки зору являв собою єдине ціле (не повинно бути інформаційних потоків, що йдуть до незахищених сервісів).*

Якщо будь-який сервіс не володіє повним набором захисних засобів, необхідне залучення додаткових сервісів, які ми будемо називати ***екрануючими***. Екрануючі сервіси встановлюються на шляхах доступу до недостатньо захищеним елементам. У принципі, один такий сервіс може екранувати (захищати) як завгодно велике число елементів.

Для забезпечення високої безперервності функціонування необхідно дотримувати наступні ***принципи архітектурної безпеки:***

- *внесення в конфігурацію тієї чи іншої форми надмірності (резервне обладнання, запасні канали зв'язку і т. п.);*

- *наявність засобів виявлення нештатних ситуацій;*
- *наявність засобів реконфігурування для відновлення, ізоляції та заміни компонентів, які відмовили або що піддалися атаці на доступність;*
- *розподіленість мережевого управління, відсутність єдиної точки відмови;*
- *виділення підмереж (сегментація мережі) і ізоляція груп користувачів один від одного. Дана міра, яка є узагальненням поділу процесів на рівні операційної системи, обмежує зону ураження при можливих порушеннях інформаційної безпеки.*

Ще один важливий ***архітектурний принцип – мінімізація обсягу захисних засобів,*** що виноситься на клієнтські системи. Причин тому кілька:

- *для доступу в корпоративну мережу можуть використовуватися споживчі пристрої з обмеженою функціональністю;*
- *конфігурацію клієнтських систем важко або неможливо контролювати.*

До необхідного мінімуму слід віднести реалізацію сервісів безпеки на мережевому і транспортному рівнях і підтримку механізмів аутентифікації, стійких до мережевих загроз.

Різноманіття варіантів побудови ІТС породжує необхідність створення різних систем захисту, що враховують індивідуальні особливості кожної з них.

Однак слід пам’ятати, ***що закон Мерфі*** актуальний і для проблем захисту інформації. Нагадаємо його зміст:

«Якщо будь-яка неприємність може трапитися, вона трапляється. Наслідки.

***1.** Все не так легко, як здається.*

***2.** Будь-яка робота вимагає більше часу, ніж ви думаєте.*

***3.** З усіх неприємностей станеться саме та, збиток від якої більше.*

***4.** Якщо чотири причини можливих неприємностей заздалегідь усунуті, то завжди знайдеться п'ята.*

***5.** Маючи змогу діяти самостійно, події мають тенденцію розвиватися від поганого до гіршого.*

***6.** Як тільки ви беретеся робити якусь роботу, знаходиться інша, яку треба зробити ще раніше.*

***7.** Будь-яке рішення плодить нові проблеми».*

Контрольні запитання

1. Назвіть сучасні технології захисту інформаційних ресурсів.
2. Назвіть основні методи забезпечення безпеки ІТС.
3. Дайте характеристику КСЗІ.
4. Для чого проводиться аудит безпеки ІТС?
5. Назвіть основні абстрактні моделі безпеки ІТС.
6. У чому полягають особливості сучасних ІТС з точки зору їх безпеки?
7. Назвіть основні принципи побудови систем безпеки ІТС.

Розділ 5. ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ЗАХИСТ ВІД РУЙНУЮЧИХ ПРОГРАМНИХ ДІЙ

ГЛАВА 10
КОМП'ЮТЕРНІ ВІРУСИ: КЛАСИФІКАЦІЯ ТА ХАРАКТЕРИСТИКА

10.1. Поняття та класифікація шкідливого програмного забезпечення

Велика група сучасних загроз пов'язана з розповсюдженням та впровадженням в комп'ютери шкідливих програм.

Шкідливі програми – це такий клас програм, які використовуються для здійснення несанкціонованого доступу до інформації та деструктивного впливу на інформацію, або ресурси інформаційної системи і які здатні викликати порушення дій комп'ютерів або комп'ютерної мережі, завдавати шкоди даним і ПЗ, або нейтралізувати засоби захисту інформації, займатись шахрайством, здирництвом та шпигувати за діями користувачів.

Деякі програми навіть можуть виконувати руйнівну функцію, тому їх називають ***руйнівними програмними засобами*** (*destructive software*).

Шкідливі програми можуть впливати на інформаційну систему наступними проявами:

- ➔ *викрадення конфіденційної інформації;*
- ➔ *надання порушникові доступу до ресурсів інформаційної системи;*
- ➔ *блокування користувацьких даних (вірус-вимагач блокує дані);*
- ➔ *перехоплення інформації, що вводиться з клавіатури (наприклад, при здійсненні операцій у різних онлайн-кабінетах). Саме з цієї причини, до речі, на багатьох сайтах, що приділяють серйозну увагу безпеці, рекомендується використовувати екранну клавіатуру;*
- ➔ *збір інформації про дії користувача;*
- ➔ *позаштатна поведінка встановленого в системі програмного забезпечення;*
- ➔ *різке зростання вхідного і вихідного трафіку і як наслідок уповільнення або повна відмова роботи комп'ютерної мережі.*

Корпорація ***Microsoft*** для визначення шкідливого ПЗ застосовує термін «***malware***»:

> ***«malware»*** *– це скорочення від malicious software, зазвичай використовується як загальноприйнятий термін для позначення будь-якого програмного забезпечення, спеціально створеного для того, щоб завдавати шкоди окремому комп'ютеру, серверу або комп'ютерної мережі незалежно від того, чи є воно вірусом, шпигунською програмою і т. п.*

Шкідливі програми можуть бути внесені (впроваджені) як навмисно, так і випадково в ПЗ із зовнішніх носіїв інформації або за допомогою мережевої взаємодії.

Втрати, викликані шкідливими програмами, можуть полягати не тільки в знищенні, спотворенні або викраденні інформації, приведення в неробочий стан програмного забезпечення, а значить, і комп'ютера в цілому, а й в значних витратах часу і сил адміністраторів на виявлення і розпізнавання атак, фільтрацію зовнішніх повідомлень, тестування і перезавантаження систем.

Перші шкідливі програми получили назву комп'ютерних вірусів, і протягом наступних десятиліть число вірусів значно перевищувала кількість всіх інших шкідливих програм разом узятих. Останнім часом з'явилися нові, невірусні технології, які використовують шкідливі програми, хоча такий термін, як «***зараження вірусом»,*** застосовуються щодо всіх шкідливих програм повсюдно. При цьому частка справжніх вірусів у загальній кількості інцидентів із шкідливими програмами за останні роки значно скоротилася.

Основними каналами поширення шкідливих програм є:

- *електронна пошта (заражені приєднані файли);*
- *телеконференції і електронні дошки оголошень у мережі Інтернет;*

- *вільне програмне забезпечення випадково або навмисно заражене вірусами;*
- *інформаційні ресурси, які містять посилання на заражені файли з елементами управління Active-X;*
- *локальні комп'ютерні мережі організацій;*
- *неліцензійні компакт-диски з програмним забезпеченням.*

Рис. 10.1. Канали поширення шкідливого ПЗ

Джерело: URL: https://zillya.ua/tipi-shkidlivikh-program-vid-trojan-do-rootkit

Хто і чому пише шкідливі програми?

Однією з головних причин, безумовно, є наявність достатньої кількості кваліфікованих програмістів, не обтяжених

морально-етичними нормами. Інша причина появи шкідливих програм взагалі є набагато серйознішою. Розробка, впровадження і поширення шкідливих програм стало невід'ємною частиною сучасної інформаційної зброї, яка, в свою чергу, стало породженням різних інформаційних воєн між конкуруючими державами, комерційними організаціями, суспільно-політичними групами і т. п. Очевидно, що ці причини появи шкідливих програм будуть мати місце протягом досить тривалого періоду часу.

Класифікувати шкідливі програми зручно *за способом проникнення, розмноження і типу шкідливого навантаження.*

За механізмами розповсюдження виділяють такі шкідливі програмні засоби:

- *комп'ютерні віруси;*
- *мережеві хробаки;*
- *трояни;*
- *люки, логічні бомби;*
- *спеціальні шкідливі програми.*

За способом проникнення шкідливе ПЗ поділяється на дві групи:

- *програми, що вимагають програм-носіїв;*
- *програми, що є незалежними.*

Програми, що вимагають програм-носіїв

До групи переважно відносяться фрагменти програм, що не можуть існувати незалежно від програм-носіїв, в ролі яких можуть виступати деякі програмні додатки, утиліти, системні програми. В цю групу входять:

- *люки, логічні бомби;*
- *трояни;*
- *віруси.*

Програми, що є незалежними

До цієї групи відносяться незалежні шкідливі програми, які можуть плануватися і запускатися операційною системою:

- *хробаки;*
- *утиліти прихованого адміністрування;*
- *шпигунські програми;*
- *шифрувальники файлів та програми-вимагателі;*
- *конструктори вірусів.*

Безфайлове шкідливе ПЗ

На сьогоднішні виділяють ще одну групу шкідливого ПЗ, так зване безфайлове шкідливе ПЗ. Можна навести такий приклад, коли цільова машина отримує шкідливі мережеві пакети, з ***експлойтом EternalBlue***. ***Експлойт EternalBlue*** використовує вразливість в реалізації мережевого протоколу ***Server Message Block (SMB)***. Вразливість дозволяє встановити ***backdoor DoublePulsar.*** Таку установку можна виконувати за допомогою командного рядка, не торкаючись файлової системи жертви. Зловмисник, сформувавши і передавши на віддалений вузол особливим чином підготовлений пакет, здатний отримати віддалений доступ до системи і запустити на ній довільний код.

Одним із найсучасніших видів шкідливого ПЗ є безфайлові шкідливі програми, які створюються на основі технології ***ROP (return oriented programing)*** – зворотно-орієнтоване програмування. При використанні цієї технології для створення шкідливого коду використовуються фрагменти інструкцій, що були знайдені в програмному забезпеченні, вже встановленому в системі (бібліотеки, модулі ОС, стеки оперативної пам’яті тощо).

Шкідливе програмне забезпечення являє собою постійно зростаючу загрозу не тільки через збільшення кількості шкідливих програм, а й через природу загроз. Це ПЗ все більше зосереджується на користувачах, змушуючи їх відвідувати заражені вебсторінки, встановлюючи шпигунське/шкідливе програмне забезпечення або відкриваючи електронні листи з шкідливим вкладенням.

10.2. Поняття та класифікація комп'ютерних вірусів

Під *комп'ютерним вірусом* прийнято розуміти програмний код, що добавляє свою копію в тіла інших програм, після чого ці програми стають «зараженими».

При запуску зараженої вірусом програми запускається вірус, який виконує задані його творцем функції, в число яких входить в першу чергу нанесення шкоди, а також подальше зараження інших програм. Прояви шкоди від вірусів можуть бути різноманітними – від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів з жорсткого диска. Поширюються віруси разом із зараженими програмами.

Тобто вірус – це програма, яка може створювати власні копії і таким чином самостійно розмножуватися. Шляхами проникнення вірусу можуть слугувати як мобільні носії, так і мережеві з'єднання – фактично, всі канали, за якими можна скопіювати файл. Зараження вірусом можливо, якщо користувач сам якимось чином його активував. Наприклад, скопіював або отримав поштою заражений файл і сам його запустив або просто відкрив.

*У **1982** році **15**-річний школяр з Пенсильванії Рік Скрента **(Rich Skrenta)** написав **Elk Cloner** – самовідтворюваний завантажувальний вірус, який інфікував **Apple II** через гнучкий магнітний диск. Під час кожного **50**-го перезавантаження ПК з'являлося повідомлення зі словами: «Він заволодіє вашими дисками, він заволодіє вашими чіпами. Так, це **Cloner!** Він прилипне до вас як клей, він вселиться в пам'ять. **Cloner** вітає вас!». Цей вірус поклав початок вірусної епохи в кіберпросторі.*

Віруси можна розділити на класи за такими основними ознаками:

- середовище проживання;
- операційна система;
- особливості алгоритму роботи;
- деструктивні можливості.

Залежно від середовища існування віруси можна розділити на:

- **файлові** – впроваджуються в виконавчі модулі програм *(* COM, *.EXE, *.SYS, *.BAT, *.DLL*), що дозволяє їм активуватися в момент запуску програми, впливаючи на її функціональність;
- **завантажувальні, або бутові** (англ. *boot* – початкове завантаження), віруси активуються у момент завантаження системи;
- **макровіруси** – заражають файли, які допускають включення в ці файли так званих макросів;
- **скриптові** – вбудовуються в HTML-документи, і запускаються браузером, причому не тільки з віддаленого сервера, а й з локального диска.

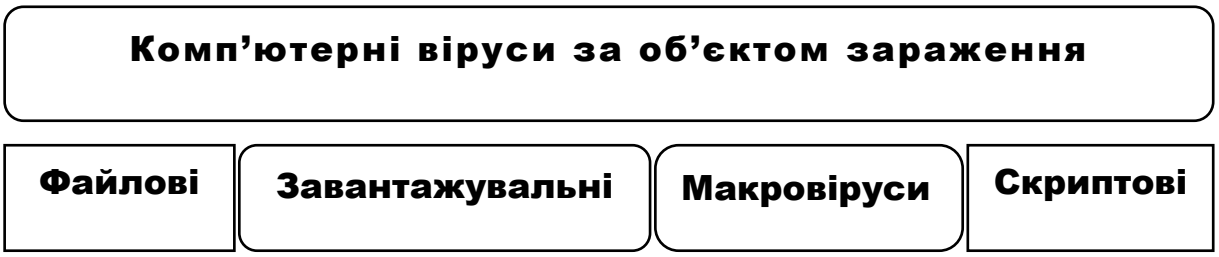


Рис. 10.2. Комп'ютерні віруси за середовищем існування

Джерело: URL: https://zillya.ua/tipi-shkidlivikh-program-vid-trojan-do-rootkit

Існує велика кількість сполучень, наприклад ***файлово-завантажувальні віруси,*** що заражають як файли, так і завантажувальні сектори дисків, або ***мережний макровірус***, який не тільки заражає документи, а й розсилає свої копії по електронній пошті.

Для вірусів характерна жорстка прив'язка до операційної системи, для якої кожен конкретний вірус був написаний. Це означає, що вірус для ***Microsoft Windows*** не працюватиме на комп'ютері з іншою встановленою операційною системою, наприклад ***Unix.*** Точно також макровірус для ***Microsoft Word*** швидше за все не буде працювати в додатку ***Microsoft Excel***.

Серед особливостей алгоритму роботи вірусів виділяються ***резидентність***. Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження і впроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними, аж до виключення комп'ютера або перезавантаження ОС. Резидентними можна вважати макровіруси, оскільки вони також присутні в пам'яті комп'ютера протягом всього часу роботи зараженого редактора.

За алгоритмом дії файлові віруси діляться на:

1. Перезаписуючі (overwriting).

Вірус записує свій код замість коду файла, знищуючи його вміст. Природно, що при цьому файл перестає працювати і не відновлюється.

2. Паразитичні (parasitic).

Віруси, які при поширенні своїх копій обов'язково змінюють вміст файлів, залишаючи самі файли при цьому повністю або частково працездатними. При зверненні до інфікованої програми спочатку запускається код вірусу, а потім і сама програма.

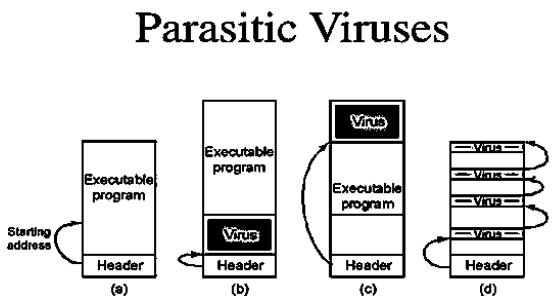


Рис. 10.3. Принцип інфікування паразитичним вірусом

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

3. Компаньон-віруси (companion).

Віруси, що не змінюють файлів, але для файлів створюється файл-двійник, причому при запуску зараженого файла управління отримує саме цей двійник, тобто вірус. Наприклад, файл ***NOTEPAD.EXE*** перейменовується в ***NOTEPAD.EXD***, а вірус записується під ім'ям ***NOTEPAD.EXE.*** При запуску управління отримує код вірусу, який потім запускає оригінальний ***NOTEPAD.***

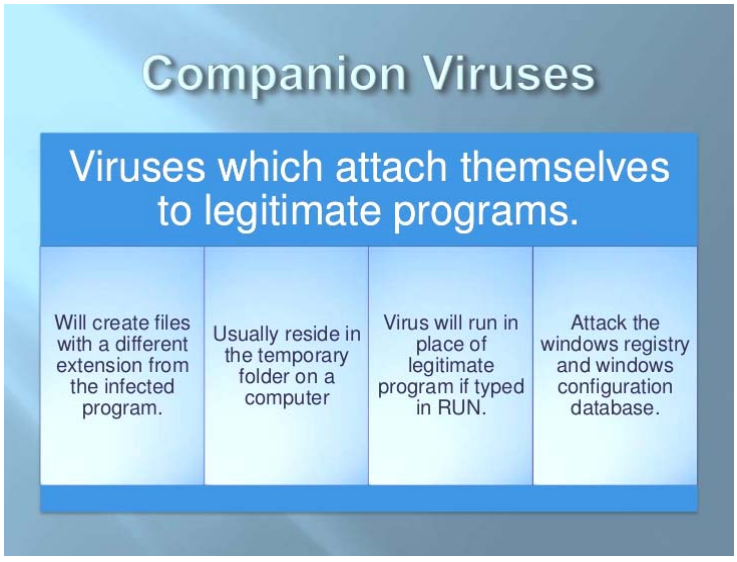


Рис. 10.4. Принцип дії компаньон-вірусів

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

4. Стелс-віруси.

Стелс-віруси – це віруси, які приховують вироблені ними зміни в системі.

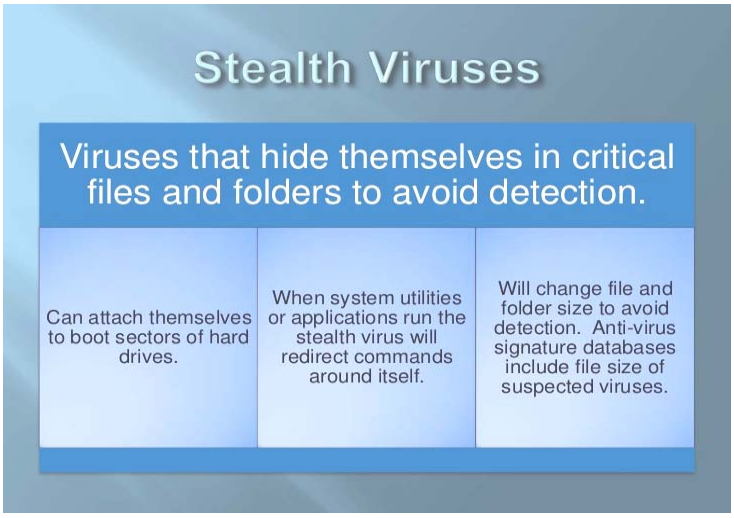


Рис. 10.5. Принцип дії стелс-вірусів

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

5. Поліморфні віруси.

Поліморфні віруси створюють різні робочі копії самих себе. Складові частини поліморфного вірусу можуть відрізнятися при кожному новому зараженні, що досягається шифруванням основного тіла вірусу. Кожна копія вірусу складається з шифратора, випадкового ключа й властиво вірусу, зашифрованого цим ключем. Це робить дуже складним його пряме виявлення за допомогою сигнатур і антивірусного програмного забезпечення.

6. Метаморфний вірус.

Метаморфний вірус – вірус, що застосовує метаморфізм до всього свого тіла для створення нових копій. ***Метаморфізм*** – створення різних копій вірусу шляхом заміни блоків команд на еквівалентні, перестановки місцями шматків коду, вставки між значущими шматками коду «сміттєвих» команд, які практично нічого не роблять.

За деструктивним можливостям віруси можна розділити на:

- нешкідливі або безпечні, які не впливають на роботу комп'ютера (крім зменшення вільної пам'яті на диску) і проявляють себе якимось графічними, чи звуковими ефектами;
- небезпечні віруси, які можуть призвести до серйозних збоїв у роботі комп'ютера;
- дуже небезпечні – в алгоритм їх роботи свідомо закладені процедури, які можуть викликати втрату програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію.

10.3. Коротка характеристика вірусів

Файлові віруси

Файлові віруси для свого розповсюдження використовують файлову систему. При зараженні файла вірус записує свій код в початок, середину або кінець файла, або відразу в кілька місць. Вихідний файл змінюється таким чином, що після відкриття зараженого файла управління негайно передається коду вірусу.

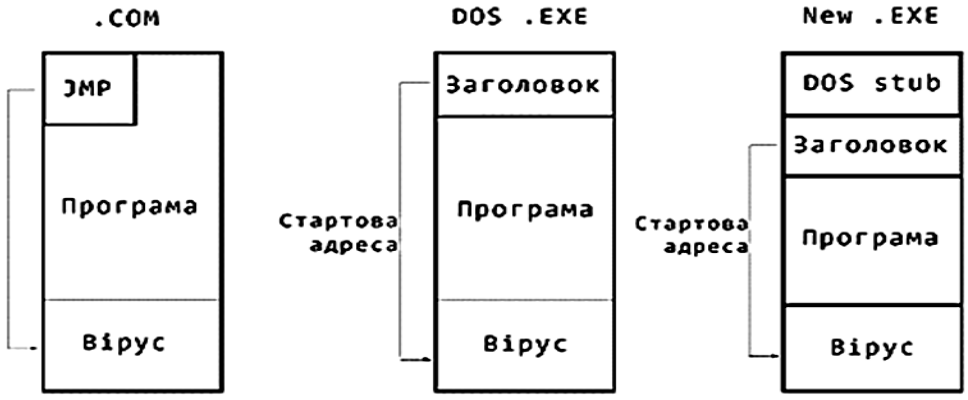


Рис. 10.6. Файлові віруси

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Після одержання керування код вірусу виконує наступну послідовність дій:

1) заражає інші файли;
2) встановлює в оперативній пам'яті власні резидентні модулі;
3) виконує інші дії, що залежать від реалізованого вірусом алгоритму;
4) продовжує процедуру відкриття файла.

Завантажувальні віруси

Завантажувальні віруси записують себе або в завантажувальний сектор диска ***(boot-сектор)***, або в сектор, що містить системний завантажувач ***(Master Boot Record),*** або змінюють покажчик на активний ***boot-сектор.*** Вірус або порушує роботу завантажувача операційної системи, що призводить до неможливості її завантаження, або змінює файлову таблицю носія з тим, щоб припинити доступ системи до файлів певного типу. При завантаженні ОС системний завантажувач зчитує інформацію з носія, розміщає зчитану інформацію в пам'ять і передає на неї (тобто на вірус) управління. Надалі завантажувальний вірус поводиться так само, як файловий: перехоплює звернення ОС до дисків і інфікує їх, залежно від встановлених умов здійснює спеціальні (іноді деструктивні) дії і може виконувати звукові або відеоефекти. Бутові віруси впроваджуються в пам'ять комп'ютера при завантаженні з інфікованого диска, тому завжди є резидентними. На жорсткому диску бутові віруси можуть дуже ефективно протидіяти антивірусним засобам, оскільки саме віруси стартують першими, ще до запуску операційної системи, і тому вони здатні залишити за собою керування критичними для їх існування ресурсами комп'ютера, зокрема, файловою системою.

Приклади. Шкідлива програма ***Virus.Boot.Snow*** записує свій код в MBR жорсткого диска. Після отримання управління вірус залишається в пам'яті комп'ютера (резидентність) й іноді проявляє себе візуальним ефектом – на екрані комп'ютера починає падати сніг.

Макровіруси

Макровіруси є програмами на макромові, що вбудовується в системи обробки даних (текстові редактори, електронні таблиці і т. п.). Для свого розмноження такі віруси використовують можливості макросів і з їх допомогою переносяться з одного зараженого файла (документа або таблиці) в інші. Найбільшого поширення набули макровіруси для програм ***Microsoft Office***, які застосовують автомакрос, перевизначають стандартні системні макроси (наприклад, ***FileSave),*** записують себе до групи глобальних макросів або автоматично запускаються після виконання певної умови. Отримавши керування, макровірус впроваджує свій код в інші файли, частіше у відкриті для редагування, рідше самостійно шукає файли на диску. При виході з ***Word*** глобальні макроси (включаючи макроси вірусу) автоматично записуються в ***DOT-файл*** глобальних макросів (зазвичай це ***NORMAL. DOT***). Таким чином, при наступному запуску ***Word*** вірус активізується в той момент, коли ***WinWord*** вантажить глобальні макроси, тобто відразу.

Макровіруси можуть заражати комп'ютери з любою ОС, якщо на даному комп'ютері встановлено текстовий редактор, повністю сумісний з ***MicrosoftWord*** (наприклад, ***MSWordfor-Macintosh***).

Відновлення файлів-документів і таблиць

Для відновлення документів, створених в ***Microsoft Office*** і знешкодження макровірусів досить зберегти всю необхідну інформацію в форматі ***RTF***, який не містить макросів. Потім слід вийти з ***Word*** або ***Excel***, знищити все заражені

Word-документи, ***Excel-таблиці***, ***NORMAL.DOT*** у ***Word*** і всі документи/таблиці в ***StartUp***-каталогах ***Word*** і ***Excel***. Після цього слід запустити ***Word*** або ***Excel*** і відновити документи/таблиці з ***RTF-файлів***. У результаті цієї процедури макровірус буде видалений з системи, а практично вся інформація залишиться без змін.

Однак цей метод має ряд недоліків. ***Основний з них*** – трудомісткість конвертування документів і таблиць в ***RTF***-формат, якщо їх число велике. До того ж у разі ***Excel*** необхідно окремо конвертувати все: ***Листи*** (***Sheets***) в кожному ***Excel-файл***. ***Другий недолік*** – втрата невірусних макросів, використовуваних при роботі. Тому перед запуском описаної процедури слід зберегти їх вихідний текст, а після знешкодження вірусу відновити необхідні макроси в первісному вигляді.

Скриптові віруси

Скриптові віруси розглядають як підгрупу файлових вірусів. Такі віруси пишуть різними мовами сценаріїв (***VBS, JS, BAT, PHP*** тощо). Вони можуть заражати інші програми-сценарії (командні та службові файли), бути компонентами багатокомпонентних вірусів, заражати файли інших форматів (наприклад, ***HTML***), якщо вони підтримують виконання сценаріїв.

Ознаки зараження ІТС вірусами

Кілька ознак зараження ІТС вірусами:

- ➔ *припинення роботи або неправильна робота програм, які раніше функціонували успішно;*
- ➔ *неможливість завантаження операційної системи;*
- ➔ *зменшення вільного обсягу пам'яті;*
- ➔ *уповільнення роботи комп'ютера;*
- ➔ *затримки під час виконання програм, збої в роботі комп'ютера;*
- ➔ *раптове збільшення кількості файлів на диску;*
- ➔ *зникнення файлів і каталогів;*

- ➔ *незрозумілі зміни у файлах;*
- ➔ *зміни дати і часу модифікації файлів без очевидних причин;*
- ➔ *незрозумілі зміни розмірів файлів;*
- ➔ *видача непередбачених звукових сигналів;*
- ➔ *виведення на екран непередбачених повідомлень або зображень.*

ГЛАВА 11
Шкідливе програмне забезпечення


11.1 Мережеві хробаки
11.2. Троянські програми
11.3. Спеціальні шкідливі програми

11.1. Мережеві хробаки

Мережеві хробаки (networm) – програми, що інфікують комп'ютери та здатні самотужки, без будь-якого втручання користувача, розповсюджуватися у комп'ютерній мережі, забезпечуючи щонайменше дві функції: передавання свого програмного ходу на інший комп'ютер і запуск свого програмного коду на ньому.

Ці шкідливі програми також здатні до створення власних копій, але, як правило, використовують цю можливість для розповсюдження по комп'ютерній мережі. Тобто така шкідлива програма не створює на одному комп'ютері безліч власних копій, (вірус може це робити), а створює свої копії на раніше не заражених вузлах мережі. Крім того, на відміну від комп'ютерних вірусів більшість хробаків не використовують як носій код іншої програми, це самостійні програми.

Хробак – це окремий файл, у той час як вірус – це код, який впроваджується в існуючі файли.

Мережеві хробаки можуть кооперуватися з вірусами – така пара здатна самостійно поширюватися по мережі (завдяки хробаку) і в той же час заражати ресурси комп'ютера (функції вірусу).

Мережеві хробаки шукають комп'ютери в глобальної або локальної мережі, підключаються до них і намагаються скопіювати себе в каталоги відкриті на читання і запис. Якщо такі каталоги не виявлені, то хробак намагається послідовним перебором паролів отримати до них доступ на запис. Отримавши доступ, хробак копіює себе на машину, в будь-яку з папок, створює завдання на запуск через планувальник завдань і запускається автоматично.

Найбільший комп'ютерний хробак в історії ***Conficker*** заразив десятки мільйонів комп'ютерів з ***ОС Windows*** в більш ніж 200 країнах. Комп'ютери уряду Великої Британії постраждали особливо сильно. ***Conficker*** призвів до хаосу на заражених комп'ютерах, відключивши важливі системні служби і програмне забезпечення безпеки, автоматично завантаживши файли і заборонивши користувачам відвідувати вебсайти, які дозволили б їм завантажувати оновлення безпеки.

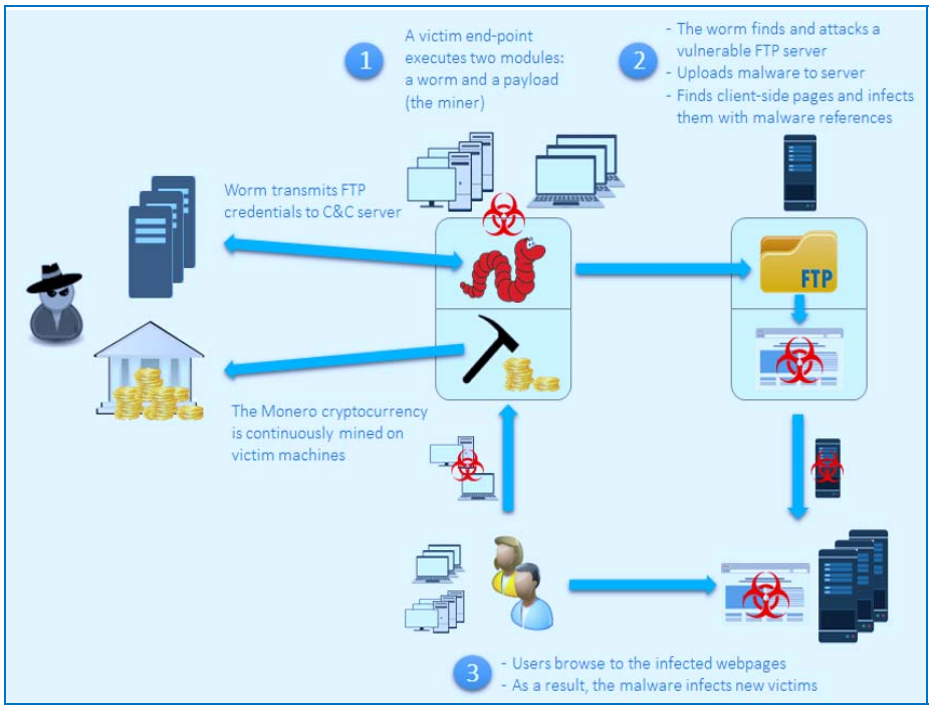


Рис. 11.1. Мережевий хробак в ролі транспорту для програми скритного криптомайнінгу

Джерело: URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/setevoy-cherv/

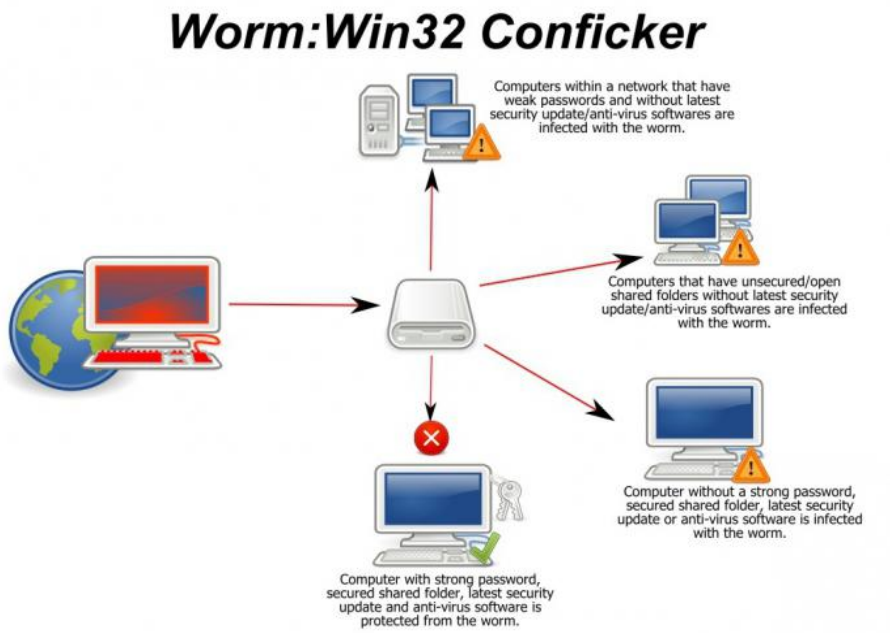
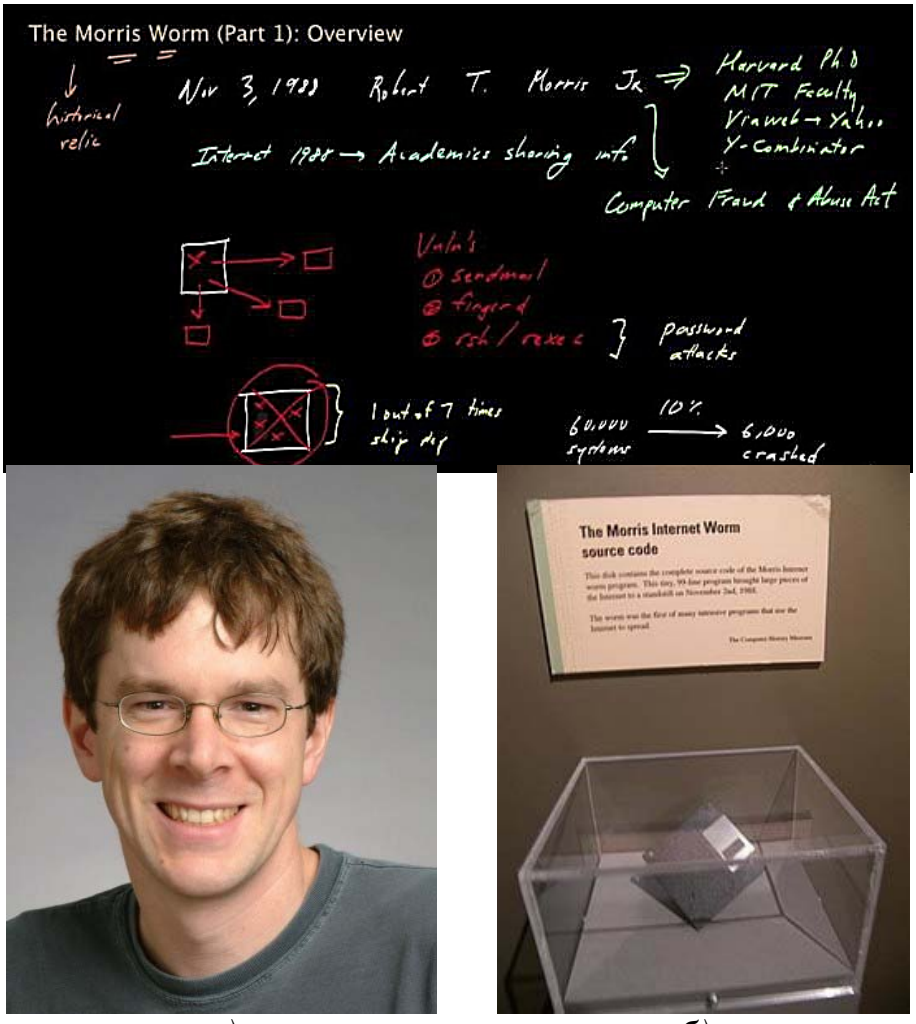


Рис. 11.2. Мережевий хробак Worm.Win32 Conficker

Джерело: URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/setevoy-cherv/

Практична історія мережевих хробаків почалася з 2 листопада 1988 року, коли в багатьох комп'ютерах університетів і лабораторій США була виявлена повна завантаженість процесорів, зайнятих виконанням якихось завдань. Завантаження процесорів перевищувала всі норми і не дозволяла користувачам і навіть адміністраторам отримати доступ до комп'ютерів. Перезавантаження комп'ютерів не давало результатів, оскільки через досить невеликий проміжок часу комп'ютери знову опинялися завантаженими різними завданнями. Цей день був пізніше оголошений ***«чорним понеділком»***, ***«атакою нового вірусу»*** (термін «хробак» ще не використовувався). Автор: студент ***MTI Роберт Морріс***.



а) *б)*

Рис. 11.3. Студент Роберт Теппен Морріс (а); дискета з кодом хробака Морріса (б) зберігається в музеї науки в Бостоні

Джерело: URL: https://uk.wikipedia.org/wiki/

Хробак Морріса – досить складний пакет програм, який реалізував такі функції:

- ➔ пошук цілей для атаки і проникнення на віддалені цілі;
- ➔ завантаження через мережу основного програмного коду, його компіляцію і запуск;
- ➔ сповіщення про зараження чергової машини;
- ➔ приховування свого існування;
- ➔ перевірку на зараженість локальної та віддалених машин для запобігання повторному зараженню.

Руйнівних функцій хробак не мав і, ймовірно, міг би бути досить довго непоміченим у мережі. Однак помилки, яких автор припустився в алгоритмах перевірки на зараження машин, призвели до того, що хробак багаторазово заражав комп'ютери.

На суді в 1989 р були оголошені втрати: інфіковано близько 6 200 машин (7,3 % всіх машин – через Інтернет), загальні втрати становили близько 98 млн дол. (робота програмістів і адміністраторів, витрати машинного часу і втрата доступу). Вирок був досить м'який: три роки випробувального терміну, 400 годин громадських робіт і 10 000 дол. штрафу. У даний час ***Роберт Моррис*** працює і викладає в ***MIT Computer Science and Artificial Intelligence Laboratory.*** Наступні хробаки з'явилися тільки через 10 років. Причому їх функціональність тільки копіювала ідеї ***Морріса.***

Крім функцій самовідтворення і саморозповсюдження сучасні хробаки, як правило, наділяються різними деструктивними функціями, або вони використовуються як носії іншого шкідливого забезпечення. Навіть якщо ніяких деструктивних дій в них не передбачено, масова розсилка хробаків може викликати перевантаження мережі і зниження її працездатності.

Основними ознаками, за якими хробаків поділяють на різні типи, є:

- спосіб їх розповсюдження;
- способи запуску хробака на комп'ютері;
- методи його впровадження в систему;
- «корисне» навантаження хробака – код, розроблений для виконання певних дій в інтересах зловмисника на цільовій машині: установка потайного ходу, установка бота, програми виконання складних математичних операцій, установка трояна.

Хробак може скопіювати свої файли на флешку та створити відповідний файл автозавантаження і як тільки флешку під'єднають до комп'ютера, на ньому одразу ж активізується хробак.

E-mail-Worm – *поштовий хробак*

До даної категорії відносяться хробаки, які для свого поширення використовують електронну пошту. При цьому хробак відсилає або свою копію у вигляді вкладення в електронний лист, або посилання на свій файл, розташований на будь-якому мережевому ресурсі (наприклад, URL на заражений файл, розташований на зламаному вебсайті). *У першому випадку* код хробака активізується при відкритті (запуску) зараженого вкладення, *у другому* – при відкритті посилання на заражений файл. В обох випадках ефект однаковий – активізується код хробака.

Мережний хробак сімейства *Net Worm.Win32.Sasser*

Класичними мережними хробаками є представники сімейства ***Net-Worm.Win32.Sasser***. Ці хробаки використовують уразливість в службі ***LSASS Microsoft Windows***. При розмноженні хробак запускає ***FTP-***службу на ***TCP-порту 5554,*** після чого вибирає ***IP***-адресу для атаки

і відсилає запит на порт 445 за цією адресою, перевіряючи, чи запущена служба ***LSASS.*** Якщо комп'ютер відповідає на запит, хробак посилає на цей же порт експлойт, який використовує вразливості в службі ***LSASS.*** У результаті успішного виконання експлойта на комп'ютері запускається командна оболонка на ***TCP-порту 9996***. Через цю оболонку хробак віддалено виконує завантаження копії хробака по протоколу ***FTP*** із запущеного раніше сервера і віддалено запускає себе, завершуючи процес проникнення і активації.

11.2. Троянські програми

Троянські програми (trojan) – це шкідливі програми, що приховано проникають до системи і виконують шкідливі, дуже часто – руйнівні функції на комп'ютері.

НА ВІДМІНУ ВІД ВІРУСІВ І ХРОБАКІВ, ТРОЯНИ САМІ НЕ РОЗМНОЖУЮТЬСЯ І НЕ СТВОРЮЮТЬ ВЛАСНІ КОПІЇ.

Програми цього типу потрапляють на комп'ютери під виглядом корисних програм, які користувачі завантажують і запускають ***ВЛАСНОРУЧ!*** При цьому програма дійсно може бути корисна, однак поряд з основними функціями вона може виконувати й інші дії, що не документуються в описі самої програми. Однак в більшості випадків, трояни проникають на комп'ютери разом з хробаком, тобто трояни – додаткове шкідливе навантаження хробака.

Трояни класифікуються за типом шкідливої функції:

- ***Trojan SPY*** – стежить за діями користувача і вишукує на комп'ютері цінну інформацію;
- ***Trojan –PSW*** – краде паролі;
- ***Trojan-Banker*** – збирає інформацію про проведення банківських операцій;

- ***Trojan – Notifier*** – сповіщає «хазяїна» про успішну атаку;
- ***Trojan-Downloader*** і ***Trojan-Dropper*** – завантажувачі та інсталятори шкідливого ПЗ;
- ***Trojan-Clicker*** – виконує несанкціоноване звернення до Internet-ресурсів;
- інші троянські програми здійснюють руйнування або зловмисну модифікацію даних і порушують роботу комп'ютера.

Trojan.Banker.Win32

Trojan.Banker.Win32 – широке сімейство троянських програм, що крадуть інформацію, яка дозволяє зловмисникові отримати доступ до банківських рахунків користувача.

Існує кілька видів троянських програм, що розрізняються механізмом отримання банківських даних:

1. ***Кейлоггери перехоплюють всю інформацію***, що вводиться з клавіатури, таким чином, зловмисник отримує все логіни і паролі для банківських і платіжних систем.

2. ***Трояни, які крадуть файли цифрових сертифікатів*** для систем клієнт-банк і файли електронних гаманців. Жертвою цього трояна стануть користувачі систем клієнт-банк, а також власники гаманців ***WebMoney, Bitcoins*** і т.п. При необхідності викрадається так само логін і пароль користувача.

3. ***Вузькоспеціалізовані троянські програми, націлені на додатки для роботи з Internet-банкінгом.*** Багато великих банків розробляють свої власні програми для роботи з сервісом *Internet-банк*, відповідно до цього, для кожної такої програми зловмисники розробляють свою програму для перехоплення переданих даних.

4. ***Саме численне сімейство – трояни, які крадуть дані кредитних карток***. Дізнавшись ім'я власника, номер пластикової картки, Expirion date і CVV2 – зловмисник швидко обчищає банківський рахунок потерпілого.

Для крадіжки даних пластикових карток, трояни застосовують такі прийоми:

- ➔ сканування файлів на комп'ютері для пошуку номерів карток (деякі користувачі зберігають всі дані про картки в звичайних текстових файлах);
- ➔ підміна офіційних сторінок банків і магазинів на фальшиві. В цьому випадку, в пам'яті комп'ютера є троянська програма, яка на ходу змінює вебсторінку в браузері і перенаправляє користувача на підроблену сторінку, або ж додає на вебсторінку підроблені поля для введення даних кредитної картки.

Рис. 11.4. Приклад дії троянської програми, яка виводить на вебсторінці підроблену форму для «перевірки кредитної картки»

Джерело: URL: https://zillya.ua/tipi-shkidlivikh-program-vid-trojan-do-rootkit

5. *Троянські програми для смартфонів* (переважно для систем Android).

У даний час безліч систем *Internet-банкінгу* прив'язане до мобільного номера клієнта. За допомогою телефону можна оплатити рахунок або зробити грошовий переказ. Перевірочні коди для здійснення операцій приходять у вигляді SMS на мобільний номер клієнта, і можуть бути легко викрадені троянської програмою. Цією особливістю поспішили скористатися зловмисники, створивши сотні троянів, замаскованих під гри і утиліти. Користувач, як правило, сам встановлює на свій телефон шкідливу програму, спокусившись скачати нову безкоштовну іграшку з *PlayMarket*. Завантажений троян отримує повний доступ до SMS повідомленнями, і починає переводити гроші, самостійно відправляючи і приймаючи SMS. Банківські трояни для мобільних телефонів є великою небезпекою, і можуть без відома користувача, швидко перевести всі його гроші на рахунок зловмисника.

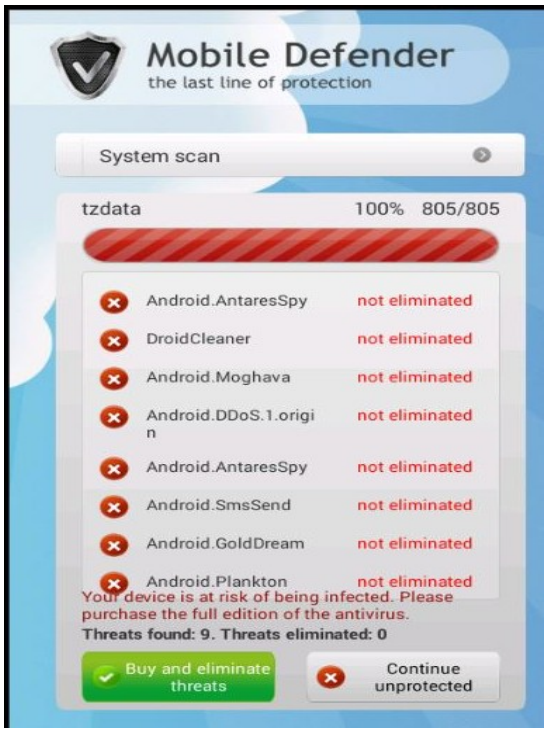


Рис. 11.5. Приклад фальшивого антивіруса для Android, який знаходить неіснуючі загрози і пропонує їх усунути після оплати

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

6. *Троянські програми перехоплюють і аналізують мережевий трафік.* Цей різновид троянів намагається знайти важливу інформацію в перехоплюваних мережевих пакетах. Зокрема цим займається троян ***OSX / CoinThief***, працює в середовищі операційної системи *MAC OS X*. Його основним завданням є крадіжка криптовалюти *Bitcoin*, для цього троян перехоплює і аналізірунет мережевий трафік.

7. *Троянські програми для крадіжки банківської інформації* часто є складні і багатокомпонентні програмні комплекси. Наприклад, один компонент видаляє антивірусне програмне забезпечення з комп'ютера, інший підміняє вебсторінки для крадіжки даних пластикової картки, третій маскує сліди своєї діяльності, четвертий займається шифруванням інформації.

Життєвий цикл троянів складається всього з трьох етапів:

➔ проникнення в систему;

➔ активація;

➔ виконання шкідливих дій.

В Україні знаковий інцидент з використанням троянів відбувся у травні 2014 року під час президентських виборів. Ряд серверів ЦВК, були заражені троянськими програмами, які змінювали роботу системи і створювали набори файлів, які модифікували вигляд офіційної сторінки результатів виборів, чим намагались спровокувати політичний конфлікт чи поставити під сумнів реальні результати виборів.

Зараження систем відбулось по класичній схемі троянізації. На одному з серверів у планувальника було поставлено завдання створити на диску два файла з конкретним вмістом, що мало призвести до модифікації офіційного сайта.

Скільки потрібно зловмисників, щоб з нуля створити і розповсюдити троян-шифрувальник

1. Фахівець з криптографії, який втілить в коді певний алгоритм шифрування.

2. Програміст, який напише код трояна, що буде забезпечувати скритність його дій в системі, так щоб він не виявлявся відомими антивірусами. Іноді для цього навіть наймають тестувальника (вже третій член команди).
3. Фахівець із соціальної інженерії, який розробляє механізм розповсюдження трояна. Троян не вірус і сам розмножуватися не вміє. Фахівець створить ескіз спам-листів і сформулює завдання на розробку фішингового сайта.
4. Вебдизайнер, який розробить фішинговий сайт.
5. Спамер, або володар ботнет-мережі.
6. Фахівець з «приховування доказів», чиє основне завдання полягає в збереженні анонімності і скритності дій всіх учасників злочинного співтовариства.

Як троян може потрапити на ПК

Пошта. Розсилка електронних листів жертвам атаки. Найчастіше у листах від атакуючих в поле «Від» стоять реальні адреси, оскільки розсилка ведеться зі зламаних аккаунтів без відома їх власників. Прикладені до таких листів «документи», які користувач відкриває, або наведенні посилання на «корисний» сайт і призводить до запуску трояна.

Шкідливі сайти. Тут є два варіанта. У першому випадку користувач, завантажуючи необхідні йому програми, або інші файли з фішингових, зламаних або просто ніким не контрольованих ресурсів (файлообмінники, торренти і т. д.), навіть і не підозрює, що разом з корисним матеріалом отримує і шкідливий код. Другий варіант ще гірше: можно нічого не завантажувати, а досить просто зайти на заражений сайт, щоб запустився скрипт, який завантажить на ПК троян і активізує його (це можливо тільки при абсолютно «небезпечних» настройках браузера і операційної системи, які і має більшість користувачів).

Змінні носії інформації. Це основний шлях зараження комп'ютерів, які або взагалі не мають підключення до мережі, або є частиною невеликих локальних мереж без виходу в Інтернет. Якщо змінний носій, будь-то флешка або знімний

жорсткий диск, заражені, а на комп'ютері не відключена функція автозапуску і немає антивірусної програми, то великий ризик того, що для активації трояна буде досить просто вставити пристрій в USB-роз'єм.

11.3. Спеціальні шкідливі програми

Крім вірусів, хробаків і троянів існує ще багато інших шкідливих програм. Серед них можна виділити наступні групи:

1. *Умовно небезпечні програми*, про які не можна однозначно сказати, що вони шкідливі. Такі програми зазвичай стають небезпечними тільки за певних умов або діях користувача. До них відносяться:

► ***рекламне ПЗ (adware)*** **–** це програми, які призначені для демонстрації реклами, перенаправлення запитів пошуку на рекламні вебсайти і збору маркетингової інформації про користувача (наприклад, якого роду сайти він відвідує), щоб реклама відповідала його інтересам.

Adware-програми можуть потрапити на комп'ютер двома основними шляхами:

- ♦ з безкоштовним або умовно-безкоштовним програмним забезпеченням;
- ♦ через заражені вебсайти.

Ці програми захищають себе від видалення і коли рекламні програми беруть під свій контроль браузер, то це називається викраденням браузера. Однак оскільки ***Adware-програми*** можуть бути присутніми комп'ютері на законних підставах, антивірусні рішення не завжди здатні визначити ступінь небезпеки конкретної ***Adware-програми***.

Для цього типу програм дуже важко провести межу між шкідливим і безпечним програмним забезпеченням, оскільки ці програми найчастіше заявляють, що є легальними програмами. У зв'язку з цим не має однозначного трактування

антивірусними компаніями чи є програма шкідливою чи ні. І якщо перевірити подібну програму за допомогою онлайн сканеру, наприклад ***VirusTotal,*** до якого зараз підключено 57 різних антивірусів, то тільки 20 скажуть, що програма є рекламним модулем, інші 37 – промовчать, показуючи, що програма нешкідлива. Чи це означає, що погано спрацювали лабораторії 37 вендорів, які не додали програму в бази, чи інші 20 вендорів помилились і у них відбулось хибне спрацювання.

До цієї групи можна також віднести і умовно-безкоштовні програми, які в якості плати за своє використання демонструють користувачеві рекламу. Після офіційної оплати і реєстрації зазвичай показ реклами закінчується і програми починають працювати в звичайному режимі. Але навіть після реєстрації такі модулі можуть автоматично не видалятися і продовжувати свою роботу в прихованому режимі.

За допомогою рекламного ПЗ вирішують такі завдання:

- ➔ змінюють параметри браузера і операційної системи з метою ослаблення захисту;
- ➔ виводять з ладу антивірусні системи й інші засоби безпеки;
- ➔ збирають інформацію про користувача (місцезнаходження, ідентифікаційні дані, набір використовуваних послуг і відвідуваних вебсайтів).

Мобільне рекламне ПЗ (madware, mobile advertising software) – це дрібниця, яка може не тільки сильно перешкодити процесу використання пристрою, а й видати зловмисникам деталі вашого місця розташування, контактні дані, а також ідентифікаційні дані пристрою. Програма типу ***madware*** непомітно потрапляє на пристрій при установці стороннього додатка, часто починає завалювати користувача спливаючими вікнами, створює ярлики, змінює настройки браузера і збирає його особисті дані.

► ***«Пасхальні яйця»*** – програмні закладки в запропонованому ПЗ, що закладаються самими виробниками ПЗ для виконання недокументованих функцій. Для запуску цих закладок слід провести складну або нестандартну сукупність дій, що робить малоймовірним випадкове виявлення цієї закладки. Назва походить від популярного в США і колишніх Британських колоніях сімейного заходу «полювання за яйцями», що влаштовується напередодні Великодня, в якому учасники повинні за допомогою підказок знайти якомога більше захованих по місцевості яєць.

2. Riskware.

Цілком легальні програми, які самі по собі не є небезпечними, але володіють функціоналом, що дозволяє зловмисникові використовувати їх зі шкідливими цілями.

Рис. 11.6. Riskware – цілком легальні програми, але дозволяють зловмисникові використовувати їх зі шкідливими цілями

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

До ***riskware*** відносяться звичайні утиліти віддаленого управління, якими часто користуються адміністратори мереж, програми для завантаження файлів з Інтернету, утиліти відновлення забутих паролів і ін.

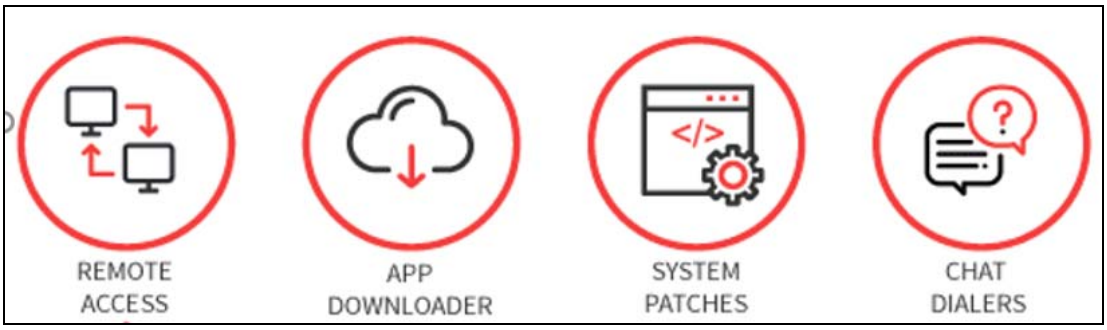


Рис. 11.7. Утиліти віддаленого управління, що відносяться до riskware

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

3. Утиліти прихованого адміністрування.

За своєю функціональністю вони багато в чому нагадують різні системи адміністрування, але особливістю їх є відсутність попередження про інсталяцію і запуск, що змушує класифікувати їх як шкідливі програми. Будучи встановленими на комп'ютер, утиліти прихованого адміністрування дозволяють робити з комп'ютером усе, що в них заклав їх автор: приймати і відсилати файли, запускати і знищувати їх, виводити повідомлення, стирати інформацію, перевантажувати комп'ютер і т. п.

1. Хакерські утиліти.

До цього виду програм відносяться програми:

➔ ***Конструктори вірусів, хробаків і троянів;***

➔ ***RootKit*** – програмні бібліотеки керування роботою комп'ютера.

Ця назва прийшла із *ОС UNIX,* де її використовували для позначення набору інструментів, що дозволяє отримати в системі права суперкористувача – root. Такий набір існує і для інших ОС.

Руткіти не обов'язково є шкідливими, проте вони можуть приховувати шкідливі дії. Зловмисники можуть отримати доступ до інформації, відстежувати дії, змінювати програми або виконувати інші функції без виявлення їх системою. Здебільш ці програми приховують від користувача роботу

шкідливого коду, дозволяючи шкідливим програмам зберігатися як можна довше. Приховуванню, як правило, піддаються ключі реєстру, що відповідають за автозапуск шкідливих об'єктів, процеси в пам'яті, що пов'язані зі шкідливим ПЗ, файли, в яких зберігається шкідливий код. Успішний руткіт потенційно може залишатися на місці роками, якщо він не виявлений. За цей час він буде красти інформацію і ресурси. Руткіти перехоплюють і змінюють стандартні процеси операційної системи. Наприклад, якщо ви попросите пристрій перерахувати всі запущені програми, руткіт може таємно видалити всі програми, про які він не хоче, щоб ви знали.

➔ ***Експлойт***.

Експлойт являє собою шкідливу програму, що використовує відому вразливість в операційній системі або прикладному програмному забезпеченні, для отримання несанкціонованого доступу до вразливого хоста або порушення його працездатності. Після того, як така програма запущена в інформаційній системі, порушник використовує вразливість штатного ПЗ для своїх потреб. Кінцевою метою експлойта може бути знищення або відключення системи, що атакується, хоча частіше це отримання несанкціонованого доступу до інформації, або виконання свого коду на локальних або віддалених машинах.

5. Bad-Joke, Hoax – програми введення користувача в оману (злі жарти).

Вказані програми не завдають будь-якої прямої шкоди, проте виводять повідомлення про те, що така шкода вже заподіяна, або буде її завдано при будь-яких умовах. До ***«злих жартів»*** відносяться, наприклад, програми, які ***«лякають»*** користувача повідомленнями про форматування диска (хоча ніякого форматування насправді не відбувається), виводять дивні вірусоподібні повідомлення і т. п. Такі програми, ***по-перше,*** відносять до шкідливих тому, що вони псують користувачеві нерви, що завдає моральної шкоди,

а ***по-друге,*** є ймовірність того, що користувач, втративши психічну рівновагу, неадекватно відреагує, що може привести до дійсної втрати інформації.

6. Програми-вимагачі (Ransomware).

Ransomware – це шкідливе ПЗ призначене для блокування комп'ютерної системи або розташованих на ній даних, до моменту здійснення викупу. Форми шкідливої поведінки у них зазвичай проявляються в тому, що вони потай зашифровують всі файли на комп'ютері-жертві. Потім, коли шифрування завершується, ці програми виводять повідомлення, що вимагають від власника системи перевести гроші на якийсь рахунок, або відправити гроші на короткий номер мобільного оператора.

Рис. 11.8. Програми-вимагачі (Ransomware)

Джерело: URL: https://www.cisco.com/c/ru_ua/solutions/security/ransomware/index.html

Найчастіше Ransomware намагається получити гроші у жертв у вигляді криптовалюти в обмін на ключ дешифрування. Але кіберзлочинці не завжди можуть виконати і розблокувати вже зашифровані файли.

Ransomware – один з найбільш прибуткових каналів доходу для кіберзлочинців, тому автори шкідливих програм постійно вдосконалюють свій код шкідливих програм, щоб краще орієнтуватися на корпоративні середовища.

Складні вимагачі як ***Spora, WannaCrypt*** (також відомий як ***WannaCry)***, ***Petya*** (також відомий як ***NotPetya***) поширюються на інші комп'ютери через мережеві ресурси. ***WannaCrypt*** використовує уразливість *Server Message Block (SMB)*.

Старі вимагачі, такі як ***Reveton***, блокують екрани замість шифрування файлів. На заблокованому екрані зображення зазвичай містить повідомлення від правоохоронних органів, в якому говориться, що комп'ютер використовувався в незаконній діяльності кіберзлочинців, і штраф повинен бути сплачений. Через це ***Reveton*** називають ***«поліцейським трояном»*** або ***«поліцейським здирником».***

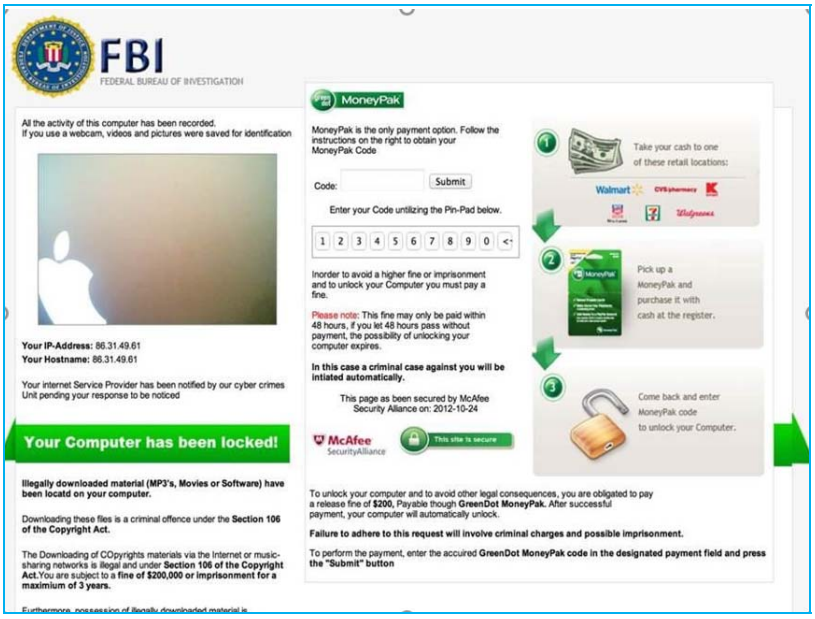


Рис. 11.9. Програми-вимагачі

Джерело: URL: https://www.cisco.com/c/ru_ua/solutions/security/ransomware/index.html#~stickynav=3

Такі вимагачі, як ***Cerber і Locky,*** здійснюють пошук і шифрування певних типів файлів, зазвичай документів

і мультимедійних файлів. Коли шифрування завершено, шкідлива програма залишає записку з вимогою викупу, використовуючи текст, зображення або файл *HTML* з інструкціями, щоб заплатити викуп за відновлення файлів. Зловмисники прагнуть робити суму порівняно невисокою, щоб люди прагнули виплачувати викуп і більшість людей платять.

7. Шпигунські програми (Spyware).

Такі програми стежать за діями користувача зараженого комп'ютера, перехоплюють інформацію, що вводиться з клавіатури, виконують копіювання екрану, фіксують інформацію про активні програми і про те, що користувач із ними робить. Шпигунські програми цікавляться системними даними, типом браузера, відвідуваними вебвузлами, іноді і вмістом файлів на жорсткому диску. Після цього посилають зібрану інформацію третій стороні – творцеві або замовникові такої програми.

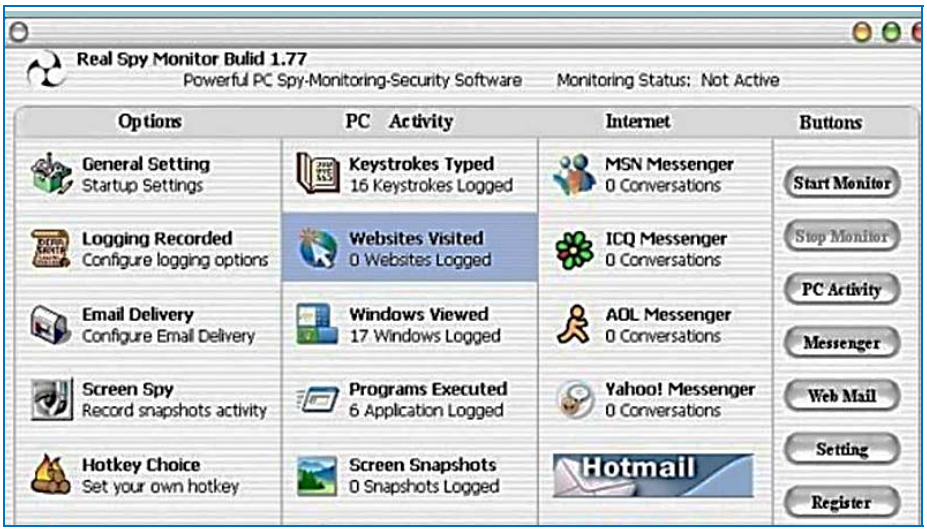


Рис. 11.10. Шпигунські програми (Spyware)

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Серед замовників таких програм – спамери, рекламщики, маркетингові агентства, злочинні угруповання, діячі промислового шпигунства. Такі програми таємно завантажуються

на комп'ютер разом з будь-яким безкоштовним софтом або при перегляді певним чином сконструйованих HTML-сторінок сайта та спливаючих рекламних вікон і встановлюються без інформування про це користувача.

Найбільш поширеним видом програм-шпигунів ***є кейлоггери*** (від англ. ***«Key» – «кнопка»*** і ***«logger» – «реєстратор»***). Ці програми можуть бути як самостійними вірусами, які впроваджуються в систему, так і спеціально встановленими утилітами стеження. Клавіатурні шпигуни призначені для реєстрації натискань всіх кнопок на клавіатурі (іноді також мишки) і збереження даних в файл. Залежно від принципу роботи кожного конкретного кейлоггера, файл може просто зберігатися на локальному жорсткому диску або періодично пересилатися до того, хто веде стеження. Для цього в налаштуваннях указують поштову адресу, на який слід надсилати файли з даними. Хороший в тому випадку, якщо вам достатньо лише знати, що користувач вводить з клавіатури і які програми запускає при цьому.

Однак цих даних може бути недостатньо. Тому були створені більш складні програмні комплекси для всебічного шпигунства.

Такі шпигунські комплекси можуть включати:

- ➔ кейлоггер;
- ➔ перехоплювач буфера обміну;
- ➔ екранний шпигун (робить скріншоти через задані проміжки часу);
- ➔ реєстратор запуску і активності програм;
- ➔ систему звуко- та відеозапису (при наявності мікрофона або вебкамери).

Програми стеження дозволяють виконувати дуже широкий спектр завдань: робити знімки екрана, стежити через вебкамеру, записувати звук з мікрофона, визначати геопозіцію лептопа, відсилати звіти разом з файлами зазначеного типу, дублювати історію браузера на випадок її видалення і робити безліч інших речей.

8. Програмні закладки (люки, потайні входи та логічні бомби).

Люк (trapdoor) – це прихована, недокументована точка входу в програмний модуль, яка дозволяє отримати доступ до програми в обхід звичайних процедур. ***Люк*** вставляється в програму в більшості випадків на етапі налагоджування для полегшення роботи, пов'язаної з коригуванням програми, в подальшому дана точка входу непотрібна і вона видаляється. Однак ***люки*** можуть зберігатися розробниками для забезпечення підтримки вже готової програми. Наприклад, ***Кен Томпсон*** – автор мови програмування ***C***, запропонував увести в компілятор ***C*** програмну закладку, яка розпізнає вихідний код утиліти *login*, що виконує автентифікацію користувача в операційній системі ***UNIX*** і в процесі компіляції додає до цієї утиліти недокументовану функцію. Завдяки цій функції після введення спеціального таємного пароля користувач получає привілейований доступ.

Висновок, що випливає з цього факту: не можна цілком довіряти програмі, написаній не власноруч, і не можна бути впевненим, що програмні продукти, навіть відомих і шанованих виробників не містять програмних закладок.

Якщо ***люк*** встановлюється зловмисниками, використовуючи вразливості програми, то в цьому випадку люк називають ***потайним входом (backdoor).***

Потайний вхід (backdoor) – це шкідлива програма, що дозволяє зловмисникові обходити контроль входу в систему для таємного доступу до даної програми. Єдиним способом виявити люк є декомпіляція – процес під назвою зворотна розробка або реверс-інжиніринг ПЗ.

Логічна бомба (програмна закладка) – це додатковий код, що поміщається в легальну програму, в тому числі і розробниками. При певних умовах цей код виконує неочікувані, руйнівні дії – ***«вибухає»*** (змінює або видаляє файли, зупиняє роботу програми або всієї системи, здійснює інші дії). Умовою для вибуху логічної бомби може бути наявність

або відсутність деяких файлів, певний день тижня або певна дата, запуск додатка певним користувачем та інше.

Приклад логічної бомби, коли її автор додав до програми код, що перевіряв наявність саме його ідентифікаційного номеру у нарахуваннях заробітної плати. Якщо цей ідентифікатор не фігурував, то ***бомба «вибухала».***

9. Псевдоантивірус (Scareware).

Це тип шкідливого ПЗ, що переконує користувача виконати конкретну дію, часто використовуючи його страх. ***Scareware*** створює спливаючі вікна, схожі на вікна діалогу операційної системи. Ці вікна висвітлюють підроблені повідомлення про те, що система знаходиться під загрозою або необхідно виконання відповідної програми для повернення до нормальної роботи. Насправді не було виявлено жодних проблем, і якщо користувач погоджується та дозволяє виконати зазначену програму, то його система буде заражена шкідливим ПЗ.

Симптоми наявності шкідливого програмного забезпечення в системі

Незалежно від того, яким типом зловмисного ПЗ інфікована система, можна виділити найпоширеніші симптоми того, що пристрій заражено:

1. Збільшується навантаження на центральний процесор.
2. Знижується швидкодія комп’ютера.
3. Комп’ютер часто зависає або дає збої.
4. Знижується швидкість перегляду вебсторінок.
5. З’являються незрозумілі проблеми з мережевими з’єднаннями.
6. Модифікуються файли.
7. Видаляються файли.
8. Наявність невідомих файлів, програм або значків на робочому столі.
9. Запущено невідомі процеси.
10. Програми самостійно знімаються з виконання або переконфігуровуються.
11. Електронна пошта надсилається без відома та згоди користувача.

ГЛАВА 12
Захист від шкідливого програмного забезпечення

12.1. Методи виявлення шкідливих програм

Найефективнішими засобами захисту від шкідливого ПЗ є спеціальні програми, здатні розпізнавати і знешкоджувати його. *Такі програми називаються антивірусами, і вони застосовуються для вирішення таких завдань*:

➔ виявлення шкідливого ПЗ в ІТС;
➔ блокування роботи шкідливого ПЗ;
➔ усунення наслідків дії шкідливого ПЗ.

У сучасних антивірусних продуктах використовуються три основних підходи (методи) до виявлення шкідливих програм:

- ❖ сигнатурний;
- ❖ поведінковий;
- ❖ евристичний.

Сигнатурні методи

Сигнатурні методи – точні методи виявлення вірусів, засновані на скануванні усіх файлів системі у пошуках пізнавальної частини коду шкідливого ПЗ – сигнатури.

Сигнатура вірусу – це послідовність коду (10–30 байт), специфічна для конкретного вірусу, що дозволяє однозначно ідентифікувати наявність вірусу у файлі (включаючи випадки, коли файл цілком є вірусом). Всі разом сигнатури відомих вірусів складають ***антивірусну базу.*** Сигнатурний метод передбачає безперервне відстеження нових екземплярів вірусів, їх опис та включення в базу сигнатур.

Практично в кожній компанії, яка випускає антивіруси, є своя група експертів, яка виконує аналіз нових вірусів і поповнює антивірусну базу новими сигнатурами. ***З цієї причини антивірусні бази в різних антивирусах відрізняються.***

Ефективність сигнатурного пошуку безпосередньо залежить від обсягу антивірусної бази і від частоти її поповнення. Саме тому сьогодні розробники антивірусних програм випускають оновлення для своїх баз мінімум раз на добу. Кращим же антивірусом буде той, для якого сигнатура нового вірусу була випущена раніше всіх.

Головний недолік сигнатурного методу – затримка реакції на нові загрози. Створити сигнатуру нового вірусу неможливо, поки вірус не потрапив на аналіз до експертів. З моменту появи вірусу в мережі Інтернет до випуску перших сигнатур зазвичай проходить кілька годин, і весь цей час вірус здатний заражати комп’ютери майже безперешкодно.

Поведінкові методи

Поведінкові методи ґрунтуються не на дослідженні коду вірусу, а на основі послідовності дій, виконуваних файлом після його запуску. Підозрілий файл запускається в спеціально створеному середовищі – ***буфері емуляцій***, або ***«пісочниці».*** Якщо в процесі виявляються будь-які підозрілі дії, то об'єкт визнається шкідливим і його запуск на комп'ютері блокується. Така «пісочниця» є абсолютно безпечною, оскільки вірус там не може розмножитися, а отже, завдати шкоди, а сам вірус не здатний відрізнити «пісочницю» від справжнього середовища і виконує в ній характерні для вірусу дії.

Перевагами поведінкових методів є висока швидкість роботи, можливість виявлення нових невідомих вірусів ще до того, як для них будуть виділені сигнатури, але поведінковий аналіз вимогливий до ресурсів комп'ютера, оскільки для цього необхідно використовувати безпечний віртуальний простір, а запуск програми на комп'ютері відкладається на час аналізу.

Евристичні методи

Евристичні методи – приблизні методи виявлення, які дозволяють припустити, що файл заражений, з певною ймовірністю. Евристичний аналіз полягає в аналізі коду програми, тобто в коді відшукуються ділянки, що відповідають за конкретні шкідливі дії, наприклад, видалення якогось файла, створення власної копії або якісь подібні типові для шкідливих програм дії. Якщо такі ділянки виявляються, то приймається рішення про те, що досліджувана програма є шкідливою.

ДЛЯ ОПТИМАЛЬНОГО АНТИВІРУСНОГО ЗАХИСТУ НЕОБХІДНО ПОЄДНАННЯ РОЗГЛЯНУТИХ ПІДХОДІВ. Прикладом успішного поєднання цих методів може слугувати технологія ***ThreatSense*** компанії ***Eset.***

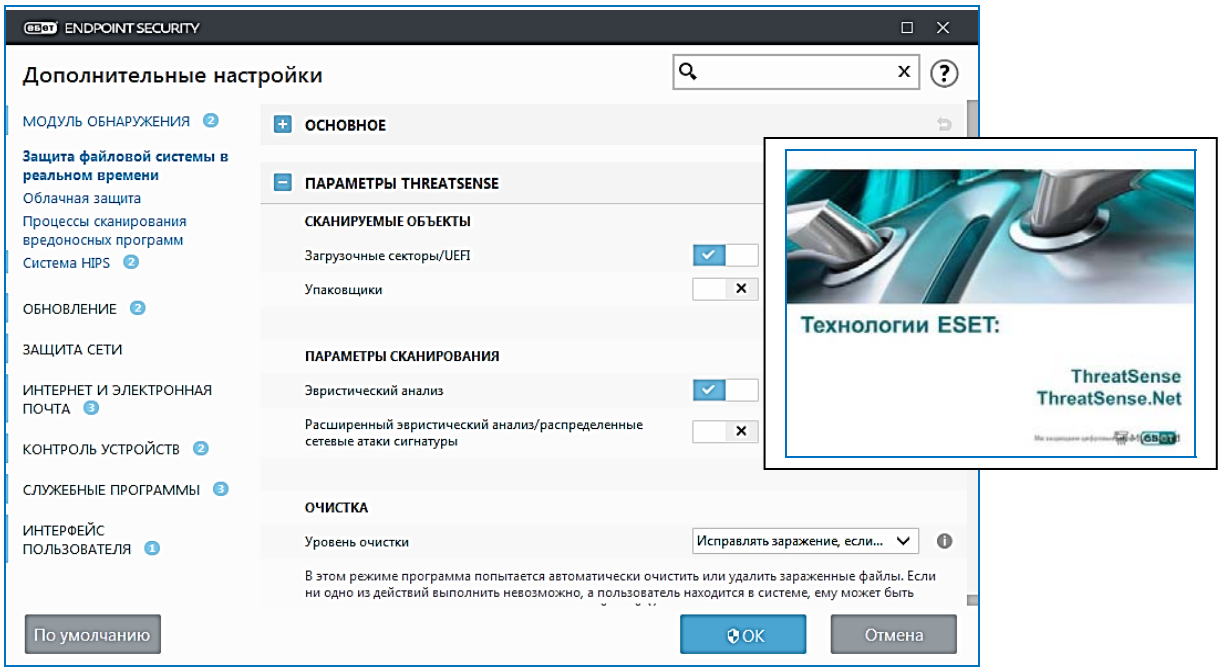


Рис. 12.1. Параметри ThreatSense

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Обсяг захисту, пропонованої антивірусними програмами, розширюється за рахунок включення, наприклад, блокувальників ***URL***, фільтрації контента, хмарних систем репутації, статичних і динамічних виявлень на основі машинного навчання і зручних для користувача засобів блокування поведінки. Якщо ці функції ідеально узгоджені з сигнатурним і евристичним виявленням, захист від загроз підвищується.

12.2. Типи і характеристики антивірусних програм

Якість антивірусної програми визначається за такими позиціями.

1. Надійність і зручність роботи.

Надійність і зручність роботи – відсутність зависань і інших технічних проблем, що вимагають від користувача спеціальної підготовки. Надійність роботи антивірусу

є найбільш важливим критерієм, оскільки навіть абсолютний антивірус може виявитися марним, якщо він буде не в змозі довести процес сканування до кінця – повисне і не перевірить частини дисків і файлів і, таким чином, залишить вірус непоміченим у системі. Якщо ж антивірус вимагає від користувача спеціальних знань, то він також виявиться марним, більшість користувачів просто проігнорують повідомлення антивірусу.

2. Якість виявлення вірусів всіх поширених типів, сканування всередині файлів документів, упакованих файлів. Відсутність «помилкових спрацьовувань». Можливість лікування заражених об'єктів.

Будь самий **«наворочений»** за своїми можливостями антивірус марний, якщо він не в змозі ловити віруси або робить це не зовсім якісно. Однак якщо при цьому антивірус з високою якістю детектування вірусів викликає велику кількість помилкових спрацьовувань, то його рівень корисності різко падає, оскільки користувач змушений або знищувати незаражені файли, або самостійно проводити аналіз підозрілих файлів, або звикає до частим помилкових спрацьовувань – перестає звертати увагу на повідомлення антивіруса і в результаті пропускає повідомлення про реальний вірус.

3. Швидкість роботи та інші корисні особливості, функції.

Відомими антивірусними програмами є ***антивірусні сканери***: ***детектори і поліфаги.*** Детектори тільки виявляють віруси, а поліфаги ще й лікують заражені файли.

Застосовуються також різного типу ***монітори (сторожа), блокіратори і імунізатори.***

Антивірусні сканери час від часу або за запитом здійснюють повне сканування файлової системи комп'ютера або вибіркове сканування заданих файлів чи каталогів. ***До переваг сканерів*** відноситься їх універсальність, до недоліків – розміри антивірусних баз, які сканерам доводиться

переносити за собою, і відносно невелика швидкість пошуку вірусів.

Антивірусні монітори (сторожа) – це резидентні програми, що відслідковують небезпечні операції (відкривання, читання, записування, переміщення файла, запуск на виконання) і повідомляють про це користувачу. ***Недоліками цих програм*** є велика кількість помилкових спрацьовувань, що і послужило причиною для практично повної відмови від подібного роду антивірусних програм.

Поведінковий блокіратор – це програма, яка аналізує поведінку запущеного додатка і блокує будь-які небезпечні дії. До основних шкідливих дій відносять:

- видалення файла;
- запис в файл;
- запис в певні області системного реєстру;
- відкриття порту на прослуховування;
- перехоплення даних, що вводяться з клавіатури;
- розсилка листів і ін.

Рис. 12.2. Види антивірусних програм

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Виконання кожної такої дії окремо не дає приводу вважати програму шкідливою. Але якщо програма послідовно виконує декілька таких дій, наприклад перехоплює дані, що вводяться з клавіатури, і з певною частотою пересилає їх на якусь адресу в Інтернеті, значить, ця програма щонайменше підозріла.

На відміну від евристичних аналізаторів, де підозрілі дії відстежуються в режимі емуляції, поведінкові блокіратори працюють в реальних умовах. До того ж блокіратор здатний виявити **руткіти**.

Особливо варто виділити таку функціональність поведінкових блокувань, як контроль цілісності додатків і системного **реєстру *Microsoft Windows*.** В останньому випадку блокіратор контролює зміни ключів реєстру і дозволяє задавати правила доступу до них для різних додатків.

Поведінковий блокіратор може запобігти поширенню як відомого, так і невідомого вірусу, що є незаперечною перевагою такого підходу до захисту. ***Недоліком поведінкових блокіраторів*** залишається спрацьовування на дії ряду легітимних програм. Для прийняття остаточного рішення про шкідливість застосування потрібне втручання користувача, що передбачає наявність у нього достатньої кваліфікації.

Карантин

У багатьох антивірусах серед допоміжних засобів є спеціальна технологія – карантин, яка захищає від можливої втрати даних у результаті дій антивіруса. Наприклад, файл детектується евристичним аналізатором як заражений і видаляється, але з певною ймовірністю антивірус міг видалити незаражений файл. Тому перед лікуванням або видаленням файлів доцільно зберегти їх резервні копії, тоді якщо виявиться, що файл був видалений помилково або втрачена важлива інформація, завжди можна буде виконати відновлення з резервної копії.

НЕ ІСНУЄ АНТИВІРУСІВ, ЩО ГАРАНТУЮТЬ СТОВІДСОТКОВИЙ ЗАХИСТ ВІД ВІРУСІВ!

Отже, можливе зараження комп'ютера, навіть якщо на ньому встановлено антивірус, але при відсутності антивірусного ПЗ, ймовірність проникнення на комп'ютер шкідливих програм багаторазово зростає.

Тестування роботи антивіруса

Як перевірити роботу антивіруса? Використовувати для тестування справжні віруси вкрай небезпечно. Якщо неправильно виконати установку або настройку антивіруса, то в процесі такого тестування він може заразити комп'ютер. Потрібен такий спосіб тестування антивірусів, який був би безпечним, але давав чітку відповідь на питання, чи коректно працює антивірус.

З огляду на важливість проблеми, організація **EICAR** за участю антивірусних компаній створила спеціальний тестовий файл, названий по імені організації – *eicar.com*.

Eicar.com – це виконуваний файл в ***COM-форматі***, який не виконує ніяких шкідливих дій, а просто виводить на екран рядок *«EICAR-STANDARD-ANTIVIRUS-TEST-FILE!»*. Отримати *eicar.com* можна на сайті організації **EICAR** за адресою: *http://www.eicar.org/anti_virus_test_file.htm*.

Рис. 12.3. Перевірка антивірусу за допомогою EICAR Test

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

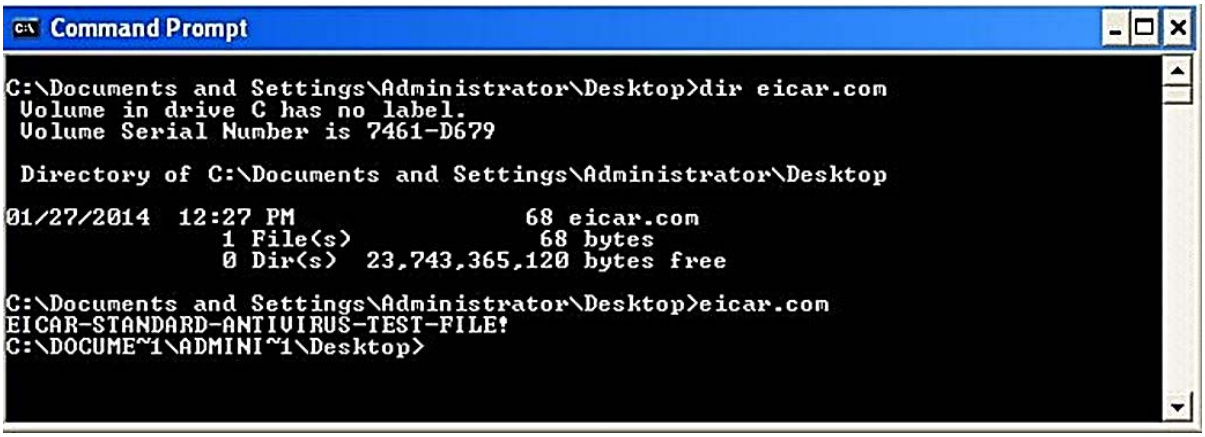


Рис. 12.4. Тестовий файл eicar.com

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

Файл *eicar.com* дозволяє протестувати, як антивірус справляється з файловими вірусами і близькими за структурою шкідливими програмами – більшістю троянів, деякими хробаками.

У світі пропонується безліч різних антивірусних засобів від різних виробників, зокрема: *Dr.Web*, *Trend Micro*, *Microsoft Security Essentials, McAfee, Eset, Panda, Avast, AWG, Norton Anti-Virus, Kaspersky Anti-Virus тощо, а також хмарні антивірусні технології.*

Крім встановлення спеціалізованих програм, можна також перевіряти файли в режимі онлайн. Річ у тім, що творці шкідливих програм зазвичай випереджають постачальників антивірусів, завжди може статися так, що якусь загрозу антивірусна програма помітить пізніше, ніж потрібно. Тому можна скористатися інтернет-сервісами, наявними майже у кожного виробника антивірусних засобів.

ВАЖЛИВО! Перед установкою антивірусного ПЗ переконайтеся, що на комп'ютері немає інших антивірусних продуктів. Якщо вони у вас вже є, обов'язково видаліть непотрібний продукт перед установкою нового. Якщо на комп'ютері будуть встановлені і запущені два різних антивірусних продуктів одночасно, можуть виникнути проблеми.

Захисник Windows Defender відключається, якщо ви встановите іншу антивірусну програму для захисту комп'ютера.

Зловмисники і шахраї іноді використовують фіктивні антивірусні програми, щоб обманним шляхом змусити встановити на комп'ютер віруси і шкідливі програми.

Три рівня антивірусного захисту

Як правило, виділяють три рівня антивірусного захисту, на кожному з яких можуть використовуватися антивірусні продукти різних виробників:

- Перший рівень включає в себе засоби захисту від шкідливих програм, що встановлюються на стику з глобальними мережами (інтернет-шлюз, міжмережевий екран, публічні сервери);
- Другий рівень – засоби захисту, що встановлюються на внутрішніх корпоративних серверах і серверах робочих груп (файлові, поштові, сервери додатків і т. д.);
- Третій рівень – засоби захисту від шкідливих програм, що встановлюються на робочих станціях користувачів, у тому числі віддалених і мобільних.

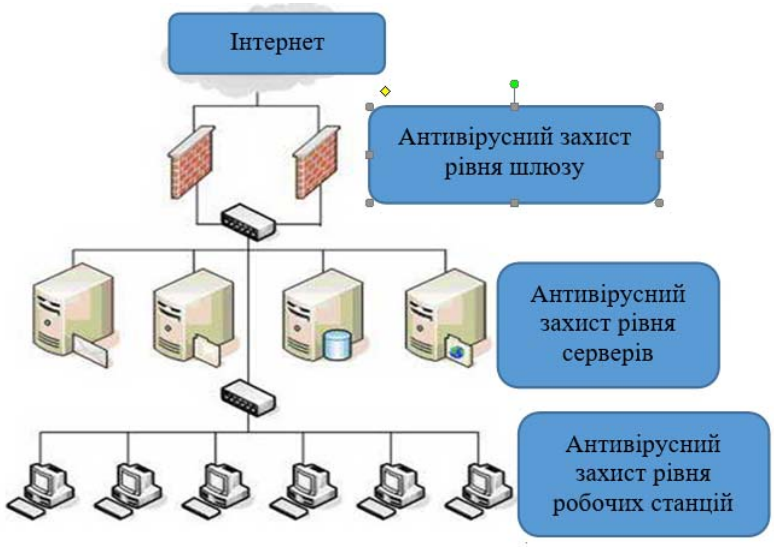


Рис. 12.5. Рівні антивірусного захисту

Джерело: URL: http://integritysys.com.ua/security/antivirus/

12.3. Технологія Whitelisting і антивірусні хмари

Технологія ***Whitelisting*** пропонує інший підхід до виявлення шкідливих програм. Її основні риси – це формування списку легітимних програм (додатків) і захист їх від зміни, а також заборона запуску програмам, що не входять до цього списку. Це дозволяє забезпечити захист не тільки від шкідливих програм (вірусів і хробаків), а й від шпигунського ПЗ та інших зайвих додатків.

Основними перевагами технології ***Whitelisting*** є:

- ➔ відсутність необхідності постійного оновлення, а також постійного сканування вхідного і вихідного трафіку (зниження навантаження процесора);
- ➔ захист від атак *zero-day;*
- ➔ захист (блокування) завантаження та інсталяції програм до яких немає довіри.

Більшість продуктів, що використовують технологію ***Whitelisting,*** дозволяють або забороняють виконання програм на основі списку довірених користувачів, довірених шляхів надходження програми і довірених виробників за допомогою цифрових сертифікатів. Деякі рішення за цією технологією ведуть величезні списки відомих файлів програм і додатків, для яких обчислені хеш-значення.

Наприклад, компанія ***Bit9*** підтримує величезний каталог програм для *ОС Windows, UNIX і Linux*, який, зокрема, містить наступні дані: *ім'я та розмір файла, дата і час створення файла, приналежність файла до продукту, джерела даних та рівень значущості файла.*

Швидкість випуску нового шкідливого ПЗ досягла тієї межі, коли звичайної системи оновлень антивірусних баз для протидії йому стало недостатньо. Час, необхідний антивірусним

компаніям для блокування вебзагроз, становить від 4,62 до 92,48 години. Подальше принципове збільшення максимальної швидкості реакції на загрози за допомогою звичайних антивірусних оновлень неможливо, оскільки витрати часу на виявлення шкідників, їх подальший аналіз і тестування формування антивірусних оновлень вже зведені до мінімуму. Не можуть збільшити швидкість реакції і евристичні методи детектування, які дозволяють блокувати загрози в момент їх появи, не чекаючи виходу антивірусних оновлень. Рівень детектування евристичних методів складає в середньому 50–70 % відповідно 30–50 % нових загроз евристичними методами **НЕ ДЕТЕКТУЄТЬСЯ.**

Одним із рішень, що дозволить збільшити швидкість реакції на нові загрози і мінімізувати розміри антивірусних баз, зберігаючи при цьому рівень захисту на високому рівні, є ***«антивірусні хмари».***

«Антивірусна хмара» являє собою інфраструктуру, яка використовується для обробки інформації, що надходить від користувачів про підозрілі шкідливі програми з метою своєчасного виявлення нових, раніше невідомих загроз. Чим більше систем підключено до хмари, тим воно краще працює: про один й той ж підозрілий об'єкт на сервер надходить інформація від багатьох користувачів, і це стимулює виробника антивірусної програми до розробки оновлення антивірусних баз. При цьому техніка зберігання і обробки даних від користувача прихована.

Класична система оновлень антивірусних баз передбачає, що вектор взаємодії антивірусної компанії і користувача завжди направлений в одну сторону – до користувача. Ніякого зворотного зв'язку з користувачем немає, тому неможливо оперативно виявляти підозрілу активність, отримувати інформацію про поширення загроз і джерелах їх поширення. При «хмарному» підході зв'язок двосторонній. Безліч ком-п'ютерів, підключених до «хмари» повідомляють «хмарі» про джерела зараження і виявлені підозрілі активності. Після обробки отриманої інформації, вона стає доступною іншим комп'ютерам, які мають з'єднання з «хмарою». Фактично, за допомогою «хмарної» інфраструктури антивірусної компанії, користувачі в змозі оперативно ділитися між собою інформацією про проведені проти них атаки і джерела таких атак. Таким чином, виходить єдина розподілена інтелектуальна антивірусна мережа, яка працює як єдине ціле. Швидкість виявлення і блокування загроз значною мірою перевершує звичайне антивірусне поновлення. Якщо сигнатурним методам для оновлення баз необхідно декількох годин, то «хмарним технологіями» на виявлення і детектування нових загроз необхідні хвилини.

Використання «хмарного» захисту дозволяє мінімізувати розміри скачуваних користувачем антивірусних баз. Це обумовлено тим, що «хмарні» бази не доставляються на комп'ютер користувача. Однак варто підкреслити, що доступ до «хмарної» інфраструктури залежить від постійної наявності мережевого з'єднання з нею. З обривом з'єднання, «хмарний» захист відразу ж припиняється.

Контрольні запитання

1. Що таке шкідливе ПЗ і як воно класифікується?
2. У чому проявляється діяльність шкідливого ПЗ?
3. Назвіть основні канали поширення шкідливого ПЗ.
4. Що таке комп'ютерні віруси і як вони класифікуються?
5. Які бувають віруси за алгоритмом дії?
6. Назвіть різницю між поліморфним і метаморфним вірусом.
7. Які ознаки зараження ІТС вірусом?
8. Що таке мережевий хробак і чим він відрізняється від вірусу?
9. Назвіть головні функції мережевих хробаків.
10. Що таке троян і чим він відрізняється від вірусів і мережевих хробаків?
11. Як класифікуються трояни?
12. Що таке adware I riskware? Наведіть приклади.
13. Що таке ransomware і як воно проявляється?
14. Що таке spyware і які завдання виконують завдяки йому?
15. Що таке програмні закладки і якими вони бувають?
16. Назвіть основні методи виявлення шкідливих програм.
17. Поясніть ідею сигнатурного методу і його слабкі сторони.
18. У чому полягає різниця між поведінковим і евристичним методами?
19. Надайте характеристику сучасним антивірусним програмам. У чому полягають переваги і недоліки використання «антивірусних хмар»?

Розділ 6. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС

ГЛАВА 13
ЗАКОНИ, НОРМАТИВНІ ДОКУМЕНТИ І СТАНДАРТИ

13.1. Законодавство України по забезпеченню кібербезпеки

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.

Структура законодавства щодо захисту інформації

Структура державного законодавства України є багаторівневою.

Перший рівень – конституційний. На ***найвищому рівні*** знаходяться норми Конституції України, які закріплюють концептуальні положення національної безпеки України, а також Стратегії національної безпеки України, Воєнної доктрини України та Закону України «Про основи національної безпеки України». Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки в усіх сферах, у тому числі й інформаційній.

Другий рівень – загальні закони (про землю, про громадянство, про власність і т. п.), які включають норми з питань інформаційної безпеки та кібербезпеки.

Третій рівень – спеціальні закони по інформатизації і захисту інформації.

Четвертий рівень – підзаконні нормативні акти (укази, постанови, рішення, державні стандарти та ін.), відомчі накази, інструкції, керівництва.

Закони 3-го рівня

Закон України «Про основні засади забезпечення кібербезпеки України».

Закон України «Про інформацію».
Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
Закон України «Про державну таємницю».
Закон України «Про електронні документи і електронний документообіг».
Закон України «Про електронний цифровий підпис».
Закон України «Про телекомунікації».

Рис. 13.1. Стуктура схеми законів 3-го рівня

Джерело: URL: https://dut.edu.ua/uploads/p_303_79299367.pdf

Держстандарт

ДСТУ 3396.0-96 – *Захист інформації. Технічний захист інформації. Основні положення.*
ДСТУ 3396.1-96 – *Захист інформації. Технічний захист інформації. Порядок проведення робіт.*
ДСТУ 3396.2-97 – *Захист інформації. Технічний захист інформації. Терміни і визначення.*
ДСТУ 4145-2002 – *Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння.*

13.2. Нормативні документи системи технічного захисту інформації

Крім законів і підзаконних актів, впроваджено багато нормативних документів, які регламентують певні аспекти діяльності у сфері захисту інформації.

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

НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

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

НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

НД ТЗІ 3.7-001-99: Методичні вказівки з розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі.

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.

НД ТЗІ 2.5-008-02: Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

НД ТЗІ 2.5-010-03: Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу.

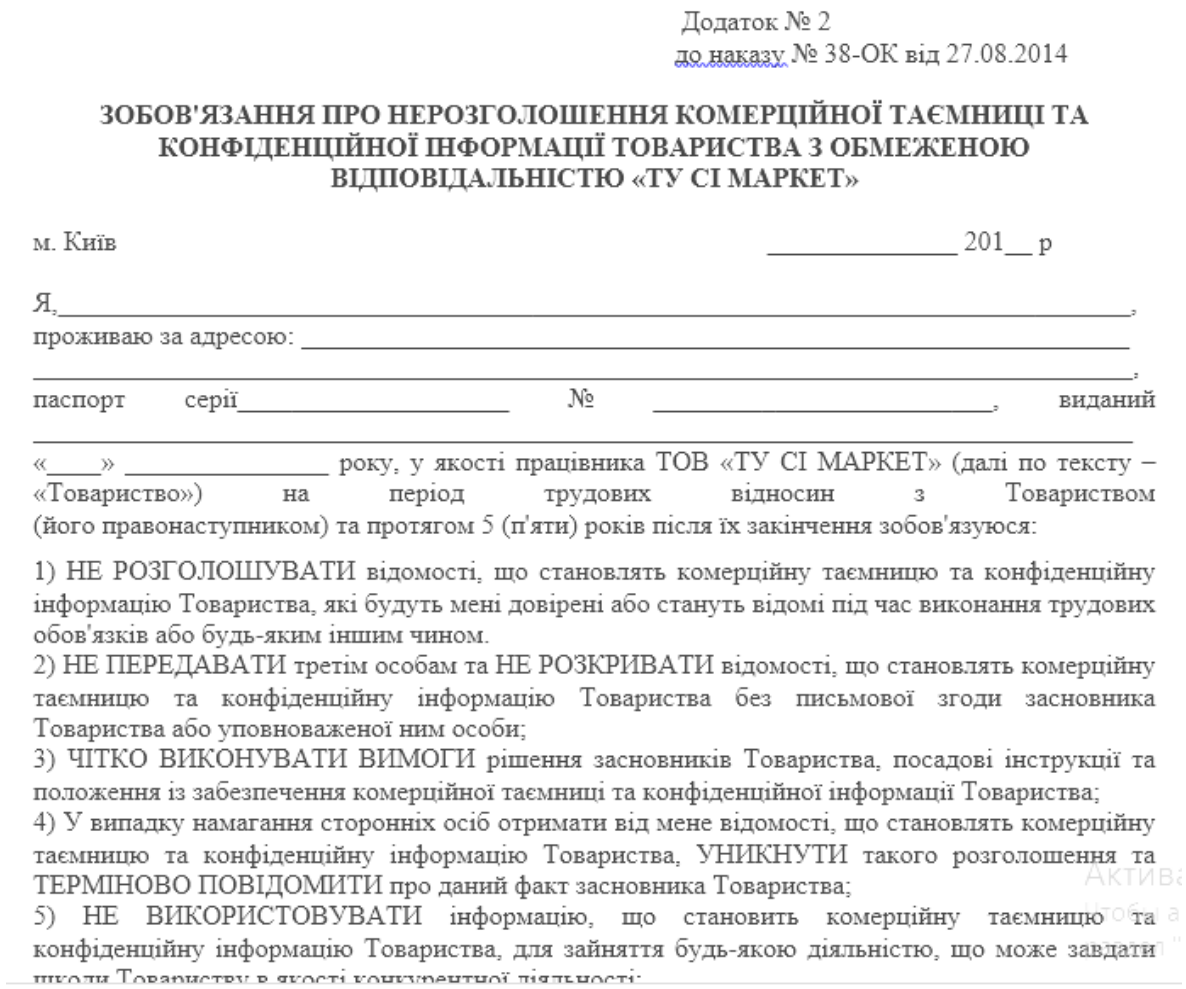
НД ТЗІ 3.7-003-05: Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

Нормативні документи організації

Опираючись на державні правові акти, конкретне підприємство (фірми, організації), розробляє власні нормативно-правові документи, орієнтовані на забезпечення безпеки ІТС.

До таких документів належать:

- *положення про збереження конфіденційної інформації;*



Додаток № 2
до наказу № 38-ОК від 27.08.2014

ЗОБОВ'ЯЗАННЯ ПРО НЕРОЗГОЛОШЕННЯ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ТА КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ТОВАРИСТВА З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ТУ СІ МАРКЕТ»

м. Київ _____ 201__ р

Я,_____,
проживаю за адресою: _____
_____,
паспорт серії_____ № _____, виданий
_____
«____» _____ року, у якості працівника ТОВ «ТУ СІ МАРКЕТ» (далі по тексту – «Товариство») на період трудових відносин з Товариством (його правонаступником) та протягом 5 (п'яти) років після їх закінчення зобов'язуюся:

1) НЕ РОЗГОЛОШУВАТИ відомості, що становлять комерційну таємницю та конфіденційну інформацію Товариства, які будуть мені довірені або стануть відомі під час виконання трудових обов'язків або будь-яким іншим чином.
2) НЕ ПЕРЕДАВАТИ третім особам та НЕ РОЗКРИВАТИ відомості, що становлять комерційну таємницю та конфіденційну інформацію Товариства без письмової згоди засновника Товариства або уповноваженої ним особи;
3) ЧІТКО ВИКОНУВАТИ ВИМОГИ рішення засновників Товариства, посадові інструкції та положення із забезпечення комерційної таємниці та конфіденційної інформації Товариства;
4) У випадку намагання сторонніх осіб отримати від мене відомості, що становлять комерційну таємницю та конфіденційну інформацію Товариства, УНИКНУТИ такого розголошення та ТЕРМІНОВО ПОВІДОМИТИ про даний факт засновника Товариства;
5) НЕ ВИКОРИСТОВУВАТИ інформацію, що становить комерційну таємницю та конфіденційну інформацію Товариства, для зайняття будь-якою діяльністю, що може завдати шкоди Товариству в якості конкурентної діяльності;

- *перелік відомостей, що становлять конфіденційну інформацію;*

Додаток № 3
до наказу № 14-К від 27.08.2014

ПАМ'ЯТКА ДЛЯ ПРАЦІВНИКА

І. ВІДОМОСТІ, ЩО СТАНОВЛЯТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ

1) До відомостей, що становлять комерційну таємницю та конфіденційну інформацію Товариства, належать:
а) собівартість товару Товариства;
б) розмір торгівельної націнки;
в) обсяги реалізації продукції
г) обсяги виробництва продукції;
д) відомості про постачальників, продавців та покупців продукції Товариства;
е) відомості про виробниче обладнання;
є) відомості про способи придбання і реалізації товару Товариства;
ж) відомості про види діяльності Товариства.
2) Технологічна інформація:
а) відомості про характер та особливості технології виробництва товару Товариства;
б) відомості про обладнання, яке використовується Товариством в процесі виробництва товару.
3) Відомості про управління Товариством:
а) відомості про способи та засоби управління Товариством;
б) відомості про засновників Товариства;
в) відомості про внутрішню структуру Товариства.
4) Відомості про фінанси Товариства:
а) відомості про систему оплати праці;
б) відомості, що розкривають показники фінансового плану;
г) майнове становище, кількість і вартість товарних запасів;
д) відомості про баланс Товариства;
е) відомості про стан банківських рахунків Товариства;
є) відомості про рівень доходів Товариства.
5) Відомості про плани Товариства:

- *інструкція про порядок допуску працівників до відомостей, що становлять конфіденційну інформацію;*
- *положення про роботу з іноземними фірмами і їх представниками та ін.*

Створюючи систему безпеки ІТС, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які наступні претензії з вашого боку до недобросовісного співробітника, клієнта, конкурента та посадової особи виявляться просто безпідставними. Якщо перелік відомостей конфіденційного характеру не доведений своєчасно до кожного співробітника (природно, якщо він допущений за посадовими обов'язками) в письмовому вигляді, то співробітник, який

вкрав важливу інформацію в порушення встановленого порядку роботи з нею, швидше за все розведе руками: ***мовляв, звідки мені це знати!*** У цьому випадку ніякі інстанції, аж до судових, не зможуть допомогти.

Вимоги забезпечення безпеки і захисту інформації відображаються в *Статуті організації*. Такі вимоги дають право адміністрації підприємства:

- *створювати організаційні структури по захисту конфіденційної інформації;*
- *включати вимоги щодо захисту інформації в договори за всіма видами діяльності;*
- *вимагати захисту інтересів підприємства з боку державних і судових інстанцій*.

При укладанні трудового договору та оформлення наказу про прийом на роботу нового співробітника робиться відмітка про обізнаність його з порядком захисту інформації підприємства. Не слід думати, що після підписання такої угоди новим співробітником таємниця буде збережена. Це попередження співробітнику, що в справу вступає система заходів щодо захисту інформації, і правова основа до того, щоб припинити його невірні або протиправні дії.

13.3. Стандарти інформаційної безпеки. Стандарт TCSEC

Безпека системи – характеристика якісна, яку неможливо виміряти. Різні фахівці пропонують різні шляхи підвищення захищеності системи і по-різному її оцінюють. Єдиний спосіб оцінити захищеність систем і узгодити думки різних фахівців – розробити стандарт, вимоги до систем і шляхи їх реалізації, а також надавав систему критеріїв і процедури оцінювання систем за цими критеріями.

Природно, що першими, хто вимагав упровадження стандартів безпеки, були військові. Оскільки інформація, якою вони володіють, має надзвичайне значення для держави, порушення безпеки інформації (як правило, розголошення) може призвести до дуже серйозних наслідків падіння міжнародного престижу держави, накладання економічних і політичних санкцій, величезних фінансових витрат на відновлення обороноспроможності, відставки уряду, зміни державного устрою і навіть до втрати державного суверенітету. Для забезпечення захисту такої інформації держави впроваджують спеціальний режим, регульований законами і державними стандартами безпеки.

Одним з перших стандартів, який вплинув на базу стандартизації безпеки в багатьох країнах, став стандарт **Міністерства оборони США «Критерії оцінки довірених комп'ютерних систем»** ***(Trusted Computer System Evaluation Criteria. TCSEC).***

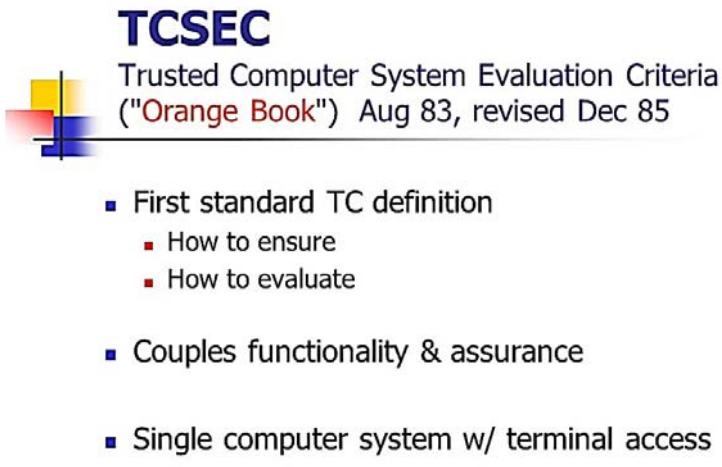


Рис. 13.2. Стандарт TCSEC ((Trusted Computer System Evaluation Criteria)

Джерело: URL: https://slideplayer.com/slide/5168978/

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 було вперше використано поширений термін ***Trusted***, який тепер здебільшого перекладають як ***«захищений»*** або ***«безпечний».*** Цей документ (частіше через колір обкладинки) називають ***«Помаранчевою книгою»***.

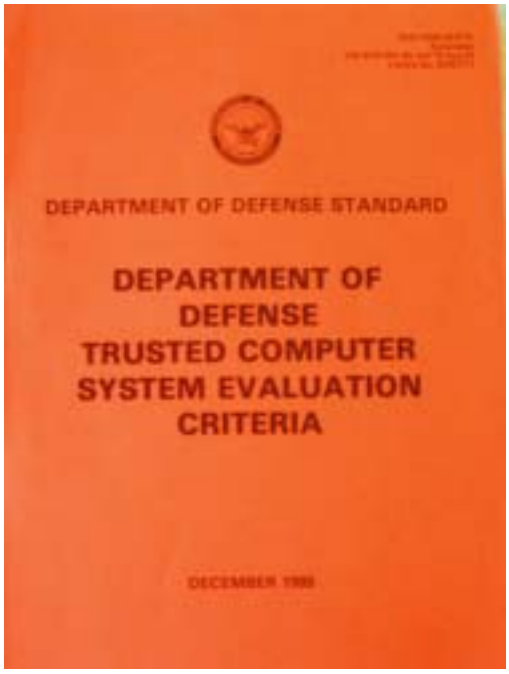


Рис. 13.3. Фотографія документа «Помаранчева книга»

Джерело: URL: https://slideplayer.com/slide/3386657/

«Помаранчева книга» пояснює поняття безпечної системи через шість фундаментальних вимог, яким повинні задовольняти такі системи, щоб пройти сертифікацію:

✹ Політика безпеки

Система має підтримувати чітко визначену політику безпеки. Можливість здійснення суб'єктами доступу до об'єктів визначається на підставі їхньої ідентифікації та набору правил керування доступом.

✹ Маркування

Для управління доступом до інформації всі об'єкти повинні бути марковані спеціальною міткою, яка надійно ідентифікує ступінь цінності об'єкта і режими допуску до нього.

✹ Ідентифікація

Усі суб'єкти мають унікальні ідентифікатори. Контроль доступу здійснюють на підставі результатів ідентифікації суб'єкта й об'єкта, підтвердження дійсності їхніх ідентифікаторів (автентифікації) і правил розмежування доступу. Дані, що використовують для ідентифікації й автентифікації, мають бути захищені від несанкціонованого доступу.

✹ Аудит

Гарантовано захищена система повинна реєструвати в захищеному файлі всі події, що відбуваються в ній і впливають на безпеку.

✹ Гарантії

Щоб гарантувати зазначені чотири вимоги з безпеки – політика, маркування, ідентифікація і аудит, необхідно передбачити набір програмних і апаратних засобів управління, який реалізує зазначені функції.

✹ Постійний захист

Усі засоби захисту мають бути захищені від несанкціонованого втручання. Такий захист має здійснюватися постійно і безперервно у будь-якому режимі функціонування системи захисту. Система не може вважатися безпечною, якщо механізми, що реалізують прийняту політику, самі не захищені.

13.4. Поняття кіберзлочинності. Класифікація кіберзлочинів

Термін *«кіберзлочинність»* часто вживається поряд з терміном *«комп'ютерна злочинність»,* причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, проте не синонімічні.

Поняття *«кіберзлочинність»* (в англомовному варіанті – ***cybercrime***) ширше, ніж *«комп'ютерна злочинність»* (в англомовному варіанті – ***computer crime***), і більш точно відображає природу такого явища, як злочинність в кіберпросторі.

*Так, Оксфордський тлумачний словник визначає приставку **«cyber-»** як компонент складного слова. Її значення – це те, що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник. Таким чином, **«cybercrime»** – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін **«computer crime»** в основному відноситься до злочинів, що скоюються проти комп'ютерів або комп'ютерних даних.*

За даними Інтерполу, кіберзлочинність є однією з найбільш швидко зростаючих сфер злочинності. Зокрема, у звіті *Європейського поліцейського управління (Європол) «Оцінка загрози організованої злочинності в Інтернеті» за 2018 рік* зазначено, що за статистичними даними ряду держав-членів Європейського Союзу кількість зареєстрованих кіберзлочинів досягає або навіть перевищує кількість традиційних злочинів.

В Україні на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини в цій сфері.

Станом на початок 2019 р. до правової основи кібернетичної безпеки України входять такі нормативно-правові акти:

- *Конституція України;*
- *Кримінальний кодекс України;*
- *Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони;*
- *Доктрина інформаційної безпеки України;*
- *Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.*

Відповідно до українського законодавства, *кібербезпека* – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (*ст. п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»)*. У глобальному розумінні, кібербезпекою є реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак.

Умовний поділ кіберзлочинів на чотири види відповідно до Конвенції про кіберзлочинність, яка є частиною українського законодавства з 11.10.2005

До першого виду належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До цього виду кіберзлочинів можна віднести всі злочини, спрямовані проти комп'ютерних систем і даних (наприклад, навмисний доступ до комп'ютерної системи або її частини; навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації; навмисне вчинення, не маючи на це права, виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, включаючи комп'ютерні програми).

До другого виду 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 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 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.

2. Комп'ютерні злочини – фальсифікація і підробка, що здійснюються з використанням комп'ютерної техніки.

3. Злочини, пов'язані з контентом – виготовлення, поширення і зберігання дитячої порнографії.

Схема Конвенції Ради Європи

У схемі, що запропонована *Конвенцією Ради Європи* й 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 ІТС в обхід заходів безпеки);*
- ➔ *незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.*

2. Шахрайство та підробка, пов'язані з використанням комп'ютерів, а саме:

- ➔ *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 щодо авторських і суміжних прав.

Усі інциденти, згідно з кодифікатором, використовуваним Міжнародною організацією кримінальної поліції – Інтерполом, мають власний ідентифікатор, який починається з літери ***Q.*** Наприклад:

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

ГЛАВА 14
Міжнародні стандарти

14.1. Класи безпеки комп'ютерних систем
14.2. Міжнародні стандарти серії ISO 27000

14.1. Класи безпеки комп'ютерних систем

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 розділені на групи A, B, C 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 С1*** 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 С2*** 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 В (мандатний захист). Основні вимоги цієї групи нормативне (мандатне) керування доступом із використанням міток безпеки, підтримка політики безпеки. У число цього рівня входять три підрівня:

▲ ***В1*** – системи, що підтримують мандатне управління доступом і взаємну ізоляцію процесів шляхом поділу їх адресних просторів;

▲ ***В2*** – система цього класу має здійснювати контроль прихованих каналів витоку інформації. Керування безпекою здійснюють адміністратори системи. Передбачені засоби керування конфігурацією. Механізми автентифікації посилені;

▲ ***В3*** – 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 А (перевірений захист). Ця група характеризується застосуванням формальних методів верифікації коректності роботи механізмів керування доступом. Група має один клас – ***А1.*** Системи цього класу еквівалентні системам класу ***В3***, 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 А***). Кожна група включає один чи кілька класів. ***Групи D і А*** містять по одному

класу (***класи D1*** і ***A1,*** відповідно), ***група С*** – ***класи С1***, ***С2***, а ***група В*** три класи – ***В1, В2, В3***, що характеризуються різними наборами вимог безпеки. Рівень безпеки зростає при русі від ***групи D*** до ***групи А***, а всередині групи – зі зростанням номера класу.

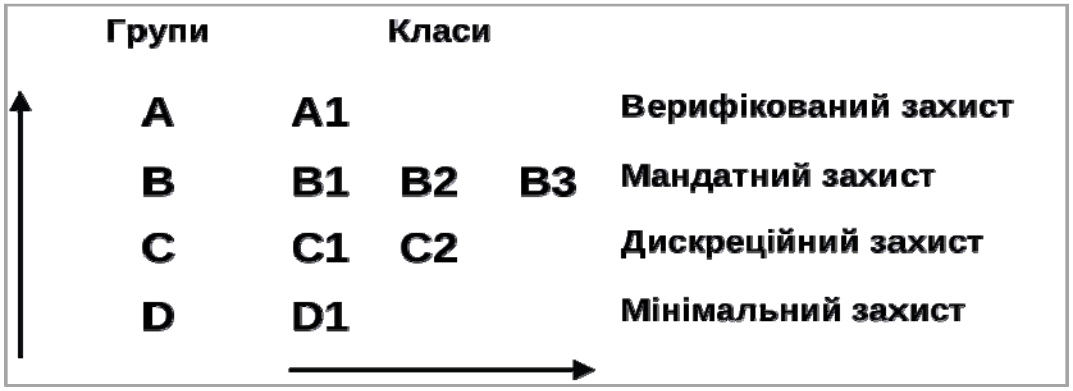


Рис. 14.1. Розподіл захисту на чотири групи, які передбачає «Помаранчева книга»

Джерело: URL: https://ktpu.kpi.ua/wp-content/uploads/2014/02/Vorobiyenko-P.P.-Telekomunikatsijni-ta-informatsijni-merezhi.pdf

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.

14.2. Міжнародні стандарти серії ISO 27000

ISO (***Міжнародна організація стандартизації***) і ***IEC*** (***Міжнародна електротехнічна комісія***) формують спеціалізовану систему всесвітньої стандартизації. ***Національні органи***, які є членами ***ISO*** або ***IEC***, беруть участь у розробці ***Міжнародних Стандартів*** через технічні комітети, створені відповідною організацією з метою роботи зі специфічними областями технічної діяльності. Технічні комітети ***ISO*** й ***IEC*** співпрацюють в областях взаємного інтересу. Інші урядові й неурядові міжнародні організації, пов'язані з ***ISO*** й ***IEC***, також беруть участь у цій роботі.

У цей час сформовано цілий ряд стандартів ***ISO/IEC*** з урахуванням їх впровадження ***у галузь «Інформаційної безпеки»:*** **стандарти серії 27000**. Основними завданнями цього проєкту 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 27001 «*Information security management systems. Requirements – Системи менеджменту інформаційною безпекою. Вимоги».*

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

ISO/IEC 27003 *«Information Security Management Systems. Guidance – Системи менеджменту інформаційної безпеки. Керівництво».*

ISO/IEC 27004 *«Information security management. Measurement – Вимірювання ефективності системи менеджменту інформаційної безпеки».*

ISO/IEC 27006 *«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 *«Guidelines for Information Security Management Systems auditing (FCD) – Керівництво для аудиту систем менеджменту ІБ».*

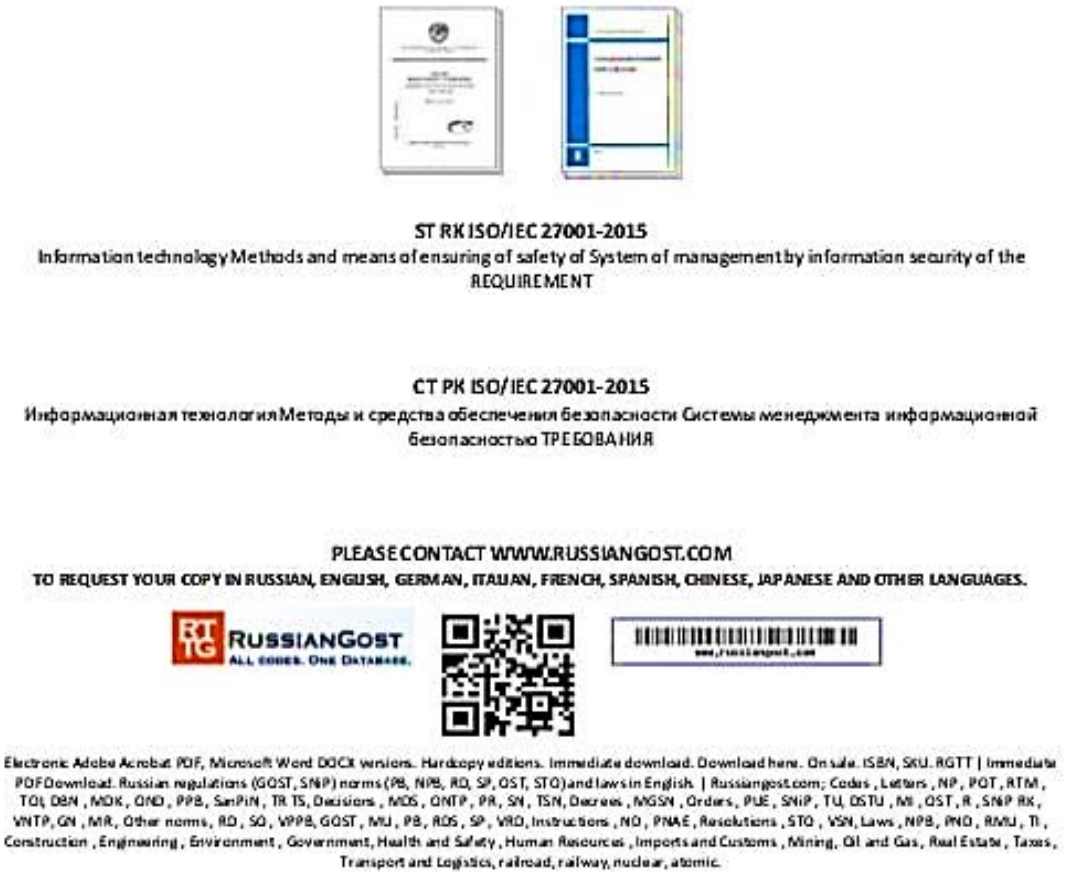


Рис. 14.2. Стандарт ISO/IEC 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник»

Джерело: URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66893

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

ISO/IEC 27001:2015 *«Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».*

(Додаток А).

А. 5. Політики інформаційної безпеки – як політики пишуться і перевіряються.

А. 6. Організація інформаційної безпеки – контроль над розподілом обов'язків.

А. 7. Безпека людських ресурсів.

А. 8. Управління активами – засоби контролю, пов'язані з інвентаризацією активів та допустимим використанням, а також для класифікації інформації і обробки носіїв.

А. 9. Контроль доступу – контролює політику контролю доступу, управління доступом користувачів, контроль доступу до системи і додатків та обов'язки користувача.

А. 10. Криптографія – засоби управління, пов'язані з шифруванням і керуванням ключами.

А. 11. Фізична і екологічна безпека – засоби контролю, що визначають безпечні зони, безпеку обладнання, безпечну утилізацію.

А. 12. Операційна безпека – управління змінами, управління потужністю, шкідливі програми, резервне копіювання, ведення журналів, моніторинг, установка.

А. 13. Безпеку зв'язку – засоби управління, пов'язані з безпекою мережі, передачею інформації, обміном повідомленнями і т. п.

А. 14. Придбання, розробка і супровід системи – засоби управління, що визначають вимоги безпеки та безпека в процесах розробки і підтримки.

А. 15. Відносини з постачальниками – контроль над тим, що включати в угоди і як контролювати постачальників.

А. 16. Управління інцидентами інформаційної безпеки – засоби контролю за повідомленнями про події та недоліки, визначення обов'язків, процедур реагування і збору доказів.

А. 17. Аспекти інформаційної безпеки управління безперервністю бізнесу – засоби управління, що вимагають планування безперервності бізнесу, процедур, перевірки і аналізу, а також надмірності ІТ.

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

Цей стандарт є офіційним документом, що описує комплексний підхід до питань інформаційної безпеки та розглядає в якості елементів управління як технічні, так і організаційно-адміністративні заходи, що забезпечують конфіденційність, цілісність, достовірність та доступність інформації. Основна ідея стандарту – допомогти комерційним та державним господарським організаціям вирішити достатньо складне завдання: забезпечення надійного захисту інформаційних ресурсів та організація ефективного доступу до даних і процесу їх обробки відповідно до визначених послуг та вимог.

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

Рис. 14.3. Стандарт ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки»

Джерело: URL: https://dnaop.com/html/62498_6.html

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*].

Стандарт використовується як стартова точка для розробки програм безпеки, на практиці часто застосовується при аудиті безпеки ІТС. Аудит по ***ISO*** складається з аналізу документації з системи менеджменту безпеки ІТС, а також вибіркового контролю в організації, який дозволяє впевнитися, що реальна практика відповідає опису системи.

Основні етапи аудиту безпеки

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.

Рекомендації, що видаються аудитором за результатами аналізу стану ІС, визначаються використовуваним 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

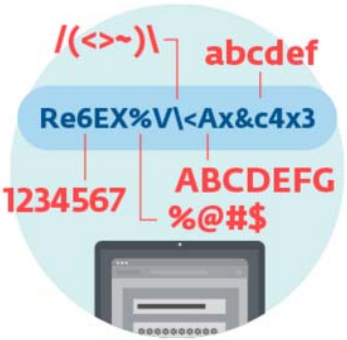
варто чекати від аудитора, як результату проведення аудиту, видачі технічного проєкту підсистеми інформаційної безпеки або детальних рекомендацій щодо впровадження конкретних програмно-технічних засобів захисту інформації. Це вимагає детальнішого опрацювання конкретних питань організації захисту, хоча внутрішні аудитори можуть брати в цих роботах найактивнішу участь.

Контрольні запитання

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. Назвіть класи безпеки комп'ютерних систем.
10. Дайте загальну характеристику міжнародним стандартам ISO 27000.

Розділ 7. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС

ГЛАВА 15
Політика безпеки



15.1. Організаційний захист

Головна мета організаційного захисту – сформувати програму робіт в області безпеки ІТС і забезпечити її виконання, виділяючи необхідні кошти і контролюючи стан справ. При цьому важливим є дотримання правил економічної ефективності – вартість реалізації програми захисту повинна бути менше можливого збитку.

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 дозволить виключити таємне проникнення сторонніх осіб, здійснити контроль за дотриманням співробітниками посадових інструкцій і режимних заходів, їх доступ до відповідного обладнання і документам.

Організація роботи з персоналом передбачає відбір персоналу, ознайомлення з ним, навчання правилам роботи з конфіденційною інформацією і розстановку персоналу в організації.

Організація роботи з інформаційними ресурсами передбачає контроль за розробкою, обліком, зберіганням і знищенням документів, робіт по налаштуванню, конфігурації і утилізації інших (непаперових) інформаційних ресурсів.

Адміністративні заходи забезпечення безпеки включають в себе:

- ➔ розробку і публікацію політик безпеки, інструкцій, процедур та настанов, що пов'язані з безпекою ІТС;
- ➔ класифікацію всієї інформації, що використовується в ІТС;

- ➔ конфігурування, тестування та контроль за системою безпеки ІТС;
- ➔ підбір персоналу, проведення тренінгів та навчань з питань безпеки;
- ➔ управління ризиками.

Ці ключові аспекти є основою програми безпеки організації чи підприємства.

Рис. 15.1. Адміністративно-організаційні заходи безпеки організації

Джерело: URL: https://dut.edu.ua/uploads/p_303_79299367.pdf

Основою адміністративного захисту є ***політика безпеки (ПБ)***, яка визначає ставлення організації до забезпечення безпеки і необхідні дії організації по захисту своїх ресурсів і активів.

Рівні політики безпеки

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, показує стратегічне і тактичне значення безпеки, вказує як все буде реалізовано.

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).

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

- організації режиму охорони;
- організації роботи з співробітниками;
- організації робота 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 ІТС 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.

15.2. Склад і структура політики 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.

Для кожної ІТС політика безпеки може бути індивідуальною і залежати від реалізованої технології обробки інформації, особливостей ІТС, фізичного середовища і багатьох інших факторів. Якщо в ІТС реалізується кілька різних технологій обробки інформації, то і політика безпеки в такій ІТС буде складовою і її частини, які відповідають різним технологіям, можуть істотно відрізнятися.

Компоненти політики безпеки

Зазвичай політика безпеки організації включає такі компоненти:

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

Базова політика безпеки встановлює, як організація обробляє інформацію, хто може отримати до неї доступ і як це можна зробити. В описі базової політики безпеки визначаються дозволені й заборонені дії, а також указуються необхідні засоби управління.

Спеціалізовані політики безпеки поділяються на дві групи:

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

До спеціалізованих політик, які зачіпають користувачів, відносяться:

➔ **Політика допустимого використання**, яка 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 самостійно встановлювати і запускати ПЗ, про регламентацію використання власного обладнання співробітників (ноутбуків, планшетів, смартфонів, USB-накопичувачів) і т. п.

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**. 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.

Приклад.

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

➔ **Політика використання Internet**.

Приклад.

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

➔ **Політика використання електронної пошти**.

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 перевірив, 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**.

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 комунебудь 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, «Любіть Україну, як сонце, любіть, як вітер, і трави, і води».
  - ► Вибрати перші літери з кожного слова: «луясля-вітів».
  - ► Набрати отриману послідовність, переключившись на англійську розкладку клавіатури: «kezckzdsnsd».
  - ► Вибрати номер символа, який буде записуватися в верхньому регістрі і після якого буде спеціальний символ. Наприклад, це буде третій символ, а в ролі 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:

- *Здійснювати періодичну перевірку – наявність пароля для доступу до інформаційних систем;*
- *Вживати заходи дисциплінарного стягнення до співробітників, які порушили правила реальної політики компанії.*

До ***спеціалізованих політик***, пов'язаних з конкретними технічними областями, відносяться:

- ❖ політика конфігурації міжмережевих екранів;
- ❖ політика щодо шифрування і управління криптоключами;
- ❖ політика використання віртуальних приватних мереж VPN;
- ❖ політика по обладнанню бездротової мережі та ін.

Три розділи кожної політики є загальноприйнятими:

- ➔ мета, яка описує, чому створена та чи інша політика;
- ➔ область прикладання політики (наприклад, політика безпеки застосовується до всіх комп'ютерних систем або політика застосовується до всіх службовців);
- ➔ відповідальність, яка визначає осіб, відповідальних за дотримання політики безпеки.

Термін ***«політика безпеки»*** може бути застосований до організації, ІТС, операційної системи, послуги, що реалізується системою (набору функцій) для забезпечення захисту від певних загроз і т. п. Наприклад, політика безпеки інформації в ІТС є частиною загальної політики безпеки організації.

Після того, як сформульована політика безпеки, приступають до складання програми її реалізації, визначають механізми і процедури реалізації політики безпеки. Під програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю виконання програми і т. п.

Розробка політики не вимагає технічних знань і не дуже приваблює ІТ-професіоналів. Крім того, не всім співробітникам сподобаються певні обмеження їх свобод, пов'язаних з дотриманням політики безпеки. Проте політика безпеки має велике значення для організації і є найбільш важливою роботою відділу безпеки.

15.3. Зразок спеціалізованої політики безпеки допустимого використання

Мета: *гарантувати використання за призначенням комп'ютерів і телекомунікаційних ресурсів Компанії її співробітниками та іншими користувачами.*

Всі користувачі комп'ютерів зобов'язані використовувати комп'ютерні ресурси кваліфіковано, ефективно, дотримуючись норм етики і законів.

Наступна політика, її правила і умови стосуються всіх користувачів комп'ютерних і телекомунікаційних ресурсів і служб компанії, де б ці користувачі не знаходилися. Порушення цієї політики тягне за собою дисциплінарні наслідки, аж до звільнення і порушення кримінальної справи. Дана політика може періодично змінюватися і переглядатися в міру необхідності.

➔ *Керівництво компанії має право, але не зобов'язана перевіряти будь-який або всі аспекти комп'ютерної системи, в тому числі електронну пошту, з метою гарантувати дотримання цієї політики.*

➔ *Комп'ютерна та телекомунікаційна системи належать Компанії і можуть використовуватися тільки в робочих цілях. Співробітники Компанії не повинні розраховувати на конфіденційність інформації, яку вони створюють, посилають або отримують за допомогою належних Компанії комп'ютерів і телекомунікаційних ресурсів.*

➔ *Користувачам комп'ютерів слід керуватися перерахованими нижче запобіжними засобами щодо всіх комп'ютерних і телекомунікаційних ресурсів і служб. Комп'ютерні та телекомунікаційні ресурси і служби включають в себе наступне: хост-комп'ютери, сервери файлів, робочі станції, автономні комп'ютери, мобільні комп'ютери, програмне забезпечення, а також внутрішні і зовнішні мережі зв'язку (інтернет, комерційні інтерактивні служби та системи електронної пошти), до яких прямо або побічно звертаються комп'ютерні пристрої Компанії.*

➔ *Користувачі повинні дотримуватися умови всіх програмних ліцензій, авторського права і законів, що стосуються інтелектуальної власності.*

➔ *Невірні, нав'язливі, непристойні, наклепницькі, образливі або протизаконні матеріали забороняється*

пересилати електронною поштою або за допомогою інших засобів електронного зв'язку, а також відображати і зберігати їх на комп'ютерах Компанії. Користувачі, які помітили або отримали подібні матеріали, повинні відразу повідомити про цей інцидент своєму керівникові.

➔ *Все, що створено на комп'ютері, в тому числі повідомлення електронної пошти та інші електронні документи, може бути проаналізовано керівництвом Компанії.*

➔ *Користувачам забороняється встановлювати на комп'ютерах і в мережі Компанії програмне забезпечення без дозволу системного адміністратора.*

➔ *Користувачам забороняється змінювати і копіювати файли, що належать іншим користувачам, без дозволу власників файлів.*

➔ *Забороняється використання комп'ютерних і телекомунікаційних ресурсів і служб Компанії для передачі або зберігання комерційних або особистих оголошень, клопотань, рекламних матеріалів, а також руйнівних програм, політичних матеріалів і будь-який інший інформації, на роботу з якої у користувача немає повноважень або призначеної для особистого використання.*

➔ *Користувач несе відповідальність за збереження своїх паролів для входу в систему. Забороняється роздруковувати, зберігати в мережі або передавати іншим особам індивідуальні паролі. Користувачі несуть відповідальність за всі транзакції, які будь-хто зробить за допомогою їх пароля.*

➔ *Можливість входу в інші комп'ютерні системи через мережу не дає користувачам права на підключення до цих систем і на використання їх без спеціального дозволу операторів цих систем.*

ГЛАВА 16
Процедури політики безпеки

16.1. Процедури реалізації політики безпеки
16.2. Оновлення ПЗ та зниження привілеїв

16.1. Процедури реалізації політики безпеки

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

Процедура управління персоналом

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. 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. 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 ІТС. Можна штучно «розщепити» пароль супер-користувача, повідомивши першу його частину одному співробітнику, а другу – іншому. Тоді критично важливі дії по адмініструванню ІТС 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

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

Ненавмисні помилки системних адміністраторів користувачів і неналежне виконання інструкцій політики безпеки загрожують ушкодженням апаратури, руйнуванням 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.

▲ *Конфігураційне управління* дозволяє контролювати і фіксувати зміни в поточній конфігурації ІТС, надаючи можливість у випадку якихось модифікацій в системі повертатися до працюючої версії, наприклад після аварії. 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 проєкти нових моделей від своїх конкурентів. Компанія вирішує обмежити доступ в ту будівлю, де розробляються моделі нових автомобілів, і пропускати туди тільки співробітників групи проєктування.

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 проєктування «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 проєктування 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 проєктування 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 зловмисника в будівлю, оскільки ідентифікує співробітників групи проєктування тільки за ознакою володіння карткою. Зловмисник 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, викупивши у фахівця, який встановив зчитувач карток, додаткову картку або викравши картку при поштовій 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 проєктування для проходу в будівлю не тільки користуватися карткою, а й вводити PIN-код. У цьому випадку завдання зловмисника 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.*

16.2. Оновлення ПЗ та зниження привілеїв

Яскравим прикладом використання організаційних заходів для підвищення безпеки ІТС є своєчасне оновлення ПЗ ІТС і зниження привілеїв користувачів ***ІТС.***

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 ***CyLab університета Карнеги*** 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 вразливість (***vulnerability***) системи. Деякі фахівці навіть вважають, що помилка в коді програми (баг) і вразливість це одне і те саме.

В якості окремої загрози, вразливість може перебувати в браузері. Під час відвідування вебсайта через такий браузер, спеціальний код на сайті може встановити шкідливе програмне забезпечення за допомогою цієї вразливості.

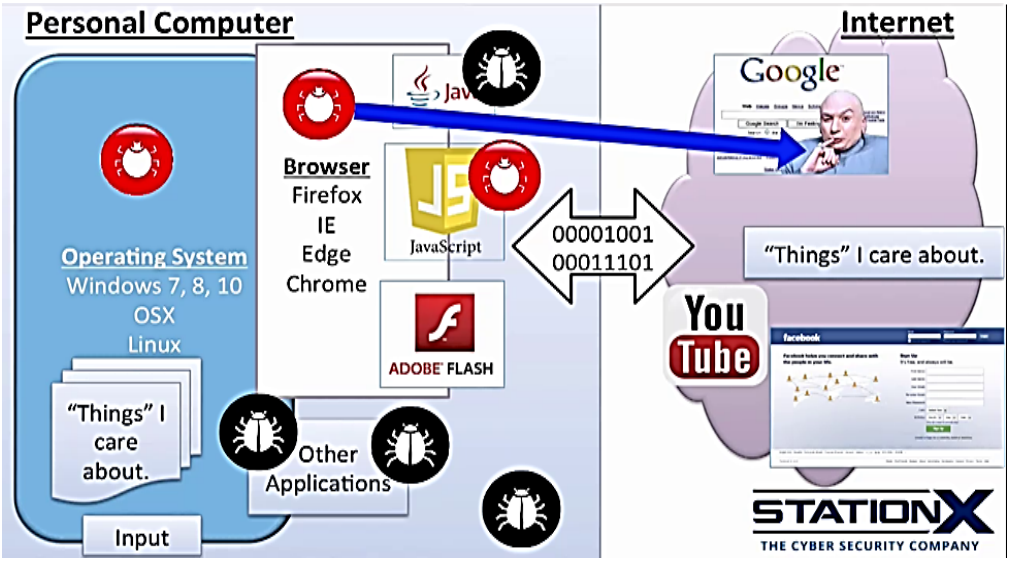


Рис. 16.1. Приклад вразливості в браузері

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Вразливості системи можуть бути ще не виявленими (***вразливості нульового дня, 0-day***), відомими тільки теоретично, або ж загальновідомими, що активно використовуються зловмисниками.

Рис. 16.2. Відомі і невідомі вразливості

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Для загальновідомих вразливостей в програмних продуктах виробники регулярно випускають виправлення, звані патчами (***patch – латка***), і якщо пропатчити систему, подібні вразливості нейтралізуються.

Патч (латка) – це програмний код, який використовується для модифікації конкретної програми. Іншими словами *латка* – це додаткова програма, яку слід запустити на виконання, якщо в уже програмному забезпеченні виявилася помилка або вразливість. При цьому часто можна встановлювати патч без видалення основної програми і навіть без завершення її роботи – в першу чергу це стосується операційних систем.

Патчінг – це вкрай важливий засіб щодо забезпечення безпеки, суть якого в регулярному оновленні програмного забезпечення. Важливо оновлювати всі програмні додатки, фірмове ПЗ, операційні системи, все. Оновлення – це 90 % виправлення виявленої вразливості в ПЗ.

Оновлення, пов'язані з нейтралізацією вразливості, 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:*
   - браузери ***Opera, Edge, Firefox, Chrome***;
   - розширення браузерів і плагіни типу ***Java, Flash, Silverlight***;
   - поштові клієнти типу ***Outlook*** або T***hunderbird***, 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 неперевірених 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.

ВАЖЛИВО!!!

1. *Якщо втрачаєте з поля зору питання установки патчів, то питання, зламають систему чи ні, навіть не виникає, це лише питання часу.*
2. *Забудьте про налаштування безпеки, якщо не виконується оновлення операційної системи.*

«Вівторок патчів» – це неофіційне позначення дати регулярних публікацій оновлень безпеки від Microsoft для їх програмних продуктів. Це відбувається в другий, а іноді в четвертий вівторок кожного місяця.

Бюлетень з безпеки від Microsoft

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 вразливості.

Якщо вибрати конкретний *патч (KB3089656),* то помітимо, яку проблему він закрив, побачимо *CVE* з певним номером *(CVE-2019-2507).* Якщо натиснути на цей номер, то потрапимо на сайт з типовими вразливостями і помилками конфігурації. На цьому сайті зазначено, що дана вразливість була виявлена групою *Hacking Team,* вони використовували цей *баг* для зламу комп'ютерів.

Якщо зайти на сайт *CVE Details* по даної вразливості, то можна побачити, що вона особливо небезпечна. Оцінка за загальною системою вразливостей *CVSS – 9.3. «Дозволяє віддаленим атакуючим виконувати довільний код».*

Подібні вразливості з віддаленим запуском довільного коду або переповненням буфера особливо небезпечні. Всі вразливості, які оцінюються як критичні, отримують цю оцінку обґрунтовано, і їх обов'язково потрібно виправляти за допомогою *патчів*.

Деталі вразливостей 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

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 залогіненого 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 безпеці комп'ютера. Тому що інші особи, дістався 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

Щоб забезпечити максимальну безпеку комп'ютера, рекомендується включити *контроль облікових записів (UAC)*. Контроль облікових записів використовується для запобігання несанкціонованим змінам на комп'ютері. При спробі внесення змін, що вимагають прав адміністратора, виводиться відповідне повідомлення і запит на введення пароля адміністратора. При цьому важливо не вводити сліпо адміністраторський пароль при виникненні запиту, а цікавитися причиною, по якій він запитується і переконатися, що це справжній запит.

Відповідно до щорічного звіту про вразливість продуктів *Microsoft* від *Avetco,* видалення адміністраторських привілеїв у користувача в *Windows* призводить до зупинки 86 % всіх загроз під *Windows*, і це неприємна статистика. Це демонструє, наскільки важливо користуватися обліковим записом не адміністратора, а звичайного користувача в *Windows.*

ГЛАВА 17
Управління ризиками

17.1. Ризики безпеки ІТС
17.2. Типові витрати на забезпечення безпеки ІТС

17.1. Ризики безпеки ІТС

Абсолютна безпека ІТС 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 ІТС можуть тільки знизити ймовірність негативних впливів або збиток від них, але не виключити їх повністю.

Виходячи з цього, метою забезпечення безпеки ІТС 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 збереження і цілісності.

Аналіз ризиків

Оцінку можливих збитків надає аналіз ризиків. Останній полягає в тому, щоб виявити існуючі загрози і вразливості, 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.

Кроки процесу аналізу ризиків

Крок 1. Визначити цінність активів.

Активи можуть бути матеріальним (комп'ютери, обладнання, матеріали) або нематеріальні (репутація, дані, інтелектуальна власність). Фактична вартість матеріального активу визначається на підставі вартості його придбання, розробки та підтримки. Наприклад, вартість сервера становить $5000, але це не є його цінністю, яка розраховується при оцінці ризиків. Цінність визначається витратами на його заміну або ремонт, втратами через зниження продуктивності, збитком від пошкодження або втрати даних, які на ньому зберігаються. Саме це визначатиме збиток для компанії у разі пошкодження або втрати сервера з тієї чи іншої причини.

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.

Крок 3. Оцінити потенційні втрати (грошова оцінка збитку) від кожної з розглянутих загроз.

Крок 4. Розрахувати загальний ризик.

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 × × 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 ІТС.

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.

Величина збитків з описом (у балах)

Величина збитків, бали	О п и с
0	*Загроза не завдає збитків або вони мінімальні*
1	*Збитки є, але фінансові операції та позиція підприємства не постраждали*
2	*Фінансові операції не проводяться протягом деякого часу*
3	*Підприємство зазнає збитків, але позиція його та клієнтура змінюється не значно. Збитки значні від підприємства, втрачається значна частина клієнтів*
4	*Збитки дуже значні. Підприємство на період до 1 року втрачає позиції на ринку. Для відновлення роботи потрібні значні фінансові кредити*
5	*Підприємство перестає існувати*

Джерело: URL: https://dut.edu.ua/uploads/p_303_79299367.pdf

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	3x5=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. 17.1. Приклад оцінки ризиків

Джерело: URL: https://dut.edu.ua/uploads/p_303_79299367.pdf

Наступним етапом є таблиця ризиків підприємства. Вона має такий вигляд (рис. 17.2):

ПРИКЛАД **розрахунку загального ризику за рік**
1. Викрадення ключової інформації – 20/61≈30% 2. Зараження системи вірусами – 15/61 ≈ 25% 3. Помилки персоналу – 8/61 ≈ 13% 4. Хакерська атака – 8/61 ≈ 13% 5. Відмови обладнання та ПЗ – 6/61 ≈ 10% 6. Наслідки стихійних лих – 4/61 ≈ 7%

Рис. 17.2. Приклад розрахунку загального ризику за рік

Джерело: URL: https://dut.edu.ua/uploads/p_303_79299367.pdf

Крок 5. Вибрати контрзаходи для протидії кожній загрозі (створити службу кібербезпеки, контролювати фізичний і логічний доступи до ІТС, встановити додаткове ПЗ і т. п.), виконати аналіз витрат обраних контрзаходів. 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.

Наприклад, компанія А вирішує захистити ряд своїх ресурсів за допомогою систем реагування на втручання ***(IPS),*** вартістю **$ 5000**. Ця ***IPS*** повинна бути протестована, щоб переконатися в безпеці і ефективності її впровадження. Після цього необхідно встановити і налаштувати сенсори і програмне забезпечення для моніторингу, налаштувати комунікаційне обладнання, направивши всі потоки трафіку

через ***IPS***, а також обмежити доступ до консолі ***IPS***, налаштувати базу даних сигнатур атак. При цьому потрібно враховувати можливе зниження продуктивності мережі, можливі незручності для користувачів, а також витрати часу і грошей на навчання персоналу і витрати на реагування при спрацюванні ***IPS***. Крім того, може виникнути необхідність закупівлі додаткових засобів оповіщення адміністратора безпеки про інциденти, виявлених IPS. Таким чином початкова ціна збільшується: **$ 5000** – сама система, **$ 2,500** – навчання персоналу, **$ 3,400** – тестування системи, **$ 2,600** – втрати продуктивності користувачів, викликані впровадженням цієї системи і ще **$ 4,000** – налаштування комунікаційного обладнання, установка ***IPS***, виявлення помилок, установка патчів. Реальна вартість цього захисного заходу складе **$ 18,000**. Якщо при цьому розрахована величина ймовірного збитку становить лише **$ 9,000**, застосування цієї ***IPS*** неефективно і призведе до перевищення бюджету.

Крок 6. Оцінити залишковий ризик.

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, або переадресація ризику* виконується шляхом укладення страхової угоди з страховою компанією.

▲ ***Уникнення ризику*** виконується шляхом припинення діяльності, що викликає ризик.

▲ ***Прийняття ризику*** – змиритися з ризиком і не витрачати гроші на захист від нього (це доцільно, якщо вартість захисних заходів перевищує величину можливого збитку).

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.

17.2. Типові витрати на забезпечення безпеки ІТС

Витрати, пов'язані з безпекою ІТС, 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 ІТС);
3. Внутрішні витрати на ліквідацію наслідків порушень політики безпеки ІТС (витрати, понесені в результаті того, що необхідний рівень захищеності НЕ був досягнутий);
4. Зовнішні витрати на ліквідацію наслідків порушення політики безпеки ІТС;
5. Витрати на технічне обслуговування системи безпеки ІТС і заходи щодо запобігання порушенням політики безпеки ІТС (попереджувальні заходи).

Витрати на формування та підтримку ланки управління системою захисту інформації

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 (визначення і підтвердження досягнутого рівня захищеності ресурсів ІТС) поділяються на:

- ➔ *контроль за дотриманням політики безпеки ІТС:*
  - ✹ витрати на контроль реалізації функцій, що забезпечують управління безпекою ІТС;
  - ✹ витрати на організацію взаємодії між підрозділами для вирішення конкретних завдань по забезпеченню безпеки ІТС;
  - ✹ витрати на проведення аудиту безпеки по кожній частині ІТС;
  - ✹ 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 підрозділах;
  - ✹ 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 проєктування 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 ІТС.

Внутрішні витрати на ліквідацію наслідків порушень політики безпеки ІТС

Внутрішні витрати на ліквідацію наслідків порушень політики безпеки ІТС (витрати, понесені в результаті того, що необхідний рівень захищеності не досягнутий) поділяються на:

➔ *перегляд політики безпеки ІТС (проводиться періодично):*

- витрати на ідентифікацію загроз безпеки ІТС;
- витрати на пошук вразливостей системи безпеки ІТС;
- оплата фахівців, які виконують роботи по визначенню можливих збитків і переоцінки ступеня ризику.

➔ *витрати на ліквідацію наслідків порушення режиму безпеки:*

- відновлення системи безпеки ІТС 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 ІТС (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 ІТС

Зовнішні витрати на ліквідацію наслідків порушення політики безпеки ІТС 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.

➔ *втрати 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 ІТС

Витрати на технічне обслуговування системи безпеки ІТС і заходи щодо запобігання порушенням політики безпеки ІТС (попереджувальні заходи) поділяються на:

➔ *витрати на управління системою безпеки ІТС:*
- витрати на планування системи безпеки ІТС;
- витрати на вивчення можливостей інфраструктури щодо забезпечення безпеки ІТС;
- витрати на технічну підтримку персоналу при впровадженні засобів захисту інформації та процедур, а також планів з безпеки ІТС;
- перевірка співробітників на лояльність, виявлення загроз безпеки ІТС;
- 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 ІТС;
- 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 ІТС:*
- витрати на контроль змін стану інформаційного середовища;
- витрати на систему контролю за діями виконавців.

➔ *забезпечення відповідності використовуваних ІТС заданим вимогам:*
- витрати на забезпечення відповідності використовуваних ІТ вимогам по безпеки, сумісності і надійності, в тому числі аналіз можливих негативних аспектів ІТС, 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 ІТС;
- розвиток нормативної бази та технічної оснащеності підрозділу безпеки.

Як бачимо, високоефективна система захисту коштує дорого, використовує при роботі істотну частину ресурсів комп'ютерної системи. Зайві заходи безпеки, крім економічної неефективності, призводять до створення додаткових незручностей і роздратування персоналу. Важливо правильно вибрати той достатній рівень захисту, при якому витрати на контрзаходи і розмір можливих збитків були б прийнятними.

Отже, мета захисту ІТС – це мінімізація ризиків для суб'єктів. Захист (забезпечення безпеки) ІТС – це безперервний процес управління ризиками, пов'язаний з виявленням інформаційних активів (цінностей), які підлягають захисту,

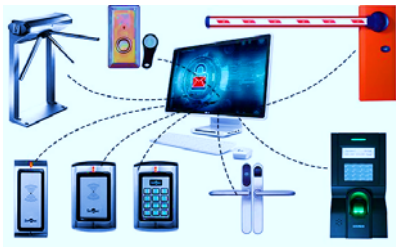
визначенням вартості цих активів, розмірів збитків та ризику, розробкою плану дій щодо захисту і вибором технологій, що реалізують цей план. На практиці це означає зведення всіх значущих для суб'єктів погроз до допустимого (прийнятного) рівня залишкового ризику, і захист найбільш важливих (критичних) інформаційних ресурсів, виходячи з існуючих можливостей і наданих фінансових коштів.

Контрольні запитання

1. Що таке організаційний захист і з чого він складається?
2. Назвіть основні адміністративні заходи забезпечення безпеки ІТС.
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 ІТС.
7. У чому полягає і для чого впроваджується принцип мінімізації привілеїв?
8. Що таке патчінг і для чого він проводиться?
9. Яке ПЗ найбільш потребує своєчасного оновлення?
10. Що таке «вівторок патчів» і в чому полягає його зміст?
11. Назвіть джерела інформації по виявленим вразливостям і методики їх усунення.
12. Що таке аналіз ризиків безпеки ІТС?
13. Назвіть основні кроки аналізу ризиків.
14. У чому різниця між кількісним і якісним підходами до аналізу ризиків безпеки?
15. Як розраховується загальний ризик? Наведіть приклад.
16. Назвіть типові витрати на забезпечення безпеки ІТС.

Розділ 8. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІТС

ГЛАВА 18
ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ



18.1. Загальна характеристика інженерно-технічних засобів безпеки

Некомпетентність і неакуратність співробітників при виконанні своїх обов'язків є однією із значущих загроз безпеки ІТС, 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 ІТС.

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.

За своїм функціональним призначенням засоби інженерно-технічного захисту інформації діляться на фізичні та технічні.

Фізичні засоби захисту

Всі фізичні засоби захисту можна розділити на три групи:

- ➔ засоби попередження (решітки, замки, сейфи та ін.);
- ➔ засоби виявлення (системи сигналізації про незаконне проникнення, системи відеоспостереження);
- ➔ засоби ліквідації загроз (система пожежогасіння, вентиляції, охолодження тощо).

Технічні засоби захисту

Технічні засоби захисту являють собою різні електронні та електронно-механічні пристрої. До цієї групи відносять:

▲ 1. Засоби захисту кабельної системи (мережі електроживлення, комп'ютерні мережі, телефоні мережі, мережі сигналізації і оповіщень, заземлення).

▲ 2. Засоби захисту від витоку інформації по різних фізичних полях, що виникають під час роботи технічних засобів (засоби виявлення шпигунської апаратури, засоби електромагнітного екранування пристроїв або приміщень, засоби активного маскування з використанням широкосмугових генераторів шумів тощо). Ці засоби захисту інформації дуже різноманітні, оскільки існує величезна кількість різних за фізичною природою каналів витоку інформації, а також фізичних принципів, на основі яких працюють системи несанкціонованого доступу.

Наприклад, відомо, що робота електронної техніки супроводжується електромагнітним випромінюванням і наведеннями на провідні лінії, що виникають внаслідок електромагнітних впливів. У деяких випадках інформацію, оброблювану засобами ЕОТ, можна відновити шляхом аналізу електромагнітних випромінювань і наведень. Для цього необхідно здійснити його прийом і декодування, що можливо навіть за допомогою загальнодоступних радіоелектронних засобів.

▲ 3. Засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється, в іншому будинку (можливо, в іншому районі або в іншому місті).

Технічні засоби за своїми можливостями поділяються на засоби захисту інформації загального призначення, розраховані на використання непрофесіоналами, і професійні комплекси, що дозволяють проводити ретельний пошук, виявлення та локалізацію загроз. Ці засоби можуть бути або вбудованими в апаратуру комп'ютера, або реалізованими у вигляді окремих продуктів, створених спеціально для вирішення проблем безпеки.

18.2. Фізичний захист

Фізичні методи захисту опираються на використання автоматизованих механічних, електричних, електронних та інших пристроїв і систем. Вони забезпечують фізичну безпеку споруд і приміщень (температура в приміщенні 10...26 °С,

вологість повітря 35–50 %), самої інформаційної системи, підтримуючої інфраструктури та допоміжного обладнання. Головні заходи з фізичного захисту мають на меті захист від вогню, води, пилу, корозійних газів, електромагнітного випромінювання, вандалізму тощо, а також захист від несанкціонованого доступу до приміщень. При цьому вимоги до кожного захисного бар'єра та місця його розташування мають визначатися цінністю інформації і ризиком порушення безпеки.

Існують наступні напрями фізичного захисту:

- ➔ захист території і приміщень ІТС від проникнення порушників (фізичне управління доступом);
- ➔ захист підтримуючої інфраструктури;
- ➔ захист апаратних засобів ІТС і носіїв інформації від розкрадання;
- ➔ захист від віддаленого відеоспостереження (підслуховування) за роботою персоналу і функціонуванням технічних засобів ІТС;
- ➔ захист від перехоплення інформації, викликане працюючими технічними засобами ІТС і лініями передачі даних.

Два останніх напрями пов'язані з технічними каналами витоку інформації.

***Заходи фізичного управління доступом* це:**

- ✹ надвисокочастотні, ультразвукові й інфрачервоні системи, призначені для виявлення об'єктів, що рухаються в межах розташування ІТС та її ресурсів з умов визначення їхніх розмірів, швидкості й напряму переміщення;
- ✹ лазерні й оптичні системи, що реагують на перетинання порушниками світлових променів;

- периметрові телевізійн системи, призначені для спостереження за охоронюваними об'єктами, в межах яких знаходиться ІТС та її ресурси;
- пропускні системи на базі технологій *smart-card*, *touch-memory*, це охорона, двері із замками, перегородки, телекамери, датчики руху і багато іншого.

Рис. 18.1. Приклади заходів фізичного управління доступом

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Все це дозволяє контролювати і обмежувати вхід і вихід співробітників і відвідувачів. Контролюватися може вся будівля організації, а також окремі приміщення, наприклад, ті, де розташовані сервери, комунікаційна апаратура і т. п. Сервери не повинні стояти відкрито на столі та ще й в незамкнутій кімнаті, куди може зайти хто завгодно (кімнати з комп'ютерами повинні закриватися на замок або перебувати під цілодобовим наглядом).

Мобільні та портативні комп'ютери – принадний об'єкт крадіжки. Їх часто залишають без нагляду, в автомобілі або на роботі, і викрасти такий комп'ютер зовсім нескладно. В організації, яка пильнує за безпекою ІТС необхідно організувати захист апаратних засобів і носіїв інформації від банального розкрадання.

Перехоплення даних може здійснюватися найрізноманітнішими способами, починаючи з читання документів у сміттєвому ящику і закінчуючи декодуванням мережевих пакетів, переданих через супутникові канали зв'язку. Існує безліч технічних каналів витоку інформації, якими може скористатися зловмисник.

18.3. Технічні канали витоку інформації

Інформаційно-телекомунікаційні системи при їх функціонуванні створюють у навколишньому просторі побічні електромагнітні, акустичні та інші випромінювання, які пов'язані з обробкою інформації. Подібні випромінювання можуть виявлятися на досить значних відстанях (до сотень метрів) і використовуватися зловмисниками для того, щоб отримати доступ до інформації. Таким чином відбувається витік інформації.

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 ІТС, можливий по технічних каналах.

Технічний канал витоку інформації, так само як і канал передачі інформації, складається з:

- ➔ джерела сигналу;
- ➔ фізичного середовища його поширення;
- ➔ приймальної апаратури зловмисника.

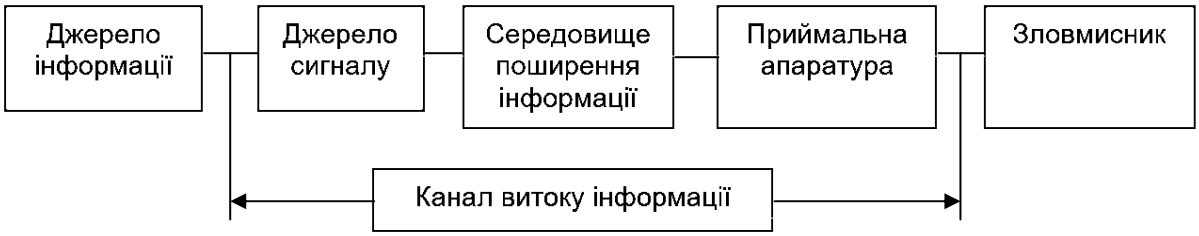


Рис. 18.2. Схема технічного каналу витоку інформації

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

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 інформації

Середовище поширення інформації визначає той маршрут, по якому сигнал з інформацією поширюється в просторі, і може бути як вільним простором, так і направляючими лініями,

наприклад, проводами, різними інженерними комунікаціями, якимись іншими конструкціями залежно від природи сигналу з інформацією.

Розподіл технічних каналів витоку інформації

Технічні канали витоку підрозділяються на:

- ➔ акустичні;
- ➔ оптичні;
- ➔ радіоелектронні.

Акустичні канали

Акустичний канал – канал, пов'язаний з поширенням звукових хвиль.

Акустичні канали можна розділити на повітряні, вібраційні, електроакустичні і оптико-акустичні.

В якості джерела в такому каналі можуть виступати людська розмова або звуковідтворююча апаратура. Середовищем поширення для даного каналу може виступати як повітря, так і рідини, або тверді тіла, у яких звукова хвиля викликає коливання.

В якості приймачів інформації для цього каналу витоку інформації використовуються: направлені і ненаправлені мікрофони, радіомікрофони, диктофони, стетоскопи та інші пристрої знімання звукової інформації. Спрямовані мікрофони дозволяють прослуховувати розмови на відстані до 300... 500 м (в умовах міста – до 50...70 м).

В основному використовуються три види спрямованих мікрофонів:

- ➢ параболічні (рефлекторні);
- ➢ трубчасті («мікрофон-труба»);
- ➢ плоскі (мікрофонні грати).

Рис. 18.3. Технічні канали витоку акустичної інформації

Джерело: URL: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

Для того щоб перехопити інформацію з використанням спрямованого мікрофону, потрібно дуже чітко направити його на джерело звукового коливання і таким чином цей сигнал можна перехопити.

Рис. 18.4. Спрямовані мікрофони

Джерело: URL: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_ Tekhnichni_kanaly_vytku_inf.pdf

Радіомікрофони або мікрофонні радіозакладки – це мініатюрні радіопередавачі з вбудованим мікрофоном. Звичайні радіомікрофони, завдяки своїм невеликим розмірам, успішно монтуються в елементи декору, технічних пристроїв, звичайні розетки електроживлення тощо. Також можуть бути приховані в елементах одягу, авторучках або запальничках.

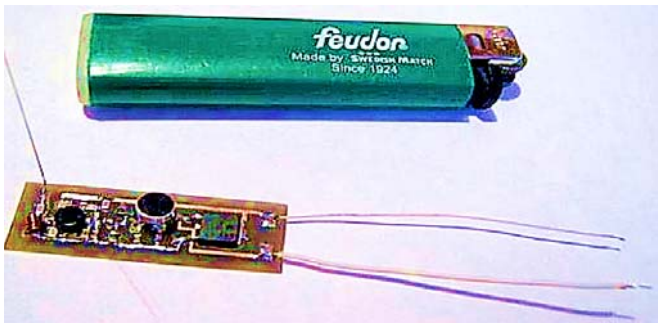


Рис. 18.5. Мікрофонні радіозакладки

Джерело: URL: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_ Tekhnichni_kanaly_vytku_inf.pdf

У вібраційних каналах середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалювання, каналізації та інші тверді тіла. Для перехоплення акустичних коливань у цьому випадку використовуються контактні мікрофони (стетоскопи).

Рис. 18.6. Середовище поширення акустичних сигналів

Джерело: URL: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

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.

Електроакустичні канали витоку інформації виникають за рахунок перетворень акустичних сигналів в електричні в тих пристроях, що мають ***«мікрофонний ефект».***

Деякі електронні елементи оргтехніки мають властивість змінювати свої параметри (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу. Зміна параметрів призводить до модуляції струмів, що протікають по цих елементах інформаційним сигналом, що міститься в акустичній хвилі. Промодульовані сигнали випромінюються в простір, де можуть бути перехоплені засобами радіорозвідки.

Отримувати інформацію можна і за допомогою ВЧ-нав'язування, при опроміненні потужним високочастотним сигналом приміщення, в якому встановлено пристрої, що володіють ***«мікрофонним ефектом»,*** і отримувати в відбитій хвилі сигнал, що модульований акустичною хвилею. (Посольство США в Москві).

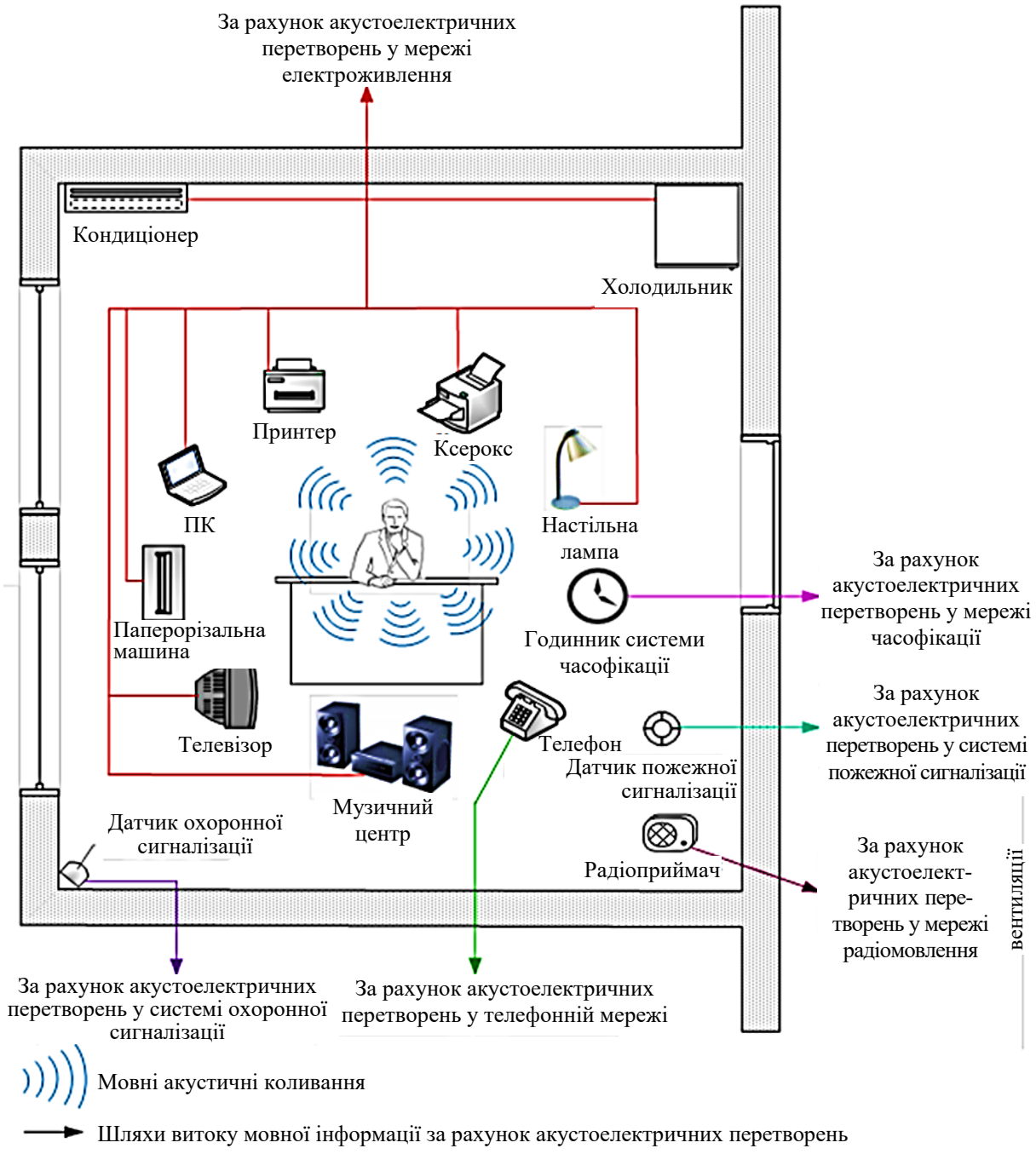


Рис. 18.7. Електроакустичні канали витоку інформації

Джерело: URL: https://tzi.com.ua/akustichn-kanali-vitoku-nformacz.html

У 1945 році посол США в СРСР Аверел Гарріман отримав в подарунок від піонерів Москви – вирізаний з дерева герб Сполучених Штатів Америки. Герб прикрашав стіну кабінету при чотирьох послах, і тільки на початку 50-х років фахівці посольства по виявленню прихованих електронних засобів побачили в ньому підслуховуючий пристрій.

*– **«Ми знайшли його, але не знали принцип дії»**, – згадує С. Пітер Карлоу, начальник служби спеціального обладнання ЦРУ.*

*– **«В гербі знаходилося пристрій, схожий на пуголовка з маленьким хвостиком. У СРСР було джерело довгохвильового сигналу, який змушував датчики всередині герба резонувати».***

Таким чином, голос людини впливав на характер резонансних коливань пристрою, дозволяючи здійснювати перехоплення слів на відстані по організованому радіоканалу.

Оптико-акустичний канал утворюється за допомогою лазера, тому іноді цей канал називають лазерним.

Рис. 18.8. Оптико-акустичний канал (лазерний канал)

Джерело: URL: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

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 встановлений в одному або різних місцях (радіус дії до 500 м).

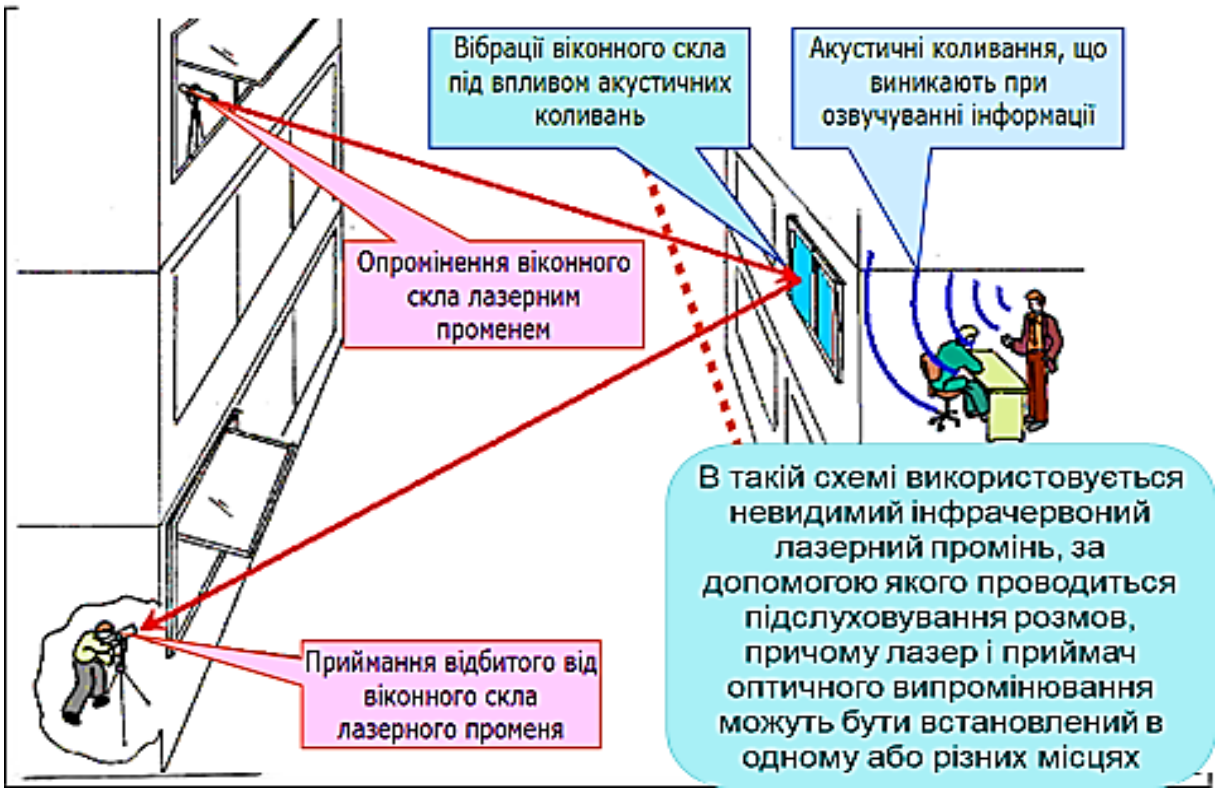


Рис. 18.9. Оптико-акустичний канал (в схемі використовується невидимий інфрачервоний лазерний промінь, за допомогою якого проводиться підслуховування розмов)

Джерело: URL: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

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.

Оптичний канал витоку інформації

Оптичний канал – канал, пов'язаний з можливістю дистанційного візуального спостереження за роботою пристроїв без проникнення в приміщення, де розташовані компоненти системи (наприклад, фотографування, відеозйомка, спостереження).

Для спостереження можуть використовуватися різні технічні засоби:

- *для спостереження вдень* – оптичні прилади (монокуляри, підзорні труби, бінокли, 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.

Відеозображення з телевізійних камер може передаватися на монітори як по кабелю, так і по радіоканалу.

Рис. 18.10. Оптичні канали витоку інформації (технічні засоби для спостережень)

Джерело: URL: http://radiotech.cv.ua/documents/book/KONSPEKT_KANAL.pdf

Електромагнітний канал витоку інформації

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 ІТС.

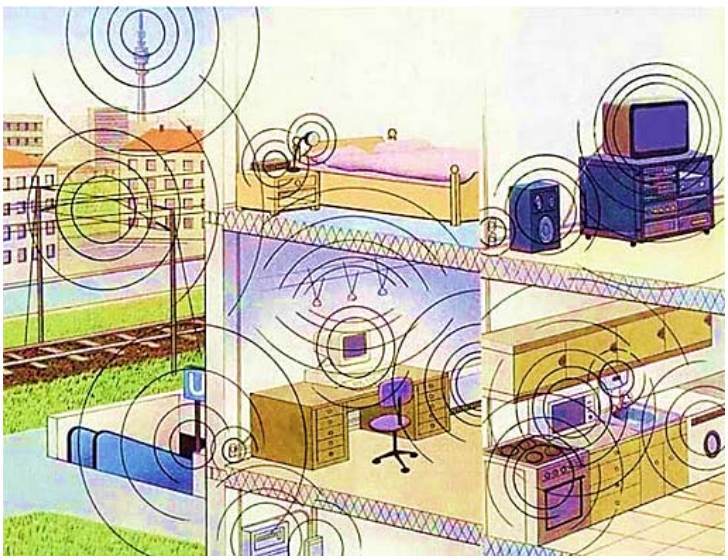


Рис. 18.11. Електромагнітний канал витоку інформації (носієм інформації – електромагнітні випромінювання)

Джерело: URL: http://radiotech.cv.ua/documents/book/KONSPEKT_KANAL.pdf

Поширюючись, це поле дає можливість приймати його і дедектувати спеціальними пристроями (*використання випромінювання*).

Крім того, виникаюче електромагнітне поле може індукціювати струм у близько розташованих дротових лініях (*використання наведення*). Випромінювання, що створюються блоками ІТС, наводяться на проводи та кабелі і можуть поширюватися по ним на великі відстані (кабелі живлення, шини заземлення, телефонна лінія, металеві труби опалення і водопостачання, дроти пожежної сигналізації і т.п.). Таким чином, виникає безліч додаткових каналів витоку. Найбільш небезпечні серед них ті, які мають вихід за межі території підприємства (організації). Перехоплення таких електромагнітних випромінювань, або наведень на кабельні системи надає можливості дистанційного доступу до інформації. Для перехоплення побічних електромагнітних випромінювань використовуються спеціальні приймальні пристрої, які називаються технічними засобами розвідки побічних електромагнітних випромінювань і наведень (ТЗР ПЕМВН).

Електромагнітний канал поділяється на канали:

- ➔ радіоканал (використання високочастотного випромінювання);
- ➔ мережевий канал (наведення на мережу електроживлення);
- ➔ канал заземлення (наведення на лінії заземлення);
- ➔ лінійний канал (наведення на лінії зв'язку, сигналізації відеоспостереження тощо).

ГЛАВА 19
Економічна розвідка і принципи захисту від неї

19.1. Технічні засоби економічної розвідки
19.2. Принципи захисту від економічної розвідки

19.1. Технічні засоби економічної розвідки

Економічна розвідка – це широке поняття, що об'єднує в собі промислову та комерційну розвідку.

Промислова розвідка – це несанкціоноване отримання науково-технічної та технологічної інформації.

Комерційна розвідка – це несанкціоноване отримання інформації, що представляє собою комерційну таємницю компанії.

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 нав'язування;*
- *стетоскопи;*

- *лазерні стетоскопи;*
- *апаратура відеоспостереження та фотозйомки;*
- *спрямовані мікрофони.*

Закладні пристрої, що використовують для передачі інформації лінії електроживлення мережі напругою 220 В, часто називають *мережевими закладками.* Вони можуть бути встановлені в електричні розетки, подовжувачі, побутову апаратуру, або безпосередньо в силову лінію. Для прийому інформації, переданої мережевими закладками, використовуються спеціальні приймачі, що підключаються до силової мережі. З використанням мережевих закладок можлива передача інформації на відстані до 300–500 м у межах одного або декількох будівель, які живляться від однієї низьковольтної шини трансформаторної підстанції.

Крім мережі електроживлення, для передачі інформації широко використовуються телефонні лінії зв'язку. Передача інформації може здійснюватися як на високій, так і на низькій частотах.

При передачі інформації по телефонній лінії на високій частоті дальність передачі інформації значно вища, ніж при передачі по мережі 220 В, і може становити кілька кілометрів.

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.

Як канали витоку великий інтерес представляють допоміжні засоби, що виходять за межі контрольованої зони, а також сторонні дроти і кабелі, що проходять через приміщення з встановленими в них основними і допоміжними технічними засобами, металеві труби систем опалення, водопостачання та інші струмопровідні металоконструкції.

Узагальнену схему можливих каналів витоку та несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі, наведено на рис. 19.1, де використано такі позначення:

Рис. 19.1. Узагальнена схема можливих каналів витоку та несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі

Джерело: URL: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

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 електрогодинника;

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

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.

Важливо, що *апаратні кейлоггери* «невидимі» для операційної системи, і їх неможливо виявити за допомогою антишпигунських програм.

Рис. 19.2. Апаратні кейлоггери

Джерело: URL: https://www.keelog.com/ru/usb-keylogger/

Однак у більшості *апаратних кейлоггеров* 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.

Відеологгери

Відеологгер – це апаратна закладка мініатюрних розмірів, встановлена в звичайний відеокабель, що з'єднує системний блок з монітором.

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 абревіатура 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 абревіатурою 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*).

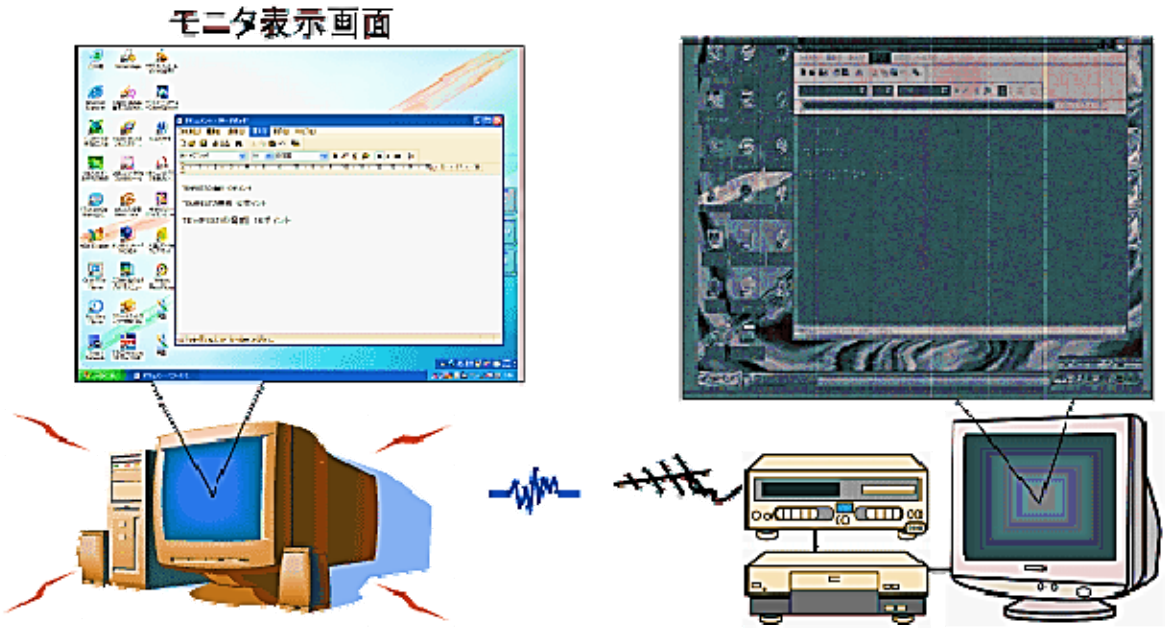


Рис. 19.3. TEMPEST-атака (можна віддалено проглядати екран вашого комп'ютера і мобільного телефона за допомогою радіохвиль)

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

19.2. 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.

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 – ***зашумленя***.

Екранування

Екранування полягає у створенні непереборного для сигналу, бар'єра між джерелом інформації і середовищем поширення інформації. Це може бути, наприклад, використання виділеної кімнати, в якій проводяться важливі переговори, з якої не проникає у відкритий простір звукові коливання. У хороших банках, у хороших організаціях, коли відвідувач заходить у касу і закриває за собою двері, переговори між відвідувачем і касиром практично не чути. Це приклад такого захисту. Навіть людина, що знаходиться в безпосередній близькості від вхідних дверей в це касове приміщення, не може почути розмову між касиром і відвідувачем.

Розсіювання

Наступним підходом до обмеження можливості порушника з перехоплення інформації по технічних каналах є *розсіювання*, яке полягає в ослабленні сигналу різними способами, наприклад, шляхом збільшення відстані від джерела сигналу до приймача сигналу, створення складних середовищ на шляху поширення сигналу інформації. Розсіювання сигналу полягає в тому, щоб збільшити відстань до такого, щоб на

межі контрольованої території перехоплення сигналу з корисною інформацією було практично виключено з тієї причини, що до цього моменту він практично згас.

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. 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.

Рис. 19.4. Просторове електромагнітне зашумлення комп'ютерного місця

Джерело: URL: https://sites.google.com/site/kanalivitokuinformaciie/metodi-ta-zasobi-zahistu-vid-vitoku-informaciie/zahodi-sodo-blokuvanna-tkvi-z-vikoristannam-aktivnih-zasobiv

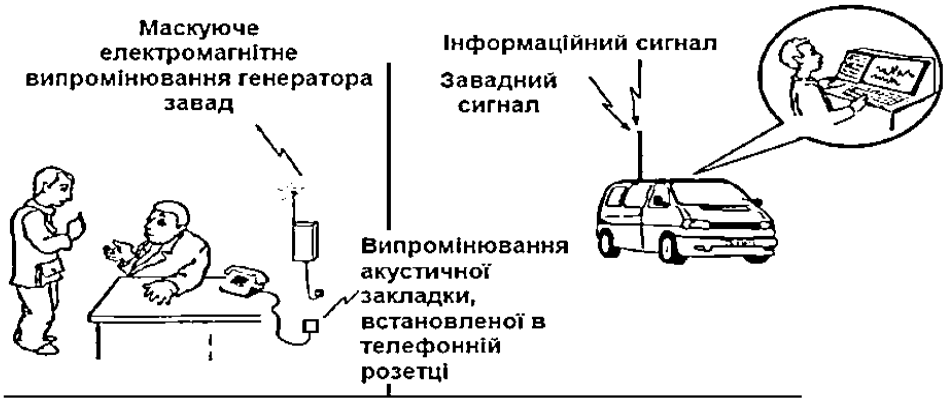


Рис. 19.5. Електромагнітне зашумлення телефонної закладки

Джерело: URL: https://sites.google.com/site/kanalivitokuinformaciie/metodi-ta-zasobi-zahistu-vid-vitoku-informaciie/zahodi-sodo-blokuvanna-tkvi-z-vikoristannam-aktivnih-zasobiv

Рис. 19.6. Створення віброакустичних завад лазерній системі розвідки

Джерело: URL: https://sites.google.com/site/kanalivitokuinformaciie/metodi-ta-zasobi-zahistu-vid-vitoku-informaciie/zahodi-sodo-blokuvanna-tkvi-z-vikoristannam-aktivnih-zasobiv

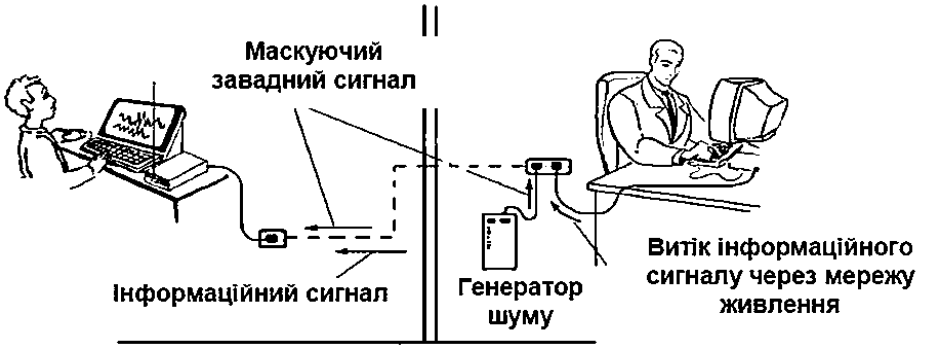


Рис. 19.7. Зашумлення ліній електроживлення

Джерело: URL: https://sites.google.com/site/kanalivitokuinformaciie/metodi-ta-zasobi-zahistu-vid-vitoku-informaciie/zahodi-sodo-blokuvanna-tkvi-z-vikoristannam-aktivnih-zasobiv

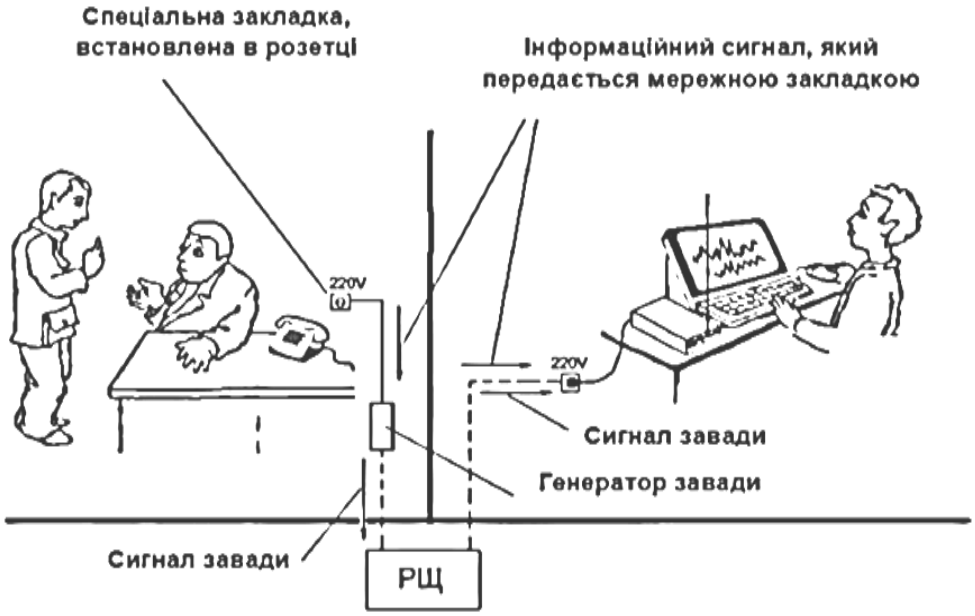


Рис. 19.8. Зашумлення сторонніх провідників і сполучних ліній

Джерело: URL: https://sites.google.com/site/kanalivitokuinformaciie/metodi-ta-zasobi-zahistu-vid-vitoku-informaciie/zahodi-sodo-blokuvanna-tkvi-z-vikoristannam-aktivnih-zasobiv

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, знаменитий китайський генерал і військовий теоретик, у своєму видатному творі «Трактат про військове мистецтво» писав: «Перша категорія шпигунів – інформатори, друга – агенти в таборі супротивника з середовища його людей, третя – агенти супротивника, використовувані проти своїх, четверта – розвідники і диверсанти, п'ята – «шпигуни життя».

«Шпигунами життя» Сунь Цзи називає таких агентів, які надсилаються до супротивника за будь-якими відомостями та від яких вимагається що б то не було повернутися живими, доставивши ці відомості.

Контрольні запитання

1. Дайте характеристику інженерно-технічних засобів безпеки.
2. Що входить до фізичних методів захисту ІТС?
3. Що таке технічний канал витоку і з чого він складається?
4. Що є джерелами сигналу для витоку інформації за межі ІТС?
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. Поясніть ідею «зашумлення» і приведіть приклади реалізації.

Розділ 9. ПРОГРАМНО-АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС

ГЛАВА 20
ІДЕНТИФІКАЦІЯ І АВТЕНТИФІКАЦІЯ


20.1. Загальна характеристика програмних засобів безпеки ІТС

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.

По відношенню до загроз, ці заходи можна розділити 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 прагнуть запобігти загрозі взагалі, тобто не допустити її реалізації. Цілі застосування превентивних механізмів захисту: випереджаюче виявлення і запобігання проблемних ситуацій, створення бар'єрів на шляху реалізації загроз, резервування, розподіл ролей, використання засобів розмежування доступу, контроль доступу в приміщення і т. п.

Заходи виявлення порушень і виявлення порушника

Заходи виявлення порушень і виявлення порушника спрямовані на виявлення факту реалізації загроз і джерела загроз. Цілі застосування детективних механізмів захисту: виявлення проблемних ситуацій і порушень безпеки під час або після їх появи, моніторинг подій безпеки, виявлення мережевих атак, антивірусне сканування, перевірка контрольних сум файлів, процедури внутрішнього аудиту і т. д.

Заходи, що локалізують порушення

Заходи, що локалізують порушення не дозволяють загрозам поширитися в системі.

Заходи відновлення безпеки інформації

Заходи відновлення безпеки інформації, в разі якщо загроза все-таки була реалізована, спрямовані на якнайшвидше усунення її наслідків.

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 є те, що вони додатково завантажують процесор, що призводить до збільшення часу реагування на запити і відповідно до зменшення ефективності роботи, а також до зменшення ємності доступної і зовнішньої оперативної пам'яті. Крім цього, жорстка орієнтація програмних засобів на певну архітектуру, а також залежність від ОС доповнює зазначені недоліки.

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 (автентифікація);
- ✹ 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 ІТС;
- контроль діяльності співробітників;
- управління безпекою.

На основі сервісів безпеки будується загальна система забезпечення безпеки інформації, яка складається з окремих підсистем, кожна з яких може включати кілька сервісів безпеки. Замість окремих підсистем екранування або тунелювання, антивірусних систем, систем виявлення і запобігання вторгнень на ринок поставляються комплексні програмно-апаратні рішення, інтегровані в структуру компанії для забезпечення інформаційного захисту на всіх рівнях. Подібна інтеграція дозволила значно знизити загальну вартість володіння засобами захисту інформації, спростити процес установки і адміністрування і в той же час підвищити рівень захищаються інформаційних ресурсів.

20.2. Ідентифікація, автентифікація та авторизація в ІТС

Застосування відкритих каналів передачі даних створює потенційні можливості для дій зловмисників. Тому одним із важливих завдань забезпечення безпеки ІТС при взаємодії користувачів є використання методів і засобів, що дозволяють одній стороні переконатися в достовірності іншої сторони.

Ідентифікація та *автентифікація* – це перша лінія оборони, «*прохідна*» інформаційного простору. З метою

забезпечення санкціонованого доступу до ресурсів ІТС кожен суб'єкт (співробітник, користувач, процес) і об'єкт (ресурс ІТС) 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).

Ідентифікація

Ідентифікація – це процес, що передбачає надання унікального імені (ідентифікатора) об′єктам та суб′єктам ІТС для подальшого розпізнавання їх системою, або порівняння запропонованого ідентифікатора з переліком привласнених ідентифікаторів.

Одні ідентифікатори автоматично генеруються ОС і додатками (ідентифікатори процесів, ідентифікатори логічних мережевих 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.

Автентифікація

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 автентифікації.

Автентифікація – це перевірка достовірності пред'явлених ідентифікаторів суб'єкта або об'єкта системи.

Мета автентифікації суб'єкта – переконатися в тому, що суб'єкт є саме тим, ким представився (ідентифікувався).

Мета автентифікації об'єкта – переконатися, що це саме той об'єкт, який потрібен.

В якості синоніма слова *«автентифікація»* 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. Автентифікація запобігає доступ до системи небажаних осіб і дозволяє вхід для легальних користувачів. Таким чином, ідентифікацію та автентифікацію можна вважати основним механізмом, який реалізує захист від несанкціонованого доступу (НСД).

За відсутності процедури автентифікації, доступ до системи нелегальних осіб стає простим завданням – достатньо просто використовувати ідентифікатор легального користувача.

Автентифікація користувачів, окрім припинення спроб доступу з боку порушника, котрий використовує ідентифікатор легально користувача, дозволяє також припинити спроби заперечення легальними користувачами вчинення ними будь-яких неправомірних дій. Тобто під час відсутності автентифікації будь-який користувач, будучи викритим в якомусь неправомірному або недбалому вчинку може стверджувати, що його ідентифікатор був використаний кимось іншим. Автентифікації-то не було, а значить, залишається можливість використання чужого ідентифікатора.

Авторизація

Наступний етап взаємодії ІТС з суб'єктами – авторизація.

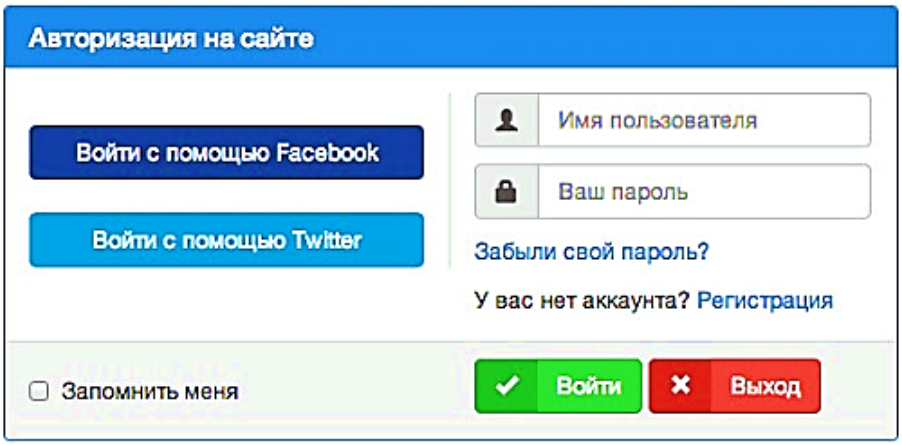


Рис. 20.1. Проста авторизація на сайті

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

Авторизація – надання автентифікованому суб'єкту відповідних прав на доступ до об'єктів системи: які дані і як він може використовувати (які операції з ними виконувати), які програми може виконувати, коли, як довго і з яких терміналів може працювати, які ресурси системи може використовувати і т. п.

Як правило, авторизація виконується після успішного проходження суб'єктом автентифікації.

Процедура проведення авторизації ще називається *управлінням доступом (access control*), тобто система надає суб'єкту тільки ті права доступу, які передбачені для даного ідентифікатора.

Якщо у користувача є в системі більше одного ідентифікатора, то права доступу для одного і того ж фізичного суб'єкта можуть бути різними для різних ідентифікаторів цього суб'єкта.

На відміну від автентифікації, яка дозволяє розпізнати легальних і нелегальних користувачів, авторизація стосується тільки легальних користувачів, які успішно пройшли процедуру автентифікації. Доступ до об'єктів, отриманий в обхід дозволів системи контролю доступу, називається несанкціонованим.

20.3. Види автентифікації суб'єктів в ІТС

У процедурі автентифікації 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 автентифікації, то це називається однофакторною автентифікацією. Для підвищення надійності

системи автентифікації використовують більш одного фактора, тобто використовують *багатофакторну автентифікацію*, коли користувачеві потрібно пройти процедури перевірки на основі більш ніж одного фактора.

Наприклад, підтвердити знання якогось секрету і одночасно пред'явити наявність якогось об'єкта. Прикладами багатофакторної автентифікації можуть бути такі пари.

Поєднання електронного ключа і пароля: тут фактори – наявність і знання. Відбиток пальця і пароль: тут фактори – володіння якоюсь ознакою і знання пароля. Відомим прикладом двофакторної автентифікації є процес реєстрації при користуванні банкоматом, коли користувач вставляє платіжну картку (то, що користувач має) і вводить PIN-код (то, що користувач знає), щоб отримати доступ до свого банківського рахунку.

Для реалізації розглянутих вище способів автентифікації необхідний первинний контакт між суб'єктом і об'єктом, в процесі якого сторони обмінюються ***автентифікаторами***. У ряді випадків такий контакт неможливий, наприклад, в системах електронного бізнесу ***B2C***. Для подібних випадків найбільш ефективна автентифікація з використанням різних форм рекомендацій від довіреного посередника, наприклад *сертифікат* або *квиток*. Зокрема, широко відомі *сертифікати X509,* що зв'язують клієнта і його ідентифікатор і які підписані цифровим підписом довіреного центру сертифікації.

Система автентифікації не позбавлена і вразливостей. Зрозуміло, що вона беззахисна проти внутрішнього порушника, який вже успішно пройшов автентифікацію і авторизацію. Можливість присвоєння порушниками чужих засобів автентифікації дозволяє йому обходити систему автентифікації.

Паролі можуть бути підглянуті або викрадені, або перехоплені, а унікальні об'єкти автентифікації також можуть бути відчужені, тобто вкрадені або відібрані силою. Абсолютно надійна автентифікація людини являє собою теоретично нездійсненне завдання. Немає такого автентифікатора, який зі стовідсотковою надійністю доводив би автентичність людини. Пароль можна перехопити, електронний ключ вкрасти, відбиток пальця підробити. Таким чином, сама система автентифікації, не будучи підтриманою ніякими іншими заходами, не в змозі повністю забезпечити захист від дій порушника в межах інформаційної системи.

У деяких випадках односторонньої автентифікації виявляється недостатньо і тоді використовують двосторонню автентифікацію. Наприклад, користувач, який звертається із запитом до корпоративного вебсервера, повинен довести йому свою легальність, але він також повинен переконатися сам, що веде діалог дійсно з вебсервером свого підприємства. Іншими словами, сервер і клієнт повинні пройти процедуру взаємної автентифікації. При встановленні сеансу зв'язку між двома пристроями також часто передбачаються процедури взаємної автентифікації пристроїв.

20.4. Парольна автентифікація

Парольна автентифікація є найпростішою формою автентифікації. Вона побудована на порівнянні *еталонного зразка автентифікаційної 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 автентифікації не пройдена.

Прийнята в організації політика безпеки, як правило, передбачає такі обов'язкові параметри використання парольної автентифікації:

- ❖ 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 парольна автентифікація може забезпечити прийнятний рівень безпеки.

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 парольної автентифікації використовуються багаторазові паролі.

Для підвищення безпеки парольної системи автентифікації на противагу багаторазовим паролям, використовуються так звані *одноразові паролі*, тобто паролі, що дійсні тільки для одного сеансу автентифікації.

Їх основна перевага – це даремність для порушника перехоплення або викрадення вже використаного пароля. Такий пароль діє тільки для одного сеансу автентифікації, 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 автентифікації 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 автентифікація 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 автентифікацію. Якщо хоча б один з одноразових паролів буде перехоплений, то порушник вже не зможе пройти автентифікацію від імені легального користувача.

Іншим варіантом забезпечення надійності одноразових паролів є синхронізація вироблення паролів з системою автентифікації. 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 парольної автентифікації є її інтелектуальна складова, тобто зв'язок з розумом і свідомістю користувача. Паролі повинні зберігатися виключно в «людській» пам'яті користувачів без запису на будь-який матеріальний носій інформації.

20.5. Автентифікація на основі PIN-коду

Найбільш поширеним методом автентифікації 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. У таких випадках єдиним контрзаходом проти несанкціонованого доступу залишається секретне значення PIN-коду. Ось чому відкрита форма PIN повинна бути відома тільки законному власнику картки. Очевидно, значення PIN потрібно тримати в секреті протягом всього терміну дії картки.

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.

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 не вимагає застосування спеціальних алгоритмів. Перевірка PIN-коду здійснюється шляхом безпосереднього порівняння введеного клієнтом PIN-коду зі значеннями, збереженими в БД серверу автентифікації, або на самій картці. Зазвичай БД зі значеннями PIN-кодів клієнтів шифрується, щоб підвищити її захищеність, не ускладнюючи процесу порівняння.

Алгоритмічний спосіб перевірки PIN-коду

Алгоритмічний спосіб перевірки PIN-коду полягає в тому, що введений клієнтом PIN-код перетворять за певним алгоритмом з використанням секретного ключа і потім порівнюють зі значенням PIN-коду, що зберігається в певній формі на картці.

Переваги цього методу перевірки – відсутність копії PIN-коду на головному комп'ютері виключає його розкриття обслуговуючим персоналом.

ГЛАВА 21
Види автентифікації

21.1. Апаратна автентифікація

В ІТС з більш високими вимогами до захищеності інформації недоліки парольної автентифікації усуваються шляхом використання апаратних пристроїв автентифікації.

Ці пристрої відносяться до категорії персональних засобів автентифікації (як і паперові документи), що дозволяє однозначно ідентифікувати суб'єктів за принципом володіння таким автентифікатором.

Апаратні автентифікатори, звані також апаратними ключами, належать до фактора автентифікації «Я маю».

Пристрої апаратної автентифікації діляться на дві групи:

1) пасивні (зберігається один фіксований автентифікатор);
2) активні (можуть генерувати різні автентифікатори).

Пасивні пристрої автентифікації

Приклади пасивних пристроїв автентифікації:

- ➔ механічні ключі;
- ➔ пластикові картки з магнітною смугою (рис. 21.1);
- ➔ елементи Touch Memory (iButton) (рис. 21.2);
- ➔ безконтактні картки Proximity і RFID-брелоки (рис. 21.3).

Рис. 21.1. Картка з магнітною смугою (а) та пристрій для читання (б)

Джерело: URL: http://dspace.onua.edu.ua/bitstream/handle/11300/11111.pdf?sequence=1&isAllowed=y

Рис. 21.2. Елемент (а) та пристрій для читання TouchMemory (б)

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

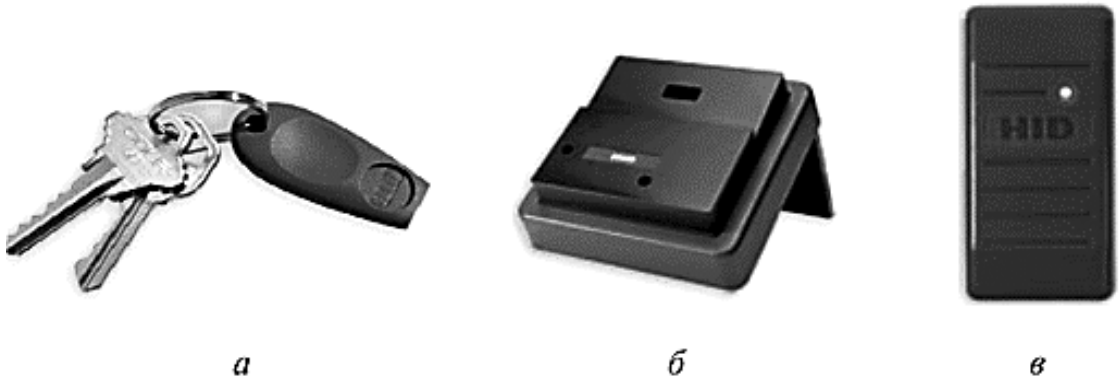


Рис. 21.3. RFID-брелок (а), програматор (б) та пристрій для читання (в)

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Для автентифікації користувача за допомогою картки досить лише надати цю картку зчитувачу і ввести свій PIN-код. Якщо введений PIN-код збігається з даними на магнітній смузі, користувач буде успішно автентифікований.

Недоліком такої картки пам'яті є те, що вона вимагає використання спеціального зчитувача для обробки інформації. Це збільшує вартість даного рішення (особливо, якщо зчитувач потрібно встановити на кожен комп'ютер компанії). Також вартість збільшує процес виготовлення («прошивки») карток пам'яті.

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, оснащеним відповідними датчиками

Недолік пасивних пристроїв автентифікації полягає в більшій простоті копіювання автентифікаційної інформації, що зберігається на них (в порівнянні з активними пристроями).

Активні пристрої автентифікації

Приклади активних пристроїв автентифікації:

- ➔ смарт-картки (пластикові картки з мікропроцесором) (рис. 21.4);
- ➔ USB-токени (USB-ключі) (рис. 21.5);
- ➔ OTP-токени (генератори одноразових паролів) (рис. 21.6);
- ➔ гибридні токени (генератори одноразових паролів) (рис. 21.7).

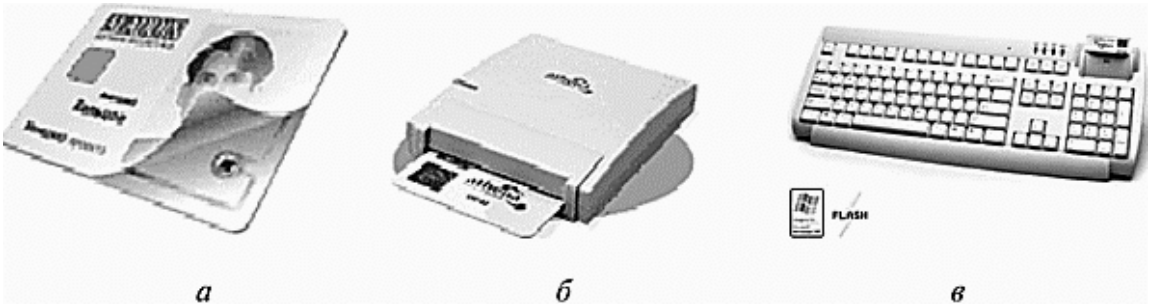


Рис. 21.4. Смарт-картка (а) і пристрій для читання (б, в)

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Рис. 21.5. USB-токен автентифікації

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

Рис. 21.6. OTP-токени. Генератори одноразових паролів

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

Основною відмінністю *смарт-карток* є їх можливості по обробці інформації. Якщо звичайна карта пам'яті може зберігати інформацію, але не може її обробляти, то смарт-картка крім зберігання інформації має необхідне апаратне і програмне забезпечення для обробки інформації.

Смарт-картки можуть бути як *контактними, так і без-контактними.*

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 автентифікації інформації.

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 автентифікації, 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. 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 автентифікацію.

Рис. 21.7. Гибридні токени

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

OTP-токени призначені для використання одноразових паролів, які і генеруються за допомогою такого токену. Вони використовуються в ІТС з автономним сервером автентифікації. У запам'ятовуючому пристрої токену зберігається таємний ключ користувача, який продубльований і на сервері автентифікації. У процедурі доступу до системи користувач вводить одноразовий пароль, що згенерував OTP-токен. Сервер автентифікації також генерує одноразовий пароль за такою ж схемою по таємному ключу користувача. Паролі користувача і серверу порівнюються і користувач получає доступ до системи, якщо паролі співпадають.

Гібридні токени мають функціональність як USB-токенів, так і OTP-токенів. Вони дозволяють проводити двофакторну автентифікацію з підключенням до USB-порту, а також безконтактну автентифікацію в випадках, коли немає доступу до такого порту.

Переваги застосування апаратної ідентифікації

Головною перевагою застосування апаратної ідентифікації є досить висока надійність, можливість використання пристроїв автентифікації для вирішення додаткових завдань (активні пристрої автентифікації – це мінікомп'ютери).

Недоліки застосування апаратної ідентифікації

Загальна проблема використання апаратних пристроїв автентифікації – це втрата, або незаконне привласнення пристрою і відповідно застосування його зловмисником.

Вирішення цієї проблеми може бути в використанні другого фактора для автентифікації, наприклад, PIN-коду.

Другим недоліком апаратної автентифікації є висока ціна пристроїв для її реалізації. Альтернативою слугують біометричні технології, які характеризуються відносними труднощами втрати автентифікатора.

На основі апаратних автентифікаторів створюють програмно-апаратні комплекси захисту від несанкціонованого доступу до комп'ютерів. Апаратний контролер такого комплексу блокує завантаження операційної системи з зовнішніх пристроїв.

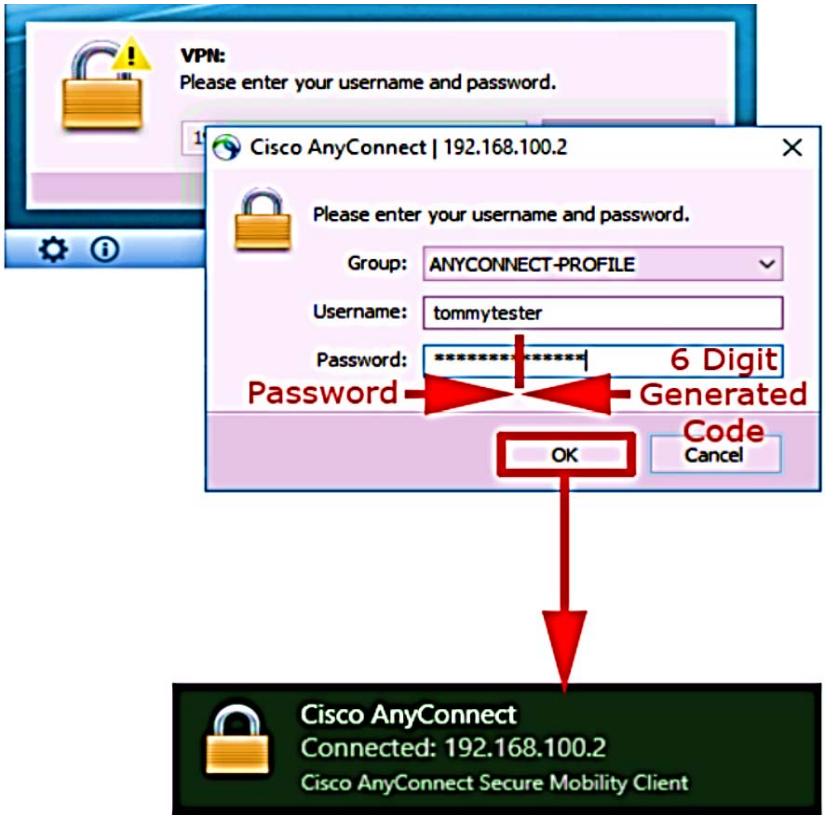


Рис. 21.8. Процедура введення двофакторної автентифікації

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Основними можливостями такого електронного замка є:

- *ідентифікація та автентифікація користувачів за допомогою ідентифікаторів Touch Memory і пароля* (операційна система завантажується з жорсткого диска тільки після успішної автентифікації, якщо користувач не пройшов автентифікацію 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).

21.2. Автентифікація за допомогою біометричних даних

Біометрія являє собою сукупність автоматизованих методів автентифікації 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.

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.

Рис. 21.9. Процедури біометричної автентифікації

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

До поведінкових характеристик відносяться параметри особистості, які виникли в процесі відтворення одні і тієї ж регулярної дії (голос, динаміка підпису, клавіатурний почерк). Аналіз підпису робиться спеціальною ручкою з перетворювачем прискорення по осях *X* і *Y*, враховується не тільки написання літер, а й швидкість і ступінь натискування на поверхню.

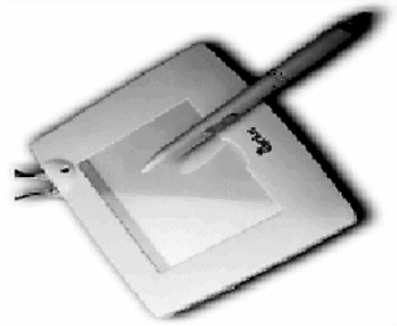


Рис. 21.10. Прилад для проведення біометричної автентифікації за аналізом динаміки підпису

Джерело: URL: https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials

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 клавіши. 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 людину є перевагою (допуск до виконання відповідальних дій, виявлення порушників).

Для роботи системи біометричної автентифікації 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 автентифікації, пред'явлені їм біометричні дані будуть порівнюватися з еталоном, що зберігаються в базі даних. Якщо вони збігаються, вважається, що автентифікація 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 автентифікації.

Мета автентифікації надати доступ до ресурсів ІТС обмеженому числу користувачів, біометричні еталони яких зберігаються в базі даних для цієї ІТС.

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 автентифікації за біометричними параметрами і додатковим унікальним ідентифікатором. За додатковим ідентифікатором біометрична система вибирає з бази даних біометричний еталон і тепер порівнює його з наданими біометричними параметрами. Збіг свідчить, що людина є та, за кого себе видає, тобто верифікація пройдена. Верифікацію можна розглядати як двофакторну автентифікацію.

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

Біометрією у всьому світі займаються дуже давно, проте довгий час все, що було пов'язано з нею, відрізнялося складністю і дорожнечею. Останнім часом попит на біометричні продукти, в першу чергу у зв'язку з розвитком електронної комерції, постійно і досить інтенсивно зростає. Це зрозуміло, оскільки з точки зору користувача набагато зручніше пред'явити себе самого, ніж щось запам'ятовувати. Попит народжує пропозицію, і на ринку з'явилися відносно недорогі апаратно-програмні продукти, орієнтовані переважно на розпізнавання відбитків пальців.

Варто зазначити, що ідентифікація людини за рисами обличчя – одна з найбільш популярна у біометричної індустрії. Привабливість цього методу заснована на тому, що він найбільш близький до того, як люди зазвичай ідентифікують один одного. Поширення мультимедійних технологій, завдяки якому все частіше можна зустріти відеокамери, встановлені на міських вулицях і площах, на вокзалах, в аеропортах та інших місцях скупчення людей, визначило розвиток цього напряму.

Переваги біометричних систем

Переваги біометричних систем безпеки очевидні:

- ➔ біометрію важко підробити. Для виявлення імітації можна застосовувати такі технології, як контроль температури, наявність 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.

21.3. Автентифікація на основі цифрових сертифікатів

Автентифікація 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 ІТС, 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 четвертій фактор автентифікації – мати рекомендації від довіреного посередника, якому вірить перевіряючий.

Сертифікати видаються спеціальними уповноваженими організаціями – *центрами сертифікації (Certificate Authority, CA)*.

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 (тобто такий, який він отримав в центрі сертифікації) і зашифрований із застосуванням свого закритого ключа. Сторона, яка проводить автентифікацію, бере з незашифрованого сертифіката відкритий ключ користувача і розшифровує з його допомогою зашифрований сертифікат. Збіг результату з відкритим сертифікатом підтверджує, що пред'явник дійсно є власником закритого ключа, яким зашифрований сертифікат. Потім за допомогою відомого відкритого ключа центра сертифікації, зазначеного в сертифікаті, проводиться розшифровка підпису цієї організації в сертифікаті. Якщо в результаті виходить той же сертифікат з тим же ім'ям

користувача і його відкритим ключем, значить, він дійсно пройшов реєстрацію в сертифікаційному центрі і вказаний в сертифікаті відкритий ключ дійсно належить йому.

При наявності сертифікатів відпадає необхідність зберігати на серверах корпорацій списки користувачів з їх паролями, натомість досить мати на сервері список імен і відкритих ключів.

21.4. Централізовані системи автентифікації. Концепція єдиного логічного входу

Традиційний спосіб автентифікації 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 автентифікації за допомогою багаторазового пароля, користувачеві доводиться пам'ятати і оновлювати досить багато паролів.

У цьому випадку на допомогу користувача приходить технологія єдиного логічного входу *(Single Sign On, SSO). Технологія SSO* дозволяє користувачу автентифікуватися через сервер автентифікації один раз, доводячи свою автентичність за допомогою будь-якого способу автентифікації, і тепер використовувати різні ресурси одного і того ж домену безпеки без необхідності повторної аутентифікації на кожному з ресурсів.

Домен – це просто набір ресурсів, доступних суб'єкту. Термін «домен безпеки» *(security domain)* ґрунтується на визначенні домену, додаючи до нього факт, що ресурси в рамках цієї логічної структури (домену) працюють з однією і тією ж політикою безпеки і керуються загальним контролером домену.

Узагальнена схема, що ілюструє ідею системи єдиного логічного входу, представлена на рис. 21.11.

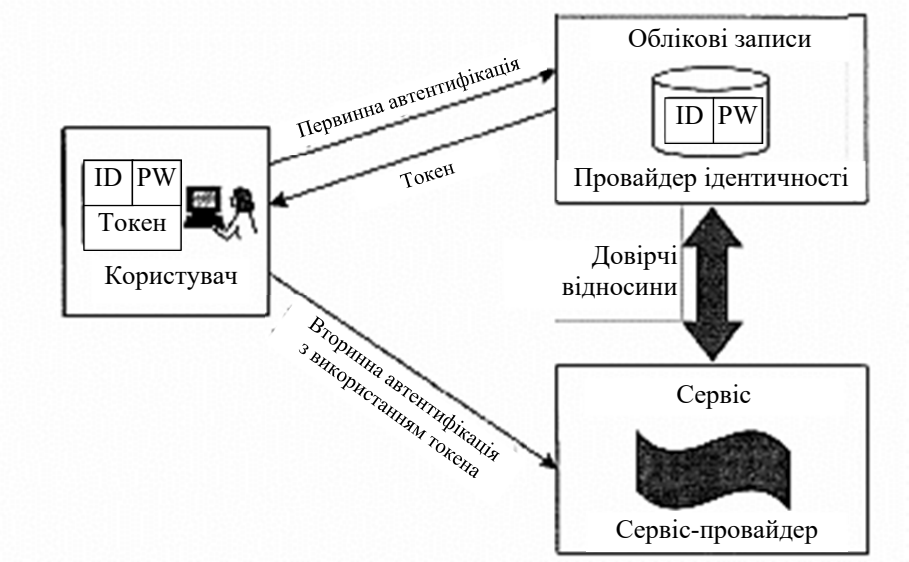


Рис. 21.11. Узагальнена схема, що ілюструє ідею системи єдиного логічного входу

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

У цій схемі є три 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 автентифікації.

- 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 автентифікації 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 автентифікації, яким ресурсний сервер довіряє автентифікувати користувачів. У цьому випадку відбувається вторинна автентифікація користувача, але для самого користувача вона прозора, оскільки пред'явленням токену доступу займається програмне забезпечення комп'ютера.

Токен доступу зазвичай має обмежений час дії, наприклад добу, тому користувач повинен його відновлювати, повторюючи процедуру з сервером автентифікації.

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 автентифікації. 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).

Прикладом системи, що реалізує процедуру єдиного логічного входу, є *мережева служба Kerberos.*

***Kerberos* – це** технологія безпеки, яка реалізує функції автентифікації. Програма працює на базі моделі клієнт-сервер і клієнтські компоненти цього програмного продукту присутні в більшості серверних операційних систем.

Основні компоненти Kerberos

Центр поширення ключів *(**KDC** – Key Distribution Center)* – зберігає секретні ключі всіх користувачів і служб. ***KDC*** реалізує службу аутентифікації і функції поширення ключів. Для цього він повинен мати обліковий запис для кожного системного об'єкта і загальний секретний ключ з кожним системним об'єктом. Для користувачів їх паролі перетворюються в значення секретного ключа. Секретний ключ використовується для передачі критичної інформації тільки між системним об'єктом і ***KDC***, а також для аутентифікації користувача. KDC – це довірений сервер аутентифікації для всіх користувачів, додатків і служб у рамках домену безпеки.

Служба надання білетів *(TGS – Ticket Granting Service)* на *KDC* генерує і передає системному об'єкту (наприклад, користувачу) білет (ticket), коли йому потрібно аутентифікуватися на іншому системному об'єкті (наприклад, сервера друку).

Призначення Kerberos

Kerberos призначений для вирішення наступного завдання.

Є відкрита (незахищена) мережа, в вузлах якої зосереджені суб'єкти – користувачі і різноманітні об'єкти – ресурси системи. Кожен суб'єкт має секретний ключ. Щоб суб'єкт ***C*** міг довести свою справжність об'єкту ***S*** (без цього об'єкт ***S*** не стане обслуговувати суб'єкт ***C***), він повинен не лише назвати себе, а й продемонструвати знання секретного ключа. Суб'єкт ***C*** не може просто послати об'єкту ***S*** свій секретний ключ, *по-перше*, тому що мережа відкрита (доступна для пасивного й активного прослуховування), а *по-друге*, тому що об'єкт ***S*** не знає (і не повинен знати) секретний ключ суб'єкта ***C***. Потрібно менш прямолінійний спосіб демонстрації знання секретного ключа.

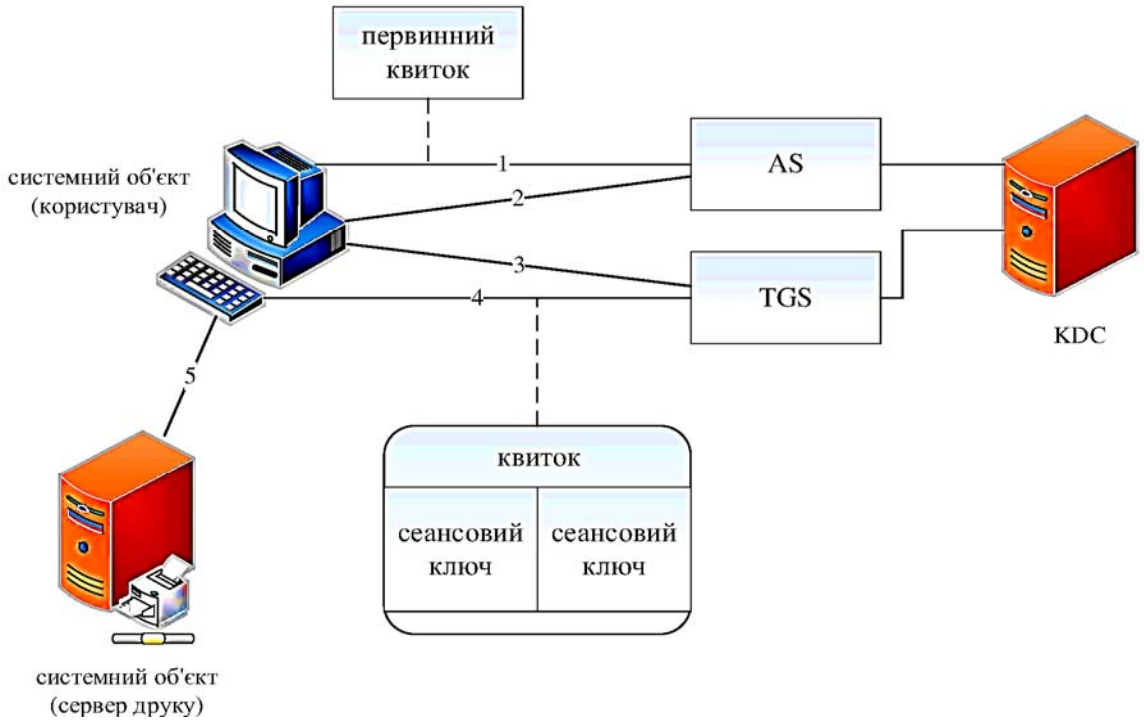


Рис. 21.12. Служба надання білетів (TGS – Ticket Granting Service) на KDC (центр поширення ключів)

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

Система ***Kerberos*** являє собою довірену третю сторону (тобто сторону, якій довіряють всі), що володіє секретними ключами всіх суб'єктів і допомагає їм в попарній перевірці справжності.

Щоб за допомогою ***Kerberos*** отримати доступ до об'єкта ***S*** (зазвичай це сервер), суб'єкт ***C*** (як правило – клієнт) посилає ***Kerberos*** запит, що містить відомості про нього (клієнта) і про запитувану послугу. У відповідь ***Kerberos*** повертає так званий квиток, зашифрований особистим ключем сервера, і копію частини інформації з квитка, зашифровану секретним ключем клієнта. Клієнт повинен розшифрувати другу порцію даних і переслати її разом з квитком серверу. Сервер, розшифрувавши квиток, може порівняти його вміст з додатковою інформацією, надісланою клієнтом. Збіг свідчить про те, що клієнт зміг розшифрувати призначені йому дані (адже вміст квитка нікому, крім сервера і ***Kerberos***, невідомий), тобто продемонстрував знання секретного ключа. Значить, клієнт – саме той, за кого себе видає. Підкреслимо, що секретні ключі в процесі перевірки автентичності не передавалися по мережі (навіть у зашифрованому вигляді) – вони тільки використовувалися для шифрування.

Контрольні запитання

1. Які основні сервіси безпеки реалізовані за допомогою програмних засобів?
2. Поясніть різницю між ідентифікацією, автентифікацією і авторизацію.
3. Які прийоми використовують для автентифікації?
4. Які особливості автентифікації в системах електронного бізнесу B2C?

5. Які обов'язкові параметри використання парольної автентифікації передбачені в політиці безпеки організації?
6. Як можна підвищити безпеку парольної системи автентифікації?
7. Наведіть приклади пасивних і активних апаратних автентифікаторів.
8. У чому відмінність USB-токенів від OTP-токенів?
9. Що таке біометрія і які фізіологічні характеристики можуть використовуватися для автентифікації?
10. Що відносять до поведінкових біометричних характеристик і в чому їх недоліки і переваги?
11. Як працює біометрична система автентифікації?
12. У чому полягає різниця між біометричною ідентифікацією і біометричною автентифікацією?
13. Дайте характеристику помилок, що виникають при роботі систем біометричної автентифікації.
14. Як вирішити проблему автентифікації для систем, де кількість користувачів вимірюється сотнями тисяч?
15. Як працюють системи централізованої автентифікації?
16. У чому полягає концепція єдиного логічного входу SSO?
17. Як працює система автентифікації Kerberos?

Розділ 10. УПРАВЛІННЯ ДОСТУПОМ І АУДИТ ІТС

ГЛАВА 22
УПРАВЛІННЯ ДОСТУПОМ

22.1. 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 витоки конфіденційних даних, і втручання у роботу системи з боку не маючих на це повноважень незареєстрованих користувачів, і порушення безпеки системи тощо.

Модель контрольованого доступу

Важливим напрямом забезпечення безпеки ІТС 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 ІТС (різноманітні пристрої, що входять до складу ІТС), а також і логічні ресурси ІТС (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 автентифікацію, 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-третє, 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.

Об'єкти і суб'єкти в рамках каталогу керуються за допомогою служби каталогу (***directory service***), що дозволяє адміністратору ІТС 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 автентифікації. Після автентифікації вебсервер відправляє веббраузеру кукі-файл (змістом якого є облікові дані і параметрами платформи з якої проходила автентифікація) 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 автентифікація, 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.

22.2. Дискреційна модель розмежування доступу

Існує три принципових підходи до керованого управління доступом:

- ➔ дискреційне (виборче) розмежування доступу;
- ➔ мандатне розмежування доступу;
- ➔ рольове розмежування доступу.

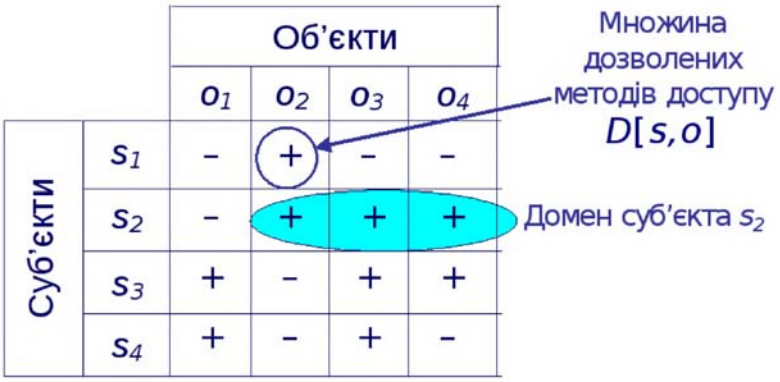


Рис. 22.1. Матриця доступу в дискреційній моделі

Джерело: URL: https://studfile.net/preview/5470392/page:4/

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.

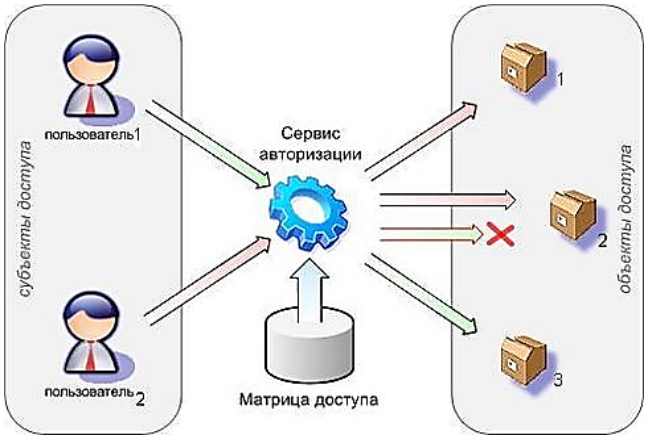


Рис. 22.2. Схема дискреційної моделі управління доступом. (Суб'єкт доступу «Користувач № 1» має право доступу тільки до об'єкта доступу № 3, тому його запит до об'єкта доступу № 2 відхиляється. Суб'єкт «Користувач № 2» має право доступу як до об'єкта доступу № 1, так і до об'єкта доступу № 2, тому його запити до даних об'єктів не відхиляються)

Джерело: URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate

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 ІТС, 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.

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 двомірного 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.

22.3. Мандатна модель розмежування доступу

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.

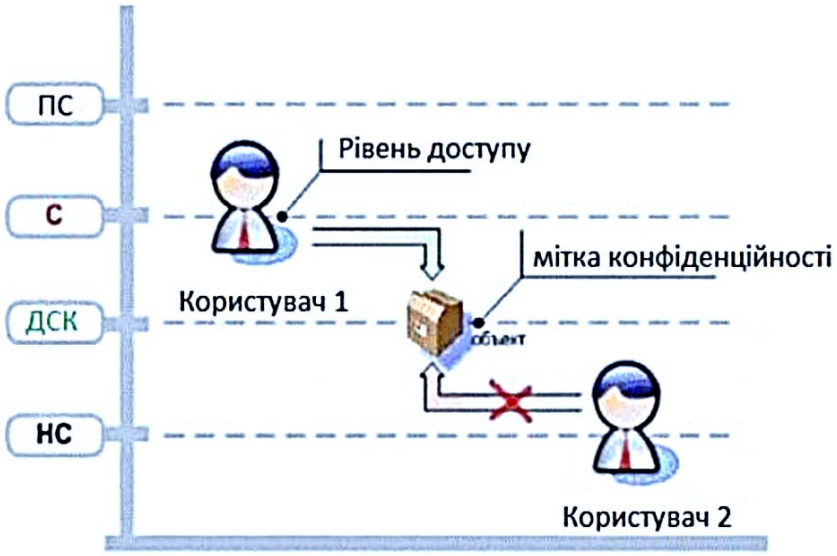


Рис. 22.3. Приклад реалізації мандатної моделі доступу

Джерело: URL: https://stud.com.ua/180191/informatika/metod_abstraktna_model_mandatnoyi_kontrolyu_dostupu

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 ІТС 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 ІТС. 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.

Дана модель доступу має такі переваги. Для її реалізації досить встановити кожному об'єкту мітку конфіденційності, а кожному суб'єкту – рівень допуску. Відповідно, це робиться значно швидше і простіше, ніж повне заповнення матриці для кожної пари суб'єкт–об'єкт. З цього

випливає, що додавання нового об'єкта або нового суб'єкта не вимагає додаткового редагування прав інших суб'єктів або об'єктів. Якщо в системі з'являється новий суб'єкт, йому встановлюється рівень допуску – і система може функціонувати далі. Якщо з'являється новий об'єкт, йому приписується мітка конфіденційності – і знову ніяких інших дій в системі не потрібно.

З цих переваг, в свою чергу, слідують і недоліки. Доступ до об'єктів одного рівня секретності надається або обмежується спільно. Немає можливості розділити 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 спроєктована та реалізує правила *MAC*.

ГЛАВА 23
Управління доступом і реєстрація подій в системі

23.1. Рольова модель розмежування доступу

Рольова модель ґрунтується на так званих ролях суб'єктів ІТС. По суті, вона є оптимізацією дискреційного розмежування доступу. Під роллю в даній моделі мається на увазі сукупність прав доступу суб'єкта до об'єктів ІТС. 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.***

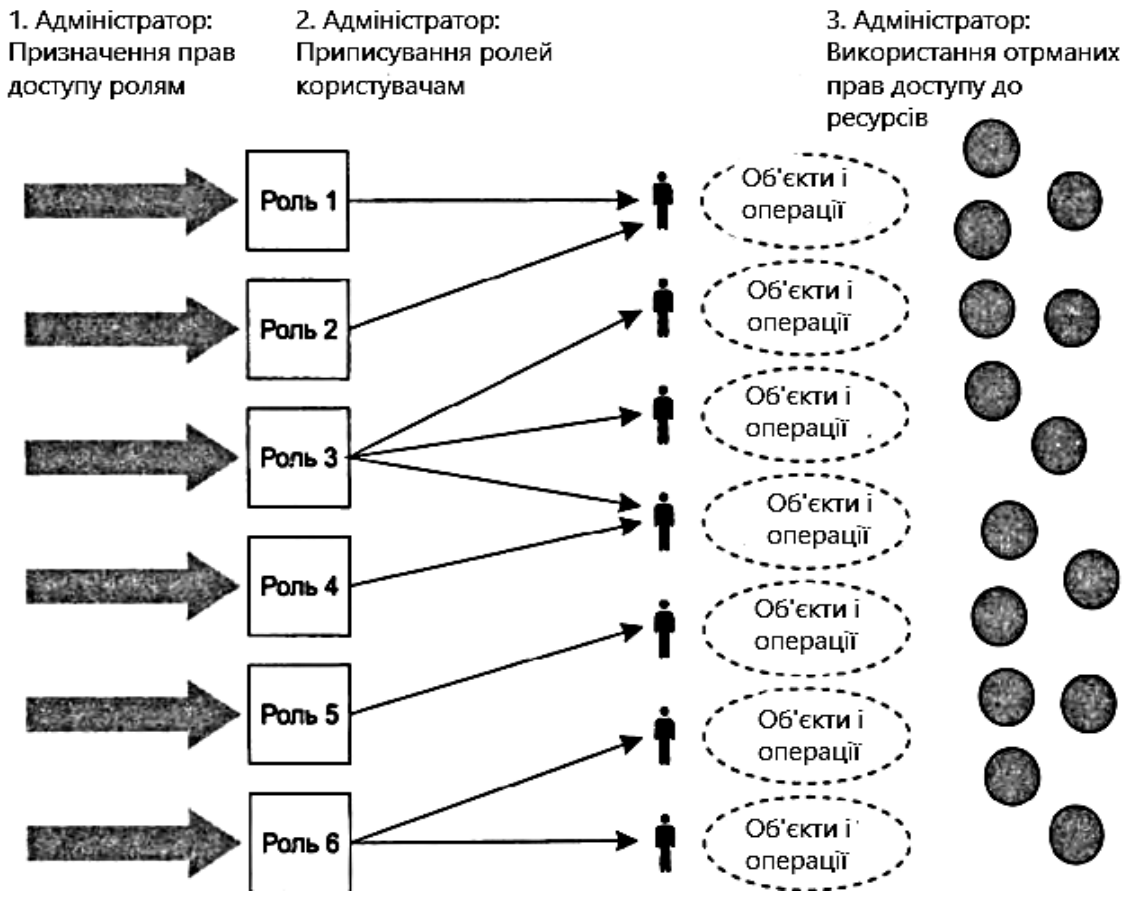


Рис. 23.1. Рольове розмежування доступу

Джерело: URL: https://studfile.net/preview/7798108/page:31/

Наприклад, може бути роль «системний адміністратор». У цьому випадку існує якийсь набір прав, який є як би стандартним для системного адміністратора. Може бути роль начальника відділу, роль оператора, роль бухгалтера. І для кожної такої ролі прописується набір прав доступу до різних об'єктів системи.

Роль – це те, чим займається користувач на підприємстві, його вид діяльності вкупі з його трудовими обов'язками.

Робота рольової системи передбачає чіткий розподіл кожного користувача по ролі, після чого доступ користувача до інформації буде залежати виключно від ролі.

Переваги у рольової 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 мандатної 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 рольової моделі розмежування доступу

Проте є й свої недоліки у рольової моделі розмежування доступу. У класичній рольової 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 формування 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.

Яку модель управління доступом вибрати?

Рольова модель краща на великих підприємствах, що здійснюють відразу кілька видів економічної діяльності та мають багаточисельний персонал. Це зумовлено її простотою та швидкодією, що буде важливо для великих компаній зі складною ієрархією. Якщо звільняється співробітник, якому була призначена певна роль, то новому співробітнику, який займе його місце, просто призначається та ж роль. Таким чином, адміністратору не потрібно постійно вносити зміни в ACL окремих об'єктів. Йому досить створити певні ролі, налаштувати необхідні цим ролям права і дозволи, а потім призначити користувачам ці ролі.

У той же час мандатна модель, яка пропонує багаторівневу ієрархію, добре підходить для закритих організацій, що оперують інформацією високої секретності, або військових підприємств, які потребують централізованого підходу до питань безпеки (в мандатній моделі така можливість передбачена). У свою чергу, дискреційна модель найпростіша.

23.2. Реєстрація подій і аудит

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 ІТС.

Аудит дозволяє виявити факти порушень, характер впливів на систему, визначити, як далеко зайшло порушення, підказати метод його розслідування і способи пошуку порушника і виправлення ситуації.

Оперативний аудит з автоматичним реагуванням на виявлені нештатні ситуації (щонайменше – засоби оповіщення адміністратора, а іноді її засоби активної протидії зафіксованим порушенням) називається ***активним***.

Обов'язкова функція аудиту – визначення користувачів, причетних до зафіксованих подій. У цілому підсистема аудиту забезпечує таку властивість захищеної ІТС як ***спостережність***.

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 автентифікації, 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

Для реєстрації подій створюється спеціальний файл (або група файлів), так званий ***журнал реєстрації***.

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.

Реалізація протоколювання і аудиту

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.

Які події реєструвати? З яким ступенем деталізації?

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

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 автентифікації;
- ➔ використання файлів, сервісів і ресурсів;
- ➔ виконання команд;
- ➔ порушення безпеки.

Контрольні запитання

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 ІТС?
7. Де знайти журнали реєстрацій подій в системі?
8. Назвіть основні події, що реєструються в системі в інтересах забезпечення безпеки.

Список рекомендованих джерел

Основний

1. Міжнародний стандарт серії ISO 2700: Інформаційні технології ; Методи захисту // Управління ризиками інформаційної безпеки, 2017. – 65 с.
2. Про рішення Ради національної безпеки і оборони України : Указ Президента України від 15 берез. 2016 р. № 96/2016 ; Про Стратегію кібербезпеки України від 27 січ. 2016 р.
3. Про основні засади забезпечення кібербезпеки України : Закон України // Відом. Верховної Ради України. – 2017. – № 45. – Ст. 403.
4. Про оборону України : Закон України // Відом. Верховної Ради України. – 2017. – № 45. – Ст. 403.
5. Методи та засоби захисту інформації : навч. посіб. / В. А. Лахно, Є. В. Василіу, В. М. Гладких та ін. – Київ : Компринт О. В., 2020. – 444 с.
6. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки : навч. посіб. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний. – Київ, 2018. – 320 с.
7. Даник Ю. Г. Основи кібербезпеки та кібероборони : підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – 2-ге вид., перероб. і доп. – Одеса : ОНАЗ ім. О. С. Попова, 2019. – 320 с.

Додатковий

1. Лахно В. А. Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак / В. А. Лахно, А. М. Терещук, Т. А. Петренко // Захист інформації. – 2016. – Т. 18. – № 2. – С. 99–106.

2. Кластеризація ознак мережевих атак в задачах аналізу захищеності інформації / В. А. Лахно, Б. С. Гусєв, А. І. Блозва та ін. // Кібербезпека: освіта, наука, техніка. – 2020. – № 1(9). – С. 45–58. – URL : https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/179/168
3. Ефективність методики розрахунку показників інвестицій в системи інформаційної безпеки об'єктів інформатизації / В. І. Чубаєвський, В. А. Лахно, О. В. Криворучко та ін. // Кібербезпека: освіта, наука, техніка. – 2021. – № 4(12). – С. 98–107. – URL : https://csecurity.kubg.edu.ua/index.php/journal/article/view/258/229
4. Модель показника поточного ризику реалізації загроз інформаційно-комунікаційним системам / В. А. Лахно, А. І. Блозва, М. Д. Місюра та ін. // Кібербезпека: освіта, наука, техніка. – 2020. – № 2(10). – С. 113–122. – URL : https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/212/189
5. Кавун С. В. Інформаційна безпека : навч. посіб. / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : ХНЕУ, 2008. – Ч.1. – 352 с. Бібліогр.: с. 338–349.
6. Єсін В. І. Безпека інформаційних систем і технологій : навч. посіб. / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Харків : ХНУ ім. В. Н. Каразіна, 2013. – 632 с.
7. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – Київ : ДУТ – КНУ, 2016. – 178 с.
8. Яремчук Ю. Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей : монографія / Ю. Є. Яремчук. – Вінниця : Книга-Вега, 2002. – 136 с.
9. Даник Ю. Г. Основи кібербезпеки та кібероборони : підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Одеса : ОНАЗ ім. О. С. Попова, 2018. – 228 с.

10. Присяжнюк М. М. Особливості забезпечення кібербезпеки / М. М. Присяжнюк, Є. І. Цифра // Реєстрація, зберігання та обробка даних. – 2017. – Т. 19. – № 2. – С. 61–68.
11. Діордиця І. Кваліфікаційні вимоги до фахівців із кібербезпеки / І. Діордиця // Підприємництво, господарство і право. – 2017. – № 2. – С. 215–219.
12. Супрунов Ю. М. Труди університету / Ю. М. Супрунов. – Київ : НУОУ. – 2011. – № 7(106). – С. 5–21.
13. Сунь-Цзи. Мистецтво війни / Сунь-Цзи ; переклад Г. Латника. – Київ : Арій, 2014. – 128 с.
14. Huang Y. Dragon's underbelly: An analysis of China's soft power / Y. Huang, & S. Ding. – East Asia. – 2006. – 23(4). – 22–44 p.
15. FM 3–12 Cyberspace and Electronic Warfare Operations, April 2017.
16. JP 3–12 Cyberspace Operations, 8 June 2018.
17. Freund J. Measuring and managing information risk. A FAIR approach / J. Freund, J. Jones. – Oxford : Butterworth of Elsevier, 2017. – 391 c.

Інтернет-джерела

1. Рекомендації CERT-UA щодо протидії APT (Advanced Persistent Threat). – URL : https://cert.gov.ua/recommendations/18
2. Перелік Кібератак. – URL : https://uk.wikipedia.org/wiki/перелік_кібератак
3. Технологія VPN може загрожувати кібербезпеці. – URL : https://detector.media/infospace/article/126505/2017-05-31-tekhnologiya-vpnmozhe-zagrozhuvati-kiberbezpetsi-inau
4. The Implementation of Network-Centric Warfare. – URL : http://www.iwar.org.uk/rma/resources/ncw/implementation-of-NCW.pdf

5. JP 3–12 Cyberspace Operations, 8 June 2018. – URL : https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
6. DOD Dictionary of Military and Associated Terms. As of January 2019. – URL : https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf
7. Isaac R. Porche III. Redefining Information Warfare Boundaries for an Army in a Wireless World / Isaac R. Porche III, Paul Christopher // RAND Corporation. – 2013. – 176 p. – 161. – URL : https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf
8. Cybersecurity a generic reference curriculum (2016). – URL : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-162 curriculum.pdf
9. National Cyber Security Strategy Good Practice Guide (2016). – URL : https://www.enisa.europa.eu/publications/ncss-good-practice-guide
10. Castro D. Boosting the Cyberworkforce / D. Castro, 2018. – URL : http://www.govtech.com/data/Boosting-the-Cyberworkforce.html
11. Get Involved with the CDM Learning Program! – URL : https://www.uscert.gov/sites/default/files/cdm_files/FNR_CGB_MTG_AprilWebinar.pdf
12. Universität der Bundeswehr München. – URL : https://www.unibw.de/home (дата звернення 27.12.2019).

Навчальне видання

ПАШОРІН Валерій Іванович,
КОСТЮК Юлія Володимирівна

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Навчальний посібник

Редактор Л. В. Білокопитова
Комп'ютерне верстання К. М. Похилюк
Дизайн обкладинки Г. В. Поліщук

Формат 60х84/16. Ум. друк. арк. 19,42. Тираж 155 пр. Зам. 295.

Видавець і виготовлювач
Державний торговельно-економічний університет
вул. Кіото, 19, м. Київ-156, Україна, 02156

Свідоцтво суб'єкта видавничої справи серія ДК № 7656 від 05.09.2022