МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

О. В. КОВАЛЬОВА

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ

НАВЧАЛЬНИЙ ПОСІБНИК

Київ
Видавничий дім Дакор
2021

УДК 004 : 34
К

Рекомендовано до друку
Вченою радою Донецького державного університету внутрішніх справ
(протокол № 19 від 26.08.2021 року)

Рецензенти
Кисько А. І. – кандидат юридичних наук, заступник начальника – начальник кримінальної поліції Головного управління Національної поліції в Донецькій області, полковник поліції;
Ісмайлов К. Ю. – кандидат юридичних наук, доцент, професор кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, майор поліції.

Ковальова О. В.

К Інформаційне забезпечення професійної діяльності : навчальний посібник / О. В. Ковальова. – Київ: ВД «Дакор», 2021. – 288 с.

ISBN 978-617-8066-04-8

Навчальний посібник підготовлений для вивчення дисципліни «Інформаційне забезпечення професійної діяльності» здобувачами та здобувачками вищої освіти за спеціальностями 081 «Право» та 262 «Правоохоронна діяльність» освітньо-кваліфікаційного рівня «бакалавр».

Навчальний посібник «Інформаційне забезпечення професійної діяльності» призначено для формування у здобувачів та здобувачок вищої освіти необхідних знань, умінь та навичок для використання сучасних інформаційних технологій у практичній діяльності поліції; удосконалення навичок професійної роботи з комп'ютерними пристроями, комп'ютерними мережами та електронними документами; оволодіння способами застосування інформаційних технологій у практиці боротьби із злочинністю з метою підготовки висококваліфікованих фахівців у галузі права для реалізації цілей Національної поліції України, здатних розв'язувати складні спеціалізовані завдання у сфері права, забезпечувати охорону прав і свобод людини, інтересів суспільства й держави, протидіяти злочинності.

УДК

ISBN 978-617-8066-04-8

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

АБД – автоматизований банк даних;
АІПС – автоматизовані інформаційно-пошукові системи;
АІС – автоматизована інформаційна система;
АСКВД – автоматизована система контролю виконання документів;
БД – база даних;
ДПС – довідкова правова система;
ЕД – електронний документ;
ЕОМ – електронна обчислювальна машина;
ЕЦП – електронний цифровий підпис;
ІЗПД – інформаційне забезпечення професійної діяльності;
ІПС – інформаційно-пошукова система;
ІС – інформаційна система;
ОС – операційна система;
ПК – персональний комп'ютер;
СЕД – система електронного документообігу;
СУБД – системи управління базами даних;
HTML – Hyper Text Markup Language – мова розмітки документів;
HTTP – Hyper Text Transfer Protocol – протокол передачі гіпертексту;
IP – Internet Protocol – міжмережевий протокол;
LAN – Locate Area Network – локальні мережі;
TCP – Transfer Control Protocol – протокол керування передачею;
WAN – Wide Area Network – глобальні мережі;
WWW – World Wide Web – Всесвітня павутина.

ВСТУП

З появою мережі «Інтернет» поширення інформації, зокрема інтернет-середовища, розуміння місця, ролі, значення людини в комунікативному просторі зазнало відповідних змін. На сьогодні технологічні системи використовуються в науці, політиці, економіці, соціальній структурі, зростає швидкість обробки інформації, створення різноманітних баз даних, мережевих та хмарних систем, що призводить до формування глобального кіберпростору. Переваги такого простору передбачають динамічні підходи використання даних і створення цифрових платформ, що забезпечує об'єктивність і швидкість рішень та позитивну співпрацю між різними суб'єктами цифровізації.

Але, незважаючи на всі ці позитивні властивості інформаційного простору, застосування людьми інформаційних технологій та перенесення суспільних відносин у цифрове поле, є й негативні наслідки, що стосуються появи нових видів провопорушень, пов'язаних із використанням новітніх комп'ютерних технологій та систем.

Метою навчального посібника «Інформаційне забезпечення професійної діяльності» є надання необхідних знань, умінь та навичок для використання сучасних інформаційних технологій у практичній діяльності поліції, удосконалення навичок професійної роботи з комп'ютерними пристроями, комп'ютерними мережами та електронними документами, напрямами використання інформаційних технологій у практиці боротьби із злочинністю та підготовка висококваліфікованих фахівців у галузі права для реалізації цілей Національної поліції України, здатних розв'язувати складні спеціалізовані завдання у сфері права, забезпечувати охорону прав і свобод людини, інтересів суспільства й держави, протидіяти злочинності.

Здобувачі та здобувачки вищої освіти, які пройшли підготовку з дисципліни ІЗПД, **повинні знати:**

1) нормативно-правову базу використання інформаційних технологій;

2) основні терміни, які використовуються в ІТ;

3) принципи побудови, функціонування та характеристики персональних комп'ютерів, комп'ютерних мереж;

4) технологію роботи з програмними продуктами MS Word, MS Excel;

5) класифікацію комп'ютерних мереж, призначення апаратного та програмного забезпечення комп'ютерних мереж;

6) характеристику та основні можливості інформаційно-пошукових систем, режиму пошуку.

Здобувачі та здобувачки вищої освіти, які пройшли підготовку з дисципліни ІЗПД, **повинні вміти**:

1) використовувати сучасні інформаційні технології в практичній діяльності;

2) користуватися сучасними програмними продуктами MS Word, MS Excel для підготовки службової і процесуальної документації;

3) користуватися різними інформаційно-пошуковими системами.

4) здійснювати предметно-орієнтований пошук інформації в інтернет-мережі, упорядковувати його результати, зберігати знайдену інформацію та використовувати її для прийняття рішень і підготовки власних документів.

Міждисциплінарні зв'язки: конституційне право, поліцейська діяльність, кримінальний процес, криміналістика, кримінологія, кримінальне право, оперативно-розшукова діяльність, юридичне документознавство, інформаційні технології.

Структурно посібник складається з восьми розділів. Особливу увагу приділено термінології та основним поняттям щодо апаратно-програмного забезпечення ПК, комп'ютерних мереж та нформаційно-пошукових систем. Після кожного розділу містяться висновки, список рекомендованих джерел, питання для самоконтролю та завдання для тестового контролю.

РОЗДІЛ 1
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ: ПОНЯТТЯ, ПРЕДМЕТ, ЗАВДАННЯ, ЗАСОБИ, ЗАКОНОДАВСТВО

1. Основні поняття, завдання ІЗПД
2. Інформаційні технології та інформаційні системи
3. Загальне уявлення про інформаційну безпеку
4. Види загроз комп'ютерній інформації
5. Нормативно-правове забезпечення ІЗПД

1. ОСНОВНІ ПОНЯТТЯ, ЗАВДАННЯ ІЗПД

Інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інформатика – це галузь науки, що вивчає структуру та загальні властивості інформації, а також питання, пов'язані з її збиранням, зберіганням, пошуком, переробкою, перетворенням, поширенням і використанням у різних сферах діяльності.

Предметом інформатики є:

- апаратне забезпечення засобів обчислювальної техніки;
- програмне забезпечення засобів обчислювальної техніки;
- засоби взаємодії апаратного і програмного забезпечення;
- засоби взаємодії людини з апаратними і програмними засобами.

На сьогодні комп'ютер та інформаційні технології є не лише предметом вивчення цілої низки навчальних дисциплін, а й засобом здійснення навчальної, наукової і професійної діяльності фахівця, який виконує свої професійні обов'язки в умовах інформаційного суспільства, у якому

інформація і технології її опрацювання перетворюються на стратегічний ресурс. Саме тому комп'ютерно-інформаційна підготовка випускника юридичного закладу вищої освіти займає одне з пріоритетних місць у процесі визначення професійної компетентності випускника та його здатності до здійснення певної професійної діяльності.

Згідно з прогнозами багатьох політологів, на сучасному етапі розвитку цивілізації відбувається поступовий перехід від індустріального до постіндустріального (або інформаційного) суспільства. Одне з його визначень таке: **інформаційне суспільство** – теоретична концепція постіндустріального суспільства; історична фаза можливого розвитку цивілізації, у якій основними продуктами виробництва є інформація і знання.

Головні риси такого суспільства:

- збільшення ролі інформації та знань;
- зростання кількості людей, зайнятих інформаційними комунікаціями та виробництвом інформаційних продуктів і послуг;
- створення глобального інформаційного простору, що забезпечує ефективну інформаційну взаємодію людей, їхній доступ до світових інформаційних ресурсів і задоволення їхніх потреб в інформаційних продуктах і послугах.

Становлення інформаційного суспільства неможливе без інформаційних відносин.

Основними принципами інформаційних відносин є:

- гарантованість права на інформацію;
- відкритість, доступність інформації, свобода обміну інформацією;
- достовірність і повнота інформації;
- свобода вираження поглядів і переконань;
- правомірність одержання, використання, поширення, зберігання та захисту інформації;
- захищеність особи від втручання в її особисте та сімейне життя.

У діяльності юриста, як і будь-якого спеціаліста, важливе значення має спілкування з іншими фахівцями, у тому числі й з інших міст, країн. Їздити – довготривало, телефонний зв'язок – неінформативно.

Такий підхід до визначення правової інформації застосовано і в *Законі України «Про інформацію», в якому зазначено, що* ***правова***

інформація *– це сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.*

Джерелами правової інформації є Конституція України, інші законодавчі та підзаконні нормативні правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

Отже, виділимо інформаційні джерела правової інформації:

1) комп'ютерні мережі (світові й локальні);

2) правові й консультаційні системи;

3) засоби отримання та обробки інформації

Дослідження в правовій інформатиці повинні враховувати як інформаційні, так і правові аспекти об'єктів, явищ і процесів, що вивчаються. Інформаційні технології довгий час розглядалися правовою інформатикою тільки з погляду ефективності організації юридичної діяльності. Проте останнім часом потреба взаємодії фахівців різних професійних галузей вимагає від юриста знання і розуміння всіх технічних та інформаційних особливостей об'єктів, що досліджуються.

У цьому розумінні правова інформатика є інструментальним засобом і джерелом знань, необхідних для вирішення безлічі проблем правового регулювання суспільних відносин.

Правова інформатика *– це міждисциплінарна галузь знання про закономірності й особливості інформаційних процесів у сфері юридичної діяльності, про їх автоматизацію, про принципи побудови й методики використання автоматизованих інформаційних систем, які створюються для вдосконалення і підвищення ефективності юридичної діяльності й вирішення правових задач на базі комплексного використання теорії та методології правових наук, засобів і методів математики, інформатики й логіки.*

Це визначення узгоджується із Законом України «Про національну програму інформатизації» від 4 лютого 1998 р., де зазначено, що **інформатизація** – це сукупність взаємозалежних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих

процесів, спрямованих на створення умов для задоволення інформаційних потреб громадян і суспільства на основі побудови, розвитку й використання інформаційних систем, мереж, ресурсів та інформаційних технологій, застосування сучасної обчислювальної і комунікаційної техніки.

Інтенсивне зближення інтересів права й інформатики є об'єктивним і закономірним процесом, викликаним нагальною потребою у взаємному використанні новітніх досягнень цих наук, який має два взаємозв'язані аспекти: прикладний і змістовий. Тобто використання останніх досягнень у галузі інформаційних технологій, пристосованих або спеціально розроблених для розвитку та функціонування юридичної науки і практики, з одного боку, і юридичне закріплення питань, пов'язаних з упровадженням у певну сферу суспільних відносин цих інформаційних технологій, – з другого.

З розвитком інформаційного суспільства збільшуються потоки інформації, швидкість її обробки й розповсюдження, у зв'язку з цим виникає необхідність у захисті інтересів суб'єктів, які використовують інформацію у своїй діяльності. Тому важливо знайти такі правові механізми, які забезпечать правове регулювання інформаційних відносин, що дозволить економічно ефективно розвивати галузь людської діяльності щодо виробництва й використання інформації, а також протистояти різним правопорушенням, пов'язаних із нею.

Розповсюдження електронних засобів фіксації, передачі й обробки інформації зумовлює безліч правових питань, що стосуються дотримання майнових і немайнових інтересів суб'єктів авторських прав. Під час захисту прав автора сайту виникає проблема ідентифікації мережевих інформаційних ресурсів як об'єкта права: чи є вони різновидом бази даних або програмою для ЕОМ, чи можна віднести сайт до засобів масової інформації тощо. Одним із найважливіших є питання безпеки й конфіденційності роботи в інтернет-мережі, тобто захист комп'ютера від зараження вірусом, запобігання несанкціонованому доступу, недопущення перехоплення особистої електронної пошти, іншої секретної інформації.

2. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

Інформаційні технології *– це сукупність процесів, що використовує засоби та методи пошуку, збирання, накопичення, зберігання, опрацювання та передавання первинної інформації для отримання інформації про стан об'єкта, процесу або явища за допомогою засобів обчислюваної та комунікаційної техніки.*

Інформаційні технології залежать від різних компонентів, зокрема:

- ✓ технічних засобів;
- ✓ персоналу, здатного використовувати їх;
- ✓ організації, яка об'єднує засоби та персонал у єдиному процесі;
- ✓ інформаційних засобів, що здійснюють формування і видачу інформації.

Інформаційні технології класифікують:

- ✓ залежно від типів даних, які опрацьовуються під час їх реалізації (наприклад, текстові, графічні, числові, мультимедійні інформаційні технології);
- ✓ за провідним інформаційним процесом, який реалізує ця технологія (наприклад, інформаційні технології передавання, опрацювання, зберігання даних);
- ✓ за основною метою здійснення інформаційних процесів (наприклад, пошуку, стиснення, передавання, кодування, захисту даних).

Термін «інформаційні технології» нерозривно пов'язаний із терміном «інформаційна система» (ІС).

Інформаційна система *– сукупність організаційних і технічних засобів для збереження та опрацювання інформації з метою забезпечення інформаційних потреб користувачів.*

Кожна інформаційна система включає в себе такі *компоненти*:

1) структура системи;
2) функції кожного елемента системи;
3) вхід і вихід кожного елемента й системи в цілому;
4) мета й обмеження системи та її окремих елементів.

До головних *завдань* належать:

1) *виявлення джерел інформації;*

2) *збирання, реєстрація, обробка та видача інформації;*
3) *розподіл інформації.*

Інформаційна система:

1) *інформаційне забезпечення* – сукупність даних для надання інформаційних послуг;

2) *технічне забезпечення* – сукупність усіх технічних засобів для функціонування та підтримання роботи інформаційної системи;

3) *програмне забезпечення* – сукупність програм для відлагодження, функціонування і перевірки роботи здатності інформаційної системи;

4) *організаційне забезпечення* – сукупність методів і засобів для організування роботи інформаційної системи;

5) *правове забезпечення* – сукупність правових норм для функціонування інформаційної системи;

6) *математичне забезпечення* – сукупність методів для реалізації роботи інформаційної системи.

Усі керовані системи, що функціонують у сфері юридичної діяльності, структурно можна поділити на суб'єкти та об'єкти керування або на підсистеми, що керують, і ті, якими керують (керовані).

Підсистеми, що керують, здійснюють керівні, регулівні та інші дії. До них належать відповідні органи державної влади, управління, суду, прокуратури, громадські організації тощо. Керовані системи піддаються діям, що керують. Об'єктом керування (керованою підсистемою) є поведінка суб'єкта – підприємства, установи, організації, посадової особи, громадянина. Взаємодія і функціонування підсистем, що керують, і керованих здійснюється через інформаційні канали прямих і зворотних зв'язків.

Для прикладу розглянемо такий важливий суспільний інститут, як кримінальна юстиція. Будь-яка система кримінальної юстиції – апарат, за допомогою якого суспільство захищає правила поведінки, необхідні для охорони інтересів як окремої особи, так і всього суспільства. Система діє, використовуючи арешт, судове переслідування і засудження тих її членів, які порушують правила спільноти. Крім негайного покарання порушника закону, будь-яка акція проти нього має на меті:

1) вилучити із суспільства людину, яка становить для нього небезпеку;

2) утримати решту членів суспільства від злочинної поведінки;

3) дати суспільству можливість зробити із злочинців законослухняних громадян.

Суб'єктами цієї системи є органи внутрішніх справ, прокуратури, суди, виправні заклади тощо; об'єктом дії – поведінка людей. Органи системи мають свої програми функціонування, насамперед юридичні та інші. Ці органи виявляють злочини, адміністративні провини тощо, тобто через канали прямого зв'язку до суб'єкта дії надходить різна соціально-правова інформація, що стосується поведінки людей. Органи юстиції (кожен по своїй лінії) збирають й обробляють цю інформацію та на її основі порушують і розслідують кримінальні справи, інші провини. Каналами зворотного зв'язку в систему надходить інформація про результати їхньої діяльності. Функціонування будь-якої системи правового характеру завжди пов'язане зі збором, обробкою та використанням інформації.

Кожна наука визначає інформаційну систему у вузькому розумінні як об'єкт свого дослідження. Тільки інформатика повинна це робити в широкому значенні, абстрагуючись від конкретних сфер застосування цих систем. Інформатика, аналізуючи поняття інформаційної системи, виділяє такі складові частини: інформація, інформаційні технології, що реалізують інформаційні процеси, і суб'єкти інформаційних процесів. Основне призначення інформаційної системи – реалізувати інформаційні процеси в тій сфері діяльності, де ця інформаційна система функціонує.

З цієї точки зору і правова система в цілому, й окремі її підсистеми (наприклад, органи прокуратури, суду, внутрішніх справ) можуть і повинні розглядатися як інформаційні системи.

У внутрішній структурі правової інформаційної системи можна виділити такі складові частини:

- ✓ суб'єкти інформаційних процесів, що відбуваються в правових утвореннях: фахівці різних галузей знань, що забезпечують функціонування інформаційної системи, суб'єкти інформаційно-правового впливу;
- ✓ соціально-правова інформація, на основі збору, систематизації та обробки якої інформаційна система вирішує поставлені завдання;

- ✓ інформаційні технології: сукупність логіко-математичних, лінгвістичних та інших методів і методик дослідження інформаційних об'єктів та обчислювальних, телекомунікаційних, інших технічних і програмних засобів обробки соціально-правової інформації.

Такий широкий підхід до визначення інформаційної системи неможливий для юридичної науки. Під час аналізу інформаційної системи як об'єкта права необхідно чітко розмежувати суб'єктний та об'єктний склади правовідносин.

Серед основних вимог, що ставляться до інформаційних систем, учені сьогодні виділяють:

1) ефективність інформаційної системи – визначається зіставленням усіх пов'язаних із розглянутими заходами витрат та одержуваних при цьому результатів;
2) якість функціонування інформаційної системи – ступінь пристосованості системи до виконання заданих функцій.

Серед основних властивостей, що визначають якість функціонування інформаційної системи, виокремлюють:

- ✓ адекватність функціонування інформаційної системи;
- ✓ наявність технічних можливостей інформаційної системи до для взаємодії, удосконалення і розвитку;
- ✓ надійність і своєчасність подання інформації та виконання функціональних технологічних операцій;
- ✓ повноту, безпомилковість, актуальність і конфіденційність інформації, що надається;

3) надійність інформаційної системи визначається надійністю технічних засобів її оснащення та помилками виконавців;

4) безпека інформаційної системи передбачає таке її функціонування, при якому забезпечується:

- ✓ захист інформації, що циркулює в цій системі (забезпечення доступності інформації для користувачів, цілісності будь-якої інформації (підтримка її актуальності й несуперечності), а також конфіденційності інформації з обмеженим доступом – захищеності від несанкціонованого використання);
- ✓ захист користувачів інформаційної системи (включаючи персонал) від шкідливої дії як інформації, що циркулює в цій системі,

так і об'єктів самої системи (ненанесення шкоди здоров'ю людей та інтересам суспільства);

✓ захист інформаційної системи та її об'єктів від несанкціонованої зміни її заданих параметрів і режиму експлуатації.

Класифікація інформаційних систем

Різноманітність сфер і форм застосування сучасних інформаційних технологій спричиняє різноманітність способів їх класифікації.

За масштабністю інформаційні системи поділяються на такі групи:

– *одиничні;*
– *групові;*
– *корпоративні;*
– *глобальні.*

За сферою застосування інформаційні системи можна умовно поділити на чотири групи:

✓ системи обробки транзакцій (операцій з базою даних) – призначені для ефективного відображення предметної області в будь-який момент часу (OLTP – OnLine Transaction Processing);

✓ системи підтримки прийняття рішень – за допомогою комплексу запитів здійснюється аналіз даних у різних аспектах: часових, просторових і т. д.;

✓ інформаційно-довідкові системи базуються на гіпертекстових документах і мультимедійних засобах. Найбільший розвиток такі системи отримали в інтернет-мережі;

✓ офісні інформаційні системи – призначені для перетворення паперових документів в електронні, для автоматизації діловодства й управління документообігом.

За способом організації автоматизовані ІС можуть бути класифіковані так: на основі архітектури файл-сервер; на основі архітектури клієнт-сервер; на основі багаторівневої архітектури; на основі інтернет-технологій.

За рівнем або сферою діяльності:

– державні;
– територіальні (регіональні);
– галузеві;
– підприємств або установ;

– технологічних процесів.

Можна класифікувати правові інформаційні системи з точки зору правової освіти, в рамках якої вони склалися і завдання якої вирішують у процесі свого функціонування, – автоматизовані системи органів прокуратури, юстиції, судів та ін.

Один з основних підходів до класифікації АІС у правовій сфері пов'язаний з видами оброблюваної соціально-правової інформації.

Так, можна виділити АІС, засновані на системі нормативних правових актів, наприклад інформаційно-пошукові по законодавству і довідкові правові системи. Для цих систем проблеми систематизації інформації стосуються питань класифікації і систематизації нормативних правових актів.

Можна виділити системи, що акумулюють та обробляють різноманітну соціально-правову інформацію ненормативного характеру: кримінологічну, криміналістичну, судово-експертну, оперативно-розшукову, науково-правову й ін.

Правова система – це база даних, у якій містяться нормативні й відомчі акти органів влади, міністерств і відомств. Основна задача, яка вирішується правовою системою, – забезпечення користувача повною, оперативною, актуальною і достовірною правовою інформацією. Серед найбільш поширених правових інформаційних систем можна назвати такі, як «Ліга: ЗАКОН», «Кодекс», «Українське законодавство». Подібні системи існують у США («LEXIS/NEXIS», «Westlaw»), у Німеччині («Juris») та в інших країнах.

У правових системах, крім баз даних нормативних документів, подані так звані тематичні пакети. Вони містять матеріали з різноманітних галузей права, словники, електронні версії різноманітних друкарських видань, консультації. Багато фірм, що поширюють системи, пропонують різноманітні послуги користувачам, що включають пошук і друкування документів за індивідуальними замовленнями.

В Україні значною правовою системою є сайт Верховної Ради України «Законодавство України», який дозволяє здійснювати пошук нормативно-правових актів України. Правова система дозволяє виконувати розширений пошук документів за реквізитами (за назвою, датою прийняття, відомчим органом), містить систему ознайомлення

з найновішими документами (прийнятими за останні 2 тижні), проєкти законодавства й інші цікаві дані не тільки для професіоналів-юристів, а й для політологів, студентів.

Експертні системи (або системи, засновані на знаннях) – це клас комп'ютерних програм, які пропонують рекомендації, проводять аналіз, виконують класифікацію, дають консультації. Вони орієнтовані на розв'язування задач, вирішення яких вимагає проведення експертизи людиною-спеціалістом. На відміну від програм, що використовують процедурний аналіз, експертні системи розв'язують проблеми у вузькій предметній площині (конкретній ділянці експертизи) на основі логічних міркувань. Такі системи часто можуть знайти розв'язання задач, які неструктуровані й неточно визначені. Вони через використання евристик компенсують відсутність структурованості, що корисно в ситуаціях, коли недостатня кількість необхідних даних або часу унеможливлює проведення повного аналізу.

Відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» автоматизована (інформаційна) система – це організаційно-технічна система, в якій реалізуються технології обробки інформації з використанням технічних і програмних засобів. А інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформаційні ресурси – окремі документи й окремі масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах).

У наш час термін «інформаційна система» використовується у двох трактуваннях. У вузькому розумінні «інформаційна система» використовується для визначення системи процедур під час роботи з даними, тобто характеризує технологічний процес, що включає виконання таких функцій: збір первинних даних (спостереження); підготовка даних до обробки; контроль; обробка даних; зберігання та пошук даних; випуск даних; переказ даних. Сукупність усіх перелічених функцій утворює процес обробки даних.

У більш широкому значенні термін «інформаційна система» використовується для позначення системи, завданням якої є

продукування інформації, що необхідна для цілей управління. Ціль побудови інформаційних систем полягає в наданні підтримки в процесі прийняття рішень.

З розвитком інформаційних технологій і техніки все більшого значення і поширення набуває такий вид інформаційних систем, як автоматизовані інформаційні системи.

Автоматизована інформаційна система є середовищем, складовими елементами якої є комп'ютери, комп'ютерні мережі, програмні продукти, бази даних та інші сучасні інформаційні технології і техніка.

Автоматизована інформаційна система (АІС) – система для організації інформаційних процесів збору, зберігання, обробки та передачі інформації, що використовує комп'ютерну інформаційну технологію.

В основі сучасних автоматизованих інформаційних систем знаходиться сукупність структурованих даних (бази даних або бази знань) та інформаційних технологій, що реалізують інформаційні процеси.

Базою даних у прямому значенні слова називають сукупність взаємопов'язаних структурованих даних. Останнім часом найбільшого поширення набули реляційні бази даних. У них інформація зберігається в одній або декількох таблицях. Зв'язок між таблицями здійснюється за допомогою значень одного або декількох співпадаючих полів.

Для взаємодії користувача з базою даних використовуються системи управління базами даних (СУБД) – комплекс програм і мовних засобів, призначених для створення, ведення та використання баз даних.

Бази знань є формою подання інформації в експертних системах, що належать до класу систем штучного інтелекту.

Базу знань можна визначити як сукупність структурованої відповідно до обраної моделі інформації про предметну область, отриманої від експертів, і правил, що описують перетворення даних у предметній області. В основі формалізації правового знання в комп'ютерних системах лежить логічна система правових норм. Логічна взаємозумовленість правових норм на різних рівнях їх змістовного функціонування, їх різноманітні логічні зв'язки і взаємини (як галузеві, так і міжгалузеві) – універсальний логічний параметр нормативно-правової системи. Кожна правова норма – певна ланка в загальній нормативній системі (як варіант) чинного законодавства. У процесі функціонування вона

логічно пов'язана з цілим арсеналом інших норм права й реалізується повною мірою лише в межах усієї системи права.

Комп'ютерна (обчислювальна) система – це об'єднання апаратних (комп'ютер) і програмних (програмне забезпечення) засобів. Обидві частини комп'ютерної системи не можуть використовуватися окремо одна від одної. Вони мають бути сумісні й обов'язково погоджені між собою за параметрами та структурою.

Комп'ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи бездротове середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило, різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали.

3. ЗАГАЛЬНЕ УЯВЛЕННЯ ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ

В обчислювальній техніці поняття «безпека» є дуже широким. Його слід розуміти як надійність роботи комп'ютера, що передбачає комплекс необхідних умов: а) збереження цінних даних; б) захист інформації від внесення в неї змін неуповноваженими особами; в) збереження таємниці листування одержуваної інформації в електронному зв'язку.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Охорона безпеки громадян здійснюється завдяки законам, але у сфері інформації, одержуваної з використанням обчислювальної техніки, систем та комп'ютерних мереж, правова практика поки що розвинута недостатньо. Законотворчий процес не встигає за розвитком технологій.

Відповідно до вимог законів України «Про інформацію», «Про державну таємницю» та «Про захист інформації в автоматизованих

системах» основним об'єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Згідно із законодавством України поняття «інформаційна безпека» має таке визначення: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації». Загалом об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Порушник – користувач, який здійснює несанкціонований доступ до інформації.

Загроза несанкціонованого доступу – це подія, що кваліфікується як факт спроби порушника вчинити несанкціоновані дії стосовно будь-якої частини інформації в інформаційній системі.

Потенційні загрози несанкціонованого доступу до інформації в інформаційних системах поділяють на цілеспрямовані (умисні) та випадкові. Умисні загрози можуть маскуватися під випадкові шляхом довгочасної масованої атаки несанкціонованими запитами або комп'ютерними вірусами.

4. ВИДИ ЗАГРОЗ КОМП'ЮТЕРНІЙ ІНФОРМАЦІЇ

Необхідність в інформаційній безпеці обумовлена самою природою мережевих служб, сервісів і послуг.

Потрібно чітко дотримуватися прийнятих протоколів обміну в мережі. Будь-яке розширення клієнтської програми може супроводжуватися певною загрозою. Рівень безпеки на кожному

комп'ютері свій. Забезпеченням режиму безпеки займається системний адміністратор.

Загроза віддаленого адміністрування. Під віддаленим адмініструванням слід розуміти несанкціоноване керування віддаленим комп'ютером. Віддалене адміністрування дає змогу брати чужий комп'ютер під своє управління. Це може дозволити копіювати та модифікувати наявні на ньому дані, установлювати довільні програми, у тому числі й шкідливі, використовувати чужий комп'ютер для вчинення злочинних дій у мережі від імені його власника.

Загроза активного змісту. Активний зміст – це активні об'єкти, вбудовані у вебсторінки. На відміну від пасивного змісту (текстів, малюнків, аудіокліпів тощо), активні об'єкти містять у собі не тільки дані, а й програмний код, що одержує клієнт вебсторінки, яка завантажується. Агресивний програмний код, що потрапив у комп'ютер, здатний поводитися як комп'ютерний вірус чи як агентська програма. Так, наприклад, він може як руйнувати дані, так і взаємодіяти з віддаленими програмами й таким способом працювати як засіб віддаленого доступу чи здійснювати підготовку для його установки.

Загроза перехоплення чи підміни даних на шляхах транспортування. З проникненням інтернету в економіку дуже гостро постала загроза перехоплення чи підміни даних на шляху транспортування. Так, наприклад, розрахунки електронними платіжними засобами (картками платіжних систем) передбачають відправлення покупцем конфіденційних даних про свою картку продавцю. Якщо ці дані будуть перехоплені на одному з проміжних серверів, немає гарантії, що ними не скористається зловмисник. Крім того, через інтернет передаються файли програм. Підміна цих файлів під час транспортування може призвести до серйозних негативних наслідків.

Загроза втручання в особисте життя. В основі цієї загрози лежать комерційні інтереси рекламних організацій. У наш час річний рекламний бюджет мережі «Інтернет» становить кілька десятків мільярдів доларів США. Прагнучи збільшити свої доходи від реклами, безліч компаній організує вебвузли, причому не стільки для того, щоб надавати клієнтам серверні послуги, скільки для того, щоб збирати про них персональні відомості. Ці відомості узагальнюються, класифікуються

і поставляються рекламним і маркетинговим службам. Процес збору персональної інформації автоматизований і дозволяє без відома клієнтів досліджувати їх пріоритети, смаки, звички.

Загроза постачання даних неприйнятного змісту. Не вся інформація, яка публікується в інтернеті, може вважатися суспільно корисною, і досить часто люди хочуть від неї захиститися.

У більшості країн світу інтернет поки не вважається засобом масової інформації. Це пов' язано з тим, що постачальник інформації не займається її копіюванням, тиражуванням і поширенням, тобто він не виконує функцій ЗМІ. Усе це робить сам клієнт у момент використання гіперпосилання. Тому звичайні закони про ЗМІ, які регламентують, що можна поширювати, а що ні, в інтернет-мережі поки не працюють.

Функції фільтрації інформації, що надходить, її змісту покладаються на браузер чи на спеціально встановлену для цієї мети програму.

Комп'ютерний злочин – це суспільно небезпечне, карне діяння (дія або бездіяльність), предметом якого є комп'ютерна інформація, направлене на заподіяння шкоди. Необхідно відзначити, що комп'ютерні злочини мають високу латентність: тільки 10–15 % комп'ютерних злочинів стають відомими. За західними джерелами, середня банківська крадіжка із застосуванням електронних засобів становить близько 15 тис. доларів, а один із найгучніших скандалів пов'язаний зі спробою викрасти 700 млн доларів з Першого національного банку в Чикаго.

Що стосується статистики злочинів у сфері використання банківських комп' ютерних систем в Україні, то її, по суті, немає, проте це не свідчить про відсутність таких злочинів.

Для визначення, аналізу та фіксації слідів комп'ютерних злочинів необхідне отримання таких даних:

1) уточнення способу порушення цілісності (конфіденційності) інформації;

2) уточнення порядку регламентації власником роботи інформаційної системи;

3) уточнення кола працівників, що мають можливість взаємодіяти з інформаційною системою, в якій відбулися зміни цілісності (конфіденційності) інформації для визначення бази свідків і виявлення кола підозрюваних осіб;

4) уточнення даних про завдану шкоду.

Класифікація комп'ютерних злочинів базується на класифікації способів учинення таких злочинів. Спосіб учинення злочину є системою взаємозумовлених, рухомих, детермінованих дій, спрямованих на підготовку, здійснення і приховання злочину, зв'язаних з використанням відповідних знарядь і засобів, а також часу, місця, об'єктивної обстановки вчинення злочину та інших обставин, що цьому сприяють.

Комп'ютерні злочини за способом їх здійснення поділяються на:

1) методи перехоплення;

2) методи несанкціонованого доступу;

3) методи маніпуляції.

Комп'ютер є об'єктом правопорушення, коли мета злочинця – викрасти інформацію або завдати шкоди системі, що цікавить його. З комп'ютером як з об'єктом пов'язані такі види злочинів:

а) вилучення засобів комп'ютерної техніки (до цієї групи належать традиційні способи здійснення звичайних видів злочинів, у яких дії злочинця направлені на вилучення чужого майна);

б) розкрадання інформації;

в) розкрадання послуг (діставання несанкціонованого доступу до якоїсь системи з метою безоплатного користування послугами, що надаються нею);

г) пошкодження системи (ця група об'єднує злочини, здійснені з метою зруйнувати або змінити дані, що є важливими для власника одного або багатьох користувачів системи – об'єкта несанкціонованого доступу);

ґ) уівинг (заплутування слідів, коли метою атаки є прагнення приховати своє ім'я і місцезнаходження).

Слід зазначити, що об'єктом правопорушення може бути пристрій, що не є комп'ютером у загальноприйнятому розумінні цього слова, наприклад, мобільний телефон, касовий апарат тощо.

Комп'ютер використовується як запам'ятовувальний пристрій (наприклад, після зламу системи створюється спеціальна директорія для зберігання файлів, що містять програмні засоби злочинця, паролі для інших вузлів, списки вкрадених номерів, кредитних карток тощо).

Залежно від способів захисту всі заходи, спрямовані на запобігання злочинам, можна класифікувати на технічні, правові та організаційні.

Технічні заходи:

1) захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем; 2) організація обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок; 3) вживання конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів; 4) установка резервних систем електроживлення, оснащення приміщень замками, сигналізацією та ін.

Правові заходи:

1) розробка норм, що встановлюють відповідальність за комп'ютерні злочини; 2) захист авторських прав; 3) удосконалення кримінального й цивільного законодавства, а також судочинства.

Організаційні заходи:

1) охорона обчислювального центру; 2) підбір персоналу, унеможливлення випадків ведення особливо важливих робіт тільки однією людиною; 3) наявність плану відновлення працездатності інформаційного центру після виходу його з ладу; 4) організація обслуговування обчислювального центру сторонньою організацією або особами, не зацікавленими в приховуванні фактів порушення роботи центру; 5) універсальність засобів захисту від усіх користувачів (у тому числі й вищого керівництва); 6) покладання відповідальності на осіб, які повинні забезпечити безпеку центру, вибір місця розташування центру тощо.

5. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІЗПД

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (дата оновлення: 04.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

8. Про Національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР (дата оновлення: 16.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text.

9. Про телекомунікації : Закон України від 18.11.2003 № 1280-IV (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text.

10. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV (дата оновлення: 07.11.2018). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

11. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII (дата оновлення: 13.02.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

12. Про затвердження Положення про Інтегровану інформаційно-пошукову систему ОВС України : наказ МВС України від 12.10.2009 № 436 (дата оновлення: 21.06.2013). URL: https://zakon.rada.gov.ua/laws/show/z1256-09#Text.

13. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 3.08.2017 № 676 (дата оновлення: 03.08.2017). URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

14. Про затвердження Порядку взаємодії ГПУ та МВС України щодо обміну інформацією з ЄРДР та інформаційних систем ОВС : спільний наказ ГПУ та МВС України від 17.11.2012 № 115/1046.

15. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 3.08.2017 № 676.

16. Методичні рекомендації щодо користування Електронною системою фіксації поліцейськими результатів реагування на події : службовий лист Національної поліції України від 16.06.2017 за 6327.

17. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14.11.2018 № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-п#Text.

ВИСНОВКИ

Інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інформаційни технології – це сукупність процесів, що використовує засоби та методи пошуку, збирання, накопичення, зберігання, опрацювання та передавання первинної інформації для отримання інформації про стан об'єкта, процесу або явища за допомогою засобів обчислюваної та комунікаційної техніки. Термін «інформаційні технології» нерозривно пов'язаний із терміном «інформаційна система» (ІС). Інформаційна система – сукупність організаційних і технічних засобів для збереження та опрацювання інформації з метою забезпечення інформаційних потреб користувачів.

Комп'ютерний злочин – це суспільно небезпечне, карне діяння (дія або бездіяльність), предметом якого є комп'ютерна інформація, направлене на заподіяння шкоди.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Відповідно до законодавства України поняття «інформаційна безпека» має таке визначення: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації». Загалом об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI (дата оновлення 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (дата оновлення: 04.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

8. Про Національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР (дата оновлення: 16.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text.

9. Про телекомунікації : Закон України від 18.11.2003 № 1280-IV (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text.

10. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV (дата оновлення: 07.11.2018). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

11. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII (дата оновлення: 13.02.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

12. Про затвердження Положення про Інтегровану інформаційно-пошукову систему ОВС України : наказ МВС від 12.10.2009 № 436 (дата оновлення: 21.06.2013). URL: https://zakon.rada.gov.ua/laws/show/z1256-09#Text.

13. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 3.08.2017 № 676 (дата оновлення: 03.08.2017). URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

14. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14.11.2018 № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-п#Text.

15. Загальні рекомендації щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет від 04.06.2021 № 24719/22-2021 / Міністерство та Комітет цифрової трансформації України.

16. Павлиш Т. Г. Навчально-методичний посібник з дисципліни «Інформаційне забезпечення професійної діяльності (+ модуль Правова статистика)» для студентів заочного відділення спеціальності 081 «Право». Кривий Ріг : Донецький юридичний інститут МВС України, 2020. 159 с.

17. Порядок взаємодії ГПУ та МВС України щодо обміну інформацією з ЄРДР та інформаційних систем ОВС : спільний наказ ГПУ та МВС України від 17.11.2012 № 115/1046. URL: https://zakon.rada.gov.ua/laws/show/v0115900-12#Text.

18. Методичні рекомендації щодо користування Електронною системою фіксації поліцейськими результатів реагування на події : службовий лист Національної поліції України від 16.06.2017 № 6327.

19. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. 256 с.

20. Іванова В. Г. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посібник.4-те вид., змін. і доп. Х. : Право, 2014. 240 с.

21. Сезонова І. К. Інформатика для правоохоронців : навч. посібник / МВС України, Харк. нац. ун-т внутр. справ, 2015. 182 с.

22. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

23. Тулінов В. С., Уткіна Г. А. Навчально-методичний посібник з дисципліни «Інформаційні технології» : для студентів ден. та заоч. форми навчання спец. 081 «Право». Кривий Ріг : Донецький юридичний інститут МВС України, 2020. 161 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Яке значення понять «правова інформатика» та «правова інформація»?

2. Що таке «інформаційні технології» та «інформаційні системи»?

3. Які ви знаєте загальні положення про інформаційну безпеку?

4. Які Ви знаєте види загроз комп'ютерній інформації?

5. У чому полягає завдання інформаційного забезпечення професійної діяльності?

6. Яке Ви знаєте нормативно-правові акти, які регламентують інформаційне забезпечення професійної діяльності?

7. Які засоби інформаційного забезпечення професійної діяльності Вам відомі?

8. У чому полягає значення інформаційного забезпечення професійної діяльності?

9. Які об'єктивні фактори зумовлюють процес інтеграції права та інформатики?

10. У чому полягає суть правової інформатики?

11. У чому полягає відмінність між даними та інформацією?

12. Що таке «правова інформація»?

13. Які Ви знаєте класифікацію інформаційних правових систем?

14. Які властивості інформації Вам відомі?

2. Практичні завдання

1. Завантажте платформу «Законодавство України» (сайт Верховної Ради України). Знайдіть та скопіюйте до документа фрагменти із Закону України «Про інформацію», а саме ст. 17 «Правова інформація» та ст. 18 «Статистична інформація».

2. Завантажте платформу «Законодавство України» (сайт Верховної Ради України). Знайдіть у Законі України «Про доступ до публічної інформації», яка інформація належить до службової із зазначенням статті. Скопіюйте знайдену інформацію до документа.

3. Теми реферативних повідомлень

1. Інформаційна культура – виклики сучасному соціуму.

2. Від інформаційного суспільства – до суспільства знань: сутність та порівняльні ознаки переходу.

3. Технологічні детермінанти сучасних соціальних концепцій.

4. Концепція електронної демократії в контексті формування інформаційного суспільства.

5. Інформаційні системи як платформа розвитку інформаційного суспільства.

6. Інформаційні автоматизовані системи як елемент інструментарію.

7. Система конфіденційного зв'язку як складова забезпечення безпеки інформаційного суспільства.

8. Поняття та сутність інформатизації.

9. Теоретико-прикладні засади оцінки інформації в умовах сучасності.

10. Забезпечення інформаційної безпеки як соціальна передумова інтелектуалізації суспільства.

11. Призначення та основні завдання Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».

ЗАВДАННЯ ДЛЯ ТЕСТОВОГО КОНТРОЛЮ

1. Згідно з Законом України «Про інформацію» захист інформації розуміють як:

а) перетворення інформації з використанням спеціальних даних з метою приховування змісту інформації, підтвердження її справжності, цілісності;
б) сукупність методів та засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру;
в) сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;
г) діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

2. Суб'єктами інформаційних відносин є:

а) фізичні особи, юридичні особи, інформація;
б) інформація, об'єднання громадян, суб'єкти владних повноважень;
в) суб'єкти владних повноважень, фізичні особи, юридичні особи;
г) юридичні особи, інформація, об'єднання громадян.

3. Предметом суспільного інтересу не вважається інформація, яка:

а) свідчить про загрозу державному суверенітету;
б) свідчить про можливість порушення прав людини, введення громадськості в оману;
в) забезпечує реалізацію конституційних прав;
г) свідчить про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

4. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

а) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;
б) про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою;
в) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;
г) про факти порушення прав і свобод людини і громадянина.

5. Укажіть принципи, які не належать до принципів інформаційних відносин:

а) рівноправність, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак, вільне отримання та поширення інформації, крім обмежень, встановлених законом;
б) відкритість, доступність інформації, свобода обміну інформацією, захищеність особи від втручання в її особисте та сімейне життя;
в) достовірність і повнота інформації, свобода вираження поглядів і переконань;
г) гарантованість права на інформацію, правомірність одержання, використання, поширення, зберігання та захисту інформації.

РОЗДІЛ 2
МЕРЕЖЕВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЇХ ВИКОРИСТАННЯ У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ

1. Комп'ютерні мережі. Їх види та призначення.
2. Поняття, структура й принципи побудови мережі «Інтернет».
3. Інтернет-сервіси.
4. Поштові адреси. Робота з гіпертекстовими сторінками World Wide Web.
5. Правова характеристика базових понять.
6. Пошук інформації в інтернет-мережі.
7. Хмарні сервіси. Поняття, значення та види.

1. КОМП'ЮТЕРНІ МЕРЕЖІ. ЇХ ВИДИ ТА ПРИЗНАЧЕННЯ

Однією з базових вимог сучасності є вчасне забезпечення особи, яка приймає рішення, актуальною інформацією. Передусім це стало можливим завдяки тому, що називають тепер «другою комп'ютерною революцією» – поєднанню обчислювальних і комунікаційних технологій у рамках глобальної мережі з неосяжним обсягом і необмеженим потенціалом. Сьогодні термін «**телекомунікації**» (від грец. «tele» – далеко та «communico» – спілкуюся) позначає здатність передавати текст, голос, зображення і навіть нематеріальні активи (грошові кошти) через мережі разом із функціональною інформацією, призначеною для управління комп'ютерними системами.

Існує багато типів мереж, що надають різні послуги. Протягом дня люди телефонують, дивляться телевізійні шоу, слухають радіо, шукають інформацію або грають у відеогру з партнером з іншої країни.

Все це було б неможливим, якби не наявність надійних мереж. Мережі об'єднують людей і пристрої незалежно від того, у якій частині світу вони розташовані. Мережі використовують, не замислюючись, як вони працюють і що було б, якби їх не існувало.

Комунікаційні технології, які використовували наприкінці 90-х років XX століття, вимагали прокладання окремих, спеціалізованих мереж. Для доступу до кожної мережі необхідні були окремі пристрої. Телефони, телевізори та комп'ютери передавали дані з використанням спеціалізованих технологій і мережевих структур. Але всім хотілося отримати легкий доступ водночас до всіх служб з одного пристрою.

Сучасні технології дали змогу створити мережу нового типу, яка надає кілька видів послуг. На відміну від некомутованих мереж, нові об'єднані системи можуть передавати голос, відеозображення і дані з використанням одного й того ж каналу зв'язку. З'явилася можливість дивитися ефірні відеопрограми на моніторі комп'ютера, телефонувати через інтернет або шукати інформацію в інтернеті, використовуючи екран телевізора. Все це стало доступним завдяки об'єднаним мережам.

На сьогодні у світі існує більше 130 млн комп'ютерів і більше 80 % з них об'єднані в різні інформаційно-обчислювальні мережі – від малих локальних мереж в офісах до глобальних мереж.

Мережа – це сукупність автономних пристроїв, сполучених лініями зв'язку. Головне призначення мереж – передача інформації. Залежно від того, рухливі передатчик / одержувач інформації або ні, розрізняють стаціонарну (фіксовану) мережу та мобільну мережу (мережа з рухомими об'єктами).

Перерахуємо мережі, які використовують щодня:

- пошта;
- телефон;
- громадський транспорт;
- локальна (корпоративна) комп'ютерна мережа;
- глобальна комп'ютерна інтернет-мережа.

Телекомунікаційна мережа – це система технічних засобів, за допомогою якої здійснюються телекомунікації. До телекомунікаційних мереж належать: а) комп'ютерні мережі (для передачі даних); б) телефонні мережі (передача голосової інформації); в) радіомережі (передача

голосової інформації – широкомовні послуги); г) телевізійні мережі (передача голосу й зображення – широкомовні послуги).

Комп'ютерні мережі (англ. network) – це сукупність ПК, розподілених на деякій території та об'єднаних для спільного використання ресурсів (даних, програм й апаратних компонентів).

Комп'ютери можна сполучити в мережу для колективного використання даних і ресурсів. Мережа може бути дуже простою (містити лише 2 комп'ютери, сполучені одним кабелем) або складною (містити сотні комп'ютерів, підключення до пристроїв, які регулюють потік інформації).

Комп'ютерною мережею називають сукупність обчислювальних машин, сполучених між собою каналами передавання даних і призначених для розподілу та колективного користування апаратними, обчислювальними та програмними засобами, інформаційними ресурсами.

Комунікаційне обладнання. Комунікаційне або мережеве обладнання – це периферійні пристрої, що здійснюють перетворення сигналів, які використовують у комп'ютері, на сигнали, що передаються через лінії зв'язку, і навпаки. Такими пристроями є модеми та мережеві адаптери. Модеми застосовують під час використання телефонних ліній зв'язку, мережеві адаптери – під час використання інших ліній.

Лінія зв'язку – це обладнання, за допомогою якого здійснюється об'єднання комп'ютерів у мережу. Мережева інтерфейсна плата (або мережевий адаптер) – спеціальний апаратний засіб для ефективної взаємодії персональних комп'ютерів у мережі. Вона встановлюється в одне з вільних гнізд розширення шини комп'ютера, а кабель передавання даних під'єднується до роз'єму на цій платі. Лінії зв'язку, що використовують кабелі для передавання сигналів, називаються дротовими, решта – бездротовими. Телефонна лінія – приклад дротової лінії зв'язку. Системи супутникового зв'язку – бездротові. Лінії зв'язку різні за складністю. Часто для з'єднання локально розташованих комп'ютерів використовується радіозв'язок. Для потужніших телекомунікацій використовується мікрохвильове або інфрачервоне випромінювання.

Комунікаційне програмне забезпечення. Комунікаційне або мережеве програмне забезпечення – це набір програм, що забезпечують роботу мережевого обладнання та обмін інформацією між комп'ютерами в мережі. Мережеве програмне забезпечення поділяють на дві групи програм. Перші працюють з мережею на так званому низькому рівні. Ці програми забезпечують управління мережевим обладнанням з метою перетворення сигналів з одного виду в інший. Програми другої групи працюють з мережею на високому рівні, вони призначені для розпізнавання та опрацювання інформації залежно від її характеру та способу організації. Усі комп'ютерні мережі поділяють на три групи: локальні, корпоративні та глобальні мережі.

Створення комп'ютерних мереж було обумовлено прагненням до економії ресурсів. Економія досягається кількома шляхами: мережа забезпечує швидкий доступ до різних джерел інформації; мережа зменшує надмірність ресурсів.

Комп'ютерна мережа забезпечує: колективне опрацювання даних користувачами, комп'ютери яких під'єднані до мережі, та обмін даними

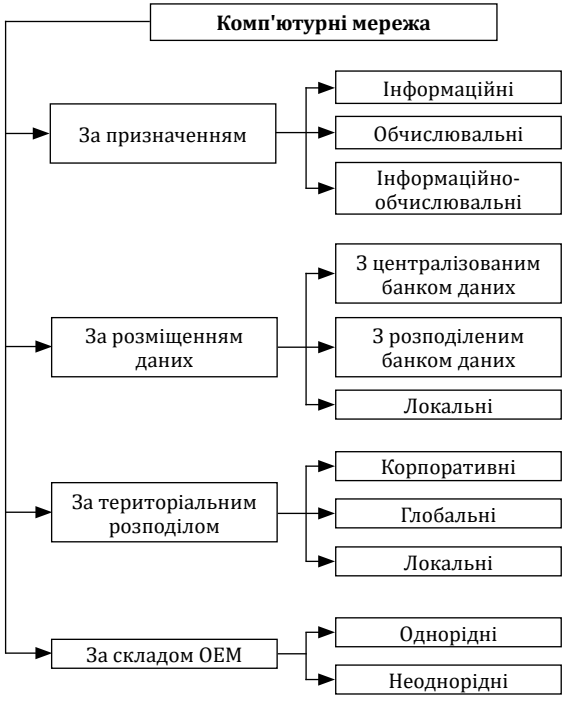
між цими користувачами; спільне використання програм; спільне використання принтерів, модемів та інших периферійних пристроїв.

Користувач, який працює на сполученому з мережею комп'ютері, має змогу використовувати всі апаратні та програмно-інформаційні ресурси мережі, на *які він отримав дозвіл від адміністратора мережі.*

Інформація, до якої здійснюють доступ за допомогою мережі, може бути сконцентрована на одному або декількох потужних комп'ютерах – серверах.

Наявні мережі прийнято ділити:

1) за призначенням;
2) за розміщенням даних;
3) за територіальною ознакою;
4) за складом ЕОМ.



Локальні мережі (LAN – Locate Area Network). Така мережа охоплює невелику територію з відстанню між окремими комп'ютерами до 10 км. Звичайно така мережа діє в межах однієї установи.

Локальну обчислювальну мережу розуміють як спільне підключення декількох окремих комп'ютерних робочих місць (робітників станцій) до єдиного каналу передачі даних. Найпростіша мережа складається як мінімум із двох комп'ютерів, з'єднаних один з одним кабелем. Це дозволяє їм використати дані спільно.

Характерною рисою локальних мереж є більша швидкість передачі даних, низький рівень помилок і використання дешевого середовища передачі даних.

Регіональні мережі. Подібні мережі існують у межах міста, району. Водночас кожна така мережа є частиною певної глобальної мережі й особливою специфікою стосовно глобальної мережі не відрізняється. Регіональні мережі поєднують кращі характеристики локальних мереж (більша швидкість передачі даних, низький рівень помилок) з більшою географічною довжиною.

Глобальні мережі (WAN – Wide Area Network). Така мережа охоплює, як правило, більші території (територію країни або декількох країн). Комп'ютери розташовуються один від одного на відстані десятків тисяч кілометрів.

Глобальні мережі часто створюються шляхом об'єднання багатьох локальних і регіональних мереж, тому вони часто є сукупністю різних технологій. Порівняно з іншими типами мереж, глобальні мережі відрізняють повільна швидкість передачі й більш високий рівень помилок.

Інтернет – це найбільша глобальна мережа, що поєднує безліч різних комп'ютерних мереж (локальних, корпоративних, глобальних) та окремих комп'ютерів (хост-комп'ютери, що постійно перебувають у ввімкненому стані), які обмінюються між собою інформацією з каналів суспільних телекомунікацій. Єдиного власника й центра керування інтернет-мережі не існує.

2. ПОНЯТТЯ, СТРУКТУРА ТА ПРИНЦИПИ ПОБУДОВИ МЕРЕЖІ «ІНТЕРНЕТ»

У суспільстві сформувалося неоднозначне ставлення до глобальної комп'ютерної мережі «Інтернет» і тих технологій, що вона підтримує. Одні вважають, що це всесвітня комунікаційна мережа; другі – величезне інформаційне звалище; треті – мегамаркет без обмежень; четверті – ідеальне середовище для злочинців; п'яті – необмежене джерело інформації тощо. Тому надано сучасне техніко-технологічне визначення.

Інтернет (Internet) *– мережа передачі даних, що має глобальну децентралізовану архітектуру, розвинені методи адресації і передачі інформації на основі протоколів TCP / IP між одно- і різнотипними мережами передачі даних, комп'ютерними системами та різноманітним термінальним (кінцевим) устаткуванням і забезпечує доступ до величезної кількості розподілених інформаційних ресурсів та надання різноманітних інформаційних послуг.*

Розвиток мережі почався на початку 60-х рр. XX ст. Для створення надійної, безвідмовної мережі зв'язку під егідою Агентства перспективних розробок Міністерства оборони США (Defence Advanced Research Project Agency – DARPA) почалася розробка і впровадження глобальної військової комп'ютерної мережі, яка з'єднувала дослідні лабораторії на території США.

Прообраз мережі «Інтернет» почав створюватися наприкінці 1960-х років за замовленням Міністерства оборони США. Днем народження мережі «Інтернет» можна вважати 2 січня 1969 р. У цей день Агентство перспективних досліджень Міністерства оборони США почало роботу над проєктом зв'язку комп'ютерів оборонних організацій. У результаті виконання цього проєкту була створена мережа «ARPANET». Формування цієї мережі мало на меті кілька цілей, однак однією з основних було створення мережі, стійкої до часткових ушкоджень. У 1986 р. Національним фондом науки США була створена опорна мережа для з'єднання своїх шести суперкомп'ютерних центрів. Мережа «Інтернет» стала використовуватися не тільки в державних (навчальних і наукових) цілях, але й у комерційних. У 1988 р. «Інтернет» стає міжнародною мережею (першими приєдналися Канада, Данія, Фінляндія, Франція, Англія, Норвегія, Швеція). На початку 90-х років до мережі «Інтернет» підключилася Україна.

Майже всі послуги інтернет-мережі побудовані за принципом «клієнт-сервер». Уся інформація в інтернеті зберігається на серверах. Обмін інформацією між серверами мережі здійснюється по високошвидкісних каналах зв'язку або магістралях.

Деякі користувачі підключаються до мережі через комп'ютери місцевих постачальників послуг інтернету, інтернет-провайдерів (Internet Service Provider – ISP), які мають постійне підключення до мережі «Інтернет». Регіональний провайдер підключається до більшого провайдера національного масштабу, що має вузли в різних містах країни. Мережі національних провайдерів поєднуються в мережі транснаціональних провайдерів або провайдерів першого рівня. Об'єднані мережі провайдерів першого рівня становлять глобальну мережу «Інтернет».

Технологія передачі інформації в інтернет-мережі побудована за принципом комутації пакетів. Визначальними для цієї технології є два поняття: протокол та адреса.

Протокол – це узгоджені правила взаємодії між двома хостами (таким терміном називають будь-які комп'ютери, що підключені до мережі, незалежно від типу, принципів дії та ін.).

Стандартний протокол забезпечує «порозуміння» між хостами в мережі та сумісність програм і даних за системою кодування і форматом.

Протокол IP (Internet Protocol) *–міжмережевий протокол* – забезпечує маршрутизацію (доставку за адресою) міжмережевих пакетів.

Протокол TCP (Transfer Control Protocol) – *протокол керування передачею* – забезпечує встановлення надійного з'єднання між двома машинами та власне передачу даних, контролюючи оптимальний розмір пакета (порції) переданих даних і здійснюючи перепосилання у разі збою. Кількість одночасно встановлюваних з'єднань між абонентами мережі не обмежується, тобто будь-яка машина може за певний проміжок часу обмінюватися даними з будь-якою кількістю інших машин по одній фізичній лінії.

TCP має механізм, який гарантує, що дані передаються без помилок, повністю і в потрібній послідовності. TCP надсилає дані у вигляді сегментів, направляє їх через IP, який забезпечує їхню маршрутизацію. З іншого боку, TCP сприймає вхідні сегменти від IP, визначає, який додаток є

приймачем даних, і передає їх цьому додатку в такому порядку, в якому їх було отримано з TCP.

Протоколи TCP / IP були написаними в 1981 р. та одержали статус стандарту США.

Адреса – це унікальний ідентифікатор хоста в інтернет-мережі. Уся мережа поділена на частини, які називаються доменами.

З розвитком комп'ютерних мереж кількість комп'ютерів, які складають їх апаратно-програмний комплекс, суттєво збільшилася. За кожним комп'ютером закріплена унікальна адреса, яка не є інтуїтивно зрозумілою для пересічних користувачів. Саме тому користувачі комп'ютерних мереж використовують так звані DNS-адреси.

DNS скорочення від **Domain Name System** – система доменних імен, що визначає всю систему адресації в інтернет-мережі. DNS з'явилася в результаті вирішення завдання створення архітектури мережі, здатної зберігати працездатність у разі значних ушкоджень. DNS часто називають регіональною системою найменувань.

Кожний рівень цієї системи називається доменом. У 80-ті роки XX ст. у США були визначені перші домени верхнього рівня:

mil – зона військових організацій;
gov – зона державних організацій;
edu – зона освітніх організацій;
com – зона компаній і комерційних підприємств;
net – зона мережевих організацій;
org – зона інших організацій.

Коли мережа «Інтернет» поширилася за національні кордони США, з'явилися національні домени. Зараз прийнято двобуквене кодування держав:

de – Німеччина;
fr – Франція;
jp – Японія;
ca – Канада;
uk – Англія;
it – Італія;
us – США;
ch – Швейцарія;

au – Австралія;
es – Іспанія;
fi – Фінляндія;
ua – Україна;
nl – Нідерланди.

Далі за доменами верхнього рівня знаходяться домени, що визначають або регіони, або організації. Потім розміщуються рівні ієрархії, які можуть бути закріплені або за невеликими організаціями, або за підрозділами більших організацій. Домени в іменах відокремлюються один від одного крапками, першою в імені стоїть назва робочої машини – реального комп'ютера з ***IP-адресою***.

IP-адреса становить послідовність чотирьох чисел, розділених крапками, – своєрідний номер комп'ютера в інтернет-мережі. Кожне число послідовності може бути дво- або тризначним. Наприклад, для комп'ютера online.kharkiv.net IP-адреса є такою: 194.44.156.18.

Для зберігання і пошуку інформації в інтернеті використовується універсальна адресація, що зветься **URL** – Uniform Resource Locator.

URL-адреса складається з трьох частин:
– використовуваний протокол;
– доменна адреса вузла;
– шлях доступу до файлу.

Схематично це можна відобразити так:

<ім'я протоколу>://адреса комп'ютера>{/<шлях до документа>}

Наприклад:

http://www.gov.ua – вебсайт органів державної влади України;

http://info.soc.org/guest/zakon/Internet/History/HIT.html – адреса вебдокумента «Мережеві інформаційні технології»;

http://www.uz.gov.ua – офіційний сайт Південної залізниці.

В електронній пошті адреса складається з імені одержувача (поштової скриньки), знака «@» та доменної адреси поштового сервера (локальної мережі), до якого приєднано одержувача. Наприклад: ivan@ukr.net.

3. ІНТЕРНЕТ-СЕРВІСИ

У мережі для користувачів підтримується низка послуг (їх також називають сервісами чи службами). Кожна послуга – це певні можливості для користувача під час роботи з мережею.

Майже всі послуги мережі побудовані за принципом «клієнт-сервер».

Сервер (у мережі «Інтернет») – це комп'ютер або програма, здатні надавати клієнтам (у міру надходження від них запиту) деякі мережні послуги.

Клієнт – прикладна програма, завантажена в комп'ютер користувача, яка забезпечує передачу запитів до сервера й одержання відповідей від нього.

Схема обміну даними АБОНЕНТ-СЕРВЕР

АБОНЕНТ	*Запит* →	Протокол обміну даними TCP / IP	*Відповідь* ←	СЕРВЕР

Соціальне значення мережі визначається тими можливостями, що їх може надати мережа для користувачів. Ці можливості реалізовані через сервіси. Різні сервіси мають різні прикладні протоколи. Найпоширенішими з них є:

- ✓ *електронна пошта (e-mail)* – для обміну електронними повідомленнями (листами) і невеликими блоками даних;
- ✓ *телеконференції (usenet)* – спосіб спілкування користувачів мережі у рамках обраних дискусійних груп (групи новин);
- ✓ *списки розсилки (maillists)* – спосіб спілкування через електронну пошту всіх, хто підписався на певний список розсилки;
- ✓ *переміщення файлів (ftp)* – копіювання файлів даних із серверів у мережі на власний комп'ютер;
- ✓ *віддалений доступ (telnet)* – спосіб керування іншим комп'ютером у мережі, яким дозволено це робити, де б він не знаходився;
- ✓ *Всесвітня павутина World Wide Web (WWW)* – спосіб доступу до інформаційних ресурсів у мережі, який реалізує концепцію гіперпосилань;

- ✓ *Gopher* – засіб розподіленого пошуку і передачі файлів у мережі;
- ✓ *IRC (Internet Relay Chat)* – спосіб спілкування з іншими користувачами мережі в режимі реального часу;
- ✓ *ICQ (I Seek You)* – безоплатна система інтернет-пейджингу (передачі коротких повідомлень у мережі), у якій кожен користувач має свій унікальний номер;
- ✓ *VoIP (Voice over Internet Protocol; IP-телефонія)* – система зв'язку, яка забезпечує передачу голосу людини через інтернет-мережу.
- ✓ *інтернет-аукціон (Internet auction)* – електронна торговельна система, у якій продаж товарів виконується безпосередньо між користувачами мережі;
- ✓ *інтернет-радіо* або *вебрадіо (realaudio)* – технологія передачі потокових аудіоданих через інтернет-мережу.
- ✓ *IP-телебачення (Internet Protocol Television,* скорочено *IPTV)* – система передачі телевізійних програм через інтернет-мережу із забезпеченням додаткових послуг з вибору контенту й керування його подачею;
- ✓ *інтернет-реклама* – медійна реклама, яка розміщується на сайтах в інтернеті. Аналогічна рекламі у друкованих ЗМІ, але наявність у банері гіперпосилання та можливість анімаційного зображення значно розширюють можливості її дії;
- ✓ *MUD* і *MOO (Multi User Dungeon* – гра серед багатьох користувачів у мережі й *Object-Oriented MUD* – об'єктно-орієнтований світ користувачів) – гра рольового характеру серед користувачів для проведення дозвілля. У віртуальному світі MOO створюються об'єкти й визначаються їхні властивості та зв'язки, що можуть застосовуватися навіть в освітніх цілях.

Зараз найбільш популярні такі інтернет-послуги: *Всесвітня павутина, вебфоруми, блоги, Вікі-проєкти (і, зокрема, Вікіпедія), інтернет-магазини, інтернет-аукціони, соціальні мережі, електронний підпис, групи новин (переважно Usenet), файлообмінні мережі, електронні платіжні системи, інтернет-радіо, інтернет-телебачення IPTV, IP-телефонія, месенджери, FTP-сервери, IRC (реалізовано також як вебчати), пошукові системи, інтернет-реклама , віддалені термінали та управління, інші послуги*.

Перегляд вебсторінки здійснюється за допомогою спеціального редактора об'єктів – браузера.

Браузер – це комп'ютерна програма у вигляді зручного для користування вікна.

Нині існує доволі багато браузерів, найбільш популярні серед них в Україні – Google Chrome, Internet Explorer, Opera, Mozilla Firefox, Safari. Свобода доступу користувачів інтернету до інформаційних ресурсів не обмежується державними кордонами і/або національними доменами, але мовні кордони зберігаються. Основною мовою інтернет-мережі є англійська. На другому місці – російська мова.

4. ПОШТОВІ АДРЕСИ. РОБОТА З ГІПЕРТЕКСТОВИМИ СТОРІНКАМИ WORLD WIDE WEB

Електронна пошта (англ. e-mail, або email, скорочення від electronic mail) – спосіб обміну цифровими повідомленнями між людьми з використанням цифрових пристроїв, таких як комп'ютери та мобільні телефони, що робить можливим пересилання даних будь-якого змісту (текстові документи, аудіо-, відеофайли, архіви, програми).

Поштові системи мають подібні основні меню, що значно полегшує роботу з ними. Принципи роботи такі. Запустивши програму і відкривши новий файл, можна в основному вікні написати лист, відповідні поля заповнити адресою адресата, адресами, кому висилати копії, а також темою листа. Щоб відправити лист, треба натиснути кнопку «Віправити». На панелях інструментів є кнопки для редагування тексту і роботи з файлами, а також кнопки для задавання таких параметрів:

- приєднання до листа ще одного файлу;
- підтвердження про отримання листа адресатом;
- підтвердження факту прочитання листа адресатом;
- перевірка граматики;
- вибір адреси з бази адрес;
- отримання довідки про програму тощо.

Електронні скриньки розміщуються на спеціальних комп'ютерах – поштових серверах. Для кожної скриньки на поштовому сервері

відводиться спеціальне місце. На одному поштовому сервері не може бути двох скриньок з однаковими назвами. Електронна адреса складається з двох частин, розділених знаком @.

Електронна пошта – засіб спілкування людей, тому вона передбачає дотримання певного етикету:

- починайте текст листа з привітання, завершуйте підписом;
- якщо звертаєтеся до людини, з якою Ви особисто не знайомі, назвіть себе; не забудьте вжити слова «будь ласка», якщо звертаєтеся до кого-небудь з проханням;
- подякуйте, якщо хтось допомагає Вам;
- слідкуйте за тоном вашого листа, намагайтеся уникати фраз, що можуть стати причиною конфлікту на релігійній, расовій, політичній та іншій основі; не надсилайте в листах неперевірені дані без посилання на їхнє джерело;
- намагайтеся не допускати граматичних помилок, використовуйте засоби перевірки орфографії, надані поштовою службою.

Робота з гіпертекстовими сторінками World Wide Web. В інтернет-мережі є низка протоколів, побудованих на базових протоколах TCP / IP, які пропонують різноманітний сервіс. Останнім часом найбільш популярним сервісом в інтернеті став сервіс WWW (World Wide Web – Всесвітня павутина). В основу цієї системи покладено поняття гіпертексту, тобто безліч окремих документів, які мають посилання один на одного. Виділені слова, що містяться в одному документі, ніби «прив'язані» до інших документів. Наприклад, якщо в змісті книжки замість номерів сторінок поставити посилання на відповідні частини тексту та створити можливість переходу за цими посиланнями, то таку книжку буде зручніше читати. Оскільки посилання можуть вказувати на документи в мережі «Інтернет» у будь-якому куточку Землі, то ця система одержала назву Всесвітньої павутини. Для роботи зі Всесвітньою павутиною використовується спеціальний протокол HTTP (Hyper Text Transfer Protocol) – протокол передачі гіпертексту.

Гіпертекст – це текст із виділеними фрагментами, що відіграють роль посилань, активізація яких спричиняє виконання певних дій, наприклад: виведення графічного зображення, відтворення звуку, відкриття нового документа тощо. Дії, які асоціюються з певними

гіперпосиланнями, можуть виконуватися автоматично (наприклад, вставка малюнка в певне місце тексту або програвання музичної мелодії під час читання документа).

Гіпертекстові документи створюються за допомогою HTML (Hyper Text Markup Language) – спеціальної мови розмітки гіпертексту. Документ у Всесвітній павутині, написаний на мові HTML і доступний для перегляду користувачем, називається вебсторінкою. Вебдокументи можна готувати в звичайному текстовому редакторі, тільки місцями в текст вставляються спеціальні коди (їх називають *тегами*), завдяки яким текст можна робити різнобарвним, вбудовувати в текст мультиплікацію, відеофрагменти тощо. Файли цих документів обов'язково повинні мати розширення імені *.htm*. Технологія WWW була розроблена Європейською лабораторією фізики елементарних частинок. Принцип роботи у Всесвітній павутині схожий на роботу з енциклопедією: Ви читаєте одну певну статтю і, користуючись посиланнями, що зацікавили Вас, читаєте ще й інші статті. Крім тексту, у документах WWW можуть знаходитися графічні зображення, звуки й відеокліпи.

Щоб почати користуватися World Wide Web, потрібно з'єднатися з інтернет-мережею і мати в наявності спеціальну програму-провідника по Всесвітній павутині. Така програма називається веббраузером (браузером-провідником), вона може відображати різноманітні типи вебінформації і переходити з теми на тему за гіпертекстовими посиланнями, які вбудовані у вебдокументи. Гіпертекстові зв'язки (посилання) виділяються на екрані кольором або (і) підкреслюються. Якщо вибрати певний гіпертекстовий зв'язок, веббраузер відобразить документ, на який вказує цей зв'язок. Найчастіше використовуються програми-браузери, які додаються до операційної системи Windows: Internet Explorer і Netscape Navigator. Крім того, деякі комерційні діалогові служби, наприклад America Online, мають свої власні браузери.

5. ПРАВОВА ХАРАКТЕРИСТИКА БАЗОВИХ ПОНЯТЬ

Визначення основних понять інтернет-технологій наведено в Законі України «Про телекомунікації». Основні з них такі:

- ✓ *адреса інтернет-мережі* – визначений чинними в інтернет-мережі міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв;
- ✓ *адресний простір інтернет-мережі* – сукупність адрес інтернет-мережі;
- ✓ *домен* – частина ієрархічного адресного простору інтернет-мережі, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється;
- ✓ *домен.UA* – домен верхнього рівня ієрархічного адресного простору інтернет-мережі, створений на основі кодування назв країн відповідно до міжнародних стандартів для обслуговування адресного простору українського сегмента мережі «Інтернет»;
- ✓ *домен другого рівня* – частина адресного простору мережі «Інтернет», що розташовується на другому рівні ієрархії імен у цій мережі;
- ✓ *Інтернет* – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами;
- ✓ *провайдер телекомунікацій* – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.

6. ПОШУК ІНФОРМАЦІЇ В ІНТЕРНЕТ-МЕРЕЖІ

Пошукова система – це вебсайт, який надає можливість пошуку інформації в інтернет-мережі. Більшість пошукових систем здійснює пошук інформації на сайтах Всесвітньої павутини, але існують системи, які здатні шукати файли на ftp-серверах, товари в інтернет-магазинах, інформацію у групах новин Usenet тощо. Є кілька моделей роботи пошукових систем. За популярністю використання варто виділити дві моделі: каталоги (довідники, директорії) та пошукові машини (індекси або пошукові покажчики).

Під час пошуку вебресурсів користувач складає запит на пошук за допомогою ключових слів. Пошукова система повинна знайти вебсторінки, що відповідають запитові. У результаті користувач має одержати гіперпосилання і короткі відомості про знайдені ресурси.

ЮРИДИЧНІ САЙТИ

1. «Юридичні послуги Online». URL: http://yurist-online.com/ukr/uslugi/

На цьому сайті Ви знайдете багато юридичної інформації як для юристів, так і для всіх, хто цікавиться українським законодавством або хоче вирішити якусь юридичну проблему. Сайт складається з чотирьох розділів:

1) послуги для громадян;
2) послуги для бізнесу;
3) послуги для юристів;
4) різне.

2. «Юридична консультація». URL: http://юрконсультация.com.ua/

Юридичний інформаційно-аналітичний сайт було створено для ефективної допомоги відвідувачам. На сайті розміщено зразки позовних заяв, юридичні аналітичні матеріали, зразки процесуальних документів, зразки договорів, судова практика, судові рішення, юридична онлайн-консультація.

3. «ЛІГА:ЗАКОН».URL: https://ligazakon.net/

Функціональні можливості системи «ЛІГА:ЗАКОН» дозволяють легко та зручно працювати з найпотужнішими базами даних, що нараховують більше 300 тисяч документів. Система «ЛІГА:ЗАКОН» – найбільш

повне джерело систематизованої та достовірної правової інформації із зручними інструментами для пошуку інформації. Дає змогу швидко знайти й проаналізувати правову інформацію на будь-який момент часу, оцінити ситуацію і прийняти правильне рішення.

4. «Всеукраїнський Юридичний Портал». URL: http://zakoni.com.ua

Це юридично-економічний інтернет-ресурс, мета якого – безкоштовне надання актуальної юридично-економічної інформації. Він містить базу законів (неповну), кодекси, Конституцію України, популярні документи, приклади договорів, документів для звернення до суду, електронні книги та багато іншого.

5. «Українська Гельсінська спілка з прав людини». URL: https://helsinki.org.ua/

Українська Гельсінська спілка сприяє розвитку гуманного суспільства, що базується на повазі до людського життя, гідності та гармонійних стосунків між людиною, державою і природою через створення платформи для співпраці між членами Спілки та іншими учасниками правозахисного руху. Її діяльність, проєкти, цілі та інші корисна інформація щодо її роботи та співпраці, доступна на офіційному сайті.

6. «Дія». URL: https://diia.gov.ua/

«Дія» – це один портал, де можна отримати всі послуги онлайн: швидко та зручно.

У сервісі доступні такі послуги, як електронний паспорт, електронне водійське посвідчення, автоцивілка, студентський квиток, військовий квиток, закордонний паспорт тощо.

Його можна безкоштовно завантажити в магазинах додатків для Android та Apple вже зараз. Кожного тижня планується надавати нові цифрові рішення для громадян.

Для ідентифікації та авторизації застосовується система Bank ID або ж додатки від Monobank та Приватбанку.

За допомогою цифрового документа українці можуть:

- ✓ здійснювати подорожі країною залізничним та повітряним транспортом;
- ✓ отримувати медичне обслуговування;
- ✓ здійснювати банківські операції;
- ✓ отримувати адміністративні та інші державні послуги;

✓ підтверджувати особу на запит правоохоронців.

«Дія. Цифрова освіта»

Проєкт запустили 21 січня 2020 року. Реєстрація дуже проста. Потрібно вказати свій номер телефону, на який надсилають sms-повідомлення. Далі необхідно ввести код з 4 цифр. Це все – Ви пройшли авторизацію.

Які серіали можна переглянути:

✓ базовий із цифрової грамотності (має три рівні знань);
✓ для вчителів;
✓ для батьків «Онлайн-безпека дітей»;
✓ «Карантин: онлайн-сервіси для вчителів».

«Дія. Бізнес»

Проєкт офіційно представили 28 лютого 2020 року. Це сайт для підприємців малого та середнього бізнесу. Портал буде працювати за двома напрямами: інформаційна платформа та служба онлайн-консультацій.

Тут можна ознайомитися з:

✓ каталогом ідей для бізнесу;
✓ шаблонами для створення бізнесу;
✓ кейсами;
✓ довідником підприємця;
✓ текстом і списком необхідних юридичних документів для відкриття бізнесу.

На сайті можна зареєструвати або закрити ФОП, такі функції пізніше будуть доступні й у додатку «Дія».

Портал «єМалятко»

Міністерство цифрової трансформації України запустило сервіс 3 січня 2020 року. Послуга значно спрощує життя батькам новонароджених дітей, адже вони можуть отримати всі необхідні послуги за 1заявою.

Послуги, якими можуть скористатися батьки:

✓ державна реєстрація народження дитини;
✓ реєстрації місця проживання народженої дитини;
✓ призначення допомоги при народженні дитини;
✓ реєстрація народженої дитини в електронній системі охорони здоров'я;

✓ реєстрація народженої дитини в Державному реєстрі фізичних осіб-платників податків;
✓ отримання посвідчень батьків багатодітної сім'ї та дитини з багатодітної сім'ї;
✓ визначення походження народженої дитини, батьки якої не перебувають у шлюбі між собою;
✓ визначення належності дитини до громадянства України;
✓ присвоєння дитині унікального номера запису в Єдиному державному демографічному реєстрі;
✓ призначення допомоги багатодітним сім'ям.

Портал з державними послугами «Дія»

Цей сервіс офіційно розпочав роботу 2 квітня 2020 року. Наразі на сайті можна оформити:

✓ довідку про несудимість;
✓ допомогу при народженні дитини;
✓ щомісячне відшкодування вартості послуг по догляду за дитиною до трьох років;
✓ низку ліцензій, дозволів чи отримати витяги з реєстрів.

Також можна подати позов до суду або отримати послуги, пов'язані з документами водія. Крім того, українці можуть перевірити наявну інформацію про себе із 5 державних реєстрів.

ГРОМАДСЬКІ ПРАВОВІ ОРГАНІЗАЦІЇ

1. «Асоціація адвокатів України». URL: https://www.uaa.org.ua/

«Асоціація адвокатів України» створена на засадах професійної належності та об'єднує адвокатів для сприяння розвитку та зміцненню інституту адвокатури в Україні, підвищення рівня правової допомоги, що надається адвокатами, зростання ролі й авторитету адвокатури в суспільстві та задоволення і захисту прав та законних інтересів членів Асоціації. Асоціація утворюється та діє із всеукраїнським статусом. Діяльність Асоціації поширюється на всю територію України.

2. «Асоціація правників України (АПУ)». URL: https://uba.ua/

«Асоціація правників України» – всеукраїнська громадська організація, заснована у 2002 році з метою об'єднання правників для створення

сильної та впливової професійної спільноти, яка стала б потужним голосом правничої громади нашої країни.

3. «Союз юристів України». URL: https://lawyersunion.org.ua/

«Союз юристів України» – всеукраїнська добровільна громадська організація, що об'єднує діячів правової сфери України. Головною метою Союзу є сприяння юристам України в задоволенні й захисті своїх професійних та соціальних інтересів, розвитку їхньої громадської активності, участі в розробці та реалізації державної правової політики. На добровільній основі та заради спільної мети в одну організацію об'єдналися судді та прокурори, працівники правоохоронних органів та органів юстиції, науковці та викладачі права, службовці органів державної влади й управління, нотаріуси, адвокати, юристи громадських організацій та інші.

ЕЛЕКТРОННІ БІБЛІОТЕКИ ПРАВОВОЇ ЛІТЕРАТУРИ

1. Електронна бібліотека Князєва. URL: https://www.ebk.net.ua/

На сайті розміщено повнотекстові книги, підручники та посібники, конспекти, що допоможуть у навчанні, реферати.

2. Правознавець. Електронна бібліотека юридичної літератури. URL: http://www.pravoznavec.com.ua/

На сайті розміщено підручники, монографії з теорії, історії і всіх галузей права України та зарубіжних країн.

3. Нормативні акти України в бібліотечній і суміжних галузях. URL: http://www.nbuv.gov.ua/node/819

На сайті розміщено повнотекстові законодавчі акти стосовно бібліотечної справи.

ОФІЦІЙНІ ПЕРІОДИЧНІ ВИДАННЯ УКРАЇНИ

1. «Вісник Верховного Суду України». URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(firstview)/vis.html?OpenDocument&Count=1000.

2. «Офіційний вісник України». URL: https://ovu.com.ua/.

3. Всеукраїнська щотижнева газета «Бухгалтерия. Налоги. Бизнес» URL: https://bnb.kiev.ua/.

4. Журнал «Податкове планування». URL: http://www.nalogovnet.com/.

5. Газета «Урядовий кур'єр». URL: https://ukurier.gov.ua/uk/.

6. Газета «Правовий тиждень». URL: http://legalweekly.com.ua/.

7. Газета «Голос України». URL: http://www.golos.com.ua/.

7. ХМАРНІ СЕРВІСИ. ПОНЯТТЯ, ЗНАЧЕННЯ ТА ВИДИ

Хмарний сервіс (public cloud services) – послуга надання хмарних ресурсів за допомогою технологій «хмарних обчислень».

Головна особливість хмарних сервісів полягає в тому, що, створюючи акаунт на такій платформі, людина зможе отримувати доступ до власної інформації з будь-якого гаджета в будь-якій точці світу. Для цього потрібно вигадати логін та пароль. Використовувати ці сервіси не лише зручно, а й безпечно. Навіть якщо з телефоном або комп'ютером щось станеться, Ваші дані не зникнуть.

Хмарні обчислення (англ. cloud computing) – це програмно-апаратне забезпечення, доступне користувачеві через інтернет-мережу або локальну мережу у вигляді сервісу, що дозволяє використовувати зручний інтерфейс для віддаленого доступу до виділених ресурсів (обчислювальних ресурсів, програм і даних). Комп'ютер користувача є при цьому рядовим терміналом, підключеним до інтернет-мережі. Комп'ютери, які здійснюють хмарні обчислення, називаються «обчислювальною хмарою». Водночас навантаження між комп'ютерами, що входять до «обчислювальної хмари», розподіляється автоматично.

Хмарні обчислення – це модель надання зручного мережевого доступу в режимі «на вимогу» до колективно використовуваного набору налаштовуваних параметрів обчислювальних ресурсів (наприклад, мереж, серверів, сховищ даних, додатків і/або сервісів), які користувач може оперативно використовувати для реалізації своїх завдань і вивільняти під час зведення до мінімуму кількості взаємодій з постачальником послуги або власних управлінських зусиль. Ця модель спрямована на підвищення доступності обчислювальних ресурсів і поєднує в собі п'ять головних характеристик, три моделі обслуговування і чотири моделі розгортання.

Уперше ідею того, що кожна людина на Землі зможе отримувати з інтернет-мережі не лише дані, а й програми, висловив думку в 1970 р.

американський учений Джозеф Карл Робнетт Ліклайдер. Розширення пропускної здатності мережі «Інтернет» дало можливість компанії «Salesforce.com» у 1999 р. першою надати своє програмне забезпечення за принципом «програмне забезпечення як зовнішній сервіс». Значну роль у подальшому розвитку хмарних сервісів відіграв розвиток технології віртуалізації. У 2006 р. компанія «Amazon» запустила перший вільно доступний сервіс під назвою «Elastic Compute Cloud», який дозволяв його користувачам запускати власні додатки.

Існує більше десяти моделей надання хмарних сервісів. Хмарні оператори виділяють три найпоширеніші з них:

- **IaaS** (Infrastructure as a Service – інфраструктура як послуга) – надання замовнику в оренду обчислювальних ресурсів у вигляді віртуальної інфраструктури;
- **PaaS** (Platform as a Service – платформа як послуга) – клієнт отримує повноцінну віртуальну платформу з різними інструментами та сервісами;
- **SaaS** (Software as a Service – програмне забезпечення як послуга) – клієнт отримує в своє розпорядження певні програмні продукти за допомогою інтернет-мережі.

Прклади популярних хмарних сервісів

- **«Google One** (Диск)» – це хмарний додаток для зберігання, редагування та синхронізації файлів, розроблений компанією «Google».

Можливості:

- можна зберігати файли будь-якого формату: фото, відео, аудіо. У кожному акаунті Google безкоштовно доступно 15 ГБ пам'яті;
- відсутня прив'язка до конкретної операційної системи;
- файли на диску можна відкривати зі смартфона, планшета або комп'ютера;
- щоб інші користувачі могли переглядати, редагувати й завантажувати файли користувача, потрібно лише відправити їм запрошення.

«Microsoft Office 365» – це хмарний сервіс, який поєднує зручні сучасні інструменти для роботи, що поширюються на основі передплати. У пакет Microsoft Office 365 входить:

- електронна пошта бізнес-класу на сервері Exchange;
- портал Sharepoint і публічний сайт-візитка з простим конструктором сторінок;
- комунікатор «Lync», за допомогою якого можна обмінюватися текстовими фразами, проводити відео- та аудіоконференції, здійснювати показ робочого столу;
- доступ до додатків останньої версії «Microsoft Office»;
- доступ до додатків «Microsoft Office» 2010, 2013 і 2016 у корпоративному тарифному плані;
- місце в «OneDrive» (1 терабайт на користувача).

«Deals» – онлайн-сервіс підписання документів електронним підписом. Сервіс допомагає оперативно приймати рішення, знижує витрати на процеси документообігу між керівником, бухгалтером, фінансистом, IT-фахівцем і юристом.

Переваги:

- збільшує кількість узгоджених вчасно документів;
- скорочує тривалість підготовки та узгодження документів;
- зменшує витрати на доставку та обмін паперовими документами між контрагентами;
- надає цілодобовий доступ до документів.

«Box» – хмарний сервіс, що більш відповідний для бізнесу і стартапів, хоча має варіанти для особистого користування. Місце у сховищі надається тільки платно: від 9 доларів за 10 ГБ. Проте версії для компаній від трьох осіб коштують від 4,5 дол. і пропонують 100 ГБ місця і більше, включаючи безлімітні сховища.

«Box» виділяється розвиненою екосистемою і зручним інтерфейсом для зберігання великих масивів даних. Доступне онлайн-редагування документів. Є інтеграція з безліччю сторонніх сервісів, включаючи таблиці й документи «Google», пакет «Office 365» і т. д.

ВИСНОВКИ

Мережа – це сукупність автономних пристроїв, сполучених лініями зв'язку. Головне призначення мереж – передача інформації. Залежно від того, рухливі передатчик / одержувач інформації або ні, розрізняють стаціонарну (фіксовану) мережу та мобільну мережу (мережа з рухомими об'єктами).

Є декілька видів мереж, які ми використовуємо щодня:

- пошта;
- телефон;
- громадський транспорт;
- локальна (корпоративна) комп'ютерна мережа;
- глобальна комп'ютерна інтернет-мережа.

Комп'ютерною мережею називають сукупність обчислювальних машин, сполучених між собою каналами передавання даних і призначених для розподілу та колективного користування апаратними, обчислювальними та програмними засобами, інформаційними ресурсами.

Усі мережі прийнято ділити:

1) за призначенням;
2) за розміщенням даних;
3) за територіальною ознакою;
4) за складом ЕОМ.

Інтернет – мережа передачі даних, що має глобальну децентралізовану будову, розвинені методи адресації і передачі інформації на основі протоколів TCP / IP.

У Законі України «Про телекомунікації» законодавець надає таке визначення поняттю «інтернет» – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами.

Технологія передачі інформації в мережі «Інтернет» побудована за принципом комутації пакетів. Визначальними для цієї технології є два поняття: протокол та адреса.

Протокол – це узгоджені правила взаємодії між двома хостами (таким терміном називають будь-які комп'ютери, що підключені до мережі, незалежно від типу, принципів дії та ін.).

Адреса – це унікальний ідентифікатор хоста в інтернет-мережі. Уся мережа поділена на частини, які називаються доменами.

З розвитком комп'ютерних мереж кількість комп'ютерів, які становлять їх апаратно-програмний комплекс, суттєво збільшилася. За кожним комп'ютером закріплена унікальна адреса, яка не є інтуїтивно зрозумілою для пересічних користувачів. Саме тому користувачі комп'ютерних мереж використовують так звані DNS-адреси.

DNS скорочення від **Domain Name System** – система доменних імен, що визначає всю систему адресації в інтернеті.

Майже всі послуги мережі побудовані за принципом «клієнт-сервер».

Сервер (в інтернет-мережі) – це комп'ютер або програма, здатні надавати клієнтам (у міру надходження від них запиту) деякі мережеві послуги.

Клієнт – прикладна програма, завантажена в комп'ютер користувача, яка забезпечує передачу запитів до сервера й одержання відповідей від нього.

Через пошукову систему маємо можливість знаходження інформації в інтернет-мережі.

Маємо змогу використовувати хмарні сервіси для зберігання інформації.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР (дата оновлення: 01.01.2020). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII (дата оновлення: 12.12.2020). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про інформацію : Закон України від 02.10.1992 № 2657-XII (дата оновлення: 16.07.2020). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI (дата оновлення: 24.10.2020). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 № 2594-IV. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI (дата оновлення: 23.04.2021). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Баженов В. А. Інформатика. Комп'ютерна техніка. Комп'ютерні технології : підручник. 4-те вид. К. : Каравела, 2012. 496 с.

8. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посібник. К. : КНЕУ, 2004. 307 с.

9. Макарова М. В. Інформатика та комп'ютерна техніка : навчальний посібник. 3-тє вид., перероб. і доп. Суми : ВДТ «Університетська книга», 2008. 665 с.

10. Маценко В. Г. Обчислювальна техніка та програмування : навчальний посібник. Чернівці : ЧНУ, 2010. 112 с.

11. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

12. Павлиш Т. Г. Навчально-методичний посібник з дисципліни «Інформаційне забезпечення професійної діяльності (+ модуль Правова статистика)» для студентів заочного відділення спеціальності 081 «Право». Кривий Ріг : Донецький юридичний інститут МВС України, 2020. 159 с.

13. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.; за заг. ред. В. Г. Іванова. Х. : Право, 2010. 240 с.

14. Редько М. М. Інформатика та комп'ютерна техніка : навчально-методичний посібник. Вінниця : Нова книга, 2007. 568 с.

15. Ярмуш О. В., Редько М. М. Інформатика і комп'ютерна техніка : навч. посібник. К. : Вища освіта, 2006. 359 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Сформулюйте визначення глобальної мережі «Інтернет».
2. З якого часу Україна має власний домен в мережі «Інтернет»?
3. Розкрийте зміст поняття «протокол передачі даних у мережі».
4. У чому полягає призначення протоколів IP?
5. У чому полягає призначення протоколів TCP?
6. Яке призначення сервісу e-mail? Назвіть його характеристики.
7. Назвіть нормативний документ, що визначає основні поняття інтернет-технологій.
8. Комп'ютерні мережі. Їх види та призначення.
9. Поняття, структура й принципи побудови мережі «Інтернет».
10. Які інтернет-сервіси Вам відомі? Які їхні особливості?
11. Правова характеристика базових понять.
12. Як здійснюється процес пошуку інформації в інтернет-мережі?
13. Хмарні сервіси. Поняття, значення та види.

2. Практичні завдання

Робота з поштовим сервісом «Google»

1. Переходимо на сайт www.gmail.com
2. На цій сторінці обираємо «Створити обліковий запис».

3. Заповнюємо всі поля форми для реєстрації.
4. Натискаємо кнопку «Далі» та потрапляємо на наступну сторінку.
5. Відмовляємося від заповнення профілю – натискаємо кнопку «Ні». Пізніше за бажанням Ви зможете додати фото для Вашого профілю. У результаті отримуємо підтвердження реєстрації.

6. Переходимо на сторінку сервісу «Google».

7. На Вашій власній сторінці можна переглянути вхідну кореспонденцію та написати лист.

8. Напишіть лист (прикріпіть картинку з побажанням для викладача). Завантажте на платформу дистанційного навчання.

9. Після того, як лист відправлено, Ви можете перейти до завантаження на диск власних документів та папок.

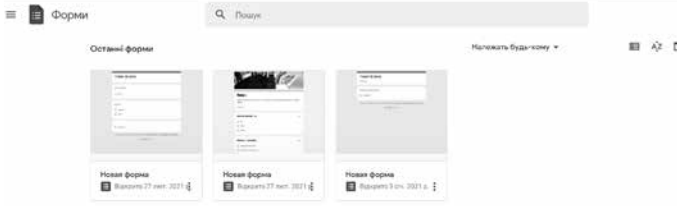
10. У відкритому вікні перейдемо до Google Диску.

11. Завантажуємо папку на Google Диск. *Увага! Попередньо необхідно створити папку та додати в неї будь-які файли, наприклад Ваші практичні роботи. Пізніше можна буде додати або видалити з неї непотрібні документи та інші папки.*

12. Аналогічно виконується завантаження файлів. Самостійно завантажте кілька файлів на диск. Після завершення завантаження документи можна переглянути у вікні.

Створіть Google-форму запрошення на конференцію «Інформаційна безпека в діяльності поліції»

1. Оберіть дію «Створити форму» в застосунку (або програмі, або в додатку): Google Документи – Google Форми – Реєстрація на захід:



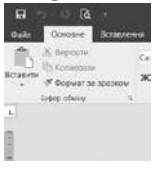
2. У формі вказати назву семінару «Інформаційна безпека в діяльності поліції» та основні питання для осіб, що реєструються, а саме:

– прізвище, ім'я, по батькові;
– місце роботи;
– посада;
– вчене звання;
– науковий ступінь;
– поштова адреса;

– контактні телефони;
– e-mail;
– назва тез.

3. Надішліть посилання на створену Google-форму на дистанційну платформу навчання.

4. Скріншоти Вашої роботи (для цього натисніть на клавіатурі кнопку «PrintScreen», а потім оберіть функцію «вставити» у MS Word) збережіть у документі Word і надішліть на сайт дистанційної освіти.



3. Теми реферативних повідомлень

1. Комп'ютерні мережі. Способи їх використання.
2. Історія розвитку глобальної комп'ютерної мережі «Інтернет».
3. Типи сервісу в інтернет-мережі.
4. Шляхи використання інтернет-мережі.
5. Електронна пошта.
6. Порівняльна характеристика найвідоміших українських провайдерів мережі «Інтернет».
7. Модеми, їхнє призначення. Види модемів.
8. Способи під'єднання до інтернет-мережі, їхні характеристики.
9. Безпровідні технології під'єднання до інтернет-мережі.
10. Адресація в інтернет-мережі. Її особливості.
11. Короткі характеристики основних служб інтернет-мережі.
12. Характеристики служб FTP, електронної пошти, IRC інтернет-мережі.
13. Характеристики служб Telnet, DNS, WWW, телеконференцій інтернет-мережі.
14. Безпека комп'ютерів під час роботи в інтернет-мережі.
15. Особливості та загальні характеристики безпровідних комп'ютерних мереж.
16. Українські регіональні комп'ютерні мережі.

ЗАВДАННЯ ДЛЯ ТЕСТОВОГО КОНТРОЛЮ

1. IP-адреса – це:
а) числова адреса мережевого комп'ютера;
б) адреса електронної пошти власника сервера;
в) адреса електронної пошти власника комп'ютера-клієнта;
г) географічні координати розташування мережевого комп'ютера.

2. Укажіть види локальних мереж:
а) глобальні;
б) інтернет-мережа;
в) з виділеним сервером;
г) однорангові.

3. Протокол – це:
а) мережеве обладнання;
б) лінія зв'язку;
в) програма;
г) набір правил обміну інформацією між комп'ютерами.

4. Через електронну пошту можна надсилати виконувані файли без архівації:
а) ні, оскільки поштові компанії самі блокують цей тип файлів;
б) так, лише за умови наявності антивірусу;
в) це можливо лише у разі зараження комп'ютера вірусом;
г) так, потрібно лише налаштувати пошту.

5. Ви давно не листувалися зі знайомим, а він раптово надіслав Вам листа з лінком, що краще зробити:
а) перейти за посиланням;
б) уточнити у знайомого, чи дійсно він відправляв цього листа;
в) негайно вимкнути комп'ютер;
г) проігнорувати листа.

РОЗДІЛ 3
ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ. ЕЛЕКТРОННИЙ ПІДПИС. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1. Поняття і значення електронного документа, електронного цифрового підпису та сучасні підходи до автоматизації документообігу.
2. Огляд сучасних систем електронного документообігу.
3. Електронний бізнес та електронна комерція.
4. Симетричні й несиметричні методи шифрування.
5. Поняття про дайджест повідомлення.
6. Поняття про криптостійкість засобів електронного цифрового підпису.

1. ПОНЯТТЯ І ЗНАЧЕННЯ ЕЛЕКТРОННОГО ДОКУМЕНТА, ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ТА СУЧАСНІ ПІДХОДИ ДО АВТОМАТИЗАЦІЇ ДОКУМЕНТООБІГУ

Усі види бізнесу й урядування неможливі без документів. Електронний бізнес та сучасне урядування використовують *електронні документи*, визначення яких міститься в Законі України «Про електронні документи та електронний документообіг», прийнятому 22 травня 2003 р. (далі – Закон). У ст. 5 Закону вказано: «*Електронний документ* – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством».

Важливим є те, що електронний документ може бути створений, переданий, збережений і перетворений електронними засобами

у візуальну форму.

При цьому «візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною» (ст. 5 Закону).

Одним із необхідних реквізитів звичайного документа є підпис або підпис з печаткою. Електронні документи теж потребують підпису – електронного. У зазначеному Законі в ст. 6 це поняття визначається так: «*Електронний підпис* є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа. Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом».

До того ж «використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах».

Крім того, електронний підпис у Законі розглянуто як засіб перевірки цілісності електронного документа. У ст. 12 указано, що «перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису».

Електронний документообіг (обіг електронних документів) – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності й у разі необхідності з підтвердженням факту одержання таких документів.

Порядок електронного документообігу регламентується державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.

У статтях 11 та 12 Закону встановлено порядок відправлення та передавання електронних документів, а також їх одержання: «Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів

інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ». Дуже важливим є визначення у Законі часу, коли був відправлений (ст. 11) та одержаний (ст. 12) електронний документ:

- «якщо автор і адресат у письмовій формі попередньо не домовилися про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання»;
- «електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

Якщо попередньою домовленістю між суб'єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа на папері. Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження».

Зверніть увагу, що, як наголошено в ст. 11 Закону, «вимоги підтвердження факту одержання документа, встановлені законодавством у випадках відправлення документів рекомендованим листом або передавання їх під розписку, не поширюються на електронні документи. У таких випадках підтвердження факту одержання електронних документів здійснюється згідно з вимогами цього Закону».

Зверніть увагу, що «дія цього Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису».

У ст. 1 Закону пояснено низку термінів і, що важливо, розрізнено поняття «електронний підпис» та «електронний цифровий підпис»:

- ✓ «*електронний підпис* – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;
- ✓ *електронний цифровий підпис* – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа».

Щоб зрозуміти це визначення, потрібно з'ясувати найважливіші поняття, які воно містить.

Одним з основних реквізитів звичайних документів є рукописний підпис. Він підтверджує факт взаємозв'язку між відомостями, що містяться в документі, та особою, що підписала документ. В основу використання рукописного підпису як засобу ідентифікації покладено гіпотезу про унікальність особистих біометричних параметрів людини. Однак його ступінь захисту зовсім недостатній. Наприклад, на фінансових документах необхідна наявність двох рукописних підписів, а також печатки юридичної особи. Якщо й цього недостатньо, то засвідчують у нотаріуса чи використовують спеціальні бланки, що мають особливі засоби захисту.

Характерною рисою рукописного підпису є його нерозривний фізичний зв'язок з носієм інформації. Тобто рукописний підпис можливий тільки на документах, що мають матеріальну природу. Обидві сторони – учасники угоди – повинні під час її складання бути присутніми, щоб особисто поставити свій підпис.

Нерозривний зв'язок між підписом і матеріальним носієм документа зумовлює важливі відмінності між оригіналом та копіями документів, одержаними засобами копіювально-множної техніки. Копії мають певні особливості порівняно з оригіналами: меншу юридичну чинність, потребують додаткових процедур засвідчення.

Ще один недолік рукописного підпису – функціональний.

Він пов'язаний з тим, що рукописний підпис забезпечує тільки ідентифікацію документа, тобто підтвердження його належності особі або зв'язку з особою, яка поставила підпис, але ніякою мірою не забезпечує аутентифікації документа, тобто його цілісності та незмінності.

Без спеціальних додаткових заходів захисту рукописний підпис не гарантує того, що документ не піддався змістовим змінам під час зберігання чи транспортування.

На відміну від рукописного підпису, електронний цифровий підпис має не фізичну, а логічну природу – це просто послідовність символів, що дозволяє однозначно «зв'язати» автора документа, зміст документа та власника електронного цифрового підпису. Логічний характер електронного цифрового підпису робить його незалежним від матеріальної природи документа. Він дозволяє позначати й аутентифікувати документи, що мають електронну природу. Електронний цифровий підпис має такі корисні властивості:

1) *можливість порівняти захисні властивості різних типів електронних цифрових підписів* – під час використання сертифікованих засобів електронного цифрового підпису його захисні властивості вищі, ніж рукописного. Їм можна дати об'єктивну (числову) оцінку, яка ґрунтується не на гіпотезі про унікальність біометричних параметрів людини, а на строгому математичному аналізі. Як наслідок, з'являється принципова можливість порівнянності захисних властивостей різних засобів електронного цифрового підпису;

2) *масштабованість* –можливість об'єктивної оцінки захисних властивостей електронного цифрового підпису зумовлює можливість застосування найпростіших засобів електронного цифрового підпису в цивільному документообігу, де загроза підробки підпису невелика. А у випадках важливих та секретних документів – застосування інших, складних спеціальних засобів електронного цифрового підпису;

3) *дематеріалізація документа* – незалежність електронного цифрового підпису від носія дає змогу здійснювати договірні відносини між віддаленими юридичними та фізичними особами без прямого чи опосередкованого фізичного контакту між ними. Ця властивість, наприклад, лежить в основі електронної комерції;

4) *рівнозначність копій* – логічна природа електронного цифрового підпису дозволяє не розрізняти копій одного документа та зробити їх

рівнозначними самому документу. Тобто будь-яка копія без додаткових заходів рівнозначна оригіналу.

Зверніть увагу, що у ст. 7 Закону України «Про електронні документи та електронний документообіг» указано: «*оригіналом електронного документа* вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу».

Є і недоліки цифрового підпису. Механізм підпису не знаходиться під безпосереднім контролем людини природними методами (наприклад, візуальними). Тому для використання електронного цифрового підпису необхідне спеціальне технічне, організаційне та правове забезпечення.

Доцільно розглянути механізм електронного цифрового підпису. Якщо стисло, то електронний цифровий підпис має за основу шифрування.

Інформаційний обмін є основою існування суспільства, тому що саме через нього реалізується дія суспільних відносин. Однією з форм інформаційного обміну є документообіг. Документообіг – це рух документів в організації з моменту їх одержання або створення до завершення виконання або відправлення. Перехід до інформаційного суспільства неминуче призводить до розширення документообігу та його якісного ускладнення. Підвищення ефективності документообігу є одним із найважливіших завдань інформатики. Вирішується воно через автоматизацію роботи з документами й використання засобів обчислювальної техніки.

Механізм документообігу має декілька стадій. Перша стадія – створення документа. Далі – його транспортування (передача), впорядковане зберігання і відтворення (або інше застосування).

Необхідною умовою переходу до автоматизованого документообігу є надання правового статусу електронним документам (ЕД). В Україні

ця проблема була вирішена з ухваленням законів України «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис». Розмежування прав доступу до тих або інших документів під час роботи в мережевому середовищі стало ще однією суттєвою проблемою, яку теж вирішено – за допомогою системи спеціальних реєстраційних імен користувачів, паролів та криптографії.

Найважче автоматизувати процеси початкової стадії документообігу – створення документів. Вони далекі від остаточної автоматизації і понині. Пояснюється це просто. Чим більша творча складова того чи іншого процесу, тим важче його автоматизувати. Водночас, чим складніший інформаційний процес, тим вища ефективність від його автоматизації, хоч би й часткової. Процес автоматизації під час створення документа ґрунтується на застосуванні стилів для оформлення деяких фрагментів документів та шаблонів документів. Водночас є можливість використання як стандартних стилів та шаблонів, так і створення нових.

Засоби автоматизації офісної діяльності (Office Automation) – текстові редактори для підготовки і коригування документів, процесори електронних таблиць, програми генерації запитів за зразком із різних БД, мережні планувальники для призначення робочих зустрічей і нарад, засоби розробки й демонстрації презентацій, словники й системи перекладу, програми відсилки і прийому факсів, електронна пошта для обміну повідомленнями й пересилання файлів. Це можуть бути окремі пакети (Word, Word Perfect, Excel, Lotus 1-2-3 тощо), інтегрований пакет програм (MS Works) або узгоджений набір пакетів (Microsoft Office або Corel Perfect Office). Для багатьох пакетів характерне використання так званих «майстрів» (Wizard), які в режимі діалогу допомагають користувачеві виконати складну процедуру.

Автоматизовані системи контролю виконання документів (АСКВД) призначені для обліку всієї документації установи, взяття на контроль і контроль за виконанням документів (нагадування про наближення строків закінчення виконання документа, повідомлення про прострочені документи тощо). Для цього в системах передбачається ведення журналу реєстрації і контролю або реєстраційно-контрольних карток документів. Такі системи побудовані на основі персональних СУБД і використовуються персоналом з діловодства і групами контролю.

Електронні архіви – системи автоматизації, призначені насамперед для фізичного збереження електронних копій документів та їх пошуку. Основою таких систем є персональна або клієнт-серверна СУБД. Документи зберігаються або в базі даних, або у файловій системі. Електронні архіви забезпечують пошук як за атрибутами, так і за змістом документів і можуть включати функції контролю за виконанням документів.

Системи керування (електронними) документами (Electronic / Enterprise Document Management System) вважаються універсальними і мають забезпечувати:

- ведення довідника користувачів на основі організаційно-штатної структури організації;
- ведення журналів реєстрації і контролю виконання документів;
- контроль термінів виконання документів, оповіщення виконавця і діловода про наближення термінів контролю та про документи, невиконані вчасно;
- збереження документів у системі;
- підтримку шаблонів документів, сполучених документів, версій і підверсій, перехресних посилань між документами;
- відстеження документів поза системою, виписування документів із системи;
- пошук документів за атрибутами, повнотекстовий та нечіткий пошук;
- розробку документів, включаючи колективну розробку;
- візування, узгодження та затвердження документів;
- документообіг – усі види маршрутизації, автоматичне розсилання повідомлень, обмін повідомленнями і дорученнями;
- всередині системи формування реєстрів відправлення до зовнішніх організацій;
- ведення класифікаторів документів (за типом, видом тощо), довідників зовнішніх і внутрішніх організацій та ін.;
- суворе розмежування повноважень у системі, підтримку ролей, протоколювання та аудит дій користувачів;
- шифрування, цифровий підпис;
- ведення справ документів, списання документів у справу, передачу справ на збереження в архів;

- формування необхідних звітів, зокрема статистичних звітів з діловодства організації.

2. ОГЛЯД СУЧАСНИХ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Електронний документообіг є сукупністю процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Електронний документообіг – високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи різноманітних підприємств, організацій, установ, органів державної влади й місцевого самоврядування. Результативність керування підприємствами й організаціями насамперед залежить від коректного вирішення завдань оперативного та якісного формування електронних документів, контролю їх виконання, а також продуманої організації їх збереження, пошуку і використання. Потреба в ефективному керуванні електронними документами й зумовила створення систем електронного документообігу (СЕД).

Розвиток суспільних відносин вимагає розроблення, удосконалення та оновлення науково-технічної і нормативно-правової бази України, створення спеціальних юридичних норм та правил регулювання сфери інформаційних документальних відносин. Верховною Радою України вже прийняті закони України: «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про Національну програму інформатизації», «Про телекомунікації», «Про Національну систему конфіденційного зв'язку», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо. У цих документах визначені основні організаційно-правові засади електронного документообігу та використання електронних документів. Отже, застосування електронного документообігу є законодавчо підкріпленим та досить поширеним на підприємствах України.

СЕД – це організаційно-технічні системи, яка забезпечують процес створення, керування доступом і розповсюдження електронних документів у комп'ютерних мережах, а також забезпечують контроль над потоками документів в організації.

Суттєвою перевагою СЕД є можливість якісного й точного виконання безлічі завдань документообігу та опрацювання великих обсягів документів. Типи файлів, що, як правило, підтримують СЕД, включають: текстові документи, зображення, електронні таблиці, аудіо- й відеодані та вебдокументи. Головне призначення СЕД – це організація збереження електронних документів, а також роботи з ними (зокрема, їх пошуку як за атрибутами, так і за змістом). У СЕД повинні автоматично відстежуватися зміни в документах, терміни їх виконання, рух, а також контролюватися всі їхні версії. Комплексна СЕД має охоплювати весь цикл діловодства підприємства чи організації: від постановки завдання на створення документа до його списання в архів, забезпечувати централізоване збереження документів у будь-яких форматах, у тому числі складних композиційних документів. СЕД повинні поєднувати розрізнені потоки документів територіально віддалених підприємств у єдину систему й забезпечувати гнучке керування документами як за допомогою точного визначення маршрутів руху, так і шляхом вільної маршрутизації документів. У СЕД має бути реалізоване чітке розмежування доступу користувачів до різних документів залежно від їхньої компетенції, займаної посади і призначених повноважень. Крім того, СЕД повинна бути налаштована відповідно до наявної організаційно-штатної структури і системи діловодства підприємства, а також інтегруватися з різними корпоративними системами.

Основними користувачами СЕД є великі державні організації, промислові підприємства, банки й усі інші структури, чия діяльність супроводжується великим обсягом створюваних, оброблюваних і збережених документів.

Згідно з основними принципами електронного документообігу він повинен функціонувати на таких засадах:

1) єдиноразова реєстрація документа;

2) можливість паралельного виконання різних операцій з метою скорочення часу руху документів і підвищення оперативності їх виконання;

3) безперервність руху документа;

4) єдина база документальної інформації для централізованого зберігання документів та унеможливлення дублювання документів;

5) ефективно організована система пошуку документа;

6) розвинена система звітності за статусами й атрибутами документів, що дозволяє контролювати поетапний рух документів.

У судовій системі України використовується автоматизована система керування документообігом «Діловодство».

Незважаючи на різноманіття систем автоматизації документообігу та діловодства, існують загальні вимоги, яким повинні відповідати ці системи:

- ✓ зручність і простота в адмініструванні та користуванні;
- ✓ масштабованість – здатність підтримувати будь-яку кількість користувачів; можливість нарощувати свою потужність має визначатися тільки потужністю відповідного апаратного забезпечення;
- ✓ розподіленість – підтримання роботи з документами в територіально розподілених організаціях та взаємодія з віддаленими користувачами;
- ✓ модульність – система має складатися з окремих модулів, інтегрованих між собою, що дає можливість замовникові вибирати й упроваджувати компоненти згідно зі своїми потребами;
- ✓ відкритість – наявність у системі відкритих інтерфейсів для можливої доробки та інтеграції з іншими системами;
- ✓ універсальність – можливість використання на різних апаратних платформах у середовищі різного системного програмного забезпечення.

3. ЕЛЕКТРОННИЙ БІЗНЕС ТА ЕЛЕКТРОННА КОМЕРЦІЯ

Перші електронні операції в мережі «Інтернет» були здійснені ще в 1995 р. Формально *електронний бізнес* є будь-якою трансакцією, здійсненою за допомогою функціональності інформаційної системи, після закінчення якої відбувається передача права власності або права користування реальним продуктом або послугою.

Разом з тим зараз відбувається поступова трансформація понять: активно вживається поняття «електронний бізнес», яке слід розуміти як реалізацію ділової активності через інтернет-мережу.

Сьогодні наявна тенденція нарощування цього сервісу й поступового перетворення вебвітрин на повноцінні інтернет-магазини. Це дає змогу бізнесу збільшити географію присутності на ринку, швидше реалізувати товар, послуги та отримати додатковий канал для маркетингу й реклами.

Проблема оплати за товар чи послугу вирішується масовим упровадженням електронних засобів платежу. Онлайнові платіжні системи, що існують сьогодні, можна розділити на три види: *пластикові* (кредитні або дебетові) картки, *електронні чеки* та *цифрові гроші* («електронний гаманець»). Головна проблема – це безпека електронних платежів. Її вирішенню сприяє поява протоколу SET (Secure Electronic Transactions – *безпечні електронні трансакції*) – міжнародного стандарту безпеки, який сьогодні є єдиним стандартом, прийнятим основними міжнародними платіжними системами для організації захищених платежів в інтернет-мережі.

Отже, сучасний електронний бізнес – це якісно нові технології, які дозволяють компанії досягти конкурентної переваги завдяки поліпшенню обслуговування своїх клієнтів та оптимізації бізнес-стосунків з партнерами. Інтернет-технології є одним з основних, але не єдиним ключовим аспектом в електронному бізнесі.

Електронна комерція як один з елементів електронного бізнесу пов'язана з виконанням функцій маркетингу, включаючи продаж товарів і послуг через інтернет-мережу споживачеві.

4. СИМЕТРИЧНІ Й НЕСИМЕТРИЧНІ МЕТОДИ ШИФРУВАННЯ

З давніх часів застосовуються різні засоби шифрування повідомлень (загальний термін – *криптографія*). Належне шифрування має забезпечувати кожній зі сторін відносну впевненість у тому, що автором повідомлення дійсно є партнер (ідентифікація партнера) і що повідомлення не було змінене в каналі зв'язку (аутентифікація повідомлення).

Метод шифрування – це формальний алгоритм, що описує порядок перетворення повідомлення в зашифроване. Ключ шифрування є набором даних, необхідних для застосування методу шифрування.

Існує нескінченна безліч методів (алгоритмів) шифрування. Наприклад, ще Гай Юлій Цезар для зв'язку з Римським сенатом використовував метод *підстановки з ключем, рівним трьом*. У повідомленні кожен символ заміщався іншим символом, що стоїть від нього в алфавіті на три позиції далі.

Розглянутий метод багатоалфавітної підстановки є класичним прикладом *симетричного шифрування*. Симетричність виявляється в тому, що обидві сторони використовують той самий ключ. Яким ключем повідомлення шифрувалося, тим же ключем і дешифрується. Це недолік, бо для використання симетричного алгоритму сторони повинні попередньо обмінятися ключами, а для цього потрібне пряме фізичне спілкування. Тому алгоритми симетричного шифрування прямо не використовуються в електронній комерції та сучасному урядуванні. Наприклад, кожному покупцю інтернет-магазину (їх тисячі) потрібно створити окремий ключ, десь ці ключі зберігати й невідомо як передавати.

В останні тридцять років з'явилися та почали розвиватися методи *несиметричної криптографії*. Саме на них ґрунтується електронний документообіг та, зокрема, електронний цифровий підпис.

Несиметрична криптографія використовує спеціальні математичні методи, на основі яких створено програмні засоби, які називаються засобами електронного цифрового підпису. Після застосування одного з таких засобів утворюється пара взаємозалежних ключів з унікальною властивістю: *те, що зашифровано одним ключем, може бути дешифровано тільки іншим і навпаки.*

Власник пари ключів залишає один ключ собі, а інший ключ розсилає своїм адресатам. Публікація ключа може відбуватися прямим розсиланням, наприклад, електронною поштою або розміщенням ключа на своєму сайті, де його зможе одержати кожен охочий. Ключ, залишений для себе, називається *закритим,* чи *особистим* ключем. Опублікований ключ – *відкритим,* чи *публічним*.

Закон України «Про електронний цифровий підпис» визначає ці поняття так: «*особистий ключ* – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу; *відкритий ключ* – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису».

Повідомлення (замовлення, договори, розпорядження тощо), які надсилаються власнику ключової пари, шифрують його відкритим ключем. Дешифрування виконується за допомогою закритого ключа.

5. ПОНЯТТЯ ПРО ДАЙДЖЕСТ ПОВІДОМЛЕННЯ

Дайджест повідомлення – це унікальна послідовність символів, що однозначно відповідає змісту повідомлення. Зазвичай дайджест має фіксовану ємність – 128 чи 168 бітів, що не залежить від довжини самого повідомлення. Дайджест вноситься до складу електронного цифрового підпису водночас із відомостями про автора та зашифровується разом з ними.

Існують більш надійні способи, щоб зловмисник не зміг змінити повідомлення так, щоб зберегти контрольну суму, якщо шифр буде зламаний і контрольна сума стане відомою зловмисникові. Це означає, що за контрольною сумою легко знайти значення цієї функції – *хеш-код.* Але за хеш-кодом неможливо відтворити контрольну суму. Мільярди мільярдів контрольних сум дають точнісінько той самий хеш-код.

До речі, так зберігають паролі, наприклад, на інтернет-сайтах. Щоб їх не вкрали, зберігають лише хеш-коди. Самих паролів немає, так що й крадіжка неможлива. У разі перевірки пароля, наданого користувачем, обробляють пароль хеш-функцією, тобто одержують його хеш-код та порівнюють з хеш-кодом, який зберігають.

Повернімося до дайджесту повідомлення. Контрольна сума обробляється хеш-функцією, щоб утворити хеш-код (аутентифікацію повідомлення). Хеш-код так само унікальний для певного повідомлення, як і відбитки пальців для людини. Це і є дайджест повідомлення. Його називають *відбитком* чи *відтиском*. Іноді – *електронною печаткою.* Дайджест повідомлення приєднується до електронного підпису і стає складовою частиною половини ключа, потім обробляє повідомлення тією ж хеш-функцією, що й відправник, після чого звіряє отриманий дайджест із тим, що містився в підписі. Якщо вони однакові, значить, повідомлення не піддалося змінам у каналі зв'язку. Усі ці дії виконуються автоматично, без участі самого користувача.

6. ПОНЯТТЯ ПРО КРИПТОСТІЙКІСТЬ ЗАСОБІВ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Електронний цифровий підпис теж може бути підданий фальсифікації. Щоб його фальсифікувати, зловмисник повинний тим чи іншим способом одержати доступ до закритого ключа. У такому разі йдеться про *компрометацію закритого ключа,* її наслідком є *компрометація електронного підпису* – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа.

Є традиційні й нетрадиційні способи компрометації. Традиційні – це викрадення ключа шляхом копіювання через несанкціонований доступ або викрадення устаткування чи викрадення через змову з особою, яка його використовує.

Захист від компрометації певною мірою забезпечує законодавство. Особи, винні у порушенні законодавства про електронний цифровий підпис, несуть відповідальність згідно з законом.

Питаннями зламу шифрів, розробкою методів, що дозволяють розшифровувати інформацію (знімати з неї захист) та оцінювати якість захисту інформації шифром (ідеться про його *криптостійкість*) займається певна галузь криптографії – *криптоаналіз.*

Можливість зламати шифр визначається продуктивністю обчислювальної техніки та ємністю ключа, яка вимірюється в бітах (двійкових

розрядах). Чим довший ключ, тим більший час перебору можливих значень. Наприклад, дуже просто оцінюється криптостійкість симетричних ключів.

Якщо довжина ключа 40 бітів, то для його реконструкції треба перебрати 240 чисел. Кілька сучасних комп'ютерів вирішать цю задачу за добу. Якщо довжина 64 біти, то необхідна мережа з декількох десятків комп'ютерів. Задача вирішується протягом декількох тижнів. 128 бітів – час реконструкції у мільйони разів більший, ніж вік Всесвіту.

Проте можна користуватися *принципом достатності шифрування та економічної доцільності* – повідомлення вважається досить захищеним, якщо його розшифровка потребує матеріальних витрат, які значно перевершують цінність інформації, яка міститься в повідомленні.

ВИСНОВКИ

Поняття «електронний документ» означає документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Одним із необхідних реквізитів звичайного документа є підпис або підпис з печаткою. Електронні документи теж потребують підпису – електронного. У ст. 6 Закону України ««Про електронні документи та електронний документообіг»» (прошу перевірити, чи правильна назва) це поняття визначається так: «*Електронний підпис* є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа. Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом».

До того ж «використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах».

Електронний документообіг (обіг електронних документів) – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Порядок електронного документообігу регламентується державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.

Існує два методи шифрування: симетричний і несиметричний.

Симетричний метод шифрування – у повідомленні кожен символ заміщався іншим символом, що стоїть від нього в алфавіті на три позиції далі.

Симетричність виявляється в тому, що обидві сторони використовують той самий ключ. Яким ключем повідомлення шифрувалося, тим ключем і дешифрується.

Несиметричний метод шифрування використовує спеціальні математичні методи, на основі яких створено програмні засоби, які називаються засобами електронного цифрового підпису. Після застосування одного з таких засобів утворюється пара взаємозалежних ключів з унікальною властивістю: те, що зашифровано одним ключем, може бути дешифровано тільки іншим і навпаки.

Проте можна користуватися *принципом достатності шифрування та економічної доцільності* – повідомлення вважається досить захищеним, якщо його розшифровка потребує матеріальних витрат, які значно перевершують цінність інформації, яка міститься в повідомленні.

Усі аспекти розглянуто переважно з точки зору застосування відповідної нормативно-правової бази.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV (дата оновлення: 07.11.2018). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

8. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII (дата оновлення: 13.02.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

9. Баженов В. А. Інформатика. Комп'ютерна техніка. Комп'ютерні технології : підручник. 4-те вид. К. : Каравела, 2012. 496 с.

10. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посібник. К. : КНЕУ, 2004. 307 с.

11. Макарова М. В. Інформатика та комп'ютерна техніка : навчальний посібник. 3-тє вид., переоб. і доп. Суми : ВДТ «Університетська книга», 2008. 665 с.

12. Клименко І. В. Електронний документообіг у державному управлінні : навч. посіб. / Нац. акад. держ. упр. при Президентові України. Х. : ФОРТ, 2009. 232 с.

13. Павлиш Т. Г. Навчально-методичний посібник з дисципліни «Інформаційне забезпечення професійної діяльності (+ модуль Правова

статистика)» для студентів заочного відділення спеціальності 081 «Право». Кривий Ріг : Донецький юридичний інститут МВС України, 2020. 159 с.

14. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.; за заг. ред. В. Г. Іванова. Х. : Право, 2010. 240 с.

15. Редько М. М. Інформатика та комп'ютерна техніка : навчально-методичний посібник. Вінниця : Нова книга, 2007. 568 с.

16. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

17. Тулінов В. С., Уткіна Г. А. Навчально-методичний посібник з дисципліни «Інформаційні технології» для студентів ден. та заоч. форми навчання спец. 081 «Право». Кривий Ріг : Донецький юридичний інститут МВС України, 2020. 161 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Які особливості електронного документа?
2. Що таке «Електронний цифровий підпис»?
3. Як здыйснюэться облік електронних документів?
4. Які сучасні підходи до автоматизації документообігу Вам відомі?
5. Механізм документообігу.
6. Електронний бізнес та електронна комерція.
7. У чому полягає суть поняття «дайджест повідомлення»?
8. Поняття крипостійкості засобів ЕЦП.
9. Організаційне забезпечення ЕЦП.
10. Дайте визначення поняттю «електронний документ».
11. Що вважається оригіналом електронного документа?
12. Дайте визначення поняттю «електронний документообіг».
13. Назвіть строк зберігання електронних документів на електронних носіях інформації.

14. Назвіть нормативно-правові акти, що регулюють відносини, пов'язані з електронним документообігом та використанням електронних документів.

2. Практичне завдання

Перегляньте відео «Основи роботи з системою електронного документообігу» за посиланням https://www.youtube.com/watch?v=q-if8LGaPak&ab_channel=IQusionIT.%D0%A1%D0%95%D0%94-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D0%BF%D1%80%D0%BE%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%B5.

3. Теми реферативних повідомлень

1. Основні правила шифрування. Використання шифроблокнота.
2. Основні особливості комп'ютерного шифрування.
3. Застосування програм шифрування з відкритим ключем під час передавання інформації у відкритих мережах зв'язку.
4. Програми захисту комп'ютерної інформації шляхом шифрування.
5. Біометрична інформація як джерело ідентифікаційних ознак особи.
6. Програмні засоби розмежування доступу до інформації.
7. Право на свободу інформації в системі конституційних прав і свобод людини та громадянина.
8. Необхідність обмеження права на свободу інформації в інтересах національної безпеки, територіальної цілісності або громадського порядку.
9. Захист персональних даних в Україні: стан та перспективи.
10. Відповідальність за порушення права на доступ до інформації в Україні.
11. Перспективи правового регулювання в інформаційній сфері України.

ЗАВДАННЯ *ДЛЯ* ТЕСТОВОГО КОНТРОЛЮ

1. Цифровий підпис – це:

а) підпис відповідальної особи, перетворений у цифрову форму, який циркулює в інформаційно-комунікаційній системі;

б) переданий факсом підпис людини;
в) знятий сканером підпис особи, що приймається як підтвердження оригінальності документа;
г) унікальний ідентифікуючий рядок символів, використовуваний як засіб перевірки й ідентифікації поштових повідомлень.

2. Сутність проблеми розподілу ключів полягає у:

а) наявності великої кількості замків для цих ключів;
б) відсутності необхідної кількості кваліфікованих слюсарів для їх виготовлення;
в) наявності великої кількості споживачів та необхідністю забезпечення секретності;
г) складністю створення великої кількості ключів.

3. Принцип шифрування заміною полягає:

а) у заміні відкритої абетки на таємну;
б) у перестановці порядку розташування літер у закритому повідомленні;
в) у заміні слів та окремих складів у закритому повідомленні;
г) немає правильної відповіді.

4. Симетричне шифрування – це:

а) шифрування з відкритим ключем;
б) кодування відкритої інформації;
в) створення закритого повідомлення з використанням таємного ключа, що відомий лише його відправнику та отримувачу;
г) приховування факту передавання інформації.

5. Асиметрічне шифрування – це:

а) шифрування з використанням разового шифроблокнота;
б) шифрування з використанням стеганографічних методів;
в) шифрування з використанням таємного та відкритого ключів;
г) немає правильної відповіді.

РОЗДІЛ 4
РИЗИКИ ТА ЗАГРОЗИ У СФЕРІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

1. Проблеми захисту інформації у сучасних ІС.
2. Загрози інформаційній безпеці.
3. Види атак.
4. Поняття і класифікація комп'ютерних вірусів.
5. Засоби захисту інформації.

1. ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У СУЧАСНИХ ІС

Захист інформації є однією з вічних проблем. Протягом історії людства способи вирішення цього питання визначалися рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми: комп'ютерні злочини стали характерною ознакою сьогодення.

Комп'ютерними називають **злочини**, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами.

Серед ***причин комп'ютерних злочинів*** і пов'язаних з ними викрадень інформації головними є такі:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного

відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їхньої надійності та збільшення кількості вразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп'ютерних злочинів, але експерти погоджуються, що відповідні суми становлять мільярди доларів. Серед основних статей варто виокремити такі:

- збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатність системи (мережі);
- вартість викрадених і скомпрометованих даних;
- витрати на відновлення роботи системи, на перевірку її цілісності, на доробку вразливих місць тощо.

Варто також ураховувати й морально-психологічні наслідки для користувачів, персоналу і власників ІС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному й військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки й безпеки держави, здоров'я і навіть для життя людей.

Економічні та юридичні питання, приватна та комерційна таємниця, національна безпека – усе це зумовлює необхідність захисту інформації та ІС.

Згідно із *Законом України «Про захист інформації в автоматизованих системах»* **захист інформації –** це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій».

Забезпечення безпеки інформаційних технологій є комплексною проблемою, яка охоплює правове регулювання використання ІТ,

удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки та витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання і можливі наслідки, вибрати адекватні засоби та побудувати надійну систему захисту.

Базовими **принципами інформаційної безпеки** є забезпечення цілісності інформації, її конфіденційності й водночас доступності для всіх авторизованих користувачів. Із цього погляду **основними випадками порушення безпеки інформації** можна назвати такі:

- несанкціонований доступ – доступ до інформації, що здійснюється з порушенням установлених в ІС правил розмежування доступу;
- витік інформації – результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації – дія, унаслідок якої інформація в ІС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
- підробка інформації – навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в ІС;
- блокування інформації – дії, наслідком яких є припинення доступу до інформації;
- порушення роботи ІС – дії або обставини, які призводять до спотворення процесу обробки інформації.

Причини настання зазначених випадків такі:

- збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережевих карт, дискових систем тощо);
- некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);
- навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи ІС, спричинення витоку інформації);

- помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);
- навмисні дії обслуговуючого персоналу та користувачів (усе сказане в попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією).

Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або витоку інформації, але передбачають втручання в роботу системи.

Основні особливості комп'ютерних злочинів:

- установлення факту вчинення злочину: на відміну від традиційних, правоохоронець не може виявити труп, відсутність матеріальних цінностей на складі, пошкоджений автомобіль. Усі сліди злочину знаходяться на матеріальних носіях комп'ютера, який може знаходитися на значній відстані від потерпілої особи;
- відсутність міждержавних кордонів для злочинців (якщо злочин вчиняється з використанням глобальної комп'ютерної мережі) та існування декількох місць учинення злочину (у разі несанкціонованого доступу до банківських комп'ютерних систем місцем учинення злочину слід вважати як саму банківську систему, що була атакована, так і місце знаходження комп'ютера, з якого здійснювали доступ, а також місце надходження коштів для отримання готівки).

Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту.

Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви: сторонні, які не знають фірму; сторонні, які знають фірму, та колишні співробітники; співробітники-непрограмісти; співробітники-програмісти.

Межа між програмістами та простими користувачами з погляду небезпечності останнім часом зникає. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку й можуть скористатися спеціальним програмним забезпеченням, яке має дружній інтерфейс і доступне на піратських CD-ROM, у спеціальних розділах BBS і на інтернет-сайтах та FidoNet. За твердженнями експертів, тільки чверть співробітників цілком лояльна, чверть налаштована щодо фірми вороже і не має моральних обмежень, лояльність решти залежить від обставин. Тому нелояльні співробітники, які мають доступ до комп'ютерів і знайомі з системою, становлять серйозну загрозу ІС. Передусім це організаційна проблема, технологія тут може відігравати тільки допоміжну роль.

Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники».

Хакери (хекери) – це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків»: за однією з легенд, слово «hack» уперше стало застосовуватися в Массачусетському технологічному інституті для позначення проєкту, який не має очевидного практичного значення і виконується лише заради задоволення від самого процесу роботи. У більш вузькому розумінні слово «хакер» позначає тих, хто одержує неправомочний доступ до ресурсів ІС тільки для самоствердження (див. приклад). Останнє відрізняє хакерів від професійних зламувачів – **кракерів** (або «крекерів», не плутати з печивом), які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень.

Найбільш криміногенною групою є **пірати –** професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, як правило, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв'язку. В усіх випадках мотивація – матеріальні інтереси, а не цікавість чи пустощі.

За даними дослідження корпорації IDG, у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % – через зовнішні проникнення із застосуванням спеціальних засобів.

Шкідники (вандали) намагаються реалізувати в кіберпросторі свої патологічні схильності: вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без будь-якої вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль.

Слід також розглянути ще одну групу, яка займає проміжне місце між хакерами та недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш тяжких наслідків, ніж спланові атаки професіоналів). Ідеться про **експериментаторів («піонерів»).** Найчастіше це молоді люди, які під час освоєння інструментальних й інформаційних ресурсів інтернет-мережі та власного комп'ютера бажають вчитися тільки на власних помилках, керуючись принципом «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією в цій групі є гра. Експерементатори стають професіоналами високого класу, зокрема й законослухняними.

Отже, **однією з основних причин порушення безпеки інформації** є незатребуваність творчого потенціалу в поєднанні з неусвідомленням усіх наслідків протиправних дій. Цей фактор існує незалежно від національності або сфери професійної діяльності. Звичайно, жодна з особистих проблем не може стати приводом для протиправної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп'ютерних злочинців. Стають відомими колосальні збитки від їхньої діяльності. Розвінчується міф про хакера як про комбінацію Гудіні та Фантомаса, адже часто своїми успіхами вони завдячують не власним навичкам, а банальним пропускам у захисті систем (звідси і нове прізвисько – «ламери»). Поширюється думка про те, що комп'ютерний злочин легше попередити, ніж потім розслідувати. Однак це не вирішує проблему повністю, адже, крім бажання розважитися і самоствердитися, є ще недбалість, холодний комерційний розрахунок, прояви садизму та хворобливої уяви. Тому комп'ютерні злочини залишаються об'єктом уваги фахівців.

2. ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Розгляд можливих загроз інформаційній безпеці здійснюється з метою визначення повного набору вимог до розроблюваної системи захисту. Зазвичай загрозу (у загальному сенсі) тлумачать як потенційно можливу подію (вплив, процес або явище), яка може зробити небажаний вплив на систему, а також на інформацію, що зберігається в ній. Далі загрозу безпеці інформаційної системи (ІС) розуміємо як можливість впливу на ІС, яка прямо або непрямо може завдати їй шкоди.

У Законі України «Про основні засади забезпечення кібербезпеки України» подано такі визначення: кіберзагроза – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів; кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Активне використання мереж, особливо дітьми та молоддю, супроводжується збільшенням різних видів загроз, що надходять з мережі. Особливо гостро ця проблема постає під час розробки та використання соціальних мереж. Найбільш активні приховані загрози, що походять з комп'ютерної мережі, можуть бути класифіковані так:

- вірусні атаки;
- кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо);

- загрози від мережевого серфінгу (кібербулінг, «дорослий» контент, незаконний вміст, насильство в онлайн-режимі, розголошення приватної інформації, платні послуги тощо).

Хакери мають багато можливостей, щоб скористатися вразливістю кібербезпеки та досягти своїх злочинних цілей.

Найпоширенішими видами таких кібератак є:

- *кардинг* – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»);
- *фішинг* – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі;
- *вішинг* – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а під час розмови запитуються конфіденційні дані власника картки;
- *онлайн-шахрайство* – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;
- *піратство* – незаконне розповсюдження інтелектуальної власності в інтернет-мережі;
- *кард-шарінг* – надання незаконного доступу до перегляду супутникового та кабельного ТБ;
- *вірус* – програма, яка встановлюється без відома та проти волі користувача на його комп'ютер або інший пристрій. Комп'ютерний вірус можна «схопити» по-різному. Наприклад, вебсторінки та поштові вкладення можуть використовуватися для безпосереднього запуску вірусу в систему. Часто вірус буває вбудований у завантажену з інтернету програму, яка «випускає» вірус на волю, після того як «жертва» її встановлює. Після зараження вірусом програма може заблоковувати доступ до файлів та системи з метою отримання викупу. При цьому сплата викупу не завжди гарантує відновлення роботи системи;

- *соціальна інженерія* – технологія управління людьми в інтернет-просторі;
- *мальваре* – створення та розповсюдження вірусів і шкідливого програмного забезпечення;
- *злам* – це умисна дія, спрямована на несанкціоноване проникнення у ПЗ або систему шляхом обходу механізму безпеки, з метою отримання несанкціонованого доступу до певного ПЗ або системи;
- *протиправний контент* – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства;
- *рефайлінг* – незаконна підміна телефонного трафіку;
- *підроблення мобільних додатків* – такі додатки з великою ймовірністю можуть містити шкідливі програми; атакуючи смартфон користувача, вони отримують доступ до особистої або банківської інформації (соцмережі, банківські операції, стан рахунків і т. д.).

З усіх цих дій кіберзлочинців виникають злочини, які посягають як на безпеку людини, так і держави в цілому:

- фінансові злочини і шахрайство;
- шпигунство;
- розкрадання інтелектуальної власності;
- військові дії (до них належать військові конфлікти між різними країнами, а також спроби заволодіти організаціями приватного сектора, особливо такими важливими інфраструктурними об'єктами національного масштабу, як енергетична, телекомунікаційна та фінансова системи);
- тероризм (атаки відбуваються терористичними групами (з можливою підтримкою з боку держави) з метою заволодіння стратегічно важливими приватними або державними інфраструктурними об'єктами;
- поширення дитячої порнографії;
- WEB-атаки, DDoS-атаки, поширення шкідливого програмного забезпечення і створення майданчиків для продажу викраденої інформації.

Проте найбільшою проблемою у сфері протидії кіберзлочинності є повільне розслідування, оскільки припинення комп'ютерного злочину та ліквідація його негативних наслідків вимагає оперативності. Згідно з чинним Кримінальним процесуальним кодексом України для одержання інформації від провайдерів та операторів, яка є необхідною для припинення злочину, ліквідації його наслідків, установлення винних правоохоронні органи витрачають багато часу на отримання відповідного судового рішення. Тому виникає потреба в наданні правоохоронним органам додаткових повноважень, пов'язаних із доступом до інформації, що має значення під час розслідування комп'ютерних злочинів.

3. ВИДИ АТАК

Порушник, здійснюючи атаку, зазвичай має на меті порушити:

- конфіденційність переданої інформації;
- цілісність і достовірність інформації, що передається;
- працездатність системи в цілому або окремих її частин.

З точки зору безпеки розподілені системи характеризуються насамперед наявністю віддалених атак, оскільки компоненти розподілених систем зазвичай використовують відкриті канали передачі даних, порушник може не тільки проводити пасивне прослуховування переданої інформації, а й модифікувати переданий трафік (активний вплив). І якщо активний вплив на трафік може бути зафіксований, то пасивний вплив майже неможливо виявити. Але оскільки в ході функціонування розподілених систем обмін службовою інформацією між компонентами системи здійснюється теж через відкриті канали передачі даних, то службова інформація стає таким самим об'єктом атаки, як і дані користувача.

Атаки доступу

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

Підслуховування (Sniffing)

Здебільшого дані передаються через комп'ютерні мережі в незахищеному форматі (відкритим текстом), що дає змогу зловмисникові,

що отримав доступ до ліній передачі даних у мережі, підслуховувати або зчитувати трафік. Для підслуховування в комп'ютерних мережах використовують сніфер. Сніфер пакетів – прикладна програма, яка перехоплює всі мережеві пакети, що передаються через певний сегмент.

На сьогодні сніфери працюють у мережах на цілком законній підставі. Вони використовуються для діагностики несправностей та аналізу трафіку. Однак через те, що деякі мережеві програми передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3 і т. д.), за допомогою сніферу можна дізнатися корисну, а іноді й конфіденційну інформацію (наприклад, імена користувачів і паролі). Запобігти загрозі сніфінгу пакетів можна завдяки таким заходам і засобам: застосування для автентифікації одноразових паролів; установка апаратних або програмних засобів, які розпізнають сніфери; застосування криптографічного захисту каналів зв'язку.

Перехоплення (Hijacking)

На відміну від підслуховування, перехоплення – це активна атака. Зловмисник перехоплює інформацію в процесі її передачі до місця призначення. Перехоплення імен і паролів створює велику небезпеку, оскільки користувачі часто застосовують одні й ті ж логін та пароль для безлічі застосунків і систем. Багато користувачів узагалі мають один пароль для доступу до всіх ресурсів і програм. Якщо застосунок чи програма працює в режимі «клієнт-сервер», а автентифікаційні дані передаються через мережу у відкритому текстовому форматі, цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів.

У найгіршому разі зловмисник отримує доступ до ресурсу користувача на системному рівні, з його допомогою створює атрибути нового користувача, які можна в будь-який момент застосувати для доступу в мережу і до її ресурсів.

Перехоплення сеансу (Session Hijacking)

Після закінчення початкової процедури автентифікації з'єднання, встановлене законним користувачем, наприклад, з поштовим сервером, перемикається зловмисником на новий вузол, а вихідному серверу надається команда розірвати з'єднання. У результаті «співрозмовник» законного користувача виявляється непомітно підміненим.

Отримавши доступ до мережі, зловмисник може:

- надсилати некоректні дані застосуванням і мережевим службам, що призводить до їх аварійного завершення або неправильного функціонування;
- наповнити комп'ютер або всю мережу трафіком, поки не відбудеться зупинка системи у зв'язку з перевантаженням;
- блокувати трафік, що призведе до втрати доступу авторизованих користувачів до мережевих ресурсів.

Атаки модифікації

Атака модифікації – це спроба неправомірної зміни інформації. Така атака можлива скрізь, де існує або передається інформація; вона спрямована на порушення цілісності інформації.

Зміна даних

Зловмисник, отримавши можливість прочитати чужі дані, зможе зробити й наступний крок – змінити їх. Дані в пакеті можуть бути змінені, навіть якщо зловмисник нічого не знає ні про відправника, ні про одержувача.

Додавання даних

Інший тип атаки – додавання нових даних, наприклад, в інформацію про історію минулих періодів. Зловмисник виконує операцію в банківській системі, унаслідок чого кошти з рахунку клієнта переміщуються на його власний рахунок.

Видалення даних

Атака видалення означає переміщення наявних даних, наприклад анулювання запису про операції з балансового звіту банку, у результаті чого зняті з рахунку грошові кошти залишаються на ньому.

Атаки типу «відмова в обслуговуванні»

Атака «відмова в обслуговуванні» (Denial-of-Service, DoS) відрізняється від атак інших типів. Вона не націлена на отримання доступу до мережі або витягу з цієї мережі будь-якої інформації. DoS-атака робить мережу організації недоступною для звичайного використання завдяки перевищенню допустимих меж функціонування мережі, операційної системи або програми. По суті, ця атака позбавляє звичайних користувачів доступу до ресурсів або комп'ютерів мережі організації.

Більшість DoS-атак розрахована на загальні слабкості системної архітектури. У разі використання деяких серверних застосувань (таких, як вебсервер або FTP-сервер) DoS-атаки можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих програм, і тримати їх в зайнятому стані, не допускаючи обслуговування звичайних користувачів. У ході DoS-атак можуть використовуватися звичайні інтернет-протоколи, зокрема TCP та ICMP (Internet Control Message Protocol).

DoS-атакам важко запобігти, оскільки для цього потрібна координація дій з провайдером. Якщо трафік, призначений для переповнення мережі, не зупинити у провайдера, то на вході в мережу це зробити вже неможливо, тому що вся смуга пропускання буде зайнята.

Якщо атака цього типу проводиться одночасно через безліч пристроїв, то йдеться *про розподілену атаку «відмова в обслуговуванні»* (DDoS, Distributed DoS).

Простота реалізації DoS-атак і величезна шкода, заподіяна ними організаціям і користувачам, привертають до цих атак пильну увагу адміністраторів мережевої безпеки.

Відмова в доступі до інформації

У результаті DoS-атаки, спрямованої проти інформації, остання стає непридатною для використання. Інформація знищується, спотворюється або переноситься в недоступне місце.

Відмова в доступі до застосунків чи програм

Інший тип DoS-атак спрямований на програми, що обробляють або відображають інформацію, або на комп'ютерну систему, в якій ці процеси здійснюються. У разі успіху подібної атаки рішення задач, які виконуються за допомогою такого застосунку чи такої програми, стає неможливим.

Відмова в доступі до системи

Загальний тип DoS-атак ставить за мету виведення з ладу комп'ютерної системи, унаслідок чого сама система, установлені на ній програми й уся збережена інформація стають недоступними.

Відмова в доступі до засобів зв'язку

Метою атаки є комунікаційне середовище. Цілісність комп'ютерної системи та інформації не порушується, однак відсутність засобів зв'язку позбавляє користувачів доступу до цих ресурсів.

Комбіновані атаки

Комбінована атака полягає в застосуванні зловмисником декількох взаємопов'язаних дій для досягнення своєї мети.

Підміна довіреного суб'єкта

Більша частина мереж та операційних систем використовують IP-адресу комп'ютера для того, щоб визначати, чи той це адресат, який потрібен. У деяких випадках можливе некоректне присвоєння IP-адреси (підміна IP-адреси відправника іншою адресою) – такий спосіб атаки називають фальсифікацією адреси або *IP-спуфінгом* (IP-spoofing).

IP-спуфінг відбувається, коли зловмисник, що знаходиться всередині корпоративної мережі або за її межами, видає себе за законного користувача. Зловмисник може скористатися його IP-адресою, що перебуває в межах діапазону санкціонованих IP-адрес, або авторизованою зовнішньою адресою, якій дозволяється доступ до певних ресурсів мережі. Зловмисник може також використовувати спеціальні програми, які формують IP-пакети так, щоб вони були схожими на вихідні з дозволених внутрішніх адрес корпоративної мережі.

Атаки IP-спуфінга часто є початком інших атак. Класичним прикладом є атака типу «відмова в обслуговуванні» (DoS), яка починається з чужої адреси, що приховує справжню особу зловмисника. Зазвичай IP-спуфінг обмежується вставкою неправдивої інформації або шкідливих команд у звичайний потік даних, що передаються між клієнтською і серверною програмами або через канал зв'язку між одноранговими пристроями.

Загрозу спуфінга можна послабити (але не усунути) за допомогою таких заходів: правильне налаштування управління доступом із зовнішньої мережі; припинення спроб спуфінга чужих мереж користувачами мережі.

Потрібно зауважити: IP-спуфінг може бути здійснений за умови, що автентифікація користувачів проходить на базі IP-адрес, тому введення додаткових методів автентифікації користувачів (на основі одноразових паролів або інших методів криптографії) дозволяє запобігти атакам IP-спуфінга.

Посередництво

Атака типу «посередництво» передбачає активне підслуховування, перехоплення даних, які передаються, невидимим проміжним

вузлом та управління ними. Коли комп'ютери взаємодіють на мережевому рівні, вони не завжди можуть визначити, з ким саме вони обмінюються даними.

Посередництво в обміні незашифрованими ключами (атака «Man-in-the-Middle» – «людина-в-середині»)

Для проведення атаки «людина-в-середині» зловмиснику потрібен доступ до пакетів, що передаються через мережу. Такий доступ до всіх пакетів, що передаються від провайдера ISP у будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніфери пакетів, транспортні протоколи та протоколи маршрутизації.

Узагалі атаки «людина-в-середині» проводяться з метою крадіжки інформації, перехоплення поточної сесії та отримання доступу до приватних мережевих ресурсів, для аналізу трафіку й отримання інформації про мережі та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії.

Ефективно боротися з атаками типу «людина-в-середині» можна тільки за допомогою криптографії. Для протидії атакам цього типу використовується *інфраструктура відкритих ключів* PKI (Public Key Infrastructure).

Атака експлоїта

Експлоїт (exploit – експлуатувати) – це комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують уразливості в програмному забезпеченні та застосовуються для проведення атаки на комп'ютерну систему. Метою атаки може бути як захоплення контролю над системою, так і порушення її функціонування (DoS-атака).

Залежно від методу отримання доступу до вразливого програмного забезпечення експлоїти поділяються на віддалені й локальні:

- віддалений експлоїт працює через мережу й використовує вразливість у захисті без якого-небудь попереднього доступу до вразливої системи;
- локальний експлоїт запускається безпосередньо у вразливій системі, вимагаючи попереднього доступу до неї. Зазвичай використовується для отримання зловмисником прав суперкористувача.

Атака експлоїта може бути спрямована на різні компоненти комп'ютерної системи – серверні застосунки чи програми, клієнтські програми або модулі операційної системи.

Парольні атаки

Метою цих атак є заволодіння паролем і логіном законного користувача. Зловмисники можуть проводити парольні атаки, використовуючи такі методи, як:

- підміна IP-адреси (IP-спуфінг);
- підслуховування (сніфінг);
- простий перебір.

Вгадування ключа

Криптографічний ключ – код або число, необхідне для розшифрування захищеної інформації. Хоча дізнатися ключ доступу важко й такі спроби вимагають значних затрат ресурсів, проте це можливо. Зокрема, для визначення значення ключа може бути використана спеціальна програма, яка реалізує метод повного перебору. Ключ, до якого отримує доступ зловмисник, називається скомпрометованим. Той, хто здійснює атаку, використовує скомпрометований ключ для отримання доступу до захищених даних без відома відправника й одержувача. Ключ дає можливість розшифровувати та редагувати дані.

Атаки на рівні програм

Ці атаки можуть проводитися декількома способами. Найпоширеніший з них полягає у використанні відомих вразливостей серверного програмного забезпечення (FTP, HTTP, вебсервера).

Головна проблема з атаками на рівні програм полягає в тому, що зловмисники часто користуються портами, яким дозволено прохід через мережеві екрани.

Відомості про атаки на рівні програм широко публікуються, щоб дати можливість адміністраторам вирішити проблему за допомогою корекційних модулів (патчів). На жаль, багато зловмисників також мають доступ до цих відомостей, що дає змогу їм вчитися.

Не можна повністю унеможливити атаки на рівні програм чи застосунків, чи додатків. Зловмисники постійно відкривають і публікують

на своїх сайтах в інтернет-мережі нові вразливі місця прикладних програм.

Тому важливо здійснювати належне системне адміністрування. Щоб зменшити вразливість від атак цього типу, можна вжити такі заходи:

- аналізувати лог-файли операційних систем і мережеві лог-файли за допомогою спеціальних аналітичних програм;
- відстежувати дані CERT про слабкі місця прикладних програм;
- користуватися найновішими версіями операційних систем і програм, останніми корекційними модулями (патчами);
- використовувати системи виявлення вторгнень IDS (Intrusion Detection Systems).

Аналіз мережного трафіку

Метою атак подібного типу є прослуховування каналів зв'язку й аналіз даних, які передаються, та службової інформації з метою вивчення топології мережі та архітектури побудови системи, отримання критичної інформації користувачів (наприклад, паролів користувачів або номерів кредитних карт, що передаються у відкритому вигляді). Атакам цього типу схильні такі протоколи, як FTP і Telnet, особливістю яких є те, що ім'я та пароль користувача передаються в межах цих протоколів у відкритому вигляді.

Мережева розвідка

Мережева розвідка – це збір інформації про мережу за допомогою загальнодоступних даних і програм. Під час підготовки атаки проти певної мережі зловмисник, як правило, намагається отримати про неї якомога більше інформації.

Мережева розвідка проводиться у формі запитів DNS, ICMP-тестування (Ping Sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цьому домену належать. ICMP-тестування адрес, розкритих за допомогою DNS, дозволяє з'ясувати, які вузли реально працюють у цій мережі. Отримавши список вузлів, зловмисники використовують засоби сканування портів, щоб скласти повний список сервісів, які підтримуються цими вузлами. У результаті отримують інформацію, яку можна використовувати для зламу.

Зловживання довірою

Цей тип дій не є атакою в прямому значенні слова. Він полягає у зловмисному використанні відносин довіри, що існують у мережі.

Типовим прикладом такого зловживання є ситуація в периферійній частині корпоративної мережі. У цьому сегменті зазвичай розташовуються сервери DNS, SMTP і HTTP. Оскільки всі вони належать до одного і того ж сегмента, злам одного з них призводить до зламу й усіх інших, тому що ці сервери «довіряють» (пропоную записати в лапках) іншим системам своєї мережі.

Ризик зловживання довірою можна знизити завдяки більш жорсткому контролю рівнів довіри в межах своєї мережі. Системи, розташовані з зовнішнього боку мережевого екрана, ніколи не повинні користуватися абсолютною довірою з боку систем, захищених мережевим екраном.

Відносини довіри повинні обмежуватися певними протоколами і за можливості автентифікуватися не тільки за IP-адресами, але й за іншими параметрами.

Фішинг (Phishing)

Фішинг є порівняно новим видом інтернет-шахрайства, мета якого – отримати ідентифікаційні дані користувачів. Сюди належать крадіжки паролів, номерів кредитних карт, банківських рахунків, PIN-кодів та іншої конфіденційної інформації, що дає доступ до грошей користувача. Фішинг не використовує технічні недоліки програмного забезпечення, а легковірність користувачів інтернет-мережі. Сам термін «phishing», співзвучний з «fishing» (з англ. – риболовля), розшифровується як «password harvesting fishing» – вивуджування пароля. Дійсно, фішинг дуже схожий на рибну ловлю. Зловмисник закидає в інтернет приманку і «виловлює» всіх «рибок» – користувачів інтернет-мережі, які клюнуть на цю приманку.

Зловмисник створює практично точну копію сайту обраного банку (електронної платіжної системи, аукціону тощо). Потім за допомогою спам- технології через електронну пошту розсилається лист, складений так, щоб бути максимально схожим на лист від обраного банку. Під час складання листа використовуються логотипи банку, імена та прізвища реальних керівників банку. У такому листі, як правило, повідомляється про те, що у зв'язку зі зміною програмного забезпечення в системі інтернет-банкінгу користувачеві необхідно підтвердити або змінити свої облікові дані. Як причини для зміни даних можуть бути названі вихід

з ладу ПЗ банку або ж напад зловмисників. Наявність правдоподібної легенди, що спонукає користувача до необхідних дій, – неодмінна складова успіху шахраїв-фішерів. У всіх випадках мета таких листів одна – змусити користувача клікнути на прикріплене чи надіслане посилання, а потім ввести свої конфіденційні дані (пароль, номер рахунку, PIN-код) на фальшивому сайті банку (електронної платіжної системи, аукціону). Зайшовши на фальшивий сайт, користувач уводить у відповідні рядки свої конфіденційні дані, а далі аферисти отримують доступ у кращому разі до його поштової скриньки, а в гіршому – до електронного рахунку.

Успіху фішинг-афер сприяє низький рівень обізнаності користувачів про правила роботи компаній, від імені яких діють злочинці. Зокрема, близько 5 % користувачів не знають простого факту: банки не розсилають листів з проханням підтвердити онлайн номер своєї кредитної картки, її PIN-код. Основним захистом від фішингу поки залишаються спам-фільтри. На жаль, програмний інструментарій для захисту від фішингу має обмежену ефективність, оскільки зловмисники експлуатують насамперед не вразливості в ПЗ, а людську психологію.

З'явилося поєднане з фішингом поняття – фармінг.

Фармінг (Pharming)

Це ще один вид шахрайства, що ставить за мету отримати персональні дані користувачів, але не через пошту, а прямо через офіційні вебсайти. Фармери замінюють на серверах DNS цифрові адреси легітимних вебсайтів на підроблені, унаслідок чого користувачі перенаправляються на сайти шахраїв. Цей вид шахрайства більш небезпечний, оскільки помітити підробку майже неможливо.

Для захисту від фішингу та фармінгу розробляються технічні засоби безпеки, насамперед плагіни для популярних браузерів. Суть захисту полягає у блокуванні сайтів, що потрапили в чорні списки шахрайських ресурсів. Наступним кроком можуть стати системи генерації одноразових паролів для інтернет-доступу до банківських рахунків та записів у платіжних системах, повсюдне поширення додаткових рівнів захисту завдяки комбінації введення пароля з використанням апаратного USB-ключа.

Застосування ботнетів

Ботнет (зомбі-мережа) – це мережа комп'ютерів, заражених шкідливою програмою, яка дозволяє кіберзлочинцям віддалено керувати

зараженими машинами (кожною окремо, частиною комп'ютерів, що входять до мережі, або всією мережею в цілому) без відома користувача. Такі програми називаються ботами.

Ботнети володіють потужними обчислювальними ресурсами, є загрозливою кіберзброєю і хорошим способом заробляння грошей для зловмисників. При цьому зараженими машинами, що входять до мережі, власник ботнету може керувати звідки завгодно: з іншого міста, країни чи навіть з іншого континенту, а організація інтернет-мережі дозволяє здійснювати це анонімно.

Управління комп'ютером, який заражений ботом, може бути прямим та опосередкованим.

У разі прямого управління зловмисник може встановити зв'язок з інфікованим комп'ютером і керувати ним, використовуючи вбудовані в тіло програми-бота команди.

У разі опосередкованого управління бот сам з'єднується з центром управління або іншими машинами в мережі, посилає запит і виконує отриману команду.

У будь-якому випадку власник зараженої машини, як правило, навіть не підозрює про те, що вона використовується зловмисниками. Саме тому заражені шкідливою програмою-ботом комп'ютери, що знаходяться під таємним наглядом кіберзлочинців, називають ще зомбі-комп'ютерами, а мережа, до якої вони входять, – зомбі-мережею. Найчастіше зомбі-машинами стають персональні комп'ютери домашніх користувачів.

Ботнети можуть використовуватися зловмисниками для вирішення кримінальних завдань різного масштабу: від розсилання спаму до атак на державні мережі.

Анонімний доступ до мережі

Зловмисники можуть звертатися до серверів в інтернет-мережі, використовуючи зомбі-машини, і від імені заражених машин здійснювати кіберзлочини, наприклад зламувати вебсайти або переказувати вкрадені гроші.

Продаж та оренда ботнетів

Один із варіантів незаконного заробітку за допомогою ботнетів ґрунтується на здачі ботнету в оренду або продажу готової мережі.

Створення ботнетів для продажу є окремим напрямом кіберзлочинного бізнесу.

Крадіжка конфіденційних даних

Цей вид кримінальної діяльності постійно приваблює кіберзлочинців, а з допомогою ботнетів «улов» у вигляді різних паролів для доступу до електронної пошти, FTP-ресурсів, вебсервісів) та інших конфіденційних даних користувачів збільшується в тисячі разів. Бот, яким заражені комп'ютери в зомбі-мережі, може завантажити іншу шкідливу програму, наприклад троянця, що краде паролі. У такому разі інфікованими троянською програмою виявляться всі комп'ютери, що входять до цієї зомбі-мережі, і зловмисники зможуть отримати паролі з усіх заражених машин. Вкрадені паролі перепродаються або використовуються, зокрема, для масового зараження вебсторінок (наприклад, паролі для всіх знайдених FTP-акаунтів) з метою подальшого поширення шкідливої програми-бота й розширення зомбі-мережі.

Перераховані атаки на IP-мережі можливі через низку причин:

- використання загальнодоступних каналів передачі даних. Найважливіші дані передаються через мережу в незашифрованому вигляді;
- вразливості в процедурах ідентифікації, реалізованих у стеку TCP / IP. Інформація для ідентифікації на рівні IP передається у відкритому вигляді;
- відсутність у базовій версії стека протоколів TCP / IP механізмів, що забезпечують конфіденційність і цілісність переданих повідомлень;
- автентифікація відправника здійснюється за його IP-адресою. Процедура автентифікації виконується тільки на стадії встановлення з'єднання, а в подальшому достовірність прийнятих пакетів не перевіряється;
- немає можливості контролю за маршрутом проходження повідомлень в інтернет-мережі, що робить віддалені мережеві атаки майже безкарними.

4. ПОНЯТТЯ І КЛАСИФІКАЦІЯ КОМП'ЮТЕРНИХ ВІРУСІВ

Вважають, що перші прототипи «електронних інфекцій» з'явилися наприкінці 1960-х – на початку 1970-х років у вигляді програм-«кроликів», які швидко поширювалися і займали системні ресурси, знижуючи у такий спосіб продуктивність комп'ютерів. Ці програми не передавалися між системами і були результатом пустощів системних програмістів. Термін «комп'ютерний вірус» уперше вжив американський студент Фред Коєн у 1984 році. Він поділив віруси на дві великі групи. До першої він зарахував ті, які написані для певних наукових досліджень у галузі інформатики, а до другої – «дикі» віруси, вироблені з метою заподіяння шкоди користувачам.

Сьогодні написання вірусів набуває ознак промислового виробництва, їхня кількість вимірюється десятками тисяч, і розуміння цієї загрози має стати необхідною вимогою для кожного користувача.

Комп'ютерний вірус – спеціально написана невелика за розмірами програма, яка може створювати свої копії, впроваджуючи їх у файли, оперативну пам'ять, завантажувальні області і т. ін. (заражати їх), та виконувати різноманітні небажані дії.

Небезпечність вірусу зростає через наявність у нього латентного періоду, коли він не виявляє себе. Для маскування вірус може використовуватися разом з «логічною» або «часовою бомбою».

Кілька ознак зараження ІС 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, несправності в роботі комп'ютера;
- раптове збільшення кількості файлів на диску;
- зникнення файлів і каталогів або перекручування їхнього вмісту;
- незрозумілі зміни у файлах;
- зміни дати та часу, модифікації файлів без очевидних причин;

- незрозумілі зміни розмірів файлів;
- видача непередбачених звукових сигналів;
- поява на екрані непередбачених повідомлень або зображень.

Віруси можна класифікувати за різними ознаками.

За середовищем існування розрізняють файлові, завантажувальні, комбіновані (файлово-завантажувальні), пакетні та мережні віруси.

Файлові віруси зазвичай заражають файли з розширеннями .com та .exe. Однак деякі їх різновиди можуть пошкодити файли й інших типів (.dll, .sys, .ovl, .prg, .bat, .mnu), вони, як правило, втрачають здатність до розмноження.

У свою чергу**, за способом зараження середовища існування** файлові віруси поділяють на резидентні та нерезидентні. Останні починають діяти тільки під час запуску зараженого файла на виконання і залишаються активними обмежений час. Резидентні віруси інсталюють свою копію в оперативній пам'яті, перехоплюють звертання операційної системи до різних об'єктів і заражають їх. Деякі віруси здатні перехоплювати досить багато різних функцій переривань. У результаті цього файли можуть заражатися у процесі перейменування, копіювання, знищення, змінювання атрибутів, перегляду каталогів, виконання, відкривання та здійснення інших операцій. Резидентні віруси зберігають активність весь час до вимикання комп'ютера.

Порівняно новою групою можна назвати **макровіруси,** які використовують можливості макросів, вбудованих у текстові редактори, електронні таблиці і т. ін. Нині поширені макровіруси у Microsoft Word і Excel. Вони перехоплюють деякі файлові функції в разі відкриття чи закриття зараженого документа і згодом інфікують решту файлів, до яких звертається програма. У певному сенсі такі віруси можна назвати резидентними, оскільки вони активні тільки у своєму середовищі – відповідному додатку.

Окрему категорію файлових вірусів становлять віруси сім'ї DIR, які не впроваджуються у файли, а виконують реорганізацію файлової системи так, що під час запуску будь-якого файла управління передається вірусу.

Завантажувальні віруси відрізняються від файлових резидентних вірусів тим, що вони переносяться із системи в систему через завантажувальні сектори. Комп'ютер заражається таким вірусом після спроби

завантаження системи з інфікованого диска, а дискета – під час читання її «змісту».

Комбіновані віруси можуть поширюватися як через завантажувальні сектори, так і через файли.

Пакетні віруси **–** це порівняно прості та старі віруси, написані мовою управління завданнями операційної системи.

Мережні віруси («черв'яки») комп'ютерною мережею, зменшуючи тим самим її пропускну здатність, уповільнюючи роботу серверів і т. ін. Вони посідають перше місце за швидкістю поширення. Найбільш відомим є так званий «черв'як Морріса». Останні моделі «черв'яків» упроваджуються у різні архіви (arj, zip та ін.) і зменшують вільний простір на диску.

За ступенем деструктивності віруси можна поділити на такі групи:

- порівняно безпечні, нешкідливі – їх вплив обмежується зменшенням вільної пам'яті та графічними або звуковими ефектами. Варто зазначити, що зменшення пам'яті в деяких випадках може призвести до збою системи, а ефекти – відволікти користувача, у результаті чого він припуститься помилки;
- небезпечні – віруси, які можуть спричинити збійні ситуації;
- дуже небезпечні – дії вірусів можуть призвести до втрати програм, знищення даних, стирання інформації в системних областях тощо.

За особливостями алгоритму віруси важко класифікувати через їхню різноманітність. Можна виокремити найпростіші – **«вульгарні» віруси**, написані єдиним блоком, який можна розпізнати в тексті програми-носія, та віруси **«роздроблені»** – поділені на частини, що нібито не мають між собою зв'язку, але містять інструкції комп'ютерові, як їх зібрати в єдине ціле і розмножити цей вірус.

З огляду на прийоми маскування розрізняють віруси-невидимки (стелс-віруси, stealth) та поліморфні віруси. Перші перехоплюють функції операційної системи, відповідальні за роботу з файлами і коригують результати звернень. Механізм «невидимості» в кожному з цих вірусів реалізується по-своєму, однак можна виокремити кілька загальних принципів:

- для приховування збільшення довжини заражених файлів вірус передає програмі перегляду каталогів зменшене значення їхньої довжини;

- для того, щоб користувач не виявив код вірусу під час перегляду файла, вірус «виліковує» його в момент відкриття і заново заражає у процесі закриття;
- для того, щоб замаскувати свою присутність у пам'яті комп'ютера, вірус стежить за діями резидентних моніторів пам'яті, у разі спроби перегляду коду вірусу система зависає.

Поліморфними називають віруси, які застосовують різноманітні способи для свого шифрування. У разі зараження чергового файла алгоритм шифрування змінюється випадковим чином. До того ж дуже важко виділити **сигнатуру** – характерну послідовність байтів у коді вірусу.

5. ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Класифікація засобів захисту інформації

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Варто зазначити, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямі сполучення програмних та апаратних засобів захисту.

Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склалися або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до зниження рівня авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ Сполучених Штатів Америки.

Правові засоби захисту – чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ.

Перехід до інформаційного суспільства вимагає удосконалення карного і цивільного законодавства, а також судочинства. Сьогодні

спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою майже неможливо, оскільки кожний закон потрібно розглядати в контексті всього законодавства. Наприклад, на положення щодо забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проєкту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи (див. матеріали сайту http://www.coe.int), було внесено зміни, оскільки його розцінили як такий, що суперечить положенням про права людини та надає урядам і поліцейським органам зайві повноваження.

Загальною тенденцією, яку можна простежити, є підвищення жорсткості кримінальних законів щодо комп'ютерних злочинців. Так, уже сьогодні у Гонконгу максимальним покаранням за такий злочин, якщо він призвів до порушень у роботі ІС або вебсайту, є 10 років позбавлення волі. Для порівняння у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування ІС, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою так, щоб найбільше ускладнити можливість порушення рівня безпеки або не допустити порушень взагалі. Вони охоплюють:

- заходи, які передбачаються під час проєктування, будівництва та облаштування об'єктів охорони (урахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.);
- заходи, що здійснюються під час проєктування, розробки, ремонту й модифікації обладнання та програмного забезпечення (сертифікація всіх технічних та програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін тощо);
- заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх

із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань і т. ін.);

- розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа та носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень і т. ін.; розробка адміністративних норм та системи покарань за їх порушення тощо).

Адміністративні засоби є необхідною частиною захисту інформації, їх значення зумовлюється тим, що вони доступні та здатні доповнити законодавчі норми там, де це потрібно організації, а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються).

Засоби фізичного (технічного) захисту інформації – це різні механічні, електро або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу й викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів ІС, стихійних лих, саботажу, диверсій і т. ін. До цієї групи належать:

- засоби захисту кабельної системи. За даними різних досліджень саме несправності кабельної системи спричиняють більш як половину відмов локальної обчислювальної машини (ЛОМ). Найкращим способом попередити подібні несправності є побудова структурованої кабельної системи (далі – СКС), у якій використовуються однакові кабелі для організації передавання даних в 1С, сигналів від датчиків пожежної безпеки, відео-інформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної

організації надійної СКС слід додержуватися вимог міжнародних стандартів;

- засоби захисту системи електроживлення. Американські дослідники з компанії Best Powerl після п'яти років досліджень проблем електроживлення зробили висновок: на кожному комп'ютері приблизно 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасового вимкнення електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, який відповідає вимогам. За умов підвищених вимог до роботоздатності 1С можливе використання аварійного електрогенератора або резервних ліній електроживлення, під'єднаних до різних підстанцій;
- засоби архівації та дублювання інформації. Якщо наявні значні обсяги інформації, доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. У разі пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);
- засоби захисту від витоку або втрати інформації по різних фізичних полях, що виникають під час роботи технічних засобів, – засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо.

До цієї ж групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні позначки, що зазначаються на документах та предметах (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього.

Як було вказано вище, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними.

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

Розглядаючи програмні засоби захисту, доцільно наголосити на стеганографічних методах. Слово «стеганографія» означає прихований запис, який не дає можливості сторонній особі дізнатися про його існування. Одна з перших згадок про застосування такого запису або стеганографії датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту – так вносилася шифрована інформація про умови складання контракту.

Комп'ютерна стеганографія базується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями, які можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення – цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

Щодо впровадження засобів програмно-технічного захисту в 1С, розрізняють два основні його способи:

- додатковий захист – засоби захисту є доповненням до основних програмних і апаратних засобів комп'ютерної системи;
- вбудований захист – механізми захисту реалізуються як окремі компоненти ІС або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати

проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом 1С. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

Захист від комп'ютерних вірусів

Для виявлення, знищення та попередження «електронних інфекцій» можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Останнім часом з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивіруси, плати, які вставляються у стандартні слоти розширення комп'ютера. Але найбільш поширеним методом залишається використання антивірусних програм – спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів.

Антивірусні програми поділяють на кілька видів.

Програми-детектори здійснюють пошук сигнатур вірусів. Недоліком детекторів є те, що вони можуть знаходити тільки ті віруси, які відомі їхнім розробникам, а отже, вони швидко стають не практичними. Деякі програми-детектори можна налаштовувати на нові типи вірусів, проте неможливо розробити програму, яка могла б виявити будь-який заздалегідь невідомий вірус. Отже, негативний результат перевірки програмою-детектором не гарантує відсутності вірусів. Багато детекторів мають режими лікування або знищення заражених файлів – функції докторів.

Програми-доктори («фаги») не тільки знаходять заражені вірусами файли, а й «лікують» їх (видаляють з файла тіло програми-вірусу), повертаючи їх у початковий стан. Перед лікуванням файлів програма очищує оперативну пам'ять. Серед фагів виокремлюють поліфаги – програми-доктори, призначені для пошуку і знищення великої кількості вірусів. Як і детектори, програми-доктори потребують постійного оновлення.

Програми-ревізори запам'ятовують початковий стан програм, каталогів і системних областей, коли комп'ютер не заражений вірусом, а згодом, періодично або за бажанням користувача, порівнюють поточний

стан системи з початковим. Як правило, перевірка здійснюється відразу після завантаження операційної системи – контролюються довжина файла, його контрольна сума, дата і час модифікації та інші параметри. До того ж деякі програми-ревізори можуть виявляти і стелс-віруси. Гібриди програм-ревізорів і докторів можуть не тільки виявляти зміни, а й повертати файли та системні області до початкового стану. Вони є більш універсальними, оскільки можуть захистити і від вірусу, не відомого на час їх створення, якщо він використовує стандартний механізм зараження.

Програми-фільтри («сторожа», «монітори») – резиденти програми, призначені для виявлення підозрілих дій під час роботи комп'ютера. Після одержання відповідного повідомлення користувач може дозволити або скасувати виконання операції. Деякі програми-фільтри перевіряють програми, які починають працювати або функціонувати, та файли, що копіюються. Недоліком подібних програм є їх «набридливість», можливі конфлікти з іншим програмним забезпеченням, а перевагами – виявлення вірусів на ранній стадії, що мінімізує втрати.

Програми-вакцини («імунізатори») модифікують програми і диски у такий спосіб, що це не відображається на роботі програм, але вірус, від якого проводиться вакцинація, вважає їх інфікованими. Це дуже неефективний спосіб захисту. Вакцини мають обмежене використання – їх можна застосувати тільки проти відомих вірусів.

Жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержуватися загальних правил (див. додатки) і користуватися останніми розробками антивірусних лабораторій.

ВИСНОВКИ

З огляду на теоретичний аспект **комп'ютерними** називають **злочини,** пов'язані із втручанням у роботу комп'ютера, і злочини, у яких комп'ютери використовуються як необхідні технічні засоби. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням,

відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами.

Основні особливості комп'ютерних злочинів:

- установлення факту вчинення злочину. Усі сліди злочину знаходяться на матеріальних носіях комп'ютера, який може знаходиться на значній відстані від потерпілої особи, що значно ускладнює процес установлення факту вчинення злочину;
- відсутність міждержавних кордонів для злочинців (якщо злочин учиняється з використанням глобальної комп'ютерної мережі) та існування декількох місць учинення злочину (у разі несанкціонованого доступу до банківських комп'ютерних систем місцем вчинення злочину слід вважати як саму банківську систему, що була атакована, так і місце знаходження комп'ютера, з якого здійснювали доступ, а також місце надходження коштів для отримання готівки).

Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники».

Найбільш активні приховані загрози, що виникають з комп'ютерної мережі, можуть бути представлені такою класифікацією:

- вірусні атаки;
- кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо);
- загрози від мережевого серфінгу (кібер-булінг, «дорослий» контент, незаконний вміст, насильство в режимі онлайн, розголошення приватної інформації, платні послуги тощо).

Завдяки можливостям інтернет-мережі маємо низку кібернетичних загроз, таких як: кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кард-шарінг, вірус, соціальна інженерія, мальваре, злам, протиправний рефайлінг, підробка мобільних додатків, поширення дитячої порнографії, вебатаки, ddos-атаки, поширення шкідливого програмного забезпечення і створення майданчиків для продажу викраденої інформації.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 р. № 2657-XII (дата оновлення 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Баженов В. А. Інформатика. Комп'ютерна техніка. Комп'ютерні технології : підручник. 4-те вид. К. : Каравела, 2012. 496 с.

8. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посібник. К. : КНЕУ, 2004. 307 с.

9. Макарова М. В. Інформатика та комп'ютерна техніка : навчальний посібник. 3-тє вид., переоб. і доп. Суми : ВДТ «Університетська книга», 2008. 665 с.

10. Маценко В. Г. Обчислювальна техніка та програмування : навчальний посібник. Чернівці : ЧНУ, 2010 112 с.

11. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

12. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / за ред.: В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін. Х. : Право, 2010. 240 с.

13. Редько М. М. Інформатика та комп'ютерна техніка : навчально-методичний посібник. Вінниця : Нова книга, 2007. 568с.

14. Ярмуш О. В., Редько М. М. Інформатика і комп'ютерна техніка : навч. посібник. К. : Вища освіта, 2006. 359 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Які сегменти належать до загального уявлення про інформаційну безпеку?

2. Які головні технологічні, організаційні та правові основи захисту даних Вам відомі.?

3. Які існують види загроз для комп'ютерної інформації?.

4. У чому полягає негативний вплив програм вірусів на комп'ютерні дані з точки зору інформаційної безпеки?

5. Сформулюйте поняття «комп'ютерний злочин».

6. Що таке «індикатори кіберзагроз»?

7. Дайте визначення «кібербезпека».

8. Назвіть правові основи забезпечення кібербезпеки України.

9. Назвіть об'єкти кібербезпеки та кіберзахисту.

2. Практині завдання

1. Відкрийте в браузері сайт «Законодавство України», здійсніть пошук Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», ознайомтеся і випишіть поняття: «захист інформації в системі», «інформаційна (автоматизована) система», «комплексна система захисту інформації», «криптографічний захист інформації», «технічний захист інформації».

2. Відкрийте в браузері сайт «Законодавство України», знайдіть Закон України «Про авторські і суміжні права». Випишіть ст. 8 «Об'єкти авторського права».

3. Теми реферативних повідомлень

1. Властивості мережі «Інтернет».

2. Витоки та сутність кіберсоціалізації.
3. Соціальні мережі з точки зору інформаційної безпеки.
4. Мережна мобілізація: питання демократії та безпеки.
5. Прогнозовані наслідки кіберсоціалізації.
6. Сутність поняття «кіберцивілізація».
7. Потенційні загрози кіберцивілізації для людства.
8. Правові основи розвитку інформаційних технологій і забезпечення інформаційної безпеки.
9. Поняття кіберзлочинності.
10. Сучасні методи технічного захисту інформації.

ЗАВДАННЯ ДЛЯ ТЕСТОВОГО КОНТРОЛЮ

1. Перші антивірусні утиліти (1984 рік) були написані:
а) Джоном Браннером;
б) Анди Хопкинсом;
в) Робертом Моррісоном;
г) Фредом Коєном.

2. Один із найбільш поширених видів комп'ютерних порушень, що полягає в одержанні користувачем доступу до об'єкта, на який у нього немає дозволу згідно з прийнятою в цій системі політикою безпеки – це:
а) несанкціонований доступ;
б) безпека інформаційної системи;
в) цілісність компонента (ресурсу);
г) доступність компонента (ресурсу).

3. Фішинг – це:
а) створення фальшивих сайтів;
б) вид шкідливого програмного забезпечення;
в) назва антивірусної технології;
г) спеціальна накладка на банкомати, для зчитування інформації з кредитних карток.

4. Скімінг – це:
а) створення фальшивих сайтів;
б) вид шкідливого програмного забезпечення;
в) назва антивірусної технології;
г) використання спеціальних накладок для банкоматів для зчитування інформації з кредитних карток.

5. Тип шкідливого програмного забезпечення, який використовується для маскування інших шкідливих програм:
а) руткіт;
б) троянська програма;
в) черв'як;
г) діалер.

РОЗДІЛ 5
КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

1. Фіксування судового процесу завдяки інформаційним технологіям.
2. Єдиний державний реєстр виконавчих проваджень.
3. Нотаріальні реєстри.
4. Автоматизована система ведення Державного земельного кадастру.
5. Автоматизація судово-експертних досліджень.

1. ФІКСУВАННЯ СУДОВОГО ПРОЦЕСУ ЗАВДЯКИ ІНФОРМАЦІЙНИМ ТЕХНОЛОГІЯМ

Інформаційна технологія – процес, що використовує сукупність засобів і методів збору, обробки і передачі даних (первинної інформації) для отримання нової інформації про стан об'єкта, процесу або явища (інформаційного продукту).

Інформаційна технологія є найбільш важливою складовою процесу використання інформаційних ресурсів суспільства. На сьогодні ця технологія має кілька еволюційних етапів, зміна яких визначалася переважно розвитком науково-технічного прогресу, появою нових технічних засобів переробки інформації. У сучасному суспільстві основним технічним засобом технології переробки інформації є персональний комп'ютер, який суттєво вплинув як на концепцію побудови та використання технологічних процесів, так і на якість результатної інформації.

Одним із напрямів інформатизації судів є використання комп'ютерних систем фіксації судового процесу. Технічна фіксація судових процесів здійснюється комп'ютерними системами, які дозволяють крім аудіозапису судового процесу отримувати анотацію (журнал, формуляр тощо) подій судового процесу згідно із аудіозаписом.

Відповідно до ст. 129 Конституції України та ст. 6 Цивільного процесуального кодексу України (далі – ЦПК України) фіксування судового процесу технічними засобами є однією з гарантій гласності судового процесу як засадничого принципу правосуддя. Порядок фіксування судового засідання технічними засобами встановлюється процесуальним законодавством (ст. 197 ЦПК України, «Інструкцією про порядок фіксування судового процесу технічними засобами», затвердженою наказом Державної судової адміністрації України від 21 липня 2005 р. № 84 «Про затвердження Інструкції про порядок фіксування судового процесу технічними засобами»).

Технічний комплекс фіксування судового процесу – це сукупність апаратно-програмних засобів, приладів і відповідних інструкцій, що забезпечують належне фіксування, зберігання, копіювання (дублювання) та використання інформації, яка відображає хід судового засідання (судового процесу).

Основним завданням систем технічної фіксації судових засідань є належне фіксування, зберігання, копіювання та використання інформації, яка відображає хід судового засідання.

Фіксування судового засідання технічними засобами – це технічний запис розгляду справи судом за допомогою звукозаписувального технічного засобу, що включає в себе створення фонограми судового засідання.

Фіксування судового засідання технічними засобами здійснює секретар судового засідання або інший працівник суду (ч. 11 ст. 6 ЦПК України), завдяки чому воно є офіційною формою фіксації судового процесу технічними засобами. Поряд із цим є неофіційні форми фіксації судових процесів. Наприклад, відповідно до ст. 6 ЦПК України учасники цивільного процесу та інші особи, присутні на відкритому судовому засіданні, мають право робити письмові записи, а також використовувати портативні технічні аудіопристрої. Для цього не потрібна згода учасників процесу та постановлення про це ухвали суду. Натомість проведення в залі судового засідання фото- і кінозйомок, відео-та звукозапису із застосуванням стаціонарної апаратури, а також транслювання судового засідання по радіо і телебаченню допускається на підставі ухвали суду за наявності згоди на це осіб, які беруть участь у справі.

Згідно з «**Інструкцією про порядок роботи з технічними засобами фіксування судового процесу (судового засідання)» від 20.09.2012 р. № 108:**

секретар або інший працівник апарату суду перед початком роботи зобов'язаний:

- включити комплекс звукозапису, зареєструватися у системі;
- перевірити годинник та календар комплексу звукозапису щодо відповідності поточним даті та часу;
- перевірити наявність вільного місця на внутрішньому носії комплексу звукозапису;
- перевірити справність пристроїв, провести тестування для перевірки того, що складові комплексу звукозапису (мікрофони, мікшер тощо) працюють нормально та запис проводиться правильно.

Звуковий запис судового засідання починається з моменту відкриття судового засідання:

Під час звукового запису секретар або інший працівник апарату суду здійснює поточний контроль якості запису судового процесу через прослуховування за допомогою навушників, контроль рівня запису в спеціальній області у програмі звукового запису та контроль працездатності комплексу звукового запису через спостереження за його станом.

За необхідності секретар або інший працівник апарату суду звертається до судді (головуючого у судовому засіданні) з проханням звернутися до учасників судового процесу (процесуальної дії) говорити голосніше.

У разі виявлення ознак несправності обладнання комплексу звукозапису секретар або інший працівник апарату суду доповідає судді (головуючому у судовому засіданні) про неможливість подальшого звукового запису судового засідання (процесуальної дії) та повідомляє про це керівника апарату й адміністратора.

Після закінчення судового засідання секретар або інший працівник апарату суду:

- зберігає, роздруковує, підписує журнал судового засідання або виготовляє та підписує протокол судового засідання та приєднує до справи (матеріалів кримінального провадження);

- створює архівну та робочу копії фонограми;
- перевіряє якість запису архівної копії фонограми;
- долучає архівну та робочу копії фонограми до судової справи (матеріалів кримінального провадження).

Фонограма судового засідання (далі – фонограма) – звуковий запис, який утворюється у процесі безпосереднього фіксування судового засідання за допомогою комплексу звукозапису та перетворений у форму електронних даних.

Обов'язкові реквізити фонограми: дата, час, місце створення запису, номер справи. Фонограма використовується для створення архівної та робочої копій.

Архівна копія фонограми – запис копії фонограми з вбудованого носія комплексу звукозапису на диск для лазерних систем зчитування (носій інформації), що має статус оригіналу та призначений для довготривалого зберігання в архіві.

Примірники фонограм записуються у вигляді архівної та робочої копій на окремі диски для лазерних систем зчитування (далі – компакт-диски). Для кожної судової справи, судового провадження надаються два компакт-диски: один – для архівної копії фонограми, інший – для робочої копії фонограми. У разі, якщо фонограми не вміщуються на один компакт-диск, надаються додаткові компакт-диски.

Фіксування судового процесу у процесуально-правовому аспекті означає відбиття, закріплення юридично значущих дій суду, інших учасників судового процесу у відповідних процесуально-документальних формах для забезпечення їх вірогідності з точки зору об'єктивності засобів фіксації судового процесу та визначення процесуальних наслідків цих дій під час розгляду справи по суті та на наступних стадіях судового процесу. Такий підхід фіксації судового процесу означає обов'язковість процесуально-документального оформлення актів-документів, які фіксують процесуальні дії суду, сторін та інших учасників судового процесу, а також обставини, факти під час розгляду справи, тобто мова йде про письмову фіксацію в судочинстві у межах, визначених законодавством.

Процесуальні кодекси не містять уніфікованого стандарту фіксування судового процесу. Наприклад, відповідно до статей 4^4, 81^1 Господарського процесуального кодексу України (далі – ГПК) судовий

процес фіксується технічними засобами та відображається у протоколі судового засідання в порядку, встановленому кодексом. Про судове засідання, огляд і дослідження письмових або речових доказів за їх місцезнаходженням складається протокол. Господарський суд може здійснювати стенографічний, а також аудіо- чи відеозапис судового засідання. ЦПК України передбачає правило повного фіксування судового засідання (ст. 197 ЦПК України). Аналогічне правило є і в Кодексі адміністративного судочинства України (ст. 41).

Однією із форм використання інформаційних технологій у судовій системі є можливість відеоконференцзв'язку.

Відеоконференція – це технологія, яка дозволяє візуалізувати взаємини, обмінюватися інформацією і спільно обробляти її в інтерактивному режимі, використовуючи можливості звичного всім комп'ютера, максимально наближаючи спілкування на відстані до реального живого спілкування. Для проведення відеоконференцій використовується спеціальна технологія – відеоконференцзв'язок. Взаємодію в режимі відеоконференцій також називають сеансом відеоконференцзв'язку.

Існують дві основні технічні проблеми, що гальмують розвиток відеоконференцзв'язку. Перша полягає в пропускній спроможності каналу зв'язку. Аналогові телефонні лінії цілком підходять для передачі аудіосигналу, але вони не в змозі забезпечити якісну трансляцію потоку відеоінформації. Друга проблема – швидкість обробки аудіо- й відеопотоку, тобто час кодування передаваної та декодування отримуваної інформації.

Вирішити проблему обробки інформації можна за допомогою двох основних підходів – програмного і апаратного. Програмний ґрунтується на спеціалізованому програмному забезпеченні, що використовує для реалізації алгоритмів кодування / декодування центральний процесор комп'ютера.

Другий підхід орієнтується на використання спеціалізованого апаратного забезпечення з попередньо встановленим на заводі програмним забезпеченням. Ці «закінчені рішення» мають високі якісні характеристики, але й високу вартість. Якщо поєднати ці два підходи, то можна отримати достатньо гнучкий програмно-апаратний комплекс

з належною якістю зв'язку і прийнятною ціною. Такі рішення і є найбільш поширеними.

Для організації відеоконференції між двома точками необхідно:

- у кожній з точок повинен бути термінал відеоконференцзв'язку. Це може бути самостійний пристрій або комп'ютер з відповідним програмним забезпеченням і, можливо, спеціальною платою;
- ці дві точки повинні бути з'єднані відповідною мережею, зазвичай по IP або ISDN.

Для організації відеоконференцій з повноцінною участю декількох сторін (більше двох) необхідна наявність спеціальних пристроїв для багатоточкових відеоконференцій. Їх зазвичай називають MCU (Multipoint Conference Unit).

Для якісної відеоконференції необхідне виконання таких правил:

- мати типове обладнання прийому / передачі;
- гарантовані високошвидкісні канали зв'язку (послуга зв'язку);
- стабільне і надійне електроживлення телекомунікаційного обладнання і відеоконференцзв'язку;
- оптимальні шумо- та ехопоглинаючі особливості приміщення;
- правильне розташування обладнання відеоконференцзв'язку відповідно до світлового фону приміщення;
- коректну настройку телекомунікаційного обладнання і відеоконференцзв'язку по обслуговуванню якості з пріоритизацією передачі даних.

Зараз спостерігаються окремі випадки використання відеоконференцзв'язку в юридичній практиці. Так, третейський суд, що постійно діє при Асоціації «Український третейський союз», розглянув позов київської фірми «Інтерон» до київського підприємства «Укрпривінвест», який був надісланий електронною поштою і підписаний електронним цифровим підписом відповідно до чинного законодавства. Судове засідання проходило в режимі відеоконференції: кожен з учасників знаходився у своєму офісі (фізично – в різних містах України) і брав участь у розгляді справи з використанням зв'язку через інтернет-мережу. Під час відеоконференції всі учасники процесу мали можливість бачити один одного, розглядати документи, ставити питання, заявляти

клопотання і виступати в судових дебатах. До того ж здійснювався відеозапис третейського розгляду. Після дослідження обставин справи і з'ясування позицій сторін представники сторін були відключені від відеоконференції, а судді працювали над рішенням у справі в закритому режимі. Після ухвалення суддями рішення представники сторін знову отримали доступ до відеоконференції, і судом було оголошено рішення у справі. Рішення третейського суду видане сторонам також і в паперовому вигляді з підписами суддів і печаткою.

Відповідно до п. 7 ч. 3 ст. 129 Конституції України, пунктів 10, 11 ст. 6 та ст. 197 ЦПК України, ст. 41 Кодексу адміністративного судочинства України, ст. 4^4 ГПК України, п. 4 ст. 9, п. 14 ст. 126 Закону України «Про судоустрій в Україні» реалізація принципу гласності судочинства забезпечується за допомогою повного фіксування судового процесу технічними засобами.

Правовий режим фіксування судового процесу технічними засобами визначається процесуальним законодавством. Так, відповідно до ч. 2 ст. 197 ЦПК України технічне фіксування судового засідання здійснює секретар або за розпорядженням головуючого інший працівник апарату суду (у будь-якому разі це повинні бути працівники, які пройшли відповідне навчання).

За вимогою особи, яка бере участь у справі, або за ініціативою суду здійснюється повне чи часткове відтворення технічного запису судового засідання (ч. 3 ст. 197 ЦПК України). Зазвичай така необхідність виникає під час порівняння показань свідків та під час застосування ч. 7 ст. 191 ЦПК України або ч. 4 ст. 182 ЦПК України тощо. Відтворення технічного запису судового засідання можливе і поза межами судового засідання з метою ознайомлення зі змістом запису (ч. 1 ст. 199 ЦПК України).

Носій інформації, на який здійснювався технічний запис судового засідання, є додатком до журналу судового засідання і після закінчення судового засідання він долучається до матеріалів справи.

Відповідно до процесуального законодавства особа, яка бере участь у справі, має право отримати роздруківку технічного запису судового засідання (повне або часткове роздрукування за плату) та копію інформації з носія, на який здійснювався технічний запис (безоплатно). Щодо отримання копії носія, на який здійснювався технічний запис,

то відповідно до Інструкції про порядок фіксації судового процесу технічними засобами за заявою осіб, які беруть участь у справі, архіваріус створює копії фонограми для зазначених осіб. Обсяг плати за роздрукування технічного запису судового засідання відповідно до ч. 6 ст. 197 ЦПК України встановлюється Кабінетом Міністрів України. Згідно з постановою Кабінету Міністрів України від 15 лютого 2006 р. № 151 «Про встановлення обсягів плати за роздрукування технічного запису судового засідання в адміністративних та цивільних справах та видачу дубліката виконавчого листа або судового наказу» плата за роздрукування однієї сторінки тексту на папері формату А4, що повністю або частково відтворює технічний запис судового засідання, встановлюється в обсязі п'яти гривень.

Єдиний державний реєстр судових рішень (далі – Реєстр) – автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень почав свою роботу з червня 2006 р. на вебсайті державного підприємства «Судовий інформаційний центр» (http://www.reyestr.court.gov.ua/). Використання Реєстру передбачено Законом України «Про доступ до судових рішень» від 22 грудня 2005 р. № 3262-IV.

Передбачений повний і загальний доступ до Реєстру. Повним доступом можуть скористатися лише судді, оскільки надається вся інформація про судову справу і про учасників судового процесу, тобто й така, що може бути конфіденційною. Загальний доступ, який відкритий для широкого загалу, не містить даних (імен, номерів телефонів й автомобілів, адрес), які дозволяють ідентифікувати особу.

Порядок доступу до Реєстру:

1. Вебсторінка доступу на сайт http://reyestr.court.gov.ua./reyestr/frame.php.

2. Вхід у Реєстр через «Загальний доступ». Відкриється форма для запиту.

3. Обов'язкові поля для заповнення: «Дата ухвалення судового рішення». Якщо невідома точна дата, необхідно вказати приблизно дату прийняття документа.

4. Результатом пошуку буде впорядкований перелік справ, які відповідають запиту, або повідомлення, що не знайдено жодного документа.

5. Для доступу до тексту документа необхідно натиснути на полі «№ рішення». Отриманий текст можна скопіювати чи зберегти для подальшої роботи.

2. ЄДИНИЙ ДЕРЖАВНИЙ РЕЄСТР ВИКОНАВЧИХ ПРОВАДЖЕНЬ

Єдиний державний реєстр виконавчих проваджень (https://asvpweb.minjust.gov.ua/#/search-debtors) – це комп'ютерна база даних, створена за допомогою автоматизованої системи, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення та надання відомостей про виконавчі дії. Цей реєстр прийнятий відповідно до:

- «Положення про Єдиний державний реєстр виконавчих проваджень», затверджене наказом Міністерства юстиції України від 20 травня 2003 р. № 43/5 «Про затвердження Положення про Єдиний державний реєстр виконавчих проваджень» і зареєстроване в Міністерстві юстиції України 21 травня 2003 р. № 388/7709;
- наказу Міністерства юстиції України від 28 травня 2004 р. № 634/7 «Про здійснення контролю за впровадженням Єдиного державного реєстру виконавчих проваджень у регіонах»;
- наказу Міністерства юстиції України від 24 лютого 2006 р. № 13/5 «Про внесення змін до Положення про Єдиний державний реєстр виконавчих проваджень та встановлення обсягів оплати за його експлуатацію»;
- наказу Міністерства юстиції України від 24 липня 2008 р. № 1270/5 «Про внесення змін до деяких нормативно-правових актів Міністерства юстиції України»;
- наказу Міністерства юстиції України від 25 липня 2008 р. № 1293/5 «Про встановлення обсягів плати за користування Єдиним державним реєстром виконавчих проваджень».

Загальні правила формування параметрів пошуку суб'єкта в базі даних Єдиного реєстру:

1) необхідно вказувати лише ті атрибути (найменування чи ПІБ або кілька значущих слів з найменування чи ПІБ, код ЄДРПОУ чи ІдН), які точно містяться в реєстровому записі про суб'єкта, якщо такий запис є в базі даних Реєстру;

2) не потрібно вказувати атрибути, які запис про суб'єкта може не містити взагалі або містити в іншій формі;

3) не треба в параметрах пошуку вказувати організаційно-правову форму юридичної особи, оскільки можливе різне написання однієї організаційно-правової форми, наприклад: «Товариство з обмеженою відповідальністю» або «ТОВ», або «ТзОВ», або навіть «ООО» (якщо має місце порушення Закону про державну мову);

4) значущими символами в найменуванні або ПІБ суб'єкта є символи кирилиці та цифри.

3. НОТАРІАЛЬНІ РЕЄСТРИ

Визначальним фактором нотаріального процесу є інформаційний аспект змісту нотаріальної діяльності, тому серед сукупності різних технологічних та організаційних рішень певне місце повинні зайняти комп'ютерні технології.

Нотаріальний реєстр – центральна база даних, у яку вноситься інформація певного виду. Бази окремих реєстрів зв'язані одна з одною; також використовуються єдині словники адміністративно-територіального устрою України, суб'єктів, документів.

Виокремлюють єдині та державні реєстри, держателями яких є:

• *Міністерство юстиції України* (https://minjust.gov.ua/);

• *Державна виконавча служба України* (https://minjust.gov.ua/ddvs).

Єдині та Державні реєстри інформаційної мережі Міністерства юстиції України створені та функціонують відповідно до законодавства України, до складу якого належать: закони України, акти Кабінету Міністрів України, відомчі нормативно-правові акти, а також інші документи правового характеру.

Адміністратором Єдиних та Державних реєстрів інформаційної мережі Міністерства юстиції України є Державне підприємство «Національні інформаційні системи» (https://nais.gov.ua/registers).

Державне підприємство «Національні інформаційні системи» (далі – ДП «НАІС») засноване Міністерством юстиції України в травні 2015 року. Організаційна структура ДП «НАІС»: головне підприємство та 24 регіональні філії в обласних центрах України. ДП «НАІС» працює лише на госпрозрахунковій основі.

Основною метою діяльності ДП «НАІС» є технічне, технологічне забезпечення, створення та супроводження програмного забезпечення ведення автоматизованих систем Єдиних та Державних реєстрів, які створюються відповідно до наказів Мін'юсту, а також інших електронних баз даних, що формуються згідно із законодавством України, надання доступу фізичним та юридичним особам до автоматизованих систем Єдиних та Державних реєстрів, забезпечення збереження та захисту даних, що містяться в автоматизованих системах Єдиних та Державних реєстрів.

Уся інформація про правові підстави функціонування Єдиних та Державних реєстрів інформаційної мережі Міністерства юстиції України, умови надання доступу та користування інформацією з них **є відкритою та розміщена на офіційних вебсайтах** Міністерства юстиції України та ДП «НАІС».

Щодо технологічних особливостей використання вказаних реєстрів слід зазначити, що всі вони побудовані за клієнт-серверною технологією. Реєстратори, тобто державні нотаріальні контори, та приватні нотаріуси, що уклали відповідні угоди з адміністратором реєстрів (Державне підприємство «Інформаційний центр»), мають повний прямий доступ до баз даних єдиних реєстрів через комп'ютерну мережу, вносять згідно з установленим порядком записи про набуття чинності та припинення дії документів і перевіряють дійсність документів шляхом запитів до єдиних реєстрів. Адміністратор здійснює комплекс організаційних заходів щодо забезпечення захисту інформації, яка міститься в єдиних реєстрах.

4. АВТОМАТИЗОВАНА СИСТЕМА ВЕДЕННЯ ДЕРЖАВНОГО ЗЕМЕЛЬНОГО КАДАСТРУ

Земельним кодексом України передбачена система державної реєстрації державних актів на землю у складі Державного реєстру земель. У ст. 193 Земельного кодексу України подано таке визначення: *«Державний земельний кадастр – це єдина державна система земельно-кадастрових робіт, яка встановлює процедуру визнання факту виникнення або припинення права власності та права користування земельними ділянками й містить сукупність відомостей і документів про місце розташування та правовий режим цих ділянок, їхню оцінку, класифікацію земель, кількісну та якісну характеристику, розподіл серед власників землі та землекористувачів».*

Закон України «Про Державний земельний кадастр» визначає Державний земельний кадастр як єдину державну геоінформаційну систему відомостей про землі, розташованих у межах державного кордону України, їх цільове призначення, обмеження у їх використанні, а також дані про кількісну і якісну характеристику земель, їхню оцінку, про розподіл земель між власниками і користувачами;

Ведення й адміністрування Державного земельного кадастру забезпечуються центральним органом виконавчої влади, що реалізує державну політику у сфері земельних відносин.

Держателем Державного земельного кадастру є центральний орган виконавчої влади, що реалізує державну політику у сфері земельних відносин.

Адміністратором Державного земельного кадастру є державне підприємство, яке належить до сфери управління центрального органу виконавчої влади, що реалізує державну політику у сфері земельних відносин, і здійснює заходи зі створення та супроводження програмного забезпечення Державного земельного кадастру, відповідає за технічне і технологічне забезпечення, збереження та захист відомостей, що містяться у Державному земельному кадастрі.

Об'єктами Державного земельного кадастру є:

- землі в межах державного кордону України;
- землі в межах території адміністративно-територіальних одиниць;

- обмеження у використанні земель;
- земельна ділянка.

Складовими частинами земельного кадастру є:

- державна реєстрація землекористувачів;
- кількісний облік земель;
- характеристика якості земель;
- економічна оцінка землі;
- кадастрові земельні карти.

5. АВТОМАТИЗАЦІЯ СУДОВО-ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ

Практика судово-експертних досліджень свідчить, що підвищення їх ефективності та наукової обґрунтованості нерозривно пов'язане з підвищенням рівня автоматизації інформаційного забезпечення цього виду юридичної діяльності.

Комп'ютерна техніка використовується в різних за змістом і метою напрямах.

1. Для автоматизації збору й обробки експериментальних даних, одержуваних під час досліджень. Таке устаткування – це переважно вимірювально-обчислювальні комплекси, змонтовані на базі приладів і ПК. Для аналізу використовуються внутрішні технологічні банки даних, що містять або набори специфічних фізико-хімічних параметрів, які характеризують речовини й матеріали, або спектрограми об'єктів, записані безпосередньо на магнітних носіях.

2. АІПС (автоматизовані інформаційно-пошукові системи) за конкретними об'єктами експертизи призначені для автоматизації деяких допоміжних обліків, таких, наприклад, систем, як «Метали» (містять відомості про склади металів і сплавів та галузі й сфери їх застосування); «Волокно» (характеристики текстильних волокон); «Марка» (характеристики автоемалі); «Взуття» (характеристики підошов взуття) тощо. Такі банки даних легко тиражувати. Вони можуть працювати як ізольовано, так і будучи вбудованими у вимірювально-обчислювальні комплекси.

3. Системи аналізу зображень. До них належать програми, що дозволяють проводити діагностичні й ідентифікаційні дослідження, наприклад, дактилоскопічні, трасологічні, портретні, складання композиційних портретів та ін. Деякі з цих систем використовуються для криміналістичної реєстрації.

4. Програмні комплекси або окремі програми виконання допоміжних розрахунків за відомими формулами й алгоритмами, які необхідні, насамперед для технічних експертиз, наприклад, для моделювання умов пожежі або вибуху для розрахунку кількісних характеристик процесів їх виникнення й розвитку. Велика кількість допоміжних розрахунків необхідна в автотехнічних, електротехнічних, технологічних експертизах. Спеціалізовані пакети прикладних програм створені також для розрахунків планово-економічних і бухгалтерських експертиз тощо.

5. Розробка програмних комплексів автоматизованого вирішення експертних завдань, що включають підготовку самого експертного висновку.

Для автоматизації експертних досліджень існують й інші програми, такі як:

Автоматизована дактилоскопічна ідентифікаційна система (далі – АДІС «ДАКТО»).

Автоматизована дактилоскопічна ідентифікаційна система (АДІС) призначена для автоматизації дактилоскопічних обліків.

АДІС «ДАКТО» реалізує такі функції:

- уведення в базу даних відбитків пальців рук (дактилокарт) і демографічних даних;
- уведення в базу даних слідів пальців рук, вилучених з місць нерозкритих злочинів;
- зберігання і керування базою даних відбитків пальців рук (дактилокарт);
- зберігання і керування базою даних неідентифікованих слідів пальців рук;
- проведення та аналіз пошуків «дактилокарта» у базі данних «дактилокарта»;
- проведення та аналіз пошуків «дактилокарта» у базі даних «неідентифікованих слідів пальців рук»;

– проведення та аналіз пошуків «слід – база даних дактилокарт»;
– проведення та аналіз пошуків «слід – база даних неідентифікованих слідів пальців рук»;
– підготовка та друк результатів пошуку;
– створення статистичних звітів;
– проведення пошуків за демографічними даними та їх комбінацій (ПІБ., дата народження і т. д.).

СКЛАД АДІС «ДАКТО»:

– комплексна АРМ (віддалене робоче місце) база до 40 000 дактилокарт / слідів: «Локальний сервер бази даних і обчислень»;
– системне програмне забезпечення – Windows XP, СКБД Oracle Enterprise Edition;
– прикладне програмне забезпечення;
– «сервер обчислень».

Автоматизована система портретної ідентифікації (АСПІ)

У розробленій АСПІ використовується багатоланкове програмне забезпечення (далі – ПЗ) (клієнтське ПЗ, серверне ПЗ, різні види сучасних промислових систем управління базами даних (СУБД), забезпечена можливість організації пакетної передачі і обробки даних на вимогу, а саме передачі між рівнями системи обмеженого обсягу даних, що, зрештою, дозволяє передавати будь-які обсяги інформації всередині системи.

Багаторівненву автоматизовану систему портретної ідентифікації – це система, що складається з підсистем територіального, регіонального та центрального рівня.

У розробленій АСПІ інформаційні потоки обробляються централізовано, а їх наповнення і використання здійснюється в різних територіальних підрозділах.

Для направлення запиту від віддаленого підрозділу в центральну автоматизовану систему портретної ідентифікації заповнюється відповідна форма, яка належить до складу використовуваної АСПІ. Підготовлений у такий спосіб запит є бінарним файлом зі складною структурою (XML, бінарний масив), який пересилається в центральну АСПІ різними способами: через відомчі e-mail, ftp, http, носії цифрових даних будь-якого виду та інші. Цей файл, потрапляючи в завантажувальний модуль центральної АІПС, автоматично ставиться в чергу обробки запитів.

Після обробки інформації центральна АСПІ формує відповідь, яка перетворюється в бінарний файл зі складною структурою, який, у свою чергу, пересилається з центральної АСПІ у віддалений підрозділ.

Такий варіант передбачає наявність віддаленої клієнтської частини АСПІ без прямого з'єднання з центральною АСПІ. Процес пересилання бінарних файлів запитів та відповідей виконується автоматично або вручну. У разі використання останнього весь процес передачі запитів і відповідей покладається на адміністраторів системи з необхідним набором прав доступу та додаткових функцій.

Розроблена система містить набір спеціалізованих засобів обміну даними для створення розподіленого обміну інформацією, запитами і результатами їх обробки.

Реалізація такого обміну здійснюється за допомогою низки засобів системи, які використовуються адміністраторами в довільній комбінації, що задовольняє поставленим завданням. Цей підхід дозволяє забезпечити максимальну гнучкість і масштабованість механізмів обміну.

Фоторобот

Система Фоторобот – програмний комплекс для автоматизації процесу створення суб'єктивних портретів шляхом компонування на екрані дисплея графічних образів з бази готових елементів обличчя.

Можливості програми:

- наявність класифікованих баз даних елементів зовнішності особи;
- бази типових осіб представників європеоїдної, монголоїдної та негроїдної рас, а також представників Кавказького і Середньоазіатського регіонів;
- база елементів обличчя, створювана користувачем;
- створення списків елементів обличчя, використовуваних користувачем;
- можливість отримання елементів обличчя із зовнішніх файлів (фотографій);
- збереження фрагментів зображення в базі елементів з їх класифікацією;
- автоматична (циклічна) заміна елементів зовнішності;

- складання суб'єктивного портрета на основі бази елементів зовнішності;
- складання суб'єктивного портрета на основі типового обличчя (узагальнене зображення);
- приведення фото зображень до єдиного масштабу;
- зміна елементів за шириною, висотою, кутом повороту та ін.;
- довільне деформування елемента (деформування на сітці);
- зміна яскравості, контрастності, гамма-корекція;
- наявність вбудованого графічного редактора (перо, пензель, виділення фрагментів і ін.);
- імпорт-експорт як окремих елементів, так і цілого зображення;
- динамічне налаштування панелі інструментів;
- вбудована довідкова система;
- багатомовна підтримка меню сайту або програми (українська, російська, англійська, можливість використання національних мов);
- збереження створеного суб'єктивного портрета у файл (jpg, bmp);
- збереження створеного суб'єктивного портрета у спеціальний файл (з урахуванням шарів і домальовувань) для подальшого складання і доопрацювання портрета;
- методичні рекомендації;
- опис команд і системи меню сайту або програми.

Автоматизована система «Відеопошук»

Автоматизована система «Відеопошук» – це комплекс математичних і програмних засобів, призначених для розпізнавання осіб у великих масивах відеоматеріалів.

Система дозволяє проводити пошук і виокремлення облич з великої кількості відеофайлів, створювати локальні бази даних облич, наявних у відеоматеріалах, і здійснювати пошук за ними, а також здійснювати всі ці функції в режимі обробки відеопотоку в реальному часі.

Особливості АС «Відеопошук»:

– спеціалізований редактор обробки зображень;
– аналіз і обробка відеофайлів (розкадровка);

– використання новітніх алгоритмів розпізнавання осіб на базі нейронних мереж, які дозволяють значно скоротити час уведення зображень облич, значно збільшити швидкість пошуку у великих масивах фото-, відеоматеріалів порівняно з традиційними алгоритмами.

Regula Forensic Studio

Програмне забезпечення «Regula Forensic Studio» – професійний програмний продукт для отримання, обробки зображень під час роботи із зовнішніми пристроями «Регула».

Функціональні можливості:

1. керування зовнішніми пристроями «регула»;
2. отримання, обробка та аналіз даних:

- візуальних (зображення);
- із зовнішніх пристроїв «регула»;
- інших пристроїв вводу: відеозахоплювачів, сканерів і т.д.;
- графічних файлів;
- інформаційно-довідкових систем та ін.
- невізуальних (інформація, яка не є зображеннями або містить будь-які дані крім графічних: наприклад, дані з rfid-мікросхем);

3. збереження результатів дослідження в локальній базі даних;
4. порівняння отриманих результатів дослідження з еталонами з інформаційно-довідкових систем.

Regula Паспорт / Passport

Містить зображення документів, їхніх елементів і засобів захисту, які відносяться до технологічного, поліграфічного і фізико-хімічного виду захисту, а також їх докладні описи.

Зміст програми:

- детальна інформація про документи та банкноти, опис їхніх елементів і засобів захисту;
- зображення:

– сторінок документів в білому, інфрачервоному 870 нм, ультрафіолетовому 254 і 365 нм діапазонах спектра;

– елементів і засобів захисту: мікротекстів, металографічного друку, водяних знаків, голограм і т. д.;
- детальний глосарій з описом та ілюстраціями елементів і засобів захисту.

Об'єм інформації програми (пропоную додати):
- 183 країни;
- 2369 документів: 2 255 паспортів, 114 віз.

Версії програми (пропоную додати):
- Brief – версія, призначена тільки для роботи у складі систем для автоматичної перевірки справжності документів зі зчитувачами «Регула»;
- Express – базова версія, що знайомить користувача з основними ознаками справжності документів;
- Forensic – розширена версія для експертного дослідження документів;
- Forensic Pro – розширена професійна версія для експертного дослідження документів, оснащена спеціальним програмним модулем «Document Builder» для додавання в інформаційно-довідкову систему власних зображень нового документа, його елементів і засобів захисту, їх описів.

Regula Автодокументи / Autodocs

Містить зображення документів, їхніх елементів і засобів захисту, які відносяться до технологічного, поліграфічного і фізико-хімічного виду захисту, а також їх докладні описи.

Зміст програми:
- детальна інформація про документи та банкноти, опис їх елементів і засобів захисту;
- зображення:
- сторінок документів в білому, інфрачервоному 870 нм, ультрафіолетовому 254 і 365 нм діапазонах спектра;
- елементів і засобів захисту: мікротекстів, металографічного друку, водяних знаків, голограм і т. д.;
- детальний глосарій з описом та ілюстраціями елементів і засобів захисту.

Об'єм інформації програми:
- 113 країн;
- 874 документа.

Версії програми:
- Brief – версія, призначена тільки для роботи в складі систем для автоматичної перевірки справжності документів зі зчитувачами «Регула»;
- Express – базова версія, що знайомить користувача з основними ознаками справжності документів;
- Forensic – розширена версія для експертного дослідження документів;
- Forensic Pro – розширена професійна версія для експертного дослідження документів, оснащена спеціальним програмним модулем «Document Builder» для додавання в інформаційно-довідкову систему власних зображень нового документа, його елементів і засобів захисту, їх описів.

Regula Валюта / Currency

Містить зображення банкнот, їхніх елементів і засобів захисту, які відносяться до технологічного, поліграфічного і фізико-хімічного виду захисту, а також їхні докладні описи.

Зміст програми:
- детальна інформація про банкноти, опис їх елементів і засобів захисту;
- зображення:
– банкнот в білому, інфрачервоному 400–530, 870 та 940 нм, ультрафіолетовому 254 і 365 нм діапазонах спектра;
– магнітних карт банкнот;
– елементів і засобів захисту: мікротекстів, металографічного друку, водяних знаків, голограм і т. д.;
- детальний глосарій з описом та ілюстраціями елементів і засобів захисту;

Об'єм інформації програми (пропоную додати):
- 168 валют за країнами і серіями випуску;
- 2 903 банкноти;

Версії програми (пропоную додати):

- Express – базова версія, що знайомить користувача з основними ознаками щодо справжності банкнот;
- Forensic – розширена версія для експертного дослідження банкнот;
- Forensic Pro – розширена професійна версія для експертного дослідження банкнот, оснащена спеціальним програмним модулем «Document Builder» для додавання в інформаційно-довідкову систему власних зображень нової банкноти, її елементів і засобів захисту, їх описів.

Regula Загальна система документів / Frontline Documents System

Містить зображення документів, їх елементів і засобів захисту, які відносяться до технологічного, поліграфічного і фізико-хімічним видам захисту, а також їх докладні описи.

Зміст програми:

- детальна інформація про документи, опис їх елементів і засобів захисту;
- зображення:
  - сторінок документів в білому, інфрачервоному 870 нм, ультрафіолетовому 254 і 365 нм діапазонах спектра;
  - елементів і засобів захисту: мікротекстів, металографічного друку, водяних знаків, голограм і т. д.;
- детальний глосарій з описом та ілюстраціями елементів і засобів захисту;

Об'єм інформації програми:

- 186 країн;
- 3 243 документа: 2 255 паспортів, 114 віз, 874 документа, пов'язаних з автотранспортом;

Версії програми:

- Brief – версія, призначена тільки для роботи у складі систем для автоматичної перевірки справжності документів зі зчитувачами «Регула»;
- Express – базова версія, що знайомить користувача з основними ознаками справжності документів;

- Forensic – розширена версія для експертного дослідження документів;

Forensic Pro – розширена професійна версія для експертного дослідження документів, оснащена спеціальним програмним модулем «Document Builder» для додавання в інформаційно-довідкову систему власних зображень нового документа, його елементів і засобів захисту, їх описів.

ВИСНОВКИ

Згідно зі ст. 129 Конституції України та ст. 6 ЦПК України фіксування судового процесу технічними засобами є однією з гарантій гласності судового процесу як засадничого принципу правосуддя. Порядок фіксування судового засідання технічними засобами встановлюється процесуальним законодавством (ст. 197 ЦПК України, «Інструкцією про порядок фіксування судового процесу технічними засобами», затвердженою наказом Державної судової адміністрації України від 21 липня 2005 р. № 84 «Про затвердження Інструкції про порядок фіксування судового процесу технічними засобами»).

Технічний комплекс фіксування судового процесу – це сукупність апаратно-програмних засобів, приладів і відповідних інструкцій, що забезпечують належне фіксування, зберігання, копіювання (дублювання) та використання інформації, яка відображає хід судового засідання (судового процесу).

Єдиний державний реєстр судових рішень – автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень почав свою роботу з червня 2006 р. на вебсайті державного підприємства «Судовий інформаційний центр».

Використання Реєстру передбачено Законом України «Про доступ до судових рішень» від 22 грудня 2005 р. № 3262-IV.

Нотаріальний реєстр – центральна база даних, у яку вноситься інформація певного виду. Бази окремих реєстрів пов'язані одна з одною; до того ж використовуються єдині словники: адміністративно-територіального устрою України, суб'єктів, документів.

Державний земельний кадастр – це єдина державна система земельно-кадастрових робіт, яка встановлює процедуру визнання факту виникнення або припинення права власності та права користування земельними ділянками й містить сукупність відомостей і документів про місце розташування та правовий режим цих ділянок, їхню оцінку, класифікацію земель, кількісну та якісну характеристику, розподіл серед власників землі та землекористувачів.

Практика судово-експертних досліджень свідчить, що підвищення їхньої ефективності та наукової обґрунтованості нерозривно пов'язано з підвищенням рівня автоматизації інформаційного забезпечення цього виду юридичної діяльності.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 р. № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Баженов В. А. Інформатика. Комп'ютерна техніка. Комп'ютерні технології : підручник. 4-те вид. К. : Каравела, 2012. 496 с.

8. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посібник. К. : КНЕУ, 2004. 307 с.

9. Макарова М. В. Інформатика та комп'ютерна техніка : навчальний посібник. 3-тє вид., переоб. і доп. Суми : ВДТ «Університетська книга», 2008. 665 с.

10. Маценко В. Г. Обчислювальна техніка та програмування : навчальний посібник. Чернівці : ЧНУ, 2010 112 с.

11. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

12. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / за ред. В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін. Х. : Право, 2010. 240 с.

13. Редько М. М. Інформатика та комп'ютерна техніка : навчально-методичний посібник. Вінниця : Нова книга, 2007. 568 с.

14. Ярмуш О. В., Редько М. М. Інформатика і комп'ютерна техніка : навч. посібник. К. : Вища освіта, 2006. 359 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Відповідно до яких нормативних актів України відбувається повне фіксування судового процесу технічними засобами?

2. Які Вам відомі техніко-технологічні функції системи технічної фіксації судових процесів?

3. Які Ви знаєте системи технічної фіксації судових засідань?

4. Які складові електронного (віртуального) судочинства?

5. Які, на ваш погляд, переваги електронного (віртуального) судочинства?

6. Які, на вашу думку, недоліки електронного (віртуального) судочинства?

7. Які, на Вашу думку, дає можливості судочинству застосування відеоконференцзв'язку?

2. Практині завдання

1. Назвіть підсистеми Єдиної судової інформаційної системи.

2. Укажіть пріоритетні напрями інформатизації судової системи України.

3. Визначте можливості системи автоматизації документообігу «Діловодство».

4. Охарактеризуйте процес забезпечення гласності судового процесу з використанням «Голосового порталу».

3. Теми реферативних повідомлень

1. Інтегровані системи та їхнє використання у правоохоронній діяльності.
2. Інтерфейс користувач-комп'ютер.
3. Прикладне програмне забезпечення загального призначення.
4. Прикладне програмне забезпечення спеціального призначення.
5. Методи маніпуляції даними та комп'ютерними програмами.
6. Наявні засоби боротьби і захисту з комп'ютерними вірусами.
7. Комп'ютерні мережі. Способи їх використання.
8. Комп'ютер – засіб для спілкування людей у всьому світі.
9. Інформаційні технології. Розвиток в сучасному світі.
10. Інформаційно-пошукові системи.
11. Інформаційно-пошукові сервери.
12. Інформаційна культура юриста.
13. Інформаційна компетентність майбутніх юристів.
14. Використання новітніх інформаційних технологій в юридичній сфері.
15. Історія розвитку комп'ютерної техніки.
16. Покоління ЕОМ. Основні етапи розвитку.

ЗАВДАННЯ ДЛЯ ТЕСТОВОГО КОНТРОЛЮ

1. У разі виявлення ознак несправності обладнання комплексу звукозапису секретар або інший працівник апарату суду доповідає судді (головуючому в судовому засіданні) про:

а) перерву судового засідання;
б) неможливість подальшого звукового запису судового засідання та повідомляє про це керівника апарату й адміністратора;
в) правільна відповідь а і б;
г) перенесення судового засідання на інший день згідно із законодавством України.

2. Збирання, зберігання, захист, облік, пошук, узагальнення та надання відомостей про виконавчі дії здійснюються:

а) ДП «НАІС»;
б) АСВП;
в) адміністратором єдиних та державних реєстрів інформаційної мережі Міністерства юстиції України;
г) усі відповіді правильні.

3. Об'єктами Державного земельного кадастру є:

а) землі в межах державного кордону України;
б) землі в межах території адміністративно-територіальних одиниць;
в) усі відповіді правильні;
г) земельна ділянка.

4. Інформаційні технології використовуються в судово-експертних дослідженях для:

а) покращення работи науково-дослідного експертно-криміналстичного центру;
б) автоматизації збору й обробки експериментальних даних, одержуваних під час досліджень;
в) відстеження нових методів дослідження;
г) розбудови нових експертиних майданчиків судово-експерних досліджень.

5. Для того, щоб знайти особу, маючи при собі її фотокартку, треба скористатися програмою:

а) Фоторобот;
б) Regula Паспорт / Passport;
в) ДП «НАІС»;
г) автоматизована система «Відеопошук».

РОЗДІЛ 6
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ЗАСОБІВ (SOFTWARE ТА HARDWARE) ЗАГАЛЬНОГО ПРИЗНАЧЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ

1. Поняття інформаційних засобів (software та hardware).
2. Функціональні можливості текстового процесора MS Word під час створення юридичних документів.
3. Робота з файлами інших форматів, що можуть містити текст.
4. Використання можливостей Excel для статистичної обробки правових даних та побудови діаграм.
5. Введення та редагування даних.
6. Сумісне використання Word та Excel. Упровадження і зв'язування об'єктів між документами різних типів.

1. ПОНЯТТЯ ІНФОРМАЦІЙНИХ ЗАСОБІВ (SOFTWARE ТА HARDWARE)

Hardware і Software – терміни, використовувані в англійській мові для позначення апаратної та програмної частини комп`ютера. Hardware є словом для позначення змісту пристрою, а поняття Software відповідає за визначення програмних характеристик.

Слово hardware має англійське походження і в комп'ютерному середовищі має відповідник «апаратне забезпечення». Це поняття пов'язано з характеристиками або параметрами комп'ютера, його корпусом і периферійним обладнанням, яке оточує пристрій. Поняття вживається відносно фізичних носіїв і пристроїв, які встановлені та працюють з комп'ютером.

До hardware належать монітор, комп'ютерна миша, клавіатура, носії інформації, різні карти (мережеві, графічні, аудіо тощо), а також модулі пам'яті, материнська плата та встановлені у неї чіпи, тобто всі об'єкти, до яких можна за бажанням доторкнутися. Однак саме по собі апаратне забезпечення здатне функціонувати тільки разом з програмним забезпеченням, тобто software. Зв'язка двох цих понять і утворює розуміння працездатної комп'ютерної системи.

Software, навпаки, визначає ту частину комп'ютера, яка не є апаратною. Програмне забезпечення включає в себе всі використовувані додатки, які вже можуть працювати. До поняття «software» належать виконувані файли, бібліотеки, скрипти. Програми виконуються на основі написаних на мові програмування інструкцій і не можуть функціонувати без апаратного компонента, який обробляє написаний програмістом код за рахунок доступних обчислювальних потужностей.

Програмне забезпечення зберігається на носіях інформації та обробляється центральним процесором через набір директив, тобто мову програмування. Інструкції складаються з низки бінарних значень, які може розрізнити й обчислити процесор, а потім видати потрібний результат через певну кількість часу.

Сучасна апаратна частина комп'ютера здатна обробляти велику кількість команд одночасно, що дозволяє створювати складні додатки, які відповідають сучасним вимогам. Чим складніша комп'ютерна програма, тим більше потрібно обчислювальних потужностей від апаратної частини. Якщо конфігурація устаткування не дозволяє виконувати запущену користувачем програму, будуть спостерігатися істотні падіння у продуктивності, а також зависання комп'ютера.

Існує безліч різновидів програмного забезпечення, які визначаються відповідно до мети їхнього застосування або специфікою їхнього функціонування і роботи.

2. ОСНОВНІ ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТЕКСТОВОГО ПРОЦЕСОРА MS WORD ПІД ЧАС СТВОРЕННЯ ЮРИДИЧНИХ ДОКУМЕНТІВ

Microsoft Office Word – текстовий процесор, доступний для Windows і Apple Mac OS X., який дозволяє створювати документи високого ступеня складності (пропоную об'єднати речення). Цей текстовий процесор підтримує технологію OLE, модулі сторонніх розробників, що підключаються, шаблони, захист документа, макроси та ін. Головними конкурентами Microsoft Office Word є OpenOffice Writer, StarOffice Writer, Corel WordPerfect і Apple Pages.

Основні можливості редактора зазначені в межах дисципліни, тому розглянемо лише окремі прийоми роботи в Microsoft Word.

Поняття шаблону. Основою кожного документа Microsoft Word є шаблон. Шаблон – це бібліотека стилів, яка визначає основну структуру документа і містить його налаштування, такі як елементи автотексту, шрифти, необхідні поєднання клавіш, макроси, меню, параметри сторінки, форматування і стилі. Шаблони дозволяють використовувати один і той самий стиль у різних текстових документах. Загальні шаблони, враховуючи шаблон Normal.dot, мають налаштування, доступні для всіх документів. Шаблони документів (наприклад, записки або факси) у діалоговому вікні «Шаблони» мають налаштування, доступні тільки для документів, створених на основі відповідних шаблонів.

Користувач може отримати доступ до таких шаблонів Microsoft Word:

- шаблони Microsoft Word на локальному комп'ютері. Для доступу до цих шаблонів потрібно обрати вкладку «Файл», потім – «Створити» і у правій панелі вікна натиснути «Шаблони на моєму комп'ютері»;
- шаблони Microsoft Office Online. Microsoft Office Online – це вебвузол, створений компанією Microsoft для допомоги користувачам Microsoft Office. На цьому вузлі розташовується довідка і підтримка, перевірка оновлень Microsoft Office, різні шаблони та пробні версії варіантів. Для доступу до цих шаблонів треба обрати вкладку «Файл», потім – «Створити» і у правій панелі вікна зазначити «Шаблони на вузлі Office Online»;

– створення файлу на підставі шаблону, розташованого на Ваших вебсерверах. Для доступу до цих шаблонів потрібно обрати вкладку «Файл», потім – «Створити» і у правій панелі вікна обрати «На моїх вебвузлах». Далі у полі «Ім'я файлу» вкажіть інтернет-адресу або адресу внутрішньої мережі та шлях до шаблону, для того, щоб відкрити, натисніть кнопку «Відкрити»;
– створення власного шаблону – ввести текст шаблону або відкрити документ, який треба перетворити на шаблон. Для створення потрібно обрати вкладку «Файл», потім «Зберегти як…», вказати тип файлу «Шаблон документа» і назвати цей шаблон. Доступ до створеного шаблону здійснюється так само, як і до шаблону на локальному комп'ютері.

Швидкий перехід по тексту – під час роботи з багатосторінковими документами доводиться здійснювати перехід у межах тексту. Для швидкого переходу треба обрати вкладку «Правка» і натиснути «Перейти» (або натиснути комбінацію клавіш Ctrl+G). З'явиться вікно з відкритою вкладкою «Перейти», а також вкладки «Знайти» і «Змінити». Вкладка «Перейти» дає змогу знайти потрібну сторінку, закладку, рядок, виноску, розділу, примітку тощо.

Пошук фрагмента тексту – виконується в багатосторінкових документах по слову або словосполученню. Результат пошуку – виділене вказане слово або словосполучення на поточній сторінці або нижче по тексту. Для пошуку фрагмента треба обрати вкладку «Правка», потім натиснути «Знайти» і ввести слово або словосполучення для пошуку. Для підвищення релевантності пошуку можна натиснути кнопку «Більше» і виконати налаштування параметрів пошуку.

Закладка – використовується для прискореного доступу до найбільш використовуваних сторінок у багатосторінковому документі. Установіть курсор у місці, на яке буде здійснюватися перехід під час використання закладки, натисніть «Вставка», а потім – «Закладка». Зазначте ім'я закладки. Ім'я закладки починається з літери і може містити тільки літери і цифри. Документ може мати декілька закладок. Для того, щоб скористатися закладкою, варто знову обрати «Вставка», а потім – «Закладка», вказати потрібну закладку й натиснути «Перейти».

Гіперпосилання – текст документа може містити елементи (слова, символи, позначки, малюнки і т. ін.), під час натискання на які буде здійснений автоматичний перехід на інший файл, який може знаходитися на вашому ПК, на ПК вашої локальної мережі або в інтернет-мережі, а також перехід в інший розділ цього документа.

Існують два види гіперпосилань: абсолютне і відносне. Абсолютне гіперпосилання – це гіперпосилання, що містить повну адресу файла або вебвузла. Приклад такої повної адреси в абсолютному гіперпосиланні: http://www.microsoft.com/support.

Відносне гіперпосилання містить адресу щодо адреси файла призначення. Адреса файла призначення також відома як база гіперпосилання.

База гіперпосилання – це спільно використовуваний у файлі шлях, що вказує на файл, у якому міститься гіперпосилання на файл призначення.

Наприклад, документ має таку базу гіперпосилання: C:\Documents and Settings\Username\My Documents.

Документ «Sales.doc» розташований за такою адресою: C:\Documents and Settings\Username\My Documents\April\Sales.doc.

Відносне гіперпосилання на документ має тільки відносну адресу Sales.doc., тому воно має таку адресу: April\Sales.doc.

Для створення гіперпосилання слід у потрібному місці документа виділити якийсь його елемент (слово, позначку, літеру, малюнок тощо), викликати контекстне меню виділеного елемента, або ж просто викликати контекстне меню і виконати команду «Гіперпосилання». У переліку «Пов'язати з…» вказати об'єкт, на який посилається гіперпосилання (файл, вебсторінку, новий документ, адресу електронної пошти). Для створення гіперпосилання на файл або вебсторінку треба задати шлях до файла або адреси вебсторінки. Щоб створити гіперпосилання на певному місці в поточному документі, це місце попередньо треба позначити закладкою і послатися на неї.

Заміна слова в тексті – використовується у разі некоректного перекладу або орфографічної помилки, що повторюється в тексті. Для виконання цієї функції треба натиснути «Правка», а потім – «Змінити», написати слово з помилкою і слово, на яке його треба замінити. Залежно від вибору користувача відбудеться заміна або першого знайденого

слова з помилкою, або в усьому тексті. Заміна виконується тільки в тій граматичній формі, у якій слово вказане у вікні «Замінити на…»

Вставка об'єкта в текстовий документ. Текстовий документ може бути оформлений різноманітними об'єктами: малюнками, таблицями, діаграмами, відеокліпами, аудіофрагментами тощо. Для їх вставки в текстовий документ треба натиснути «Вставка», а потім – «Об'єкт».

Якщо об'єкт вже існує у вигляді файла відповідного типу, перейдіть на вкладку «Створення із файлу» и за допомогою кнопки «Огляд» вкажіть шлях до потрібного файлу та тип зв'язку з відповідним додатком. Текстовий редактор Word підтримує технологію OLE – технологію роботи з документом, складові частини якого (об'єкти) розроблені в різних додатках. Для подальшої роботи з упровадженими об'єктами Word автоматично завантажте потрібний додаток.

Якщо об'єкт треба створити, то на вкладці «Створити» варто вказати тип об'єкта і за допомогою відповідного додатка створити його або обрати з переліку наявних файлів.

Створення списків. Багаторівневі списки використовуються для переліку об'єктів за відповідною класифікацією. Наприклад:

1. Апаратна частина ПК:

1) системна плата;

2) накопичувачі;

3) периферійні пристрої.

2. Програмне забезпечення ПК:

1) системне ПЗ;

2) операційні системи;

3) утиліти;

4) інструментальне ПЗ.

Для створення багаторівневого списку треба виділити потрібні абзаци, які містять його елементи, викликати контекстне меню, і натиснути «Список». У вікні, що з'явилося, обрати вкладку «Багаторівневий» і обрати потрібний тип списку (у цьому разі другий тип).

Після цього слід виділити елементи другого рівня, викликати контекстне меню і зробити збільшення відступу. Аналогічно створюються елементи третього рівня (для їх створення потрібно двічі натиснути

кнопку «Збільшити відстань», оскільки під час кожного її натискання відбувається переміщення на наступний рівень).

Стильове форматування – це форматування тексту з використанням стилів. Якщо задати для абзацу потрібний стиль, то редактор автоматично відформатує цей абзац, обравши певний шрифт, параметри абзацу, мову, обрамлення, нумерацію і т. ін. Якщо змінити характеристики стилю, то також автоматично зміняться відповідні характеристики всіх абзаців згідно з обраним стилем. У текстовому редакторі Word існує велика кількість стилів, але зазвичай використовуються такі:

- Заголовок 1 – для назви розділів;
- Заголовок 2 – для назви параграфів;
- Звичайний – для звичайного тексту.

Для того, щоб обрати потрібний стиль треба встановити курсор на відповідному абзаці. Потім обрати потрібний стиль з розкритого списку в панелі інструментів або натиснути «Формат», потім обрати «Стилі й форматування» і у правій частині вікна вказати необхідний стиль.

Зміст документа – це список назв розділів, параграфів тощо із зазначенням сторінки. Для автоматичного створення змісту потрібно заголовки розділів і підрозділів виділити відповідними стилями. Заголовки розділів першого рівня (наприклад, ВСТУП, ВИСНОВОК, назви розділів) виділяємо стилем Заголовок 1, заголовки підрозділів – стилем Заголовок 2 і т. д. Потім треба встановити курсор на місці формування змісту і натиснути «Вставка», потім обрати «Посилання», а після цього – «Заголовок і показники». У вікні, що з'явилося, потрібно обрати вкладку «Заголовок» і вказати кількість рівнів змісту (якщо в документі є тільки розділи і підрозділи, то буде всього два рівні, якщо у підрозділах є параграфи – це три рівні і т. д.).

Для автоматизації багаторазового виконання часто виконуваних з документом робіт створюються макроси, наприклад, для прискорення часто виконуваних операцій редагування або форматування, об'єднання декількох команд (для вставки таблиці з вказаними обсягами і межами та певною кількістю рядків і стовпців), спрощення доступу до параметрів у діалогових вікнах, автоматизації обробки складних послідовностей дій в документах тощо.

Макрос (або макрокоманда) – це послідовність заданих користувачем команд, що має ім'я і зберігається у формі стандартного програмного модуля на мові програмування «Visual Basic for Application» (VBA) або «Visual Basic для додатків». VBA є середовищем програмування, розробленим спеціально для створення макросів у додатках. Це мова програмування, яка підтримується всіма додатками пакета Microsoft Office. Макрос об'єднує всі інструкції в одному сценарії, який потім можна викликати за допомогою команди меню, кнопки панелі інструментів або комбінації клавіш. Список інструкцій, складових макроса, як правило, складається з макрооператорів.

Для створення макросів у Microsoft Word існують два методи:

I. Використання засобу для розробки макросу.

1. У вкладці «Сервіс» натисніть «Макрос» й оберіть «Почати запис».

2. У вкладці «Ім'я макроса» запишіть ім'я нового макроса. Ім'я повинне починатися з букви, мати тільки букви і цифри.

3. У списку «Макрос доступний для…» оберіть шаблон або документ, у якому зберігатиметься макрос.

4. Опишіть макрос у вкладці «Опис».

5. Якщо макросу не потрібно призначати кнопку панелі інструментів, команду меню або поєднання клавіш, натисніть кнопку ОК, щоб почати запис макроса.

6. Щоб призначити макросу кнопку панелі інструментів або команду меню, натисніть кнопку «Панелі», а потім – вкладку «Команди». Оберіть записуваний макрос в списку «Команди» і перетягніть його на панель інструментів або в меню. Натисніть кнопку «Закрити», щоб почати запис макроса.

7. Щоб призначити макросу поєднання клавіш, натисніть кнопку «Клавіатура». Оберіть записуваний макрос у списку «Команди», введіть поєднання клавіш у поле «Нове поєднання клавіш» і натисніть кнопку «Призначити». Натисніть кнопку «Закрити», щоб почати запис макроса.

8. Виконайте дії, які варто додати до макроса.

Під час запису нового макроса допускається застосування комп'ютерної миші тільки для вибору команд і параметрів. Для запису таких дій, як виділення тексту, необхідно використовувати клавіатуру. Наприклад, за допомогою клавіші F8 можна виділити текст, а за допомогою клавіші END – перемістити курсор у кінець рядка.

9. Для завершення запису макроса натисніть кнопку «Зупинити запис».

II. Програмування макроса за допомогою Visual Basic для додатків.

1. Натисніть «Сервіс» й оберіть «Макроси».

2. Із списку «Макроси» оберіть шаблон або документ, у якому зберігатиметься макрос.

3. У полі «Ім'я макроса» введіть ім'я нового макроса.

4. Натисніть кнопку «Створити», щоб відкрити редактор Visual Basic.

Поради щодо запису і використання макросів

1. Перед записом макроса заплануйте заздалегідь кроки й команди, які він повинен виконати. Якщо під час запису буде допущена помилка, то в макросі також запишуться всі виправлення. Непотрібні інструкції можна буде прибрати пізніше завдяки редагуванню макроса.

2. Ім'я макроса повинне починатися з букви, у ньому не можна використовувати пропуски та символи пунктуації.

3. Під час створення макроса, пов'язаного з форматуванням символів, для запису таких дій, як виділення тексту, не слід використовувати клавіші зі стрілками. Текст можна виділити за допомогою клавіші F8, а перемістити на початок і кінець рядка – за допомогою клавіш Home і End відповідно. Дії та параметри можна обирати за допомогою миші, проте рухи комп'ютерної миші не протоколюються. Наприклад, комп'ютерну мишу не можна використовувати для виділення, копіювання, вставки і перетягування елементів. Для запису цих дій треба користуватися клавіатурою.

4. Якщо макрос викликає команду «Знайти» або «Змінити», натисніть кнопку «Більше» на вкладці «Знайти» або «Змінити», а потім виберіть параметр «Усюди» у списку «Напрямок». Якщо макрос виконує пошук тільки вперед або назад, то після досягнення кінця або початку документа Word припинить виконання макроса і запропонує продовжити пошук у частині документа, що залишилася.

5. Текст, що вводиться під час створення макроса, записується в ньому. Це дозволяє, наприклад, за допомогою макроса отримувати таблиці, у першому рядку яких (у так званій «шапці таблиці») будуть представлені необхідні заголовки стовпців.

6. Перед використанням макроса, записаного в іншому документі, переконайтеся, що він не залежить від змісту цього документа.

7. Якщо певний макрос використовується надто часто, призначте йому кнопку панелі інструментів, команду меню або поєднання клавіш. Це дозволить швидко викликати макрос без відкриття діалогового вікна «Макроси».

Захист документа. Засоби Word дозволяють захистити документ від:

– форматування і/або редагування. Треба натиснути «Сервіси» й обрати функцію «Захистити», у правій панелі вікна встановити потрібні режими і ввести пароль;
– відкриття. Треба натиснути «Сервіси», далі обрати «Параметри», а потім – «Безпека» і встановити пароль для відкриття файла. Там же обираються параметри сумісного використання для цього документа.

3. РОБОТА З ФАЙЛАМИ ІНШИХ ФОРМАТІВ, ЩО МОЖУТЬ МІСТИТИ ТЕКСТ

PDF (Portable Document Format) – це формат електронних документів, розроблений компанією Adobe Systems, переносний формат документів, створений як засіб міжплатформеного обміну даними. Насамперед він призначений для представлення в електронному вигляді поліграфічної продукції; переважна частина сучасного професійного друкарського устаткування може обробляти PDF безпосередньо.

Формат не накладає ніяких обмежень на зовнішній вигляд документа. Документ у форматі pdf може містити текст, векторну і растрову графіку, шрифти, графіку, мультимедійні елементи, об'єднані довільно, що гарантує правильне відображення незалежно від операційної системи програмного забезпечення і призначених для користувача налаштувань конкретного комп'ютера. Саме ця властивість – зберігати початковий вигляд – і робить його привабливим. Необхідність швидкого переміщення по сторінках і об'єктах документа зумовила ієрархічну структуру даних PDF. На початку файла знаходиться зміст, що вказує на те, які об'єкти у ньому розташовані й де саме, потім зазначаються самі дані. Будь-які дії можливі за наявності всього PDF-файла, оскільки

фрагмент даних, який знадобиться першим, може знаходитися в будь-якій його частині, у тому числі й у самому кінці файла. Для документів з очевидним переважанням тексту і векторної графіки формат PDF, як правило, забезпечує помітне скорочення об'єму файла (з відповідним скороченням часу пересилки по мережі і т. д.).

Для читання документів використовують як безкоштовну програму Adobe Acrobat Reader, так і сторонні розробки. Зазвичай програми перегляду розповсюджуються безкоштовно, а програми, що дозволяють не тільки переглядати, а й редагувати pdf-файли – на комерційній основі.

Формат PDF має такі переваги:

✓ кросплатформеність: документ містить необхідні для правильного відображення елементи і виглядає однаково на будь-якій платформі й за будь-якого застосування. Кросплатформеність формату створює зручні умови для організації електронного документообігу;
✓ компактність: різні алгоритми компресії (архівації) дозволяють ефективно стискати як текст, так і графіку;
✓ інтерактивність: у pdf-файлі можна використовувати мультимедіа (відео-, аудіоролики), гіперпосилання, форми, відомості, які зберігаються в зовнішніх базах даних;
✓ безпека: формат підтримує багаторівневий механізм захисту й перевірки достовірності. Є можливість встановити пароль на перегляд / редагування, створити електронний підпис для ідентифікації автора.

Недоліки у форматі також є. PDF охоплює безліч стандартів, що не дозволяє ефективно використовувати його в конкретних цілях. Наприклад, формат можна використовувати для створення сторінок або сайтів вебсервером, але html справляється з цим завданням краще. PDF зберігає точну візуальну копію документа, але не його логічну структуру. Як наслідок, PDF достатньо складно редагувати.

Інші програми для роботи з файлами у форматі PDF в Microsoft Windows:

✓ Microsoft Office 2007 – у пакет оновлень SP2 вбудована функція експорту будь-яких документів у PDF, тобто перетворення pdf-файлів у doc не вимагає використання додаткових програм.

- ✓ Foxit Reader – умовно-безкоштовна програма для перегляду PDF-файлів у Microsoft Windows. Ємність програми складає 3,5 Мб, установки не вимагає.
- ✓ Sumatra PDF – вільна (GPLv2) програма для перегляду PDF-файлів у Microsoft Windows.
- ✓ ABBYY PDF Transformer – власна програма для Windows NT версії від 5.0 для створення і перетворення PDF-файлів з будь-якого офісного застосування і перетворення PDF-файлів в документи редагованих форматів (Microsoft Word, RTF і ін.).
- ✓ PDFCreator вільна програма для створення файлів PDF. Може використовуватися з будь-яким додатком Microsoft Windows, що має можливість друку документів.
- ✓ Scientific and technical documentation utility (STDU) Viewer – безкоштовна для некомерційного використання програма для читання PDF і DJVU файлів, Converter – платна програма для перетворення формату DJVU в PDF.
- ✓ Формат DjVu (від фр. deja vu - вже бачене) графічний формат, розроблений фірмою AT&T, оптимізований для зберігання відсканованих документів. Існує два традиційні способи зберігання відсканованої книги: розпізнавання (OCR) з подальшою підготовкою повноцінного текстового електронного документа або скани – відскановані картинки, часто зібрані в pdf- документ. У першому випадку потрібно багато клопіткої роботи, у другому –формуються файли обсягом у десятки і навіть сотні мегабайт. Компромісним варіантом є перетворення відсканованих картинок у формат DjVu. До того ж текст і контрастні малюнки зберігаються зі здатністю 300dpi, все решта вважається фоном і зберігається із зниженим дозволом. Це дозволяє стиснути електронний документ без втрати можливості його прочитання. Суть технології DjVu полягає в автоматичному діленні зображення на декілька ділянок (наприклад, текст, логотип фірми і растрова фотографія), для кожного з яких обирається оптимальний для цього графічного образу алгоритм стиснення. Технологія DjVu забезпечує для файлів з чорно-білими монохромними зображеннями стиснення близько 500:1. Формат DjVu приблизно в 20 разів переважає над форматом GIF щодо обсягу файлу. У DjVu обсяг файла відсканованої книги можна одержати в межах декількох мегабайт, що цілком прийнятно. Особливого значення цей формат набуває для перенесення в мережу технічної, зокрема математичної літератури, де велику кількість схем і формул робить розпізнавання і переклад у текстовий формат практично нездійсненним. Він також ефективний у випадках, коли необхідно передати всі нюанси оформлення, наприклад, історичних документів, де важливе значення має не тільки зміст, а й колір і фактура паперу, дефекти пергаменту (тріщини, сліди від складання), виправлення, плями, відбитки пальців; сліди, залишені іншими предметами.

Формат DjVu стає фактичним стандартом для електронних бібліотек технічної і наукової літератури.

Величезна кількість книг у цьому форматі доступна в файлообмінних мережах.

Формат оптимізований для передачі мережею у такий спосіб, що сторінку можна проглядати ще до завершення скачування. DjVu-файл може містити текстовий (OCR) шар, що дозволяє здійснювати повнотекстовий пошук по файлу. Крім того, DjVu- файл може мати вбудований інтерактивний зміст і активні ділянки посилання, що робить зручною навігацію в DjVu-книгах.

4. ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ EXCEL ДЛЯ СТАТИСТИЧНОЇ ОБРОБКИ ПРАВОВИХ ДАНИХ ТА ПОБУДОВИ ДІАГРАМ

Електронна таблиця – це засіб інформаційних технологій, прикладна програма, що дозволяє вирішувати такі завдання:

- ✓ автоматизацію обчислень – автоматичну реалізацію обчислювальних завдань, які раніше можна було виконати тільки шляхом програмування;
- ✓ математичне моделювання – використання математичних формул дозволяє описати взаємозв'язок між різними параметрами

системи або процесу. Можливість автоматичного обчислення формул і функцій під час зміни значень вхідних у них операндів робить електронну таблицю зручним інструментом для організації чисельного експерименту:

1) підбір параметрів;
2) прогноз поведінки модельованої системи;
3) аналіз залежностей;
4) планування;

✓ використання електронної таблиці як бази даних. Електронні таблиці дозволяють виконувати дії, властиві СУБД, – пошук інформації за заданими умовами і сортування інформації;

✓ графічне представлення (у вигляді графіків, діаграм) числової інформації, що міститься в таблиці.

Одним із найпопулярніших табличних процесорів є MS Excel, що входить до складу пакета Microsoft Office.

Microsoft Excel – програма для роботи з електронними таблицями, створена корпорацією Microsoft для Microsoft Windows, Windows NT і Mac OS. Вона надає можливості економіко-статистичних розрахунків, графічні інструменти і мову макропрограмування VBA. Microsoft Excel входить до складу Microsoft Office, і на сьогодні Excel є одним із найбільш застосовуваних у світі.

Створення і редагування таблиць. Документ Excel називається робочою книгою. Робоча книга – це сукупність робочих листів, розділених на рядки і стовпці, на перетині яких утворюються комірки. Імена рядків – це їх номери. Рядки мають номери від 1 до 65536. Імена стовпців – літери латинського алфавіту від A до Z, потім від AA до AZ, BA до BZ і т. д. Додати або видалити лист можна, викликавши контекстне меню ярлика листа в лівому нижньому кутку і виконавши команду «Додати» або «Видалити». У комірку робочого листа можна вводити константи і формули. Константи поділяються на такі категорії: числові значення, текстові значення, значення дати й часу, логічні значення і помилкові значення.

Якщо стандартна ширина стовпця недостатня для розміщення в ній даних, то Excel виводить або округлене значення, або рядок символів ###. Обсяги комірок можуть бути змінені: встановити курсор на

роздільнику заголовків стовпців або на роздільнику між номерами рядків і виконати буксирування.

Для розташування даних у комірці в декілька рядків треба викликати контекстне меню виділених комірок і натиснути «Формат комірок», далі – «Вирівнювання», встановити «Відображення» й обрати «Переносити за словами» та змінити обсяг комірок. Вибір режиму «Автопідбір ширини» зменшує обсяг символів у виділеній комірці так, щоб вони повністю помістилися у ній.

Для виділення блоку комірок треба виконати такі дії:

– для виділення суміжних комірок – буксирування по комірках;
– для виділення несуміжних комірок –натиснути на першій сукупності комірок, потім за умови того, що затиснута клавіша [Ctrl], натиснути на решту сукупностей комірок;
– виділення всіх комірок робочого листа –натиснути клавішею комп'ютерної миші на кнопку, розташовану на перетині адресних смуг.

5. ВВЕДЕННЯ ТА РЕДАГУВАННЯ ДАНИХ

Щоб почати редагування, треба натиснути на комірці та ввести дані. Для редагування змісту комірки двічі натиснути на комірці та зазначити виправлення. Для переміщення даних слід виділити комірку, підвести курсор до межі виділеної комірки так, щоб він перетворився на звичайну стрілку миші, виконати буксирування до комірки, у яку переміщуються дані.

Для встановлення маркера заповнення треба натиснути «Сервіс», далі – «Параметри», потім обрати вкладку «Правка» й «Переміщення комірок». До того ж у нижньому правому кутку виділеної комірки з'являється маленький чорний квадрат – маркер заповнення. Під час установки маркера заповнення покажчик комп'ютерної (пропоную додати) миші приймає вигляд тонкого чорного хрестика.

Маркер заповнення використовується для автоматичного введення в таблицю значень із списку автозаповнення, який створюється у такий спосіб (пропоную додати):

– відкрити «вихідний список», натиснути на вкладку «Сервіс», потім – «Параметри», обрати вкладку «Списки» – «Виділити новий список» і ввести елементи списку, розділяючи їх комами;
– із значень, наявних у таблиці, визначити діапазон комірок, де містяться потрібні значення і виконати такі дії (пропоную додати): натиснути на вкладку «Сервіс», потім – «Параметри», далі обрати вкладку «Списки» й «Імпорт».

Для використання списку автозаповнення треба ввести в комірку будь-який елемент зі списку і відбуксирувати маркер заповнення в будь-якому напрямку, щоб ввести елементи списку в суміжні комірки.

Для використання автоматичного введення даних з постійною зміною слід ввести в першу комірку діапазону початкове значення, виділити діапазон для автоматичного заповнення даними і виконати такі дії (пропоную додати): натиснути «Правка», далі – «Заповнити», а потім обрати вкладку «Прогресія».

Дані в таблиці зображаються на екрані в певному форматі. Якщо дані не відповідають заданому формату, то вони неправильно відображаються. Щоб установити потрібний формат, треба викликати контекстне меню комірок, і виконати такі дії (пропоную додати): натиснути «Формат комірок» й обрати вкладку «Кількість».

Сортування даних – це впорядкування записів у таблиці. Для виконання сортування варто виділити блок комірок і виконати такі дії: натиснути «Дані», обрати вкладку «Сортування» та вказати порядок сортування.

Фільтрація даних – дозволяє знаходити і відбирати для обробки частину записів. Дані зображаються на екрані у вигляді відфільтрованого списку, тобто лише ті рядки, які містять певні значення або відповідають певним критеріям. Excel має два варіанти фільтрації: автофільтр і розширений фільтр.

Автофільтр здійснює швидку фільтрацію списку відповідно до змісту комірок або відповідно до простого критерію пошуку.

Для використання автофільтру потрібно:
✓ установити курсор всередині таблиці;
✓ обрати команди «Дані», потім – «Фільтр» й «Автофільтр».
✓ заголовний рядок списку в режимі автофільтра містить у кожному стовпці кнопку зі стрілкою. Клацання розкриває списки, елементи якого беруть участь у формуванні критерію. Кожне поле (стовпець) може використовуватися як критерій;
✓ розкрити список стовпця, за яким проводитиметься вибірка;
✓ обрати значення або умову і задати критерій вибірки в діалоговому вікні «Автофільтр користувача».

Для відновлення всіх рядків початкової таблиці потрібно виділити рядок «Усе» у списку фільтра, який відкривається, або виконати команду «Дані», обрати вкладку «Фільтр» і натиснути «Відобразити все».

Для того, щоб відмінити режим фільтрації потрібно встановити курсор усередині таблиці, повторно обрати команду «Дані», потім «Фільтр», обрати «Автофільтр» і зняти відмітку з цієї функції.

Автофільтр можна використовувати для знаходження заданого числа найбільших або найменших елементів списку, пошуку порожніх комірок, текстових значень у заданому алфавітному діапазоні тощо;

Розширений фільтр дає змогу формувати множинні критерії вибірки і здійснювати складнішу фільтрацію даних електронної таблиці, указуючи умову відбору за декількома стовпцями. Фільтрація записів із використанням розширеного фільтру виконується так: виділивши комірку, треба виконати такі дії (пропоную додати): натиснути «Дані», потім – «Фільтр», обрати «Розширений фільтр», у вікні «Розширений фільтр» зазначити умови фільтрації.

6. СУМІСНЕ ВИКОРИСТАННЯ WORD ТА EXCEL. УПРОВАДЖЕННЯ І ЗВ'ЯЗУВАННЯ ОБ'ЄКТІВ МІЖ ДОКУМЕНТАМИ РІЗНИХ ТИПІВ

Технологія OLE (Object Linking and Embedding) – технологія зв'язування і впровадження об'єктів, розроблена корпорацією Microsoft.

OLE дозволяє передавати частину роботи від однієї програми редагування до іншої та повертати результати назад.

Під час використання OLE в обміні інформацією беруть участь два додатки – додаток-джерело і додаток-приймач. Додаток-джерело використовується для створення і редагування OLE-об'єктів. Після того, як об'єкт створений, його розміщують у додатку-приймачі.

Зв'язування – OLE-зв'язаний об'єкт підключається до окремого файла. Керування відображенням OLE-об'єкта в додатку-приймачі здійснюється на основі інформації, що зберігається у файлі додатку-джерела. Якщо цей файл змінюється в додатку-джерелі, OLE-об'єкт відповідно оновлюється. OLE-об'єкт не міститься в документі-приймачі. Замість цього додаток-приймач запам'ятовує джерело об'єкта. Обсяг файла-приймача збільшується тільки на обсяг посилання на файл-джерело. Початковий файл повинен залишатися доступним на комп'ютері або в мережі та слугувати джерелом оригінальних даних. Для зв'язування таблиці Excel і документа Word треба:

- виділити таблицю в додатку-джерелі, викликати контекстне меню, і натиснути «Копіювати»;
- відкрити документ Word, установити курсор на місце вставки таблиці й виконати такі дії (пропоную додати): натиснути «Правка», далі – «Спеціальна вставка» й обрати «Зв'язати». Зазначити тип об'єкта, що зв'язується з документом.

Тепер у разі змін у таблиці, що виконуються в Excel, ці зміни автоматично будуть відображатися в таблиці, що зв'язана з документом Word.

Упровадження – упроваджений OLE-об'єкт повністю міститься у файлі додатку-приймача, тому він не пов'язаний із зовнішнім файлом.

Об'єкт, розміщений в документі, «пам'ятає», звідки він узявся. MS Office забезпечить можливість його редагування в тому додатку, у якому цей об'єкт був створений, а не в тому, у якому він зараз відображається. Обсяг файла-приймача збільшується на обсяг усього файла-джерела, а не тільки впроваджених даних. Для впровадження таблиці Excel в документ Word треба:

- виділити таблицю в додатку-джерелі, викликати контекстне меню і натиснути «Копіювати»;
- відкрити документ Word, установити курсор на місці вставки таблиці і виконати такі дії (пропоную додати): натиснути «Правка», потім – «Спеціальна вставка» й обрати вкладку «Вставити». Зазначити тип об'єкта, що впроваджується в документ.

Для редагування впровадженого об'єкта необхідно двічі натиснути на впроваджених даних, що дасть можливість редагування

фрагмента у вікні додатку-приймача, а за допомогою рядка меню і панелей інструментів – додатку-джерела. Під час відкриття файлу на іншому комп'ютері впроваджений об'єкт можна буде переглядати, навіть не маючи доступу до початкових даних. Оскільки впроваджений об'єкт не має жодних зв'язків з початковим файлом, він не оновлюється під час зміни початкових даних.

Буксирування є найпростішим способом створення OLE-об'єкта. За допомогою комп'ютерної (пропоную додати) миші можна обрати елемент у додатку-джерелі, відбуксирувати його в додаток-клієнт, після чого він автоматично стає OLE-об'єктом. У разі звичайного буксирування виділеного об'єкта він стає OLE-впровадженим об'єктом. Якщо буксирування виділеного об'єкта здійснюватиметься під час натиснутої клавіші [Ctrl] або [Shift], він стає OLE-зв'язаним об'єктом.

Впровадження і зв'язування дозволяють вставляти в документ дані, з якими додаток-приймач не може працювати безпосередньо. Наприклад, під час додавання звуку чи відео в тексті з'явиться значок, натиснувши на який можна відтворити необхідне – звук чи відео.

ВИСНОВКИ

Microsoft Office Word – текстовий процесор, доступний для Windows і Apple Mac OS X, який дозволяє створювати документи високого ступеня складності (пропоную об'єднати ці два речення). Цей текстовий процесор підтримує технологію OLE, модулі сторонніх розробників, що підключаються, шаблони, захист документа, макроси та ін.

PDF (Portable Document Format) – це формат електронних документів, розроблений компанією Adobe Systems, переносний формат документів, створений як засіб міжплатформеного обміну даними. Насамперед він призначений для представлення в електронному вигляді поліграфічної продукції; переважна частина сучасного професійного друкарського устаткування може обробляти PDF безпосередньо.

Електронна таблиця – це засіб інформаційних технологій, прикладна програма, що дозволяє вирішувати такі завдання:

- автоматизацію обчислень – автоматичну реалізацію обчислювальних завдань, які раніше можна було виконати тільки через програмування;
- математичне моделювання – використання математичних формул дозволяє описати взаємозв'язок між різними параметрами системи або процесу.

Технологія OLE (Object Linking and Embedding) – технологія зв'язування і впровадження об'єктів, розроблена корпорацією Microsoft.

OLE дозволяє передавати частину роботи від однієї програми редагування до іншої та повертати результати назад.

Сучасна апаратна частина комп'ютера здатна обробляти велику кількість команд одночасно, що дозволяє створювати складні додатки, які відповідають сучасним вимогам. Чим складніша комп'ютерна програма, тим більше потрібно обчислювальних потужностей від апаратної частини. Якщо конфігурація устаткування не дозволяє виконувати запущену користувачем програму, будуть спостерігатися значне зниження рівня продуктивності, а також зависання комп'ютера (пропоную додати).

Існує безліч різновидів програмного забезпечення, які визначаються відповідно до мети їх застосування або специфікою їх функціонування і роботи.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 р. № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Баженов В. А. Інформатика. Комп'ютерна техніка. Комп'ютерні технології : підручник. 4-те вид. К. : Каравела, 2012. 496 с.

8. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посібник. К. : КНЕУ, 2004. 307 с.

9. Макарова М. В. Інформатика та комп'ютерна техніка : навчальний посібник. 3-тє вид., переоб. і доп. Суми : ВДТ «Університетська книга», 2008. 665 с.

10. Маценко В. Г. Обчислювальна техніка та програмування : навчальний посібник. Чернівці : ЧНУ, 2010 112 с.

11. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

12. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / за ред. В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін. Х. : Право, 2010. 240 с.

13. Редько М. М. Інформатика та комп'ютерна техніка : навчально-методичний посібник. Вінниця : Нова книга, 2007. 568 с.

14. Ярмуш О. В., Редько М. М. Інформатика і комп'ютерна техніка : навч. посібник. К. : Вища освіта, 2006. 359 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Що таке «software» та «hardware»?
2. Які характеристики текстового процесора Microsoft Word?

3. Які Ви знаєте засоби роботи в текстовому процесорі Microsoft Word?

4. Що таке «табличний процесор»? Яке його призначення та можливості?

5. Що таке «Табличний процесор Microsoft Excel»?

6. Які основні об'єкти табличного процесора MS Excel?

7. Як відбувається автоматизація введення даних?

8. Як здійснюються обчислення в електронних таблицях?

9. Як здійснюється аналіз результатів, сортування й фільтрування даних у MS Excel?

10. Який Ви знаєте процес побудови діаграм і графіків?

11. У чому полягає сумісне використання Word та Excel? Як здійснюється впровадження і зв'язування об'єктів між документами різних типів?

12. Що таке «файлова система» та її складові: папка, файл, ярлик?

13. За допомогою якої програми були створені такі файли: 1)*.**txt** 2)*.**html** 3)*.**exe** 4)*. **hlp**5)*.**jpg?**

14. Що таке «сервісне програмне забезпечення», «комп'ютерний вірус»?

15. Яке призначення антивірусних програм?

2. Практині завдання

Завдання № 1.

1. На своєму комп'ютері (пропоную додати) запустити програму «**Провідник»**.

2. Обрати диск **D** і відкрити папку **«2 курс»** (якщо її немає, то створити).

3. У папці «**2 курс»** створити папку з номером взводу (наприклад, **102**)

4. Відкрити папку з номером взводу та створити нову папку (назва папки – Ваше прізвище).

5. У власній папці створити текстовий документ. Дати назву – **«Особисті дані»**.

6. Скопіювати документ **«Особисті дані»** в папку **з номером взводу**.

7. Відкрити папку з номером взводу й змінити назву документа **«Особисті дані»** на назву **«Мої дані»**.

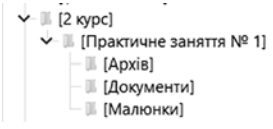
8. Перемістити документ **«Мої дані»** із папки з **номером взводу** у власну папку.

9. У власній папці для документа **«Особисті дані»** створити ярлик.

10. Створити ярлик для документа **«Мої дані»** на Робочому столі. Перевірити як він працює (відкрити).

11. Видалити із власної папки всі створені документи. Із Робочого столу видалити **ярлик** для документа (пропоную додати) **«Мої дані»**.

12. Створити у власній папці таку структуру папок:



13. Знайти 10 файлів з розширенням docx. Знайдені файли скопіювати до папки **«Документи»**, що знаходиться на диску **D:\ 2 Курс\ Номер взводу\Прізвище**.

14. Створити архів для папки **«Документи»,** розмістивши його у папці **Архів**, використовуючи для цього контекстне меню.

15. Проаналізувати вміст папки **«Документи»** і архіву **«Документи.rar».**

16. Створити SFX-архів (англ. self-extracting archive) для папки **«Документи»** і помістити його у папку **Архів**.

17. Порівняти розміри двох створених вами архівів **rar** і **sfx (exe).**

18. Відшукати на комп'ютері графічні файли з розширенням bmp, оберіть будь-які два знайдених файли, скопіюйте їх в папку Малюнки.

19. Створити для них архів з іменем **«Малюнок.rar»** в папці **«Архів»**, установивши параметри максимального стиснення.

20. Відкрити програму-антивірус, встановлену на комп'ютері.

21. Перевірити диск D на наявність вірусів.

22. Показати результати роботи викладачу. Почистити вміст Корзини (видалити документи **«Особисті дані»**, **«Мої дані»**, **Ярлик для «Мої дані»**, **Ярлик для «Особистих даних»**). Закрити всі відкриті вікна і вийти на **Робочий стіл.**

Завдання № 2.

1. Створіть новий текстовий документ Word та збережіть його у папці Word, що знаходиться у вашому каталозі (якщо такої папки не існує,

то створіть її), з ім'ям **Оригінал.** Збережіть ще раз цей текстовий документ з ім'ям **Форматування** у власній папці.

2. У цьому текстовому документі встановіть параметри сторінки: розмір: А4; поля: ліве – 3 см; праве – 1 см; верхнє, нижнє – 2 см; орієнтація сторінки – **книжкова**.

3. Установіть відступи для першого рядка абзацу **1 см 25 мм**. Міжстроковий інтервал –**1 см 50 мм**, вирівнювання – **по ширині** , шрифт – Times New Roman , розмір кегля – 14 пт.

4. Виберіть мову введення тексту – **українську**.

5. Наберіть текст із запропонованих викладачем додатків.

6. Додайте декілька слів у довільних місцях тексту. Поміняйте 2-й і 3-й абзаци місцями.

7. Виконайте пошук слів, які Ви додали до тексту.

8. Виконайте розрив сторінки після першого абзацу.

9. Для другого абзацу встановіть такі параметри: розмір шрифту **16**, **напівжирний курсив**, **зеленого** кольору, назва шрифту **Comic Sans MS**, міжсимвольний інтервал – **розріджений**, вирівнювання **по центру**.

10. Для третього абзацу застосуйте форматування з урахування різних інших налаштувань щодо шрифтів (тип, розмір, накреслення, інтервал, видозміна, масштаб, колір тощо).

11. Для введеного тексту застосуйте **Автоматичну розстановку перенесення** слів.

12. Оберіть режим перегляду документа – **Режим читання**.

13. Укажіть масштаби зображення сторінки на екрані: **75 %**, **дві сторінки**.

14. Збережіть файл у своєму каталозі.

15. На другому аркуші створіть автоматичний нумерований список і застосуйте до тексту певні параметри, виконавши такі дії: оберіть вкладку «Розмітка сторінки», потім натисніть «Межі сторінки», у вікні, що відкрилося, натисніть «Межі», потім оберіть вкладку «Рамка», обравши рамку для свого тексту, натисніть «Застосувати до абзацу» і «ОК».

16. Розташуйте в тексті малюнок.

17. Установіть такі параметри: розмір шрифту **12** , **напівжирний** для першого абзацу, назва шрифту Arial, міжсимвольний

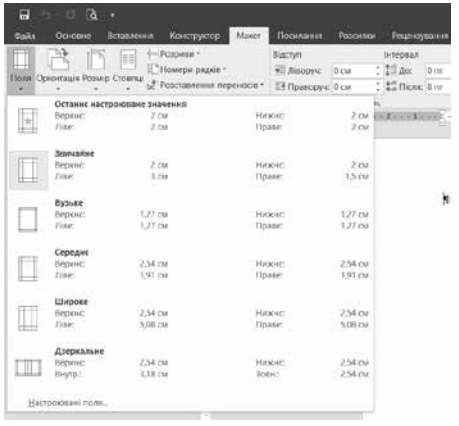
інтервал – **розріджений**, вирівнювання **по лівому краю,** границю до абзацу, малюнок – **обтікання тексту по контуру**.

18. Завантажте результати роботи на платформу дистанційного навчання.

Завдання № 3

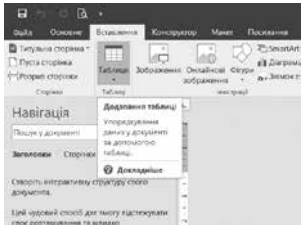
1. Завантажити Microsoft Word.

2. Установити параметри сторінки: **Поля** –верхнє: 1,5 см, нижнє: 1,5 см, ліве: 3 см, праве: 1 см; **Орієнтація** –книжна; розмір аркуша – 210 х 297 мм.



3. Зберегти документ у власній папці з назвою **Статистика**.

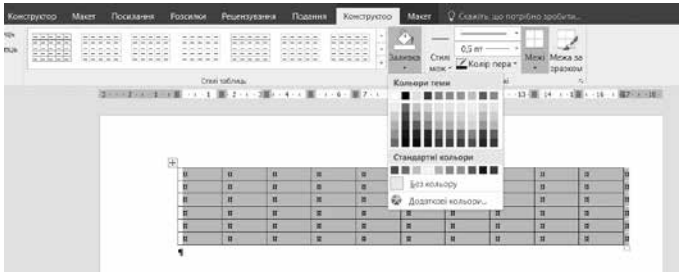
4. Створити документ відповідно до зразка 1. Розміри шрифту **Times New Roman** для таблиці: 10–12 пт. Параметри абзацу: міжрядковий одинарний.



Зразок 1 (пропоную додати, якщо це і є зразком)

1) Вставка – «таблиця» – «Вставити таблицю» – вказати кількість рядків і стовпчиків.

5. Зробити заливання сірим кольором верхнього рядку таблиці: виділити рядок, натиснути «Конструктор», далі – «Заливка» й обрати сірий колір.



6. Зберегти документ у власній папці Word, з ім'ям: **Статистика**, тип файлу: **Документ Word**.

3. Теми реферативних повідомлень

1. Операційна система. Складові частини ОС.
2. Переваги та недоліки операційних систем сімейства Windows. Можливості операційної системи Windows.
3. Інтегровані системи.
4. Інтерфейс користувача – комп'ютера.
5. Прикладне програмне забезпечення загального призначення.
6. Прикладне програмне забезпечення спеціального призначення.
7. Зовнішня пам'ять персонального комп'ютера. Перспективи розвитку.
8. Пристрої для друку. Сучасний стан та перспективи.
9. Методи маніпуляції даними та комп'ютерними програмами.
10. Наявні засоби боротьби і захисту з комп'ютерними вірусами.
11. Комп'ютерні мережі. Способи їх використання.

ЗАВДАННЯ ДЛЯ ТЕСТОВОГО КОНТРОЛЮ

1. Програму Microsoft Word можна відкрити такими способами:

а) за допомогою команди головного меню *пуск / програми / Microsoft Word*;
б) за допомогою ярлика програми, розміщеного на робочому столі Windows;
в) створити новий файл;
г) будь-яким з перелічених способів.

2. Під час форматування символу у TP Word можна задати:

а) лише його колір;
б) розмір і колір шрифту;
в) розмір, накреслення, гарнітуру та колір.
г) фон тексту.

3. Для того, щоб надрукувати документ Word на принтері, потрібно:

а) скористатися кнопкою панелі інструментів *«друк»*;
б) скористатися командою меню «*формат» / «друк»*;
в) скористатися командою меню «*файл» / «роздрукувати документ».*
г) усі відповіді правильні.

4. Команди меню «Файл» програми Microsoft Word призначені для:

а) налаштування програми;
б) роботи з документами;
в) створення нових файлів;
г) роботи з вікнами документа.

5. Переглянути створений документ у TP Word можна:

а) натиснувши комп'ютерною мишею на піктограму *«Попередній перегляд»*;
б) правильної відповідь немає;
в) виконати дії *Файл / Відкрити*;
г) виконати дії *Формат / Табуляція.*

РОЗДІЛ 7
ІНФОРМАЦІЙНІ ЗАСОБИ ЯК ДЖЕРЕЛА ІНФОРМАЦІЇ ЩОДО ОБСТАВИН ЗЛОЧИНУ

1. Особливості проведення огляду місця події (інших слідчих дій) під час розслідування комп'ютерних злочинів.
2. Загальні правила вилучення комп'ютерних засобів та їх упакування.
3. Особливості вилучення окремих видів комп'ютерної техніки.
4. Типові помилки під час проведення слідчих дій та рекомендації для їх запобігання.
5. Організація процесу комп'ютерно-технічної експертизи.
6. Комп'ютерно-технічна експертиза.

1. ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОГЛЯДУ МІСЦЯ ПОДІЇ (ІНШИХ СЛІДЧИХ ДІЙ) ПІД ЧАС РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Після прибуття на місце події слідчо-оперативній групі потрібно вжити заходів щодо охорони місця події та забезпечення збереження інформації на комп'ютерах і периферійних запам'ятовуючих пристроях (ПЗП). Для цього необхідно:

- заборонити доступ до комп'ютерної техніки персоналу, який працює на об'єкті;
- персоналу об'єкта заборонити вимикати електропостачання комп'ютерної техніки;
- у разі, якщо на момент початку огляду місця події електропостачання об'єкта вимкнено, то до його відновлення потрібно відключити від електромережі всю комп'ютерну техніку, яка знаходиться в приміщенні, що оглядається;

- не робити ніяких маніпуляцій із засобами комп'ютерної техніки, якщо їх результат заздалегідь невідомий;
- за наявності в приміщенні, де знаходиться комп'ютерна техніка, небезпечних речовин, матеріалів або обладнання (електромагнітних, вибухових, токсичних тощо) прибрати або перенести їх в інше місце.

Після вживання вказаних вище невідкладних заходів можна починати безпосередній огляд місця події і вилучення речових доказів. До того ж потрібно брати до уваги:

- спроби персоналу пошкодити комп'ютерну техніку з метою знищення інформації, якщо до скоєння злочину причетні працівники цього об'єкта;
- наявність в комп'ютерній техніці спеціальних засобів захисту від несанкціонованого доступу, які, не отримавши у встановлений час спеціальний код, автоматично знищать всю інформацію;
- наявність в комп'ютерній техніці інших засобів захисту від несанкціонованого доступу.

Під час обшуків і виїмок, пов'язаних з вилученням ЕОМ, носіїв інформації виникає ряд загальних проблем, пов'язаних зі специфікою технічних засобів, що вилучаються. Так, необхідно передбачати заходи безпеки, що здійснюються злочинцями з метою знищення речових доказів. Наприклад, вони можуть використати спеціальне обладнання, яке в критичних випадках створює сильне магнітне поле, що стирає магнітні записи. Відома історія про хакера, який створив у дверному отворі магнітне поле такої сили, що воно знищувало магнітні носії інформації під час винесення їх з його кімнати. Злочинець має можливість включити до складу програмного забезпечення своєї машини програму, яка примусить комп'ютер періодично вимагати пароль, і, якщо за декілька секунд правильний пароль не введений, дані в комп'ютері автоматично зникнуть (як варіант, щоб уникнути повтору). Винахідливі власники комп'ютерів встановлюють іноді приховані команди, що знищують або архівують з паролями важливі дані, якщо деякі процедури запуску машини не супроводжуються спеціальними діями, відомими тільки їм.

Об'єктами огляду у справах цієї категорії є місце події та його обстановка, окремі комп'ютерні засоби й комплектуючі, інші предмети, документи.

Під час підготовки до огляду або обшуку необхідно з'ясувати факт наявності комп'ютерних засобів в обстежуваному приміщенні. У разі виявлення таких варто визначитися з низкою показників:

- кількість комп'ютерів та їхні типи;
- наявність носіїв комп'ютерних даних, які використовуються;
- наявність локальної мережі й виходу в інші мережі за допомогою модема, радіомодема або виділених ліній;
- системне й прикладне програмне забезпечення, яке використовується;
- наявність систем захисту інформації, їхні типи; можливості використання засобів невідкладного знищення комп'ютерної інформації;
- кваліфікація користувачів.

Це дозволить слідчому одержати всю криміналістично значиму інформацію, що зберігається в комп'ютерних пристроях; максимально підвищити її доказове значення.

Під час підготовки до огляду або обшуку корисно допитати (опитати) обслуговуючий персонал (системного адміністратора, операторів) і з'ясувати такі питання:

- які операційні системи встановлені на кожному з комп'ютерів;
- яке використовується програмне забезпечення;
- які застосовуються системи захисту й шифрування;
- де зберігаються загальні файли даних і резервні копії;
- які паролі встановлені на комп'ютери та паролі (пропоную додати) адміністраторів системи;
- які зареєстровані імена й паролі користувачів, які паролі та логіни використовуються для зв'язку в загальній інтернет-мережі?

Для успішного проведення огляду або обшуку важливе значення має фактор раптовості. Інакше підозрюваний (обвинувачуваний) може швидко знищити усі докази, що знаходяться в комп'ютері або на магнітних носіях. Якщо отримано відомості про те, що комп'ютери організовані в локальну мережу, треба, якщо це можливо, встановити

місцезнаходження всіх комп'ютерних пристроїв, підключених до цієї мережі. Також (за можливості) проводиться груповий обшук або огляд одночасно у всіх приміщеннях, де встановлені комп'ютерні засоби, в іншому разі насамперед треба проводити огляд головного комп'ютера (сервера).

З місця огляду або обшуку необхідно видалити всіх сторонніх осіб і припинити подальший доступ до комп'ютерів. Але під час обшуку обов'язково повинен бути присутнім представник об'єкта, який обшукується, для надання відповідних пояснень.

Якщо комп'ютер на (пропоную прибрати) початку огляду (обшуку) виявився ввімкненим, необхідно оцінити інформацію, зображену на моніторі, і визначити, яка програма зараз виконується (дії описати). У разі роботи стандартного програмного забезпечення (наприклад, на екрані зображені стандартні вікна операційних оболонок Windows, Volkov Commander або Total Commander) не можна починати будь-які маніпуляції без попереднього візуального огляду технічних засобів. Екран монітора бажано сфотографувати. Відключити всі телефонні лінії та мережеві лінії, підключені до комп'ютера (якщо такі з'єднання є). Зачинити всі програми, що працюють, програмно завершити роботу комп'ютера (наприклад, у системі Windows – кнопка «Пуск» – «Завершення роботи» – «ОК»), тільки після цього вимкнути комп'ютер з електромережі.

У протоколі слідчої дії слідчий описує основні фізичні характеристики пристроїв, що вилучають, їхні видимі індивідуальні ознаки, конфігурацію комп'ютерних засобів (їхню комплектацію); номера моделей і серійні номери кожного із пристроїв.

2. ЗАГАЛЬНІ ПРАВИЛА ВИЛУЧЕННЯ КОМП'ЮТЕРНИХ ЗАСОБІВ ТА ЇХ УПАКУВАННЯ

Завершальним етапом огляду, обшуку або виїмки у справах, пов'язаних з використанням комп'ютерних технологій, є фіксація й вилучення комп'ютерних засобів. Від того, як зроблене вилучення, транспортування й зберігання цих об'єктів часто залежить їхнє доказове значення. Тому речові докази у вигляді ЕОМ, носіїв інформації

вимагають особливої обережності під час вилучення, транспортування та зберігання. Їм протипоказані різкі кидки, удари, підвищені температури (вище кімнатних), вологість, тютюновий дим. Усі ці зовнішні чинники можуть спричинити втрату даних, інформації та властивостей апаратури. Не треба забувати під час огляду й обшуку про можливість збору традиційних доказів, наприклад, прихованих відбитків пальців на клавіатурі, вимикачах та ін.

Під час вилучення засобів комп'ютерної техніки необхідно забезпечити суворе дотримання кримінально-процесуального законодавства. Для цього необхідно акцентувати увагу понятих на всіх діях, що проводяться, та їх результатах. У разі потреби (щоб уникнути повтору) понятим дають необхідні пояснення, оскільки багатьом учасникам слідчої дії можуть бути незрозумілі маніпуляції, що проводяться.

Усі вилучені системні блоки та інші пристрої повинні бути упаковані й опечатані так, щоб не допустити можливість їхнього пошкодження, включення в мережу й розбирання.

Предмети та документи, виявлені під час слідчої дії, які, ймовірно, можуть мати значення для слідства, повинні бути вилучені відповідно до вимог процесуального кодексу. У зв'язку з цим у протоколі повинні бути точно вказані місце, час і зовнішній вигляд предметів, що вилучаються, і документів.

Вилучення комп'ютерних засобів повинно відбуватися відразу. У разі відсутності транспорту варто організувати охорону вилученого обладнання у спеціальному приміщенні.

Неприпустиме надання вилучених засобів, або їх частини у розпорядження організації (установи) із причин «виробничої необхідності», тому що в процесі роботи можуть бути внесені зміни у файли інформації або програми. Такі дії можуть спричинити пошкодження або знищення наявної комп'ютерної інформації.

Відомі зовсім неприпустимі випадки використання вилучених речових доказів комп'ютерних засобів слідчими й співробітниками оперативних апаратів для складання процесуальних документів, звітів, комп'ютерних ігор. Такі дії повинні рішуче припинятися, а винні притягуватися до відповідальності, навіть якщо у слідчому відділі, що розслідує злочин, припинили працювати всі службові комп'ютери.

Під час перевезення комп'ютерних засобів необхідно попередити їхні механічні ушкодження й взаємодію з хімічно активними речовинами. Варто екранувати від впливу електромагнітних полів як комп'ютерні пристрої, так і магнітні носії інформації. Такий вплив може призвести до псування або знищення інформації шляхом розмагнічування. Оскільки комп'ютерні засоби потрапляють на дослідження в експертні установи, особливу увагу варто звернути на огородження вилучених об'єктів від впливу широко використовуваних у цих установах магнітоутримуючих засобів криміналістичної техніки (наприклад, магнітних підйомників, магнітних пензликів для виявлення слідів рук та ін.).

Під час розміщення вилучених об'єктів на зберігання треба дотримуватися встановлених правил зберігання і складування електронних технічних засобів. Не можна ставити системні блоки комп'ютерів у штабель вище трьох штук, а також розміщувати на них будь-які інші предмети. Зберігають комп'ютери й їх комплектуючі в сухому, опалювальному приміщенні. Варто впевнитися, що в ньому немає гризунів (мишей і пацюків), які часто є причиною несправності апаратури. Крім того, категорично не рекомендується палити, приймати їжу і утримувати тварин у приміщеннях, призначених для зберігання комп'ютерної техніки й магнітних носіїв.

3. ОСОБЛИВОСТІ ВИЛУЧЕННЯ ОКРЕМИХ ВИДІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Системний блок ПК та периферійні пристрої

Персональний комп'ютер – комплекс пристроїв, який призначений для створення, зберігання, обробки та передачі інформації. Найрозповсюдженіші процеси, які здійснює ПК, – це набір, обробка та зберігання текстової інформації (документи, таблиці, бази даних), введення, обробка, зберігання та відтворення фото- та відеозображень, оперування (передача, отримання) інформацією у локальних та глобальних комп'ютерних мережах.

Складовими частинами ПК є:

1) системний блок (повна назва – системний блок персонального комп'ютера, скорочено – СБПК). До системного блока ПК зазвичай належать: системна (материнська) плата, процесор, оперативна пам'ять, графічний адаптер, накопичувач на оптичних дисках, накопичувач на жорстких магнітних дисках (НЖМД);

2) монітор;

3) клавіатура;

4) маніпулятор «миша» (далі – миша);

До периферійного обладнання відносять зовнішні пристрої ПК, зокрема й ті, без яких ПК не може працювати (миша, клавіатура), також принтери, сканери, музичні колонки, модем, ігрові джойстики тощо (далі комплекс ПК та інших додаткових пристроїв буде визначатися як «комп'ютерна система»).

Методика проведення пошуку та вилучення

За наявності даних про те, що особа використовує комп'ютерну систему як знаряддя вчинення злочину, вірогідність того, що ПК має докази злочинної діяльності, є дуже великою. Таке твердження також правильне, якщо достовірно відомо, що злочинець вже знищив інформацію (її в подальшому, зазвичай, можна відновити).

Слід зазначити, що основним об'єктом, який може зберегти сліди злочину є системний блок ПК, зокрема, його основна складова – накопичувач на жорстких магнітних дисках.

На практиці трапляються випадки, коли на вимогу обшукуваних працівники міліції вилучають лише НЖМД, відмонтовуючи його на місці проведення слідчої дії від системного блока ПК. Такі дії слід вважати неправильними та неприпустимими, оскільки вони унеможливлюють проведення деяких видів експертних досліджень, зокрема, експертного експерименту, через відсутність інших частин системного блока ПК.

На початку слідчої дії слід заборонити будь-кому бути присутнім біля ПК, оскільки нехтування цим може призвести до того, що особа натисканням декількох клавіш може безповоротно знищити важливу доказову інформацію.

Також треба звернути увагу на мережеві кабелі, якими один ПК з'єднаний з іншими ПК. Якщо до ПК підключені мережеві кабелі, то їх

варто від'єднати, указавши про це в протоколі слідчої дії. За допомогою мережі знищення інформації з ПК можливо також здійснити з іншого ПК, під'єднаного за допомогою мережевих кабелів. Ця рекомендація актуальна, якщо кількість приміщень значна, а контролювати дії всіх у них присутніх неможливо.

У разі відсутності спеціаліста слід керуватися такими **рекомендаціями з відключення ПК**:

- від'єднати мережеві кабелі;
- описати відображення на екрані монітору;
- коректно завершити роботи комп'ютера;
- від'єднати кабель енергоживлення від ПК,
- від'єднати всі кабелі від системного блока ПК.

Під час вилучення блоків ПК варто звернути увагу на записні книжки підозрюваного та інші папери, які знаходяться біля ПК, оскільки вони можуть мати записи з паролями до програм та зашифрованих файлів. Нерідко трапляються випадки, коли для успішного проведення дослідження не вистачало лише правильного пароля.

Опис системного блока ПК та периферійних пристроїв

Під час вилучення блока ПК завжди виникає необхідність це в протоколі слідчої дії та на паперовій етикетці упаковки. Зазвичай, системний блок ПК не має серійного номеру, за винятком деяких видів дорогих блоків. Тому слід описувати блок, беручи до уваги його колір, наліпки на передній та задніх панелях з написами, а також габаритні розміри: довжина, ширина та глибина системного блока ПК.

Під час опису моніторів, сканерів, принтерів треба звернути увагу на спеціальну заводську наліпку, яка розташована на їхніх корпусах та на якій є відомості про виробника, модель пристрою та його серійний номер.

Під час опису клавіатури та комп'ютерної (пропоную додати) миші варто вказати назву фірми виробника та модель пристрою, відомості, що розташовані на корпусі або на етикетці. У деяких випадках етикетки мають також серійний номер.

Упакування

Під час вилучення комп'ютерної системи кожна його складова (принтер, сканер, монітор, системний блок ПК) має бути упакована окремо від інших, окрім дрібних речей (клавіатури, миші). Дрібні речі доцільно упакувати разом.

Зважаючи на великий розмір окремих частин комп'ютерної системи, наприклад, системного блока, монітора, ідеальним пакувальним матеріалом може бути заводська картонна коробка. Зазвичай власники рідко викидають упакування виробника та зберігають його вдома, оскільки гарантійні зобов'язання продавця повною мірою можуть бути реалізовані за наявності упаковки. Тому доцільно попросити власника принести коробки для упакування.

Клапани коробки слід обклеїти липкою стрічкою, а саму коробку треба перев'язати капроновою ниткою методом «хрест-навхрест».

Паперову етикетку з описом предмета, що знаходиться в коробці, потрібно прикріпити до нитки, обклеївши її кінці папером з відбитком печатки, яку керівник слідчої дії повинен підготувати заздалегідь.

У разі відсутності упаковки виробника, необхідно мати інший пакувальний матеріал, що заздалегідь має бути підготовлений членами слідчо-оперативної групи. Таким матеріалом можуть бути міцні поліетиленові пакети для сміття. Так, для упакування стандартного за розміром блока ПК достатньо одного пакета для сміття об'ємом 160 літрів. Блок ПК вміщується в пакет, горловина якого щільно обмотується капроновою ниткою, до якої кріпиться паперова етикетка з відповідними написами.

Слід вважати неправильним упакування (яке дуже часто зустрічається на практиці), коли правоохоронці не упаковують системний блок ПК, а просто намагаються заклеїти важливі для роботи ПК гніздa або кнопки паперовими етикетками. У разі допущення подібної помилки, за умови звинувачення особи у протиправному використанні комп'ютерної програми операційної системи Microsoft Windows, відсутність цілісності упаковки завадить доведенню факту присутності або відсутності сертифіката відповідності на корпусі блока ПК.

Неефективність такої упаковки також пояснюється тим, що клей за своєю здатністю не передбачений для надійного склеювання паперу

та металу або фарби металу та паперу. Наклеєний у такий спосіб папір після висихання клею відривається, не залишаючи будь-яких слідів, але таку ситуацію не можна допустити за жодних умов.

Також трапляються випадки, коли гнізда та кнопки заклеєні липкою технічною стрічкою (т. з. «скотч»), а під нею знаходиться паперова етикетка з написами. Такий вид упаковки є теж неправильним з огляду на ненадійність склеювання пофарбованого металу та технічної стрічки. У разі такого пакування власники системних блоків, наполягаючи на його ненадійності, можуть вимагати (щоб уникнути повтору) переустановлення програм ПК працівником поліції, що суттєво уповільнює процес розслідування справи або її розгляд у суді.

Особливості вилучення ноутбуків

Ноутбуки слід вилучати разом із пристроєм для живлення акумуляторних батарей. Упакуванням для ноутбуку може слугувати його сумка. Замки «блискавки» зшиваються між собою, а до кінців нитки приклеюється паперова етикетка з відповідними написами.

Кожен ноутбук має на нижній панелі наліпку виробника із вказаними моделлю та серійним номером. Цей номер варто зазначити у протоколі та на паперовій етикетці. Часто також на задній панелі ноутбука наклеєно сертифікат відповідності комп'ютерної програми Microsoft Windows, що свідчить про правомірне використання комп'ютерної програми. Цей сертифікат складається із 25 унікальних цифр та літер, що можуть також чітко індивідуалізувати ноутбук.

4. ТИПОВІ ПОМИЛКИ ПІД ЧАС ПРОВЕДЕННЯ СЛІДЧИХ ДІЙ ТА РЕКОМЕНДАЦІЇ ДЛЯ ЇХ ЗАПОБІГАННЯ

Можна виокремити деякі правила роботи з комп'ютерами, вилученими під час розслідування злочинів у сфері комп'ютерної інформації, а також запропонувати загальні рекомендації, які можуть бути корисні у процесі обробки комп'ютерних доказів в операційних системах DOS чи Windows.

Помилка 1. Робота на комп'ютері

Головне правило, що неухильно повинне виконуватися, полягає в тому, щоб ніколи і за жодних умов не працювати на вилученому комп'ютері. У цьому правилі наголошується на тому, що вилучений комп'ютер – це насамперед об'єкт дослідження фахівців, речовий доказ. Тому його бажано навіть не включати до передачі експертам, оскільки категорично заборонено виконувати будь-які програми на вилученому комп'ютері без вживання необхідних заходів безпеки (наприклад, захисту від модифікації або створення резервної копії). Якщо на комп'ютері встановлена система захисту (наприклад, пароль), то його включення може призвести до знищення інформації, що знаходиться на жорсткому диску. Не допускається завантаження такого комп'ютера з використанням його власної операційної системи.

Таке застереження пояснюється досить просто: злочинцеві зовсім неважко встановити на своєму комп'ютері програму для знищення інформації на жорсткому чи гнучкому магнітному диску, записавши спеціальні програми-«пастки» в операційну систему.

Після того, як сама програма знищила дані, ніхто не зможе з певністю сказати, чи був «підозрюваний» комп'ютер спеціально оснащений такими програмами, або це результат недбалості під час дослідження комп'ютерних доказів.

Помилка 2. Допуск до комп'ютера власника або користувача комп'ютера

Суттєвою помилкою є допуск до досліджуваного комп'ютера власника для отримання допомоги під час його експлуатації. У багатьох зарубіжних літературних джерелах описуються випадки, коли підозрюваному на допитах, пов'язаних з комп'ютерними злочинами, був наданий доступ до вилученого комп'ютера. Пізніше він розповідав своїм знайомим, як шифрував файли поряд з поліцейськими, а ті про це навіть не здогадувалися. Враховуючи такі наслідки, фахівці з комп'ютерних досліджень почали робити резервні копії комп'ютерної інформації перед тим, як надавати до них доступ.

Інша проблема пов'язана з можливістю спростування в суді ідентичності пред'явленого на процесі програмного забезпечення, яке

перебувало на цьому комп'ютері до вилучення. Щоб уникнути таких ситуацій, комп'ютер потрібно, не включаючи, опечатати у присутності понятих. Якщо ж співробітник правоохоронних органів приймає рішення оглянути комп'ютер на місці, то насамперед треба зробити копію жорсткого магнітного диска і всіх носіїв інформації, які будуть вилучатися як речові докази. Це означає, що до проведення будь-яких операцій з комп'ютером необхідно зафіксувати його стан на момент проведення слідчих дій.

Помилка 3. Відсутність перевірки комп'ютера на наявність вірусів і програмних закладок.

Для перевірки комп'ютера на наявність вірусів і програмних закладок необхідно проводити завантаження комп'ютера не з операційної системи, яка знаходиться на ньому, а зі своєї попередньо підготовленої дискети, або зі стендового жорсткого диска. Перевірці підлягають усі носії інформації: дискети, компакт-диски, жорсткі диски та інші носії. Цю роботу варто робити залученим для участі в слідчих діях фахівцям за допомогою спеціального програмного забезпечення.

Не можна допустити, щоб у суді з'явилася можливість звинуватити слідство у навмисному зараженні комп'ютера вірусами, у некомпетентності під час проведення слідчих дій або просто в недбалості, оскільки довести, що вірус був у комп'ютері до початку дослідження, навряд чи можливо, а подібне звинувачення змусить сумніватися у праці експерта та достовірності його висновків.

Це найбільш типові помилки, які часто зустрічаються під час дослідження комп'ютерів у справах, пов'язаних з розслідуванням комп'ютерних злочинів.

Для запобігання помилок у процесі проведення слідчих дій на початковому етапі розслідування, які можуть призвести до втрати або руйнування комп'ютерної інформації, потрібно дотримуватися заходів безпеки.

5. ОРГАНІЗАЦІЯ ПРОЦЕСУ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Виокремлюють такі етапи організації процесу комп'ютерно-технічної експертизи:

1. Отримання дозволу про призначення експертизи – ці дії вважаються законними у разі отримання ухвали слідчого судді. Судова експертиза може бути організована за особистою ініціативою учасників судочинства, наприклад, позивачем, відповідачем, обвинуваченим, потерпілим, адвокатом, або за клопотанням прокурора чи слідчого за погодженням із прокурором. Після схвалення запиту складається список питань, на які фахівець повинен дати розгорнуту відповідь у строки, відповідні ухвалі.

2. Направлення комп'ютерної техніки та програмних продуктів до вказаного в ухвалі слідчого судді експертного центру.

3. Безпосереднє проведення досліджень і надання відповідей на поставлені питання, визначені у Наказі Міністерства юстиції України.

4. Отримання висновку експерта. У разі неможливості дати висновок експерт зобов'язаний скласти пояснювальну записку, у якій повинен пояснити причини відмови від експертизи. До найбільш поширених причин відмови належать: непридатність матеріалів і об'єктів досліджень; недостатність кваліфікованих кадрів; відсутність сучасних технологій, що не дає змогу вирішити завдання експертизи.

6. КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА

З метою дослідження комп'ютерів, їх комплектуючих і тієї інформації, яка в них знаходиться, призначається **комп'ютерно-технічна експертиза** – новий вид інженерно-технічних експертиз. Основою цієї експертизи є спеціальні знання в галузі інформатики й обчислювальної техніки (комп'ютерних технологій і програмного забезпечення).

Комп'ютерно-технічна експертиза – це дослідження технічних властивостей цифрового обладнання (комп'ютерів, накопичувачів інформації, мобільних телефонів тощо) та програмного забезпечення

з метою отримання фактичних даних, що відносяться до обставин скоєного злочину або предмета цивільного позову. Експертиза дає змогу виявити суттєві ознаки злочину (інциденту) і створити цілісну доказову базу шляхом дослідження інформації.

Залежно від мети дослідження в межах комп'ютерно-технічної експертизи виокремлюють: технічну експертизу комп'ютерів та їх комплектуючих і експертизу програмного забезпечення.

Завданнями, що вирішуються в межах проведення комп'ютерно-технічної експертизи, є:

- встановлення виду (типу, марки), властивостей апаратного засобу, а також його технічних і функціональних характеристик;
- встановлення фактичного стану та справності апаратного засобу;
- виявлення і дослідження функціональних властивостей, а також налаштувань програмного забезпечення, часу його інсталяції;
- з'ясування (щоб уникнути повтору) потрібної інформації, встановлення її властивостей та виду відображення в комп'ютерній системі;
- відновлення видаленої та зашифрованої інформації на різного виду носіях;
- виявлення ознак діяльності шкідливого програмного забезпечення;
- встановлення слідів активності в інтернет-мережі, змісту електронного листування, історії обміну повідомленнями у програмах для спілкування та інше.

Об'єктами комп'ютерно-технічної експертизи є як апаратні засоби (системні блоки комп'ютерів та їх комплектуючі, сервери, ноутбуки, жорсткі диски, флеш-накопичувачі, модеми, маршрутизатори та ін.), так і **програмні продукти** (комп'ютерні програми, бази даних тощо).

Типові питання, які вирішуються судовою комп'ютерно-технічною експертизою.

✓ Чи містяться на наданих для дослідження об'єктах серед наявних та видалених файлів інформація щодо ключових слів: «****», «***», «**»? Якщо так, то які атрибути (дата та час створення, редагування, друку, видалення тощо) файлів, що мають зазначену

інформацію?

- ✓ Чи є на наданих для дослідження об'єктах серед наявних та видалених файлів документи формату «doc», «docx», «pdf» та електронні таблиці формату «xls», «xlsx»?
- ✓ Чи є на наданих для дослідження об'єктах серед наявної та видаленої інформації графічні або відеофайли з ознаками порнографічної продукції? (виключно під час призначення комплексної комп'ютерно-технічної та мистецтвознавчої експертизи).
- ✓ Чи містяться на наданих для дослідження об'єктах файли листів електронної пошти? У разі наявності скопіювати зазначену інформацію на окремий носій.
- ✓ До яких вебадрес інтернет-мережі та коли здійснювався доступ з наданих для дослідження об'єктів?
- ✓ Чи є на наданих для дослідження об'єктах облікові дані (логіни та паролі) для доступу до інтернет-ресурсів?
- ✓ Чи встановлені на наданих для дослідження об'єктах програми, призначені для спілкування в інтернет-мережі («Viber», «Skype», «Telegram», «Whatsapp» та інші)? Якщо так, то чи містять вони інформацію щодо історії повідомлень та дзвінків?
- ✓ Чи є на наданих для дослідження об'єктах програмне забезпечення, призначене для віддаленого керування комп'ютером («teamviewer», «ammyy admin», «radmin», «ultravnc» та інше)? Якщо так, то чи містяться на наданих для дослідження об'єктах лог-файли використання виявлених програм?
- ✓ Чи наявні на наданих для дослідження об'єктах програми (клієнти) для дистанційного банківського обслуговування (ДБО) типу «клієнт-банк», «інтернет-банкінг»? Якщо так, то чи містять вони лог-файли використання вказаних програм?
- ✓ Чи є на наданих для дослідження об'єктах певне (зазначити назву або функціональне призначення, а також вид – встановлене чи не встановлене) програмне забезпечення? (стосовно грального бізнесу програми «iConnect», «iChampion», «G-slot», «Gaminator», «Superomatic», «iGaming Casino», «Megasuperomatic»).
- ✓ Чи можливо виконання певних дій (вказати яких саме) за допомогою цього програмного продукту?

- ✓ Чи можливе вирішення певного завдання (вказати якого саме) за допомогою цього програмного продукту?
- ✓ Чи реалізовані в цьому програмному продукті функції, передбачені технічним завданням для його розробки?
- ✓ Чи містяться на наданому для дослідження відеореєстраторі відеозаписи, створені в певний (пропоную додати) період часу (вказати дату та час, за які потрібні відеозаписи)? Якщо так, то ці відеозаписи треба скопіювати на окремий носій.
- ✓ Чи містяться в пам'яті наданих для дослідження мобільних телефонів інформація щодо списку контактів, журналу дзвінків, текстових та мультимедійних повідомлень, вебісторії, повідомлень в інтернет-мережі, а також текстових, графічних, відеофайлів користувача? У разі наявності зазначеної інформації треба скопіювати її на окремий носій інформації.

ВИСНОВКИ

Комп'ютерно-технічна експертиза – це дослідження технічних властивостей цифрового обладнання (комп'ютерів, накопичувачів інформації, мобільних телефонів тощо) та програмного забезпечення з метою отримання фактичних даних, що відносяться до обставин скоєного злочину або предмета цивільного позову. Експертиза дає змогу виявити суттєві ознаки злочину (інциденту) і створити цілісну доказову базу шляхом дослідження інформації.

Комп'ютерно-технічна експертиза має на меті: встановлення виду (типу, марки), властивостей апаратного засобу, а також його технічних і функціональних характеристик; з'ясування (щоб уникнути повтору) фактичного стану та справності апаратного засобу; виявлення і дослідження функціональних властивостей, а також налаштувань програмного забезпечення, часу його інсталяції; виявлення потрібної інформації, встановлення її властивостей та виду відображення в комп'ютерній системі; відновлення видаленої та зашифрованої інформації на різного виду носіях; виявлення ознак діяльності шкідливого програмного забезпечення; виявлення слідів активності в інтернет-мережі, змісту електронного листування, історії обміну повідомленнями у програмах для спілкування та інше.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 р. № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Баженов В. А. Інформатика. Комп'ютерна техніка. Комп'ютерні технології : підручник. 4-те вид. К. : Каравела, 2012. 496 с.

8. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посібник. К. : КНЕУ, 2004. 307 с.

9. Макарова М. В. Інформатика та комп'ютерна техніка : навчальний посібник. 3-тє вид., переоб. і доп. Суми : ВДТ «Університетська книга», 2008. 665 с.

10. Маценко В. Г. Обчислювальна техніка та програмування : навчальний посібник. Чернівці : ЧНУ, 2010 112 с.

11. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

12. Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу

комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. URL: https://ojs.naiau.kiev.ua/index.php/scientbul/article/view/1229.

13. Шорохова Г. М. Проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України : матер. шостої міжнародної науково-практичної конференції НАНР Економіко-правові виклики 2016 року, м. Львів 12 січня 2016 р. Львів: Національна академія наукового розвитку, 2016. Том 2. С. 184–186.

14. Шульга Б. С. Комп'ютерно–технічна експертиза: поняття, предмет, об'єкти, завдання. Особливості проведення огляду місця події при комп'ютерних злочинах, правила вилучення комп'ютерних засобів та їх упакування. Сучасні криміналістичні експертизи в розслідуванні злочинів. 2015. URL: http://elar.naiau.kiev.ua/bitstream/123456789/9141/1/СУЧАСНІ%20КРИМІНАЛІСТИЧНІ_p069-073.pdf.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Які особливості проведення огляду місця події (інших слідчих дій) у разі комп'ютерних злочинів?

2. Загальні правила вилучення комп'ютерних засобів та їх упакування.

3. Укажіть особливості вилучення окремих видів комп'ютерної техніки.

4. Які типові помилки під час проведення слідчих дій та рекомендації для їх запобігання?.

5. Організація процесу комп'ютерно-технічної експертизи.

6. Комп'ютерно-технічна експертиза: об'єкти та питання, які вирішує.

2. Практині завдання

Завдання № 1

1. Назвіть основні частини системного блоку.

2. Укажіть найпоширеніші місця розташування заводських наліпок на системному блоці комп'ютера.

Завдання № 2

Назвіть пристрій, зображений на малюнку нижче, та зазначте його призначення.

Завдання № 3

Однією постановою призначена експертиза за різними видами об'єктів (сервери та персональні комп'ютери разом з мобільними телефонами та планшетними комп'ютерами). Чи доцільно призначати за цими об'єктами експертизу однією постановою? Доведіть свою думку.

Завдання № 4

Укажіть, які питання доцільно ставити для вирішення експертизи щодо історії спілкування в інтернет-мережі (оберіть з перелічених):

– Чи наявні на носієві інформації файли листів електронної пошти?

– Чи встановлені на наданих для дослідження об'єктах програми, призначені для спілкування в інтернет-мережі («Viber», «Skype», «Telegram», «WhatsApp»)? Якщо так, то чи містять вони інформацію щодо історії повідомлень та дзвінків?

– Чи є на наданих для дослідження об'єктах певне (зазначити назву або функціональне призначення, а також вид – встановлене чи не встановлене) програмне забезпечення? (стосовно грального бізнесу – програми «iConnect», «iChampion», «G-slot», «Gaminator», «Superomatic», «iGaming Casino», «Megasuperomatic»)?

– Чи можливе виконання певних дій за допомогою цього програмного продукту?

– Чи можливе вирішення певного завдання за допомогою цього програмного продукту?

– Чи реалізовані у цьому програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

3. Теми реферативних повідомлень

1. Значення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів.

2. Смартфони – як джерело інформації про кіберзлочини.

ЗАВДАННЯ ДЛЯ ТЕСТОВОГО КОНТРОЛЮ

1. Об'єктами огляду кіберзлочинів є:

а) місце події і його обстановка;
б) окремі комп'ютерні засоби і комплектуючі;
в) усі відповід правильні;
г) інші предмети та документи.

2. Складовими частинами ПК є:

а) системний блок;
б) текстовий процесор Microsoft Word;
в) графічний адаптер;
г) інформація, яка зберігається на ПК.

3. Огляд місця події злочинів, скоєних за допомогою технічних засобів, проводить:

а) прокурор;
б) слідчий;
в) експерт;
г) усі відповіді правильні.

4. Порядок Ваших дій, якщо Ви знайшли мобільний телефон неповнолітньої особи, що зникла, на якому є уся інформація про цю особу, але телефон заблоковано:

а) провести огляд місця події; вилучити мобільний телефон як доказ; оглянути телефон щодо наявності відбитків пальців;
б) правильної відповідь немає;
в) провести огляд місця події без вилучення речових доказів;
г) провести огляд місця події; відправити телефон на експертизу.

5. Комп'ютерно-технічна експертиза – це:

а) дослідження технічних властивостей цифрового обладнання тільки комп'ютерів з метою отримання фактичних даних;
б) дослідження технічних властивостей комп'ютерів та програмного забезпечення з метою отримання фактичних даних;

в) дослідження технічних властивостей цифрового обладнання програмного забезпечення комп'ютерів з метою отримання фактичних даних;
г) дослідження технічних властивостей цифрового обладнання комп'ютерів, накопичувачів інформації, мобільних телефонів та програмного забезпечення з метою отримання фактичних даних.

РОЗДІЛ 8
ЄДИНА ІНФОРМАЦІЙНА СИСТЕМА МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ: СТРУКТУРА, ЗАГАЛЬНІ ЗАСАДИ ФУНКЦІОНУВАННЯ, ПОРЯДОК ЇЇ ФОРМУВАННЯ ТА ВИКОРИСТАННЯ

1. Загальні питання.

2. Мета, завдання та функції єдиної інформаційної системи МВС України.

3. Структура єдиної інформаційної системи МВС України.

4. Загальні засади функціонування та використання єдиної інформаційної системи МВС України.

5. Повноваження власника, служби та адміністратора єдиної інформаційної системи МВС України.

6. Обліки МВС України.

1. ЗАГАЛЬНІ ПИТАННЯ

Єдина інформаційна система Міністерства внутрішніх справ України (далі – єдина інформаційна система МВС України) – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку й супроводження їхньої діяльності та становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних і технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію.

Функціональні підсистеми єдиної інформаційної системи МВС України – це сукупність технічних засобів та програмних комплексів,

які автоматизують службові процеси суб'єктів єдиної інформаційної системи МВС України до рівня стандартів операційних процедур та автоматизованого робочого місця користувача, забезпечують формування, зберігання, спільне використання і верифікацію інформаційних ресурсів єдиної інформаційної системи МВС України.

Суб'єкти єдиної інформаційної системи МВС України – апарат МВС України та його територіальні органи з надання сервісних послуг МВС України, Національна гвардія, заклади, установи і підприємства, що належать до сфери управління МВС України (далі – система МВС України), центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ, інші державні органи, які обробляють інформацію в єдиній інформаційній системі МВС України для реалізації своїх повноважень.

Інформаційні ресурси єдиної інформаційної системи МВС України – визначені групи взаємозв'язаних задокументованих одиниць інформації, які формуються і об'єднуються в автоматизованих інформаційних системах суб'єктів єдиної інформаційної системи МВС України за певними ознаками, у тому числі зазначених у переліку пріоритетних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ, затвердженому Постановою Кабінету Міністрів України від 14 листопада 2018 р. № 1024.

Інтеграція інформаційних ресурсів єдиної інформаційної системи МВС України – комплекс методів та процедур, спрямованих на логічне функціональне об'єднання інформаційних ресурсів єдиної інформаційної системи МВС України у визначених форматах, за узгодженими показниками, для їх автоматизованої обробки, використання та надання користувачам в уніфікованому вигляді.

Користувачі єдиної інформаційної системи МВС України – фізичні особи та уповноважені посадові особи суб'єктів єдиної інформаційної системи МВС України, яким в установленому порядку надано відповідні права доступу до інформації в єдиній інформаційній системі МВС України.

Сервіс єдиної інформаційної системи МВС України – спеціальний програмний засіб, що забезпечує доступ користувачів єдиної

інформаційної системи МВС України до інформаційних ресурсів єдиної інформаційної системи МВС України.

Згідно з Постановою Кабінету Міністрів України від 14.11.2018 р. № 1024 «Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів» (пропоную додати) власником і розпорядником єдиної інформаційної системи МВС України є держава в особі МВС України.

Володільцем інформації, що обробляється в центральній підсистемі єдиної інформаційної системи МВС України, є саме Міністерство внутрішніх справ.

Володільцями інформації, що обробляється у функціональних підсистемах єдиної інформаційної системи МВС України, є відповідні суб'єкти єдиної інформаційної системи МВС України, які забезпечують захист інформації від випадкової втрати або знищення, незаконної обробки та незаконного доступу до інформації.

Мета обробки інформації у функціональних підсистемах єдиної інформаційної системи МВС України установлюється нормативно-правовими актами, які регулюють діяльність відповідних суб'єктів єдиної інформаційної системи МВС України, окремо для кожного визначеного пріоритетного інформаційного ресурсу.

МВС України визначає структурний підрозділ апарату Міністерства, який забезпечує реалізацію пріоритетних напрямів інформатизації системи МВС України та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ (далі – служба єдиної інформаційної системи МВС).

Адміністратором єдиної інформаційної системи МВС України є державне підприємство, яке належить до сфери управління МВС України.

2. МЕТА, ЗАВДАННЯ ТА ФУНКЦІЇ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС УКРАЇНИ

Єдина інформаційна система МВС України функціонує з метою оптимізації інформаційної взаємодії суб'єктів єдиної інформаційної системи МВС України на рівні загальнодержавних інформаційних ресурсів в інтересах національної безпеки, захисту прав та законних інтересів громадян, суспільства і держави у сферах:

- забезпечення охорони прав і свобод людини, інтересів суспільства та держави, протидії злочинності, підтримання публічної безпеки та порядку;
- захисту державного кордону й охорони суверенних прав України в її виключній (морській) економічній зоні;
- цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;
- міграції (імміграції та еміграції), зокрема протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Завданнями єдиної інформаційної системи МВС України є:

- створення єдиного інформаційного простору системи МВС України та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ шляхом логічного об'єднання їх інформаційних ресурсів, оптимізація процесів спільного використання технічних та програмних ресурсів;
- інформаційна підтримка діяльності суб'єктів єдиної інформаційної системи МВС України під час виконання завдань та функцій, покладених на них законодавством, з метою підвищення її ефективності;
- створення умов для електронної взаємодії суб'єктів єдиної інформаційної системи МВС України з метою оперативного

виконання завдань, покладених на них законодавством, зменшення часових та фінансових витрат на адміністративно-управлінські, інформаційно-пошукові, розрахункові та аналітичні роботи, формування звітності;
- забезпечення інформаційної взаємодії з державними органами, органами місцевого самоврядування, міжнародними організаціями, суб'єктами господарювання та правоохоронними органами інших держав, у тому числі з використанням загальнодержавних інформаційно-телекомунікаційних систем, а саме системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» та інтегрованої системи електронної ідентифікації.

Функціями єдиної інформаційної системи МВС України є:
- інтеграція інформаційних ресурсів єдиної інформаційної системи МВС України;
- обробка інформації, що формується у процесі діяльності суб'єктів єдиної інформаційної системи МВС України;
- перевірка своєчасності внесення, достовірності та повноти інформації, яка відповідно до законодавства обробляється суб'єктами єдиної інформаційної системи МВС України;
- систематизація та узагальнення інформації, перетворення її на формат, придатний для проведення подальшого аналізу та забезпечення роботи автоматизованих підсистем підтримки прийняття рішень, сигнальних та контрольних сервісів;
- автоматизація та верифікація процесів інформаційної діяльності суб'єктів єдиної інформаційної системи МВС України в інтерактивному режимі реального часу;
- забезпечення електронної інформаційної взаємодії та електронного документообігу між суб'єктами єдиної інформаційної системи МВС України;
- розмежування прав доступу та надання контрольованого доступу користувачам єдиної інформаційної системи МВС України до інформаційних ресурсів єдиної інформаційної системи МВС України;
- забезпечення резервного копіювання, зберігання та комплексного захисту інформації, що міститься в інформаційних ресурсах єдиної інформаційної системи МВС України.

3. СТРУКТУРА ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС УКРАЇНИ

Єдина інформаційна система МВС України складається з:

1) центральної підсистеми;

2) функціональних підсистем;

3) транспортної мережі передачі даних;

4) центрів обробки даних, телекомунікаційних мереж суб'єктів єдиної інформаційної системи МВС України;

5) комплексних систем захисту інформації підсистем єдиної інформаційної системи МВС України з підтвердженою в установленому законодавством порядку відповідністю.

Центральна підсистема єдиної інформаційної системи МВС України – обчислювальне середовище функціонування автоматизованих сервісів, яке забезпечує безперервність їх обслуговування в інтерактивному режимі реального часу та високий рівень продуктивності.

Центральна підсистема єдиної інформаційної системи МВС України функціонує в основному та резервному центрах обробки даних, які забезпечують середовище для її роботи.

До складу центральної підсистеми єдиної інформаційної системи МВС України належать:
- центральне сховище даних – програмно-технічний комплекс, який складається із серверів баз даних та програмного забезпечення, призначених для безперервної обробки та зберігання інформації, ведення та зберігання системних журналів аудиту роботи користувачів єдиної інформаційної системи МВС України, системних журналів реєстрації роботи програмних засобів і журналів аудиту засобів безпеки;
- центральний сервер обробки даних – програмно-технічний комплекс, який складається з основного та резервних серверів, баз даних, програмного забезпечення, призначених для безперервного виконання операцій з інформаційного обміну між центральним сховищем даних та суб'єктами і користувачами єдиної інформаційної системи МВС України, записування

та зберігання системних журналів аудиту приймання-передачі інформації;
- сервери додатків – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для безперервного функціонування програмних засобів обробки інформації в інтерактивному режимі реального часу, архівування та синхронізації інформації, записування та зберігання системних журналів аудиту приймання-передачі інформації, реєстрації роботи програмних засобів і журналів аудиту засобів безпеки;
- шлюзові сервери – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для забезпечення захисту інформації під час її приймання та передавання до центрального сховища даних, а також для запобігання можливості блокування доступу до програмно-апаратних ресурсів єдиної інформаційної системи МВС України;
- інші сервери та телекомунікаційне обладнання, які можуть використовуватися в разі розширення завдань та функцій єдиної інформаційної системи МВС України у процесі її роботи;
- автоматизовані робочі місця користувачів центральної підсистеми єдиної інформаційної системи МВС України – робочі місця, обладнані програмно-технічними засобами доступу до відповідних програмно-інформаційних комплексів функціональних підсистем єдиної інформаційної системи МВС України, призначені для забезпечення користувачам можливості обробляти інформацію відповідно до наданих прав;
- автоматизовані робочі місця адміністраторів центральної підсистеми єдиної інформаційної системи МВС України – робочі місця, обладнані технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних засобів, аналізу порушень у роботі єдиної інформаційної системи МВС України, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів центральної підсистеми єдиної інформаційної системи МВС України;

- автоматизовані робочі місця адміністраторів безпеки єдиної інформаційної системи МВС України.

Функціональними підсистемами єдиної інформаційної системи МВС України є:
- національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства;
- інформаційний портал Національної поліції України;
- Єдиний державний реєстр транспортних засобів;
- Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху;
- система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі;
- система екстреної допомоги населенню за єдиним телефонним номером 112;
- інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон;
- інформаційно-телекомунікаційна система прикордонного контролю «Гарт-1»;
- інші системи, реєстри та бази (банки) даних, створені суб'єктами єдиної інформаційної системи МВС України в межах реалізації владних повноважень.

Структура та порядок роботи функціональних підсистем єдиної інформаційної системи МВС України визначаються положеннями про ці підсистеми, які розробляються суб'єктами єдиної інформаційної системи МВС України з урахуванням затвердженого МВС України Типового положення про функціональну підсистему єдиної інформаційної системи МВС України та затверджуються в установленому законодавством порядку.

Транспортна мережа передачі даних – це універсальна мережа, що реалізує функції транспортування / комутації та об'єднує окремі мережі доступу із забезпеченням транзиту трафіку між ними високошвидкісними каналами.

Комплексні системи захисту інформації забезпечують захист інформації в підсистемах єдиної інформаційної системи МВС України через

здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого ознайомлення з нею та/або її модифікації.

4. ЗАГАЛЬНІ ЗАСАДИ ФУНКЦІОНУВАННЯ ТА ВИКОРИСТАННЯ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС УКРАЇНИ

Для забезпечення належного функціонування єдиної інформаційної системи МВС України власник системи розробляє та видає відповідні нормативно-правові акти, а суб'єкти цієї системи забезпечують своєчасне: внесення до єдиної інформаційної системи МВС України достовірної та повної інформації;

- надання / позбавлення доступу користувачам єдиної інформаційної системи МВС України до функціональних підсистем відповідно до законодавства;
- інформування адміністратора єдиної інформаційної системи МВС України про проблеми, що виникають під час функціонування єдиної інформаційної системи МВС України.

Доступ до відкритої інформації єдиної інформаційної системи МВС України реалізується через сервіси на офіційних вебсайтах суб'єктів єдиної інформаційної системи МВС України без електронної ідентифікації особи.

Доступ фізичної особи до інформації про себе, що обробляється в єдиній інформаційній системі МВС України, здійснюється з використанням засобів електронної ідентифікації особи, що відповідають вимогам законодавства.

Доступ уповноважених працівників до сервісів єдиної інформаційної системи МВС України здійснюється з використанням засобів електронної ідентифікації, що відповідають вимогам законодавства, у межах реалізації своїх повноважень.

Користувачі єдиної інформаційної системи МВС України зобов'язані дотримуватися визначеного МВС України порядку роботи з інформаційними

ресурсами єдиної інформаційної системи МВС України та використовувати отриману інформацію відповідно до законодавства.

Інформаційні ресурси єдиної інформаційної системи МВС України, що створені в системі МВС України, зберігаються в центральній підсистемі єдиної інформаційної системи МВС України, а інформаційні ресурси інших суб'єктів єдиної інформаційної системи МВС України – у центрах обробки даних відповідних суб'єктів єдиної інформаційної системи МВС України.

Інформація, що обробляється в єдиній інформаційній системі МВС України, може бути змінена засобами функціональних підсистем єдиної інформаційної системи МВС України уповноваженим працівником суб'єкта єдиної інформаційної системи МВС України лише у випадках, передбачених положеннями про функціональні підсистеми єдиної інформаційної системи МВС України.

Строки зберігання інформації, порядок видалення та знищення інформації в єдиній інформаційній системі МВС України визначаються положеннями про відповідні функціональні підсистеми єдиної інформаційної системи МВС України з урахуванням вимог законодавства.

5. ПОВНОВАЖЕННЯ ВЛАСНИКА, СЛУЖБИ ТА АДМІНІСТРАТОРА ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС УКРАЇНИ

МВС України здійснює організаційне забезпечення функціонування єдиної інформаційної системи МВС України, а також визначає права і обов'язки персоналу служби та адміністратора єдиної інформаційної системи МВС України.

Служба єдиної інформаційної системи МВС України:

- здійснює методичне та методологічне забезпечення функціонування єдиної інформаційної системи МВС України;
- контролює процес (щоб уникнути повтору) дотримання суб'єктами єдиної інформаційної системи МВС України вимог законодавства щодо використання інформаційних ресурсів єдиної інформаційної системи МВС України;

- проводить аналіз структури та змісту інформаційних ресурсів єдиної інформаційної системи МВС України з метою підвищення рівня інформаційної взаємодії її суб'єктів;
- забезпечує інтеграцію інформаційних ресурсів єдиної інформаційної системи МВС України;
- визначає механізми інформаційного обміну, забезпечує розроблення та впровадження регламенту електронної взаємодії суб'єктів єдиної інформаційної системи МВС України;
- забезпечує взаємодію єдиної інформаційної системи МВС України з іншими інформаційними системами, реєстрами та базами (банками) даних;
- проводить перевірку стосовно повноти та актуальності інформаційних ресурсів єдиної інформаційної системи МВС України, вживає заходів щодо усунення виявлених порушень;
- здійснює систематичний моніторинг та проводить аналіз ефективності функціонування єдиної інформаційної системи МВС України.

Адміністратор єдиної інформаційної системи МВС України повинен (пропоную додати):

1) забезпечувати:
- адміністрування, технічну підтримку та безперебійне функціонування центральної підсистеми єдиної інформаційної системи МВС України;
- розроблення програмного забезпечення центральної підсистеми єдиної інформаційної системи МВС України;
- електронну інформаційну взаємодію суб'єктів єдиної інформаційної системи МВС України;
- розроблення та здійснення заходів щодо захисту єдиної інформаційної системи МВС України та інформації, що міститься в ній;
- гарантоване збереження інформації, що міститься в єдиній інформаційній системі МВС України;

2) здійснювати:
- постійний моніторинг технічного стану єдиної інформаційної системи МВС та захищеності інформації, що міститься в ній;

- впровадження механізмів електронної ідентифікації особи, зокрема для доступу до інформаційних ресурсів єдиної інформаційної системи МВС України;
- надання доступу користувачам єдиної інформаційної системи МВС України до інформаційних ресурсів єдиної інформаційної системи МВС України;
- надання / позбавлення доступу користувачам єдиної інформаційної системи МВС України до центральної підсистеми відповідно до законодавства;
- ведення обліку користувачів єдиної інформаційної системи МВС України, яким надано доступ до інформаційних ресурсів єдиної інформаційної системи МВС України з використанням засобів електронної ідентифікації особи, з фіксуванням відомостей про дату і час отримання доступу, обсяг інформації, до якої отримано доступ;
- технічну та інформаційну підтримку користувачів єдиної інформаційної системи МВС України, зокрема за допомогою відкритих вебресурсів, телефонного інформаційного центру тощо;

3) проводить навчання користувачів суб'єктів єдиної інформаційної системи МВС України під час її впровадження та функціонування.

6. ОБЛІКИ МВС УКРАЇНИ

Стаття 25 Закону України «Про Національну Поліцію» регламентує повноваження поліції у сфері інформаційно-аналітичного забезпечення, а саме поліція в межах інформаційно-аналітичної діяльності формує бази (банки) даних, що належать до єдиної інформаційної системи Міністерства внутрішніх справ України; користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; виконує інформаційно-пошукову та інформаційно-аналітичну роботу; здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

Формування інформаційних ресурсів регламентує стаття 26 Закону України «Про Національну Поліцію»:

1. Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно:

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;

3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;

4) розшуку осіб, зниклих безвісти;

5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;

6) зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;

7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);

8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;

9) зареєстрованих кримінальних та адміністративних правопорушень, пов'язаних з корупцією, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;

10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;

11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;

12) викрадених (втрачених) документів за зверненням громадян;

13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;

14) викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;

15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;

16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;

17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;

18) бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону.

2. Під час наповнення баз (банків) даних, визначених у пункті 7 частини першої цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК).

Стаття 27 Закону України «Про Національну Поліцію» регламентує використання поліцією інформаційних ресурсів, а саме поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних».

Інтегрована інформаційно-пошукова система (далі – ІІПС) органів Національної поліції України (далі – НП України) створена з метою об'єднання наявних в органах та підрозділах системи МВС України інформаційних ресурсів в єдиний інформаційно-аналітичний комплекс із використанням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання для підтримки оперативно-службової діяльності органів і підрозділів НП України та значного зміцнення їхньої спроможності щодо протидії та профілактиці злочинності.

ІІПС має трирівневу ієрархічну структуру, що відповідає організаційній побудові органів НП України: *перший рівень* – центральний вузол (банк даних) ІІПС, який розташовано в спеціально виділених службових приміщеннях Департаменту інформаційно-аналітичного забезпечення МВС України; *другий рівень* – регіональні (обласні) банки даних ІІПС, які розміщено (щоб уникнути повтору) в спеціально виділених службових

приміщеннях управлінь (відділів) інформаційно-аналітичного забезпечення; *третій рівень* – територіальний вузол ІІПС, який розміщується і функціонує безпосередньо в міських, районних управліннях (відділах).

Інтегрована інформаційно-пошукова система у своїй структурі має такі бази даних:

Інформаційна підсистема (далі – ІП) «Факт» – база даних, у якій обліковуються відомості про події, кримінальні та адміністративні правопорушення, надзвичайні події, зазначені в заявах (повідомлення, рапорти), що зареєстровані в чергових частинах НП України.

ІП «Доставлені» – база даних, у якій обліковуються особи, затримані та доставлені до органу НП України для встановлення їх особистості та з'ясування обставин учиненого правопорушення.

ІП «Особа» – база даних, у якій обліковуються особи, які вчиняють протиправні діяння, становлять групу ризику, стосовно яких здійснюється профілактична робота.

ІП «Угон» – база даних, у якій обліковуються відомості про транспортні засоби (автомобілі, мотоцикли, мопеди, плавзасоби), які розшукуються органами внутрішніх справ, правоохоронними органами держав-учасниць СНД.

ІП «Розшук» та «Пізнання» – бази даних, у яких обліковуються підозрювані, обвинувачені та підсудні, що переховуються від органів досудового слідства, слідчого судді та суду; засуджені до покарання у вигляді позбавлення волі, які ухиляються від відбування кримінального покарання; безвісти зниклі особи; невпізнані трупи; невідомі хворі та діти, які не можуть повідомити інформацію про себе; особи, які переховуються від правоохоронних органів інших країн, країн-членів Інтерпола;

ІП «Річ» – база обліку речей, викрадених, вилучених у громадян (належність яких не встановлена) з ознаками підроблення, заборонених або обмежених у цивільному обігу, знайдених або вилучених з камер схову вокзалів, портів, аеропортів та зданих до органів НП України. База даних «Річ» складається з підсистем «Номерна річ», «Антикваріат».

ІП «Зареєстрована зброя» – база даних, що містить інформацію про вогнепальну та холодну зброю, яка легально використовується фізичними та юридичними особами та зареєстрована в дозвільній системі органів НП України.

ІП «Кримінальна зброя» – база відомостей про зброю, викрадену, утрачену, знайдену, здану до органів Національної поліції України, вилучену працівниками органів Національної поліції з кількості тієї, що незаконно зберігалася, незалежно від її технічного стану, що має індивідуальні заводські (фабричні) номери або номери деталей.

ІП «Адміністративне правопорушення» – база даних, у якій обліковуються відомості про зареєстровані адміністративні правопорушення, за матеріалами яких уповноваженими на те працівниками поліції складено протоколи про адміністративні правопорушення.

ІП «Мігрант» – база даних, у якій обліковується інформація про осіб, затриманих за порушення законодавства України про державний кордон, про правовий статус іноземців та осіб без громадянства.

ІП «Корупція» – база даних, у якій обліковуються відомості про зареєстровані корупційні правопорушення, за матеріалами яких уповноваженими працівниками органів Національної поліції у сфері протидії корупції складено протоколи про вчинення корупційних правопорушень, а осіб, які вчинили ці правопорушення, рішеннями судів притягнуто до відповідальності за корупційні правопорушення.

Криміналістичні обліки створюються з метою їх використання для запобігання, виявлення, розкриття і розслідування злочинів та інших правопорушень під час здійснення оперативно-розшукової діяльності й досудового розслідування, а також підвищення рівня інформаційного забезпечення проведення експертних досліджень.

Джерелами формування криміналістичних обліків є об'єкти (їх копії, зображення) та (або) відомості про них, що надходять з органів досудового розслідування, прокуратури, судів, підрозділів, які відповідно до чинного законодавства мають право здійснювати оперативно-розшукову діяльність, з Міністерства охорони здоров'я України, Міністерства юстиції України, інших органів виконавчої влади, а також Національного банку України.

Система криміналістичного обліку має різні види і охоплює:

1) трасологічний облік;
2) дактилоскопічний облік;
3) балістичний облік;
4) облік холодної зброї;

5) облік грошових знаків, бланків документів, цінних паперів та пластикових платіжних карток;

6) облік осіб за ознаками зовнішності;

7) вибухотехнічний облік;

8) пожежно-технічний облік;

9) облік наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів;

10) облік генетичних ознак людини;

11) облік записів голосів та мовлення осіб;

12) облік ідентифікаційних позначень транспортних засобів та реквізитів документів (підписів, печаток, штампів);

13) облік матеріалів, речовин та виробів.

Залежно від вирішуваних завдань криміналістичні обліки поділяються на оперативно-пошукові та інформаційно-довідкові, а залежно від рівня концентрації інформації – на центральні, обласні (регіональні) та місцеві.

Оперативні обліки призначені для отримання інформації про особу, яка причетна до вчинення злочину; ідентифікації особи, знаряддя злочину (транспортного засобу, зброї, обладнання тощо, які використовувалися під час учинення злочину); установлення спільної родової (групової) належності матеріалів та речовин; інших фактичних даних, які свідчать про вчинення злочинів конкретною особою; отримання іншої інформації щодо вчинених злочинів та запобігання їм.

Ці обліки (колекції) формуються з об'єктів (їх копій, зображень) та (або) відомостей про них, вилучених або отриманих, як правило, під час огляду місця події, проведення інших слідчих (розшукових) дій, оперативно-розшукових заходів тощо, а також отриманих під час криміналістичної реєстрації дактилокарт, фото- та відеозображень, записів голосів і мовлення осіб, ДНК-профілів. До них належать: дактилоскопічні обліки, колекції слідів злому, взуття, транспортних засобів, волокон, замків і ключів, підроблених рецептів і бланків документів, кулегільзотеки, колекції суб'єктивних портретів та ін.

Розшукові обліки призначені для надання допомоги щодо:

1) встановлення місцезнаходження безвісти зниклих людей;

2) встановлення осіб, які втратили пам'ять;

3) пошуку мобільних телефонів;

4) розшуку тих, хто переховується від органів влади;

5) пошуку викрадених культурних цінностей;

6) пошуку паспорта громадянина України серед викрадених та втрачених;

7) перевірки транспортних засобів та зброї, які знаходяться у розшуку;

8) перевірки легітимності довідки про судимість.

ВИСНОВКИ

Єдина інформаційна система МВС України функціонує з метою оптимізації інформаційної взаємодії суб'єктів єдиної інформаційної системи МВС України на рівні загальнодержавних інформаційних ресурсів в інтересах національної безпеки, захисту прав та законних інтересів громадян, суспільства і держави у сферах:

- забезпечення охорони прав і свобод людини;
- захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні;
- цивільного захисту населення і територій;
- міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Єдина інформаційна система МВС України складається з:

1) центральної підсистеми;

2) функціональних підсистем;

3) транспортної мережі передачі даних;

4) центрів обробки даних, телекомунікаційних мереж суб'єктів єдиної інформаційної системи МВС України;

5) комплексних систем захисту інформації підсистем єдиної інформаційної системи МВС України з підтвердженою в установленому законодавством порядку відповідністю.

Система криміналістичного обліку має різні види і охоплює:

1) трасологічний облік;

2) дактилоскопічний облік;

3) балістичний облік;

4) облік холодної зброї;

5) облік грошових знаків, бланків документів, цінних паперів та пластикових платіжних карток;

6) облік осіб за ознаками зовнішності;

7) вибухотехнічний облік;

8) пожежно-технічний облік;

9) облік наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів;

10) облік генетичних ознак людини;

11) облік записів голосів та мовлення осіб;

12) облік ідентифікаційних позначень транспортних засобів та реквізитів документів (підписів, печаток, штампів);

13) облік матеріалів, речовин та виробів.

Розшукові обліки призначені для надання допомоги щодо:

1) встановлення місцезнаходження безвісти зниклих людей;

2) встановлення осіб, які втратили пам'ять;

3) пошуку мобільних телефонів;

4) розшуку тих, хто переховується від органів влади;

5) пошуку викрадених культурних цінностей;

6) пошуку паспорта громадянина України серед викрадених та втрачених;

7) перевірки транспортних засобів та зброї, які знаходяться у розшуку;

8) перевірки легітимності довідки про судимість.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР (дата оновлення: 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

3. Про Інформацію : Закон України від 02.10.1992 р. № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

4. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

5. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

6. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. Баженов В. А. Інформатика. Комп'ютерна техніка. Комп'ютерні технології : підручник. 4-те вид. К. : Каравела, 2012. 496 с.

8. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посібник. К. : КНЕУ, 2004. 307 с.

9. Макарова М. В. Інформатика та комп'ютерна техніка : навчальний посібник. 3-тє вид., переоб. і доп. Суми : ВДТ «Університетська книга», 2008. 665 с.

10. Маценко В. Г. Обчислювальна техніка та програмування : навчальний посібник. Чернівці : ЧНУ, 2010 112 с.

11. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте відповіді на запитання

1. Яка структура єдиної інформаційної системи МВС України?

2. Які загальні засади функціонування та використання єдиної інформаційної системи МВС України.?

2. Практині завдання

Завдяки інформації з відкритих реєстрів та баз даних державних органів України, знайти за допомогою інтернет-мережі певну інформацію.

1. Використавши єдину базу даних електронних адрес, номерів факсів суб'єктів владних повноважень, знайти: ЄДРПОУ, адресу електронної

пошти, номер факсу (телефаксу), поштову адресу, юридичну адресу Головного управління Національної поліції в Донецькій області. Зробити знімок екрана та вставити в документ Word.

2. Послуговуючися базою даних поштових індексів та відділень поштового зв'язку України, знайти поштові індекси всіх корпусів Донецького державного університету внутрішніх справ. Індекси скопіювати та додати в документ Word.

3. На сайті Єдиного державного реєстру судових рішень знайти номери та форми судових рішень, що стосуються судової справи за номером 263/14702/20. У чому полягає сутність цієї справи?

4. Використавши інформацію щодо судових експертів України, знайти судових експертів із прізвищем «Гостілова». Інформацію щодо наявних допусків вставте в документ Word.

5. Використавши інформацію з єдиного реєстру адвокатів України, знайти перелік адвокатів міста Маріуполя, що мають прізвище «Іванова».

6. Послуговуючися публічною кадастровою картою України, знайти місцерозташування ділянки з кадастровим номером 1412336600:01:007:0499 та визначити цільове призначення на цій ділянці.

7. Набравши на телефоні комбінацію *#06#, визначте IMEI свого мобільного та перевірте його в базі «Перевірка коду IMEI мобільних телефонів» МВС України.

3. Теми реферативних повідомлень

1. Специфіка інформаційних систем аналітичної обробки інформації.
2. Інформаційні війни в межах сучасних світових процесів: виклики та ризики.
3. Причини інформаційних війн з позиції глобалізаційних змін.
4. Особливості технологій ведення інформаційних війн.
5. Безпека України та інформаційні війни: стан та перспективи.
6. Проблеми захисту та збереження інтелектуальної власності.
7. Удосконалення інформаційної безпеки України.
8. Специфіка організації інформаційних послуг.

ЗАВДАННЯ ДЛЯ ТЕСТОВОГО КОНТРОЛЮ

1. Назва інформаційного підрозділу районного рівня МВС України:

а) відділення інформаційних технологій;
б) обчислювальний центр;
в) відділення обліку та реєстрації злочинів;
г) відділення інформаційно-аналітичного забезпечення.

2. Базовий рівень накопичення інформації в МВС України:

а) територіальний;
б) регіональний;
в) центральний;
г) міждержавний.

3. Первинне накопичення інформації в МВС України здійснюється на:

а) міждержавному рівні;
б) центральному рівні;
в) регіональному рівні;
г) територіальному рівні.

4. Основна мета системи інформаційного забезпечення МВС України:

а) збір, обробка та узагальнення оперативної інформації;
б) всебічна інформаційна підтримка діяльності МВС України у боротьбі зі злочинністю;
в) забезпечення захисту інформації;
г) забезпечення інформаційної взаємодії усіх підрозділів МВС України.

5. Загальними формами здійснення оперативно-розшукової діяльності органів Національної поліції України є:

а) оперативна розробка;
б) взаємодія з органами управління та населенням;
в) ведення криміналістичних та оперативних обліків;
г) усі відповіді правильні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальні питання криміналістики та судової експертизи : матеріали Всеукр. наук.-практ. конф. (Київ, 19 листоп. 2020 р.). Київ : Нац. акад. внутр. справ, 2020. 461 с.

2. Бараненко Р. В. Дослідження особливостей функціонування програмного забезпечення системи централізованого управління нарядами патрульної служби «ЦУНАМІ». *Юридичний бюлетень : наук. журн*. Випуск 2. Одеса, ОДУВС, 2016.

3. Безпечний онлайн шопінг – поради кіберполіції. URL. https://cyberpolice.gov.ua/article/bezpechnyj-onlajn-shoping---porady-kiberpolicziyi-5967/.

4. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. 256 с.

5. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

6. Великий тлумачний словник сучасної української мови. Донецьк : ТОВ «Глорія Трейд», 2012. 864 с.

7. Використання інформаційно-пошукових систем в діяльності поліції. Правові інформаційно-пошукові системи. URL. https://arm.naiau.kiev.ua/books/inform_tekhnolohii/lection/lec3.html.

8. Використання штучного інтелекту в кримінальній юстиції. URL. https://ua.112.ua/statji/maliuska-khoche-vykorystovuvaty-shtuchnyi-intelekt-u-kryminalnii-iustytsii-naskilky-tse-mozhlyvo-535538.html.

9. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія. Запоріжжя : ГУ «ЗІДМУ», 2003. 250 с.

10. Давидюк В. М. Інтернет, як соціальне середовище роботи з конфідентами. Актуальні питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків). МВС України, Харків. нац. ун-т внутр. справ; Координатор проєктів ОБСЄ в Україні. Харків : ХНУВС, 2018. 436 с.

11. Денисова О. О. Інформаційні системи і технології в юридичній діяльності. К. : КНЕУ, 2003. 315 с.

12. Державна служба фінансового моніторингу України. Кіберзлочинність та відмивання коштів URL: www.minfin.gov.ua/file/link/396800/file/tipolog2013.pdf.

13. Дубинський О. Ю. Судова експертиза як форма застосування спеціальних знань при розслідуванні злочинів, чинених з використанням комп`ютерних технологій. URL: http://eir.nuos.edu.ua/xmlui/bitstream/handle/123456789/2292/Dubinskyi.PDF?sequence=1&isAllowed=y.

14. Загальні рекомендації щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет від 04.06.2021 р. № 24719/22-2021. Міністерство та Комітет цифрової трансформації України.

15. Іванова В. Г. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посібник.4-те вид., змін. і доп. Х. : Право, 2014. 240 с.

16. Інструкція про призначення та проведення судових експертиз та експертних досліджень : затв. наказом Міністерства юстиції України від 08.10.1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

17. Шапошнікова І. В. Основні аспекти вибору типу і проведення експертизи у справах про кіберзлочинність. 2017. URL: https://yur-gazeta.com/publications/practice/inshe/osnovni-aspekti-viboru-tipu-i-provedennya-ekspertizi-u-spravah-pro-kiberzlochinnist.html.

18. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР (дата оновлення 01.01.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

19. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

20. Лазебний А. М., Бичок Т. П., Огляд місця події (правові, організаційні та техніко-криміналістичні проблеми). *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. № 1–2. С. 228–236. URL: file:///C:/Users/User/Downloads/muvnudp_2018_1-2_39.pdf.

21. Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : затв. наказом Міністерства юстиції України від 08.10.1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

22. Муляр Г. В., Ховпун О. С. Особливості доказування кіберзлочинів. *«Право. Людина. Довкілля»*. Том 10, № 3. 2019. С. 132–138. URL: file:///C:/Users/%D0%9D%D0%B0%D1%83%D1%87%D0%BD%D1%8B%D0%B9%20%D0%BE%D1%82%D0%B4%D0%B5%D0%BB/Downloads/12631-28679-1-PB.pdf.

23. Методичні рекомендації щодо користування Електронною системою фіксації поліцейськими результатів реагування на події. Службовий лист Національної поліції від 16.06.2017 № 6327.

24. Москаленко Д. Ю. Історія розвитку та сучасний стан інформаційного забезпечення правоохоронної діяльності. Інформаційні технології в освіті та практиці : матеріали Всеукраїнської науково-практичної конференції. Львівський державний університет внутрішніх справ. 2020. № 6. С. 102–103.

25. Павлиш Т. Г. Навчально-методичний посібник з дисципліни «Інформаційне забезпечення професійної діяльності (+ модуль правова статистика)» для студентів заочного відділення спеціальності 081 «Право». Кривий Ріг : Донецький юридичний інститут МВС України, 2020. 159 с.

26. Пефтієв О. В. Єдиний аналітичний сервісний центр Головного управління Національної поліції в Донецькій області. Актуальні питання забезпечення публічної безпеки, порядку в сучасних умовах: поліція та суспільство – стратегії розвитку і взаємодії : тези доп. Всеукр. наук.-практ. конф. (м. Маріуполь, 12 трав. 2018 р.). МВС України, ДВНЗ «Приазовський державний технічний університет». Маріуполь, 2018. С. 345–351.

27. Проблеми використання електронних доказів у протидії кіберзлочинності. 2020. URL: http://univd.edu.ua/general/publishing/konf/27_05_2020/pdf/26.pdf.

28. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14.11.2018 р. № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-п#Text.

29. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII (дата оновлення: 12.12.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

30. Про Національну програму інформатизації : Закон України від 04.02.1998 р. № 74/98-ВР (дата оновлення: 16.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text.

31. Про Інформацію : Закон України від 02.10.1992 р. № 2657-XII (дата оновлення: 16.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

32. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

33. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

34. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI (дата оновлення: 23.04.2021). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

35. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР (дата оновлення: 04.07.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

36. Про судову експертизу : Закон України від 25 лютого 1994 р. № 4038-XII (дата оновлення: 03.07.2020). URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text.

37. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV (дата оновлення: 24.10.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text.

38. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (дата оновлення: 07.11.2018). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

39. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII (дата оновлення: 13.02.2020). *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

40. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : Наказ Міністерства внутрішніх справ від 3.08.2017 р. № 676 (дата оновлення: 03.08.2017). URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

41. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса. 2020. 112 с.

42. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія. Одеса : ТЕС, 2020. 372 с.

43. Сезонова І. К. Інформатика для правоохоронців : навч. посіб МВС України, Харк. нац. ун-т внутр. справ, 2015. 182 с.

44. Спільний наказ ГПУ та МВС України «Порядок взаємодії ГПУ та МВС України щодо обміну інформацією з ЄРДР та інформаційних систем ОВС» від 17.11.2012 р. № 115/1046. URL: https://zakon.rada.gov.ua/laws/show/v0115900-12#Text.

45. Співаковський О. В., Шерман М. І., Стратонов В. М., Лапінський В. В. Інформаційні технології в юридичній діяльності: базовий курс : навчальний посібник. Херсон : ХДУ, 2012. 220 с.

46. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. 2017. URL: file:///C:/Users/User/Downloads/5aUExaN-edUw0w3RvChG7g3kV17pvRho.pdf

47. Тулінов В. С., Уткіна Г. А. Інформаційні технології : навчально-методичний посібник для студентів ден. та заоч. форми навчання спец. 081 «Право». Кривий Ріг : Донецький юридичний інститут МВС України, 2020. 161 с.

48. Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Національної академії внутрішніх справ. 2020. URL: https://ojs.naiau.kiev.ua/index.php/scientbul/article/view/1229/1232.

49. Шорохова Г. М. Проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України : матеріали шостої міжнародної науково-практичної конференції НАНР Економіко-правові виклики 2016 року (12 січня 2016 року). Львів : Національна академія наукового розвитку, 2016. Том 2. 202 с.

50. Шульга Б. С. Комп'ютерно-технічна експертиза: поняття, предмет, об'єкти, завдання. Особливості проведення огляду місця події при комп'ютерних злочинах, правила вилучення комп'ютерних засобів та їх упакування. Сучасні криміналістичні експертизи в розслідуванні злочинів. 2015. URL: http://elar.naiau.kiev.ua/bitstream/123456789/9141/1/СУЧАСНІ%20КРИМІНАЛІСТИЧНІ_p069-073.pdf.

ДОДАТОК 1

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС РОБОТИ В МЕРЕЖІ «ІНТЕРНЕТ»

1. Зберігання та передача даних

Недотримання окремих правил безпеки під час здійснення службових обов'язків працівниками органів виконавчої влади місцевого самоврядування, посадовими особами державних підприємств, установ, організацій може призвести до втрати чи крадіжки мобільних телефонів, персональних ноутбуків, магнітних носіїв інформації тощо. Указане ставить під загрозу збереження персональних даних та може призвести до розголошення інформації з обмеженим доступом.

Сприятливі умови для реалізації кіберзагроз виникають через порушення базових вимог законодавства про захист інформації в інформаційно-телекомунікаційних системах (далі – ІТС), а також унаслідок таких чинників:

- здійснення несанкціонованого доступу до баз даних;
- копіювання та передача через незахищений канал мережі «Інтернет» документальних матеріалів, що містять службову інформацію;
- використання особистих технічних засобів у складі виробничих автоматизованих систем (USB-флеш-накопичувачі);
- підключення до комп'ютерних систем технічних засобів із модулями передачі даних (Bluetooth, GSM тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;
- незахищеність ІТС за допомогою актуальних версій антивірусного програмного забезпечення.

З метою уникнення негативних наслідків у разі втрати або викрадення носіїв інформації необхідно:

- встановити паролі на всі пристрої, що перебувають у користуванні, а також паролі / коди на доступ до всіх облікових записів;
- систематично здійснювати резервне копіювання важливих файлів;
- блокувати пристрої щоразу після закінчення роботи з ними.

2. Соціальні мережі

З метою уникнення несанкціонованого доступу до персональних акаунтів, зареєстрованих у соціально-орієнтованих ресурсах мережі «Інтернет», необхідно:

- встановити надійний пароль для входу в обліковий запис. До того ж рівень захищеності акаунта та інформації, яка в ньому міститься, залежить від складності встановленого пароля;
- використовувати функцію подвійної авторизації. Щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника акаунта. На вказаний номер телефону чи на поштову скриньку буде надіслано повідомлення з кодом підтвердження або необхідно буде ввести один із паролів, які попередньо були збережені через інший обраний спосіб підтвердження;
- здійснити додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованого доступу до ресурсів з невідомого пристрою або інтернет-браузера;
- під час створення акаунтів у соціальних мережах використовувати у якості логіна поштову адресу надійного сервісу (наприклад «Google», «Yahoo») або українських поштових сервісів. Не рекомендується користуватися російськими сервісами;
- не здійснювати авторизацію особистих чи робочих, корпоративних профілів з незнайомих чи незахищених пристроїв. Існує імовірність, що після завершення роботи не буде здійснено вихід із облікового запису або пристрій запам'ятає вказаний під час входу логін та пароль. Крім того, існує імовірність ураження такого пристрою шкідливим програмним забезпеченням, що

може збирати та передавати відомості щодо паролів та логінів зацікавленим особам;

– не відкривати вкладень у підозрілих повідомленнях від адресатів, щодо яких виникають сумнів;

• пам'ятайте, що саме фішинг (*фішинг – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі «Інтернет» персональних даних клієнтів, сервісів із переказу або обміну валюти, інтернет-магазинів*) є найпоширенішим способом отримання зловмисниками паролів до поштових скриньок та сторінок у соціальних мережах.

Також варто враховувати, що під час гібридної агресії з боку Російської Федерації соціальні мережі активно використовуються для збору додаткових відомостей щодо місць регулярного перебування особи, її родичів, колег, особистих уподобань та іншої приватної інформації.

З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації стосовно особи, членів її сім'ї, колег рекомендується:

• не публікувати в соціальних мережах інформацію, що може загрожувати особистому життю особи, життю членів її сім'ї та інших осіб;

– обмежити доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі. Обрати налаштування, які найбільше захищають додаткові відомості про власника акаунта. Зокрема, не зазначати геолокацію (місце розташування);

– періодично переглядати список «друзів» у соціальній мережі. Якщо серед них є незнайомі або підозрілі акаунти, необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. Надалі необхідно бути уважними під час додавання до списку «друзів» нових користувачів;

– не використовувати російські соціальні мережі «Вконтакте» та «Одноклассники», а також російські пошукові системи «Mail.ru» та «Yandex» (у т. ч. із застосуванням сервісів VPN), доступ до яких обмежено згідно з Указом Президента України № 184/2020, оскільки відповідно до федеральних законів

Російської Федерації власники вказаних ресурсів можуть передавати російським спецслужбам відомості щодо персональних даних користувачів акаунтів (e-mail, номер мобільного телефону, дата та IP-адреса реєстрації, дата та IP-адреса останнього відвідування тощо).

Слід зазначити, що за розповсюдження через соцмережі матеріалів із закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України, передбачена кримінальна відповідальність,

Також варто звернути увагу на те, що окремі публікації, розміщені посадовими особами органів виконавчої влади на їх персональних сторінках у соціальних мережах, можуть слугувати інформаційним приводом, який у подальшому буде використаний для зниження рівня авторитету державної влади в цілому, штучного загострення суспільно-політичної ситуації в державі та здійснення інших деструктивних дій на шкоду державним інтересам України.

3. Використання додатків до смартфонів

Під час встановлення тих чи інших додатків на власний телефон ці програмні продукти можуть вимагати доступу до певної інформації на використовуваному пристрої, насамперед геолокації, списку контактів, акаунтів у соціальних мережах та поштових скриньок.

За наявними даними більшість шпигунських програм додають саме в мобільні додатки, які цікавлять конкретну аудиторію. Тому необхідно бути уважним під час встановлення додатків, особливо якщо робити це з невідомих та неперевірених сервісів.

З метою унеможливлення завантаження на особистий пристрій програм-шпигунів необхідно дотримуватися таких правил:

• встановлювати додатки лише офіційних та перевірених сервісів («Chrome Store», «Google Play Store» для Android, «App Store» для iOS);

• заборонити операційній системі смартфона автоматично встановлювати додатки з невідомих джерел, обравши відповідні налаштування пристрою;

- періодично здійснювати видалення усіх додатків, які не використовуються.

4. Електронне листування

Щоб уникнути зламу електронної поштової скриньки, необхідно:

- увімкнути двофакторну автентифікацію за допомогою мобільного пристрою. У такому разі під час спроби отримання паролю до поштової скриньки сторонніми особами буде надходити попередження на мобільний телефон у вигляді SMS-повідомлення про спробу зламу;
- встановити надійний пароль;
- не використовувати для відновлення пароля російські сервіси («Yandex.ru», «Mail.ru» тощо);
- не запускати на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.bat», «.cmd», «.vbs», «.doct», «.xlst» тощо;
- державні службовці повинні пам'ятати, що службові електронні скриньки не слід використовувати для приватного листування.

5. Доступ до мережі «Інтернет»

Одним із найпоширеніших способів доступу до мережі «Інтернет» у публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони є безплатними та доступ до них здійснюється без введення паролів. Саме відсутність пароля робить їх вразливішими для зламу зацікавленими особами, які мають на меті отримати персональні дані та відомості, що зберігаються на телефоні, планшеті тощо.

Щоб уникнути перехоплення даних сторонніми особами, необхідно:

- під час здійснення доступу до інтернет-мережі використовувати лише ті точки Wi-Fi, які мають протоколи безпеки для захисту безпровідного з'єднання WPA и WPA-2;
- у публічних місцях найкраще користуватися особистим Wi-Fi модемом або здійснювати достут до мережі «Інтернет» з мобільного пристрою за передплаченим пакетом послуг мобільного оператора;
- на мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi».

Рекомендації посадовій особі органу виконавчої влади:

- пресслужбам державних органів під час суспільно-політичних подій в країні необхідно надавати коментарі та роз'яснення рішень для того, щоб уникнути інтерпретацій та спотворень інформації у процесі обговорення тієї чи іншої ситуації в загальнодоступних та соціально-орієнтованих ресурсах мережі «Інтернет»;
- державним органам, установам необхідно розробити та затвердити чіткий план дій для оприлюднення представниками їхніх пресслужб інформації у разі виникнення резонансних інцидентів;
- офіційні представники органів державної влади повинні оприлюднювати суспільно значущу інформацію, якщо вона не належить до тієї категорії, що не підлягає оприлюдненню. Не варто забувати, що приховування такої інформації від суспільства може знизити рівень (пропоную додати) довіри до них;
- представникам органів державної влади під час надання коментарів, інтерв'ю, брифінгів не рекомендується використовувати оціночні судження, що можуть призвести до неоднозначного тлумачення наданої інформації її споживачами;
- органам державної влади необхідно розробити правила використання офіційних сторінок та акаунтів у соціальних мережах для уникнення непорозумінь з користувачами та окреслення формату комунікації через соціальні мережі. Крім того, вважається за доцільне здійснити верифікацію офіційних представництв органів державної влади та установ, які у своїй діяльності використовують акаунти в соціальних мережах, насамперед «Facebook», «Twitter» та канали у відеохостингу «Youtube»;
- держслужбовцям, а також іншим особам, які відповідно до своїх функціональних обов'язків працюють з інформацією з обмеженим доступом, необхідно пам'ятати, що у процесі оформлення допуску до державної таємниці під час заповнення відповідних анкет вони повинні вносити достовірні дані про свої контакти з іноземними громадянами, наявність власних елктроних скриньок, сайтів, профілів у соціальних мережах та тематичних форумах.

ДОДАТОК 2

НОРМАТИВНО-ПРАВОВІ ДОКУМЕНТИ (ВИТЯГИ)

КОНСТИТУЦІЯ УКРАЇНИ

(Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141)

Стаття 17. Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

(Зі змінами та доповненнями станом на 2021 рік)

Розділ XVI
КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Примітка. Значною шкодою у статтях 361–363^{-1}, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 361^1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк до п'яти років.

Стаття 361^2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від двох до п'яти років.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363[1]. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

ЗАКОН УКРАЇНИ
ПРО НАЦІОНАЛЬНУ ПРОГРАМУ ІНФОРМАТИЗАЦІЇ

(Відомості Верховної Ради України (ВВР), 1998, № 27–28, ст. 181)

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Основні терміни та поняття

У цьому Законі наведені нижче терміни та поняття вживаються у такому значенні:

база даних – іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області;

база знань – масив інформації у формі, придатній до логічної і смислової обробки відповідними програмними засобами;

засоби інформатизації – електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій;

інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами;

інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

інформаційний суверенітет держави – здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави;

локалізація програмних продуктів – приведення програмних продуктів, які використовуються в Україні, у відповідність із законами України та іншими нормативно-правовими актами, нормами і правилами, що діють в Україні;

нерезиденти – юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням за межами України, які створені й діють відповідно до законодавства іноземної держави, у тому числі юридичні особи та інші суб'єкти підприємницької діяльності, створені за участю юридичних і фізичних осіб;

окреме завдання – комплекс проєктів інформатизації, взаємопов'язаних і взаємопогоджених за термінами реалізації, складом виконавців та спрямованих на досягнення конкретних цілей;

проєкт інформатизації – комплекс взаємопов'язаних заходів, як правило, інвестиційного характеру, що узгоджені за часом, використанням певних матеріально-технічних, інформаційних, людських, фінансових та інших ресурсів і мають на меті створення заздалегідь визначених інформаційних і телекомунікаційних систем, засобів інформатизації та інформаційних ресурсів, які відповідають певним показникам якості;

резиденти – юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням на території України, які здійснюють свою діяльність відповідно до законодавства України.

ЗАКОН УКРАЇНИ ПРО ІНФОРМАЦІЮ

(Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650)

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

суб'єкт владних повноважень – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Розділ II
ВИДИ ІНФОРМАЦІЇ

Стаття 10. Види інформації за змістом

За змістом інформація поділяється на такі види:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- інші види інформації.

Стаття 11. Інформація про фізичну особу

1. Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення повноважень щодо верифікації та моніторингу державних виплат не потребує згоди фізичних осіб на отримання та обробку персональних даних.

Стаття 12. Інформація довідково-енциклопедичного характеру

1. Інформація довідково-енциклопедичного характеру – систематизовані, документовані, публічно оголошені або іншим чином

поширені відомості про суспільне, державне життя та навколишнє природне середовище.

2. Основними джерелами інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-телекомунікаційними системами.

3. Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 13. Інформація про стан довкілля (екологічна інформація)

1. Інформація про стан довкілля (екологічна інформація) – відомості та/або дані про:

стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;

фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);

стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;

інші відомості та/або дані.

2. Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Стаття 14. Інформація про товар (роботу, послугу)

1. Інформація про товар (роботу, послугу) – відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

2. Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

3. Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 15. Науково-технічна інформація

1. Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані у процесі науково-дослідної, дослідно-конструкторської, проєктно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

2. Правовий режим науково-технічної інформації визначається Законом України «Про науково-технічну інформацію», іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Стаття 16. Податкова інформація

1. Податкова інформація – сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

2. Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами.

Стаття 17. Правова інформація

1. Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

2. Джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

3. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Стаття 18. Статистична інформація

1. Статистична інформація – документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

2. Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

3. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом.

4. Правовий режим державної статистичної інформації визначається Законом України «Про державну статистику», іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 19. Соціологічна інформація

1. Соціологічна інформація – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

2. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 20. Доступ до інформації

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Стаття 21. Інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

3. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

4. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932–1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

5^{-1}) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або

територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

ЗАКОН УКРАЇНИ ПРО ЕЛЕКТРОННІ ДОКУМЕНТИ ТА ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ

(Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275)

Розділ I ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

адресат – фізична або юридична особа, якій адресується електронний документ;

дані – інформація, яка подана у формі, придатній для її оброблення електронними засобами;

посередник – фізична або юридична особа, яка в установленому законодавством порядку здійснює приймання, передавання (доставку), зберігання, перевірку цілісності електронних документів для задоволення власних потреб або надає відповідні послуги за дорученням інших суб'єктів електронного документообігу;

обов'язковий реквізит електронного документа – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;

автор електронного документа – фізична або юридична особа, яка створила електронний документ;

суб'єкти електронного документообігу – автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу.

Стаття 2. Сфера дії Закону

Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Стаття 3. Законодавство про електронні документи та електронний документообіг

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про телекомунікації», «Про обов'язковий примірник документів», «Про Національний архівний фонд та архівні установи», цим Законом, а також іншими нормативно-правовими актами.

Розділ II
ЕЛЕКТРОННИЙ ДОКУМЕНТ

Стаття 5. Електронний документ

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Стаття 6. Електронний підпис

Для ідентифікації автора електронного документа може використовуватися електронний підпис.

(Частина перша статті 6 в редакції Закону № 1206-VII від 15.04.2014).

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням удосконалених та кваліфікованих електронних підписів, регулюються Законом України «Про електронні довірчі послуги».

(Частина третя статті 6 в редакції Закону № 2155-VIII від 05.10.2017)

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Стаття 7. Оригінал електронного документа

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги».

(Частина перша статті 7 із змінами, внесеними згідно із Законом № 1206-VII від 15.04.2014; у редакції Законів № 675-VIII від 03.09.2015, № 2155-VIII від 05.10.2017).

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, у тому числі у паперовій копії.

Електронна копія електронного документа засвідчується у порядку, встановленому законом.

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Стаття 8. Правовий статус електронного документа та його копії

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;

2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

ЗАКОН УКРАЇНИ
ПРО ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.400)

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі терміни вживаються в такому значенні:

1) автентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних;

2) блокування сертифіката відкритого ключа – тимчасове зупинення чинності сертифіката відкритого ключа;

3) вебсайт – сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі «Інтернет», разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу;

4) відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

5) відокремлений пункт реєстрації – представництво (філія, підрозділ, територіальний орган) надавача електронних довірчих послуг або

юридична чи фізична особа, яка на підставі наказу надавача електронних довірчих послуг (його керівника) або договору, укладеного з ним, здійснює реєстрацію підписувачів з дотриманням вимог цього Закону та законодавства у сфері захисту інформації;

6) Довірчий список – перелік кваліфікованих надавачів електронних довірчих послуг та інформації про послуги, що ними надаються;

7) електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги;

8) електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;

9) електронна печатка – електронні дані, які додаються створювачем електронної печатки до інших електронних даних або логічно з ними пов'язуються і використовуються для визначення походження та перевірки цілісності пов'язаних електронних даних;

10) електронна позначка часу – електронні дані, які пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу;

11) електронна послуга – будь-яка послуга, що надається через інформаційно-телекомунікаційну систему;

12) електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;

13) електронні дані – будь-яка інформація в електронній формі;

14) засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

15) засіб електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки;

16) засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;

17) засіб кваліфікованого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення,

які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам цього Закону;

18) засіб удосконаленого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення удосконаленого електронного підпису чи печатки, та/або перевірки удосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа удосконаленого електронного підпису чи печатки;

19) ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;

20) ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, у результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи;

21) інтероперабельність – технологічна сумісність технічних рішень, що використовуються під час надання електронних послуг, та їх здатність взаємодіяти між собою;

22) кваліфікована електронна печатка – удосконалена електронна печатка, яка створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки;

23) кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

24) кваліфікований надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;

25) кваліфікований сертифікат відкритого ключа – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам цього Закону;

26) компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;

27) користувачі електронних довірчих послуг – підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону;

28) надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну або більше електронних довірчих послуг;

29) собистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

30) пара ключів – особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення;

31) перевірка – процес засвідчення справжності та підтвердження того, що електронний підпис чи печатка є дійсними;

32) підписувач – фізична особа, яка створює електронний підпис;

33) поновлення сертифіката відкритого ключа – відновлення чинності попередньо заблокованого сертифіката відкритого ключа;

34) програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг (далі – програмно-технічний комплекс), – апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов'язаних з наданням електронних довірчих послуг;

35) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів – електронна база даних, у якій містяться відомості про сертифікати відкритих ключів, сформовані надавачем електронних

довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом, їх статус та списки відкликаних сертифікатів відкритих ключів;

36) реєстрована електронна доставка – послуга, яка дає змогу передавати електронні дані між третіми сторонами за допомогою електронних засобів, засвідчувати обробку переданих електронних даних, у тому числі підтверджувати відправлення та отримання електронних даних, та захистити відправлені електронні дані від втрати, крадіжки, пошкодження або несанкціонованих змін;

37) самопідписаний сертифікат відкритого ключа – сертифікат відкритого ключа, який формується центральним засвідчувальним органом або засвідчувальним центром з використанням особистого ключа центрального засвідчувального органу або засвідчувального центру;

38) сертифікат відкритого ключа – електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію вебсайту;

39) скасування сертифіката відкритого ключа – зупинення чинності сертифіката відкритого ключа;

40) створювач електронної печатки – юридична особа, яка створює електронну печатку;

41) схема електронної ідентифікації – система електронної ідентифікації, у якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб;

42) технологічна нейтральність національних технічних рішень – невтручання органів, що здійснюють державне регулювання у сфері електронних довірчих послуг, у процес розроблення програмно-технічних комплексів, засобів електронного підпису чи печатки та засобів криптографічного захисту інформації, який не перешкоджатиме досягненню інтероперабельності між ними;

43) удосконалена електронна печатка – електронна печатка, створена за результатом криптографічного перетворення електронних даних, з якими пов'язана ця електронна печатка, з використанням засобу удосконаленої електронної печатки та особистого ключа, однозначно пов'язаного із створювачем електронної печатки, і який дає змогу

здійснити електронну ідентифікацію створювача електронної печатки та виявити порушення цілісності електронних даних, з якими пов'язана ця електронна печатка;

44) удосконалений електронний підпис – електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов'язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов'язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов'язаний цей електронний підпис.

2. Інші терміни вживаються у значеннях, наведених у Цивільному кодексі України, законах України «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про стандартизацію», «Про технічні регламенти та оцінку відповідності», «Про наукову і науково-технічну експертизу», «Про Національний банк України».

Розділ III
ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ

Стаття 14. Засоби електронної ідентифікації

1. Електронна ідентифікація здійснюється за допомогою засобів електронної ідентифікації, що підпадають під схему електронної ідентифікації, затверджену Кабінетом Міністрів України.

2. Міжнародні договори України щодо електронних довірчих послуг повинні передбачати порядок подання повідомлень та визнання схем електронної ідентифікації (із зазначенням рівня довіри для засобів електронної ідентифікації).

Стаття 15. Схеми електронної ідентифікації

1. Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. Схема електронної ідентифікації визначається Кабінетом Міністрів України.

2. Низький, середній та високий рівні довіри до засобів електронної ідентифікації повинні відповідати таким критеріям:

- низький рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в

контексті схеми електронної ідентифікації, яка забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності;

- середній рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності;
- високий рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних особи і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є запобігання зловживанню повноваженнями або підміні особи.

3. Використання кваліфікованих електронних підписів та печаток забезпечує високий рівень довіри до схем електронної ідентифікації.

Використання удосконалених електронних підписів та печаток забезпечує середній рівень довіри до схем електронної ідентифікації.

Розділ IV
ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ

Стаття 16. Вимоги до електронних довірчих послуг

1. Електронні довірчі послуги надаються, як правило, на договірних засадах надавачами електронних довірчих послуг.

2. До складу електронних довірчих послуг входять:

- створення, перевірка та підтвердження удосконаленого електронного підпису чи печатки;

- формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки;
- формування, перевірка та підтвердження чинності сертифіката автентифікації вебсайту;
- формування, перевірка та підтвердження електронної позначки часу;
- реєстрована електронна доставка;
- зберігання удосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами.

Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися як окремо, так і в сукупності.

3. Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному рахунку зі спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менш як 1000 мінімальних розмірів заробітної плати.

4. Розподіл ризиків збитків, що можуть бути заподіяні користувачам електронних довірчих послуг та третім особам фізичними або юридичними особами, не внесеними центральним засвідчувальним органом до Довірчого списку, визначається суб'єктами правових відносин на договірних засадах.

Стаття 17. Використання електронних довірчих послуг

1. Електронна взаємодія фізичних та юридичних осіб, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях не повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в інформаційних системах, у яких здійснюється обробка таких електронних даних, можуть здійснюватися з використанням електронних довірчих послуг або без отримання таких

послуг, за умови попередньої домовленості між учасниками взаємодії щодо порядку електронної ідентифікації учасників таких правових відносин.

2. Електронна взаємодія фізичних та юридичних осіб, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в складових частинах інформаційних систем, у яких здійснюється обробка таких електронних даних та володільцями інформації в яких є органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, повинні здійснюватися з використанням кваліфікованих електронних довірчих послуг.

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори, нотаріуси та інші суб'єкти, уповноважені державою на здійснення функцій державного реєстратора, для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа, а для реалізації повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи відповідно до закону, застосовують виключно засоби кваліфікованого електронного підпису чи печатки, які мають вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.

3. Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності встановлюється Кабінетом Міністрів України.

4. Нотаріальні дії з використанням кваліфікованого електронного підпису чи печатки або інших засобів електронної ідентифікації вчиняються в порядку, визначеному головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері нотаріату.

5. Здійснення правосуддя з використанням кваліфікованого електронного підпису чи печатки або інших засобів електронної ідентифікації вчиняється в порядку, встановленому законом.

6. Використання електронних довірчих послуг не змінює порядку вчинення правочинів, встановленого законом.

Правочини, що підлягають нотаріальному посвідченню та/або державній реєстрації у випадках, встановлених законом, вчиняються в електронній формі виключно із застосуванням кваліфікованих електронних довірчих послуг та у встановленому порядку.

7. Результати надання кваліфікованих електронних довірчих послуг повинні визнаватися в усіх державних установах та іншими користувачами цих послуг.

Стаття 18. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки

1. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки надається кваліфікованим постачальником електронних довірчих послуг та включає:

- надання користувачам електронних довірчих послуг засобів кваліфікованого електронного підпису чи печатки для генерації пар ключів та/або створення кваліфікованих електронних підписів чи печаток, та/або перевірки кваліфікованих електронних підписів чи печаток, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки;
- технічну підтримку та обслуговування наданих засобів кваліфікованого електронного підпису чи печатки.

2. Кваліфікований електронний підпис чи печатка вважається таким, що пройшов / пройшла перевірку та отримав / отримала підтвердження, якщо:

- перевірку кваліфікованого електронного підпису чи печатки проведено засобом кваліфікованого електронного підпису чи печатки;
- перевіркою встановлено, що відповідно до вимог цього Закону на момент створення кваліфікованого електронного підпису чи

печатки був чинним кваліфікований сертифікат електронного підпису чи печатки підписувача чи створювача електронної печатки;

- за допомогою кваліфікованого сертифіката електронного підпису чи печатки здійснено ідентифікацію підписувача чи створювача електронної печатки;
- під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки;
- під час перевірки підтверджено цілісність електронних даних в електронній формі, з якими пов'язаний цей кваліфікований електронний підпис чи печатка.

3. Електронний підпис чи печатка не можуть бути визнані недійсними та позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки.

4. Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

5. Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов'язана.

6. Обов'язкові вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

7. Випуск та обіг засобів електронної ідентифікації з функціями кваліфікованого електронного підпису як документів, що посвідчують особу, регулюються законодавством.

Вимоги до кваліфікованих електронних довірчих послуг, які надаються з використанням засобів електронної ідентифікації з функціями кваліфікованого електронного підпису як документів, що

посвідчують особу, встановлюються цим Законом та іншими актами законодавства.

Стаття 19. Засоби кваліфікованого електронного підпису чи печатки

1. Засоби кваліфікованого електронного підпису чи печатки повинні забезпечувати:

- належний рівень унікальності пари ключів, що ними генеруються;
- конфіденційність особистих ключів під час їх генерації, зберігання та створення кваліфікованого електронного підпису чи печатки;
- захист від доступу до особистих ключів сторонніх осіб.

Засоби кваліфікованого електронного підпису чи печатки не повинні змінювати електронні дані, з якими пов'язаний цей кваліфікований електронний підпис чи печатка, або перешкоджати доступу до них підписувача чи створювача (уповноваженого представника створювача) електронної печатки.

2. Засоби кваліфікованого електронного підпису чи печатки під час перевірки кваліфікованого електронного підпису чи печатки повинні надавати користувачеві електронних довірчих послуг результат процесу перевірки та виявляти всі події, що стосуються порушень захисту інформації.

3. Вимоги до засобів кваліфікованого електронного підпису чи печатки встановлюються Кабінетом Міністрів України.

Відповідність засобів кваліфікованого електронного підпису чи печатки зазначеним вимогам підтверджується документами про відповідність або позитивними експертними висновками за результатами їх державної експертизи у сфері криптографічного захисту інформації.

4. Встановлення обов'язкових вимог до засобів кваліфікованого електронного підпису чи печатки, а також перевірка їх дотримання здійснюються відповідно до вимог, установлених Кабінетом Міністрів України.

Стаття 20. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає:

- створення умов для генерації пари ключів особисто підписувачем чи створювачем (уповноваженим представником створювача) електронної печатки за допомогою засобу кваліфікованого електронного підпису чи печатки;
- формування кваліфікованих сертифікатів електронного підпису чи печатки, що відповідають вимогам цього Закону, та видачу їх користувачу електронної довірчої послуги;
- скасування, блокування та поновлення кваліфікованих сертифікатів електронного підпису чи печатки у випадках, передбачених цим Законом;
- перевірку та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки шляхом надання третім особам інформації про їхній статус та відповідність вимогам цього Закону;
- надання доступу до сформованих кваліфікованих сертифікатів електронних підписів та печаток шляхом їх розміщення на офіційному вебсайті кваліфікованого надавача електронних довірчих послуг, за умови згоди підписувача чи створювача електронної печатки на публікацію кваліфікованого сертифіката електронного підпису чи печатки.

2. Формування та видача кваліфікованих сертифікатів електронного підпису чи печатки, що не відповідають вимогам цього Закону, заборонені.

3. Обов'язкові вимоги до кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Стаття 21. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту включає:

- формування кваліфікованого сертифіката автентифікації вебсайту, що відповідає вимогам цього Закону, та передачу його користувачу електронної довірчої послуги;

- створення умов для генерації пари ключів особисто користувачем цієї електронної довірчої послуги за допомогою засобу кваліфікованого електронного підпису чи печатки;
- скасування, блокування та поновлення кваліфікованого сертифіката автентифікації вебсайту у випадках, передбачених цим Законом;
- перевірку та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту шляхом надання третім особам інформації про його статус та відповідність вимогам цього Закону;
- надання доступу до кваліфікованого сертифіката автентифікації вебсайту шляхом розміщення його на офіційному вебсайті кваліфікованого надавача електронних довірчих послуг, за умови згоди особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті автентифікації вебсайту, на публікацію кваліфікованого сертифіката автентифікації вебсайту.

2. Обов'язкові вимоги до кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Стаття 22. Ідентифікація особи під час формування та видачі кваліфікованого сертифіката відкритого ключа

1. Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються.

2. Ідентифікація фізичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

3. Допускається ідентифікація фізичної особи кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

4. Ідентифікація іноземців здійснюється відповідно до законодавства.

5. Під час перевірки цивільної правоздатності та дієздатності юридичної особи кваліфікований надавач електронних довірчих послуг зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

6. Кваліфікований надавач електронних довірчих послуг під час формування та видачі кваліфікованого сертифіката відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог цього Закону, а також перевіряє обсяг його повноважень за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, кваліфікованому надавачу електронних довірчих послуг подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

Стаття 23. Кваліфіковані сертифікати відкритих ключів

1. Під час надання кваліфікованих електронних довірчих послуг використовуються кваліфіковані сертифікати електронного підпису, кваліфіковані сертифікати електронної печатки та кваліфіковані сертифікати автентифікації вебсайту.

2. Кваліфіковані сертифікати відкритих ключів обов'язково повинні містити:

1) позначку, що сертифікат відкритого ключа виданий як кваліфікований сертифікат відкритого ключа;

2) позначку, що сертифікат відкритого ключа виданий в Україні;

3) ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа (далі – суб'єкти, які видали сертифікат), у тому числі обов'язково:

для юридичної особи: найменування та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено її державну реєстрацію;

для фізичної особи-підприємця: прізвище, ім'я, по батькові (за наявності) та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний податковий орган і мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), за якими здійснено її державну реєстрацію;

4) ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг, у тому числі обов'язково:

прізвище, ім'я, по батькові (за наявності) підписувача та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний податковий орган та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта) або;

найменування або прізвище, ім'я, по батькові (за наявності) створювача електронної печатки та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено його державну реєстрацію, або унікальний номер запису в Єдиному державному демографічному реєстрі, або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний податковий орган та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

5) місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;

6) значення відкритого ключа, який відповідає особистому ключу;

7) відомості про початок та закінчення строку дії кваліфікованого сертифіката відкритого ключа;

8) серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;

9) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені суб'єктом, який видав сертифікат;

10) відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;

11) відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;

12) відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

13) відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

14) ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації вебсайту).

(Частина друга статті 23 зі змінами, внесеними згідно із Законом № 440-IX від 14.01.2020)

3. Кваліфіковані сертифікати відкритих ключів можуть містити інші ідентифікаційні дані фізичних або юридичних осіб, необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

4. Обов'язкові вимоги до кваліфікованих сертифікатів відкритих ключів, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

5. Правочин, учинений в електронній формі, може бути визнаний судом недійсним у разі, коли під час його вчинення використовувався кваліфікований електронний підпис чи печатка, кваліфікований

сертифікат якого / якої не містить відомостей, передбачених частиною другою цієї статті, або містить недостовірні відомості.

Стаття 24. Чинність кваліфікованих сертифікатів відкритих ключів

1. Кваліфікований сертифікат відкритого ключа вважається чинним у разі, якщо на момент перевірки чинності:

строк дії, зазначений у кваліфікованому сертифікаті відкритого ключа, не закінчився;

суб'єктом, який видав сертифікат, статус кваліфікованого сертифіката відкритого ключа не змінено на скасований або блокований з підстав, визначених цим Законом;

за попередніми двома ознаками був чинним кваліфікований сертифікат відкритого ключа суб'єкта, який видав сертифікат.

2. Суб'єкти, які видають сертифікати відкритих ключів, не повинні видавати кваліфіковані сертифікати відкритих ключів зі строком дії, що перевищує строк дії їх власних кваліфікованих сертифікатів відкритих ключів.

3. Інформація про статус кваліфікованих сертифікатів відкритих ключів надається суб'єктами, що видали сертифікати, засобами їх інформаційно-телекомунікаційної системи цілодобово.

4. Доступ до кваліфікованих сертифікатів відкритих ключів надається суб'єктами, що видали сертифікати, з урахуванням вимог законодавства у сфері захисту персональних даних.

Стаття 25. Скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів

1. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин скасовується суб'єктом, який видав сертифікат, у разі:

1) подання користувачем електронних довірчих послуг заяви про скасування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача;

2) надходження до суб'єкта, який видав сертифікат, документа, що підтверджує:

- смерть фізичної особи-підписувача;
- припинення діяльності створювача електронної печатки;
- зміни ідентифікаційних даних користувача електронних довірчих послуг;

- факт державної реєстрації припинення підприємницької діяльності фізичної особи-підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи;
- надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката відкритого ключа;
- факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;
- набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

2. Самопідписаний сертифікат електронної печатки центрального засвідчувального органу не пізніше ніж протягом 24 годин скасовується центральним засвідчувальним органом у разі:

- підтвердження факту компрометації особистого ключа центрального засвідчувального органу, виявленого ним самостійно або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;
- набрання законної сили рішенням суду про скасування самопідписаного сертифіката електронної печатки центрального засвідчувального органу.

У разі подання повідомлення про прийняття кваліфікованим надавачем електронних довірчих послуг рішення про припинення діяльності з надання кваліфікованих електронних довірчих послуг центральний засвідчувальний орган або засвідчувальний центр на основі відповідного рішення скасовує кваліфікований сертифікат відкритого ключа, виданий цьому надавачу відповідно до вимог цього Закону.

4. Кваліфікований сертифікат відкритого ключа вважається скасованим з моменту зміни суб'єктом, який видав сертифікат, статусу

кваліфікованого сертифіката відкритого ключа на скасований.

5. Скасований кваліфікований сертифікат відкритого ключа поновленню не підлягає.

6. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин блокується суб'єктом, який видав сертифікат, у разі:

- подання користувачем електронних довірчих послуг заяви про блокування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача;
- повідомлення користувачем електронних довірчих послуг або контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг;
- набрання законної сили рішенням суду про блокування кваліфікованого сертифіката відкритого ключа;
- порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг.

7. Кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також блокується у разі прийняття рішення контролюючим органом про блокування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача електронних довірчих послуг за результатами здійснення державного нагляду (контролю) відповідно до вимог цього Закону.

8. Кваліфікований сертифікат відкритого ключа вважається заблокованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на заблокований.

9. Кваліфікований сертифікат відкритого ключа, статус якого змінено на заблокований, у період блокування не використовується.

10. Заблокований кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин поновлюється суб'єктом, який видав сертифікат, у разі:

- подання користувачем електронних довірчих послуг заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);

- повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або контролюючим органом, який раніше повідомив про цю підозру;
- надходження до суб'єкта, який видав сертифікат, повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката відкритого ключа, що набрало законної сили.

11. Заблокований кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також поновлюється відповідно до вимог цього Закону в разі:

- відновлення статусу кваліфікованого надавача електронних довірчих послуг;
- набрання законної сили рішенням суду на користь надавача електронних довірчих послуг.

12. Кваліфікований сертифікат відкритого ключа, який був заблокований, відновлює свою чинність з моменту його поновлення.

13. Кваліфікований сертифікат відкритого ключа вважається поновленим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на поновлений.

14. Суб'єкт, який видав кваліфікований сертифікат відкритого ключа, повинен забезпечити доступ до інформації про дату та час зміни статусу кваліфікованого сертифіката відкритого ключа.

Стаття 26. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає:

- формування кваліфікованої електронної позначки часу;
- передачу кваліфікованої електронної позначки часу користувачеві електронної довірчої послуги.

Кваліфікована електронна позначка часу має презумпцію точності дати та часу, на які вона вказує, та цілісності електронних даних, з якими ці дата та час пов'язані.

2. Кваліфікована електронна позначка часу повинна забезпечувати:

- зв'язок дати і часу з електронними даними в такий спосіб, що цілком виключає можливість непомітної зміни електронних даних;

- точність часу в програмно-технічному комплексі кваліфікованого надавача електронних довірчих послуг, що синхронізується із Всесвітнім координованим часом (UTC) з точністю до секунди.

3. До кваліфікованої електронної позначки часу додається створений для неї удосконалений електронний підпис чи удосконалена електронна печатка.

4. Використання кваліфікованої електронної позначки часу для постійного зберігання електронних даних є обов'язковим.

5. Обов'язкові вимоги до процедур надання кваліфікованої електронної довірчої послуги, надання кваліфікованої електронної позначки часу, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

ЗАКОН УКРАЇНИ ПРО ТЕЛЕКОМУНІКАЦІЇ

(Відомості Верховної Ради України (ВВР), 2004, № 12, ст.155)

Глава I ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення основних термінів

1. У цьому Законі терміни вживаються в такому значенні:

абонент – споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі;

абонентна плата – фіксований платіж, який може встановлювати оператор телекомунікацій для абонента за доступ на постійній основі до своєї телекомунікаційної мережі незалежно від факту отримання послуг;

абонентський номер – сукупність цифрових знаків для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі;

адреса мережі «Інтернет» – визначений чинними в інтернет-мережі міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв;

адресний простір мережі «Інтернет» – сукупність адрес мережі «Інтернет»;

безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ) – електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися зі збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру;

взаємоз'єднання телекомунікаційних мереж – встановлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватися інформацією;

власник (володілець) кабельної каналізації електрозв'язку – суб'єкт господарювання, у власності (володінні) якого перебувають уся інфраструктура кабельної каналізації електрозв'язку або окремі її елементи, набуті на належній правовій підставі, призначені для забезпечення доступу до телекомунікаційної мережі загального користування;

голосова телефонія – обмін інформацією голосом у реальному часі з використанням телекомунікаційних мереж;

дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки;

домен – частина ієрархічного адресного простору мережі «Інтернет», яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється;

домен.UA – домен верхнього рівня ієрархічного адресного простору мережі «Інтернет», створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі «Інтернет»;

домен другого рівня – частина адресного простору мережі «Інтернет», що розташовується на другому рівні ієрархії імен у цій мережі;

електрозв'язок – див. «телекомунікації»;

загальнодоступні (універсальні) телекомунікаційні послуги – мінімальний набір визначених цим Законом послуг нормованої якості, доступний усім споживачам на всій території України;

Інтернет – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

інформаційна система загального доступу – сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних;

інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації;

інформація – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

кабельна каналізація електрозв'язку – обладнання та споруди, призначені для прокладання, монтажу та експлуатаційного обслуговування кабелів телекомунікацій, що включають трубопроводи (канали кабельної каналізації), закладні та оглядові пристрої в колодязях, кабельних шафах, шахтах, колекторах, мостах, естакадах, тунелях, будівлях, а також приміщення для вводу кабелів і розміщення лінійного обладнання;

канал електрозв'язку – сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і який характеризується смугою частот та/або швидкістю передачі;

канал кабельної каналізації електрозв'язку – окремо виділені місця в колекторах, телекомунікаційних колодязях, тунелях, акведуках, шляхопроводах, на мостах, мостових переходах, естакадах, трубопроводах, а також інші надземні та підземні інженерні споруди, що призначені для прокладання або використовуються для прокладання магістральних, з'єднувальних та розподільних проводових і оптоволоконних кабелів електрозв'язку, а також розміщення супутніх лінійних технічних засобів телекомунікацій;

кінцеве обладнання – обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг;

монопольний (домінуючий) оператор телекомунікацій – оператор, який відповідно до законодавства України займає монопольне (домінуюче) становище на ринку певних телекомунікаційних послуг на території держави чи певного регіону;

Національний план нумерації –нормативно-правовий акт, який визначає структуру, регламентує розподіл та умови використання номерного ресурсу в телекомунікаційних мережах;

номерний ресурс – сукупність цифрових знаків, що використовуються для позначення (ідентифікації) мереж, послуг, пунктів закінчення мережі в телекомунікаційних мережах загального користування;

оператор телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;

оператор, провайдер телекомунікацій з істотною ринковою перевагою на ринку телекомунікаційних послуг – оператор, провайдер телекомунікацій, частка доходу якого на визначеному національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, ринку певних телекомунікаційних послуг протягом року, що передує проведенню аналізу ринку, перевищує 25 відсотків сумарного доходу всіх операторів, провайдерів телекомунікацій, отриманого на цьому ринку за той самий період часу, або якщо внаслідок технологічного процесу надання послуги іншому оператору, провайдеру телекомунікацій її може бути надано тільки в мережі певного оператора, провайдера телекомунікацій;

передавання даних – передавання інформації у вигляді даних з використанням телекомунікаційних мереж;

перенесення абонентського номера – телекомунікаційна послуга, що надається абоненту за його заявою, яка полягає у збереженні за абонентом наданого йому оператором телекомунікацій абонентського номера з метою використання цього номера для отримання телекомунікаційних послуг у мережі іншого оператора телекомунікацій, що надає телекомунікаційні послуги на території України;

персональний номер – абонентський номер, що присвоюється зареєстрованому абоненту за його заявою у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку

та інформатизації, централізовано адмініструється і може використовуватися цим абонентом для отримання відповідно до договору телекомунікаційних послуг незалежно від географічного регіону України і типу цих послуг;

послуга пропуску трафіка – телекомунікаційна послуга щодо здійснення термінації та/або транзиту трафіка, що надається оператором телекомунікацій іншим операторам;

провайдер телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку;

проводовий електрозв'язок – передавання і приймання інформації із застосуванням проводових ліній з металевими або волоконнооптичними жилами;

пропуск трафіка – проходження трафіка між елементами однієї або різних телекомунікаційних мереж;

пункт закінчення телекомунікаційної мережі – місце стику (з'єднання) мережі телекомунікацій та кінцевого обладнання;

ресурси телекомунікаційних мереж – наявні в телекомунікаційних мережах кількість номерів (номерний ресурс), кількість і пропускна спроможність проводових ліній з металевими жилами, оптичними волокнами, радіоліній, каналів, трактів для передавання інформації, комутаційних станцій та вузлів, радіочастотний ресурс;

ринок телекомунікаційних послуг – сфера обігу визначених телекомунікаційних послуг, на які протягом певного часу і в межах певної території є попит і пропозиція;

розподіл номерного ресурсу – виділення номерного ресурсу з визначеного діапазону номерів для надання телекомунікаційних послуг;

розрахункова такса – сума, що визначає розмір оплати за доступ до технічних та технологічних ресурсів мереж операторів телекомунікацій (здійснення доступу) для пропуску одиниці трафіка і застосовується для операторів, які є суб'єктами господарської діяльності на території України;

розрахункова такса за послугу пропуску трафіка – розмір плати за термінацію або транзит одиниці трафіка між телекомунікаційними мережами операторів;

роумінг національний – телекомунікаційна послуга, яка забезпечує можливість абонентам одного оператора телекомунікацій, що надає послуги рухомого (мобільного) зв'язку на території України, отримувати телекомунікаційні послуги в телекомунікаційній мережі іншого оператора (операторів) у межах України;

рухомий (мобільний) зв'язок – електрозв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного зі споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції;

споживач телекомунікаційних послуг (споживач) – юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб;

споруди електрозв'язку – будівлі, вежі, антени, що використовуються для організації електрозв'язку;

сталість телекомунікаційної мережі – властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників;

суб'єкти ринку телекомунікацій – оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій;

телекомунікації (електрозв'язок) – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах;

телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

телекомунікаційна мережа загального користування – телекомунікаційна мережа, доступ до якої відкрито для всіх споживачів;

телекомунікаційна мережа доступу – частина телекомунікаційної мережі між пунктом закінчення телекомунікаційної мережі та найближчим вузлом (центром) комутації включно;

телекомунікаційна послуга (послуга) – продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій;

телемережі – телекомунікаційні мережі загального користування, що призначаються для передавання програм радіо- та телебачення, а також інших телекомунікаційних і мультимедійних послуг і можуть інтегруватися з іншими телекомунікаційними мережами загального користування;

термінація трафіка – встановлення, підтримка фізичного та/або логічного з'єднання, пропуск трафіка між телекомунікаційною мережею, з якої надходить виклик або ініціюється з'єднання, та кінцевим обладнанням, до якого спрямовується виклик або ініціюється з'єднання;

технічні вимоги – (технічний) документ, що встановлює вимоги, які повинні бути виконані під час побудови та функціонування телекомунікаційних мереж, застосування технічних засобів та об'єктів телекомунікацій чи отримання телекомунікаційних послуг;

технічні засоби телекомунікацій – обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж;

транзит трафіка – встановлення, підтримка телекомунікаційною мережею оператора фізичного та/або логічного з'єднання, пропуск трафіка між двома іншими телекомунікаційними мережами;

транспортна телекомунікаційна мережа – мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу;

трафік – сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію;

фіксований зв'язок – телекомунікації, що здійснюються із застосуванням стаціонарного (нерухомого) кінцевого обладнання.

2. Термін «благодійне телекомунікаційне повідомлення» вживається в цьому Законі у значенні, наведеному в Законі України «Про благодійну діяльність та благодійні організації».

Стаття 9. Охорона таємниці телефонних розмов, телеграфної та іншої кореспонденції, безпека телекомунікацій

1. Охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України.

2. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом.

3. Оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Глава VI
СПОЖИВАЧІ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

Стаття 32. Права споживачів телекомунікаційних послуг

1. Споживачі під час замовлення та/або отримання телекомунікаційних послуг мають право на:

1) державний захист своїх прав;

2) вільний доступ до телекомунікаційних послуг;

3) безпеку телекомунікаційних послуг;

4) вибір оператора, провайдера телекомунікацій;

5) вибір виду та кількості телекомунікаційних послуг;

6) безоплатне отримання від оператора, провайдера телекомунікацій вичерпної інформації щодо змісту, якості, вартості та порядку надання телекомунікаційних послуг;

7) своєчасне і якісне одержання телекомунікаційних послуг;

8) отримання від оператора, провайдера телекомунікацій наявних відомостей щодо наданих телекомунікаційних послуг;

9) обмеження оператором, провайдером телекомунікацій доступу споживача до окремих видів послуг на підставі його власної письмової заяви;

10) повернення від оператора, провайдера телекомунікацій невикористаної частини коштів у разі відмови від передплачених телекомунікаційних послуг у випадках і порядку, визначених правилами надання і

отримання цих послуг, а також договором приєднання щодо виконання благодійного телекомунікаційного повідомлення (у разі укладення такого договору);

11) відмову від телекомунікаційних послуг у порядку, встановленому договором про надання телекомунікаційних послуг;

12) відшкодування збитків, заподіяних унаслідок невиконання чи неналежного виконання оператором, провайдером телекомунікацій обов'язків, передбачених договором зі споживачем чи законодавством;

13) оскарження неправомірних дій операторів, провайдерів телекомунікацій шляхом звернення до суду та уповноважених державних органів;

14) відмову від оплати телекомунікаційної послуги, яку вони не замовляли;

15) отримання відомостей щодо можливості та порядку відмови від замовленої телекомунікаційної послуги;

16) безоплатне отримання від оператора, провайдера телекомунікацій рахунків за надані телекомунікаційні послуги. За особистим зверненням споживача з урахуванням технічної можливості обладнання телекомунікаційної мережі нарахована до оплати сума за надані послуги повинна бути розшифрована тільки за той розрахунковий період, до якого споживач має претензії, із зазначенням номера абонента, якого викликав споживач, виду послуги, часу початку і закінчення кожного сеансу зв'язку, обсягу наданих послуг, суми коштів до сплати за кожний сеанс зв'язку. Телекомунікаційні послуги, які надаються знеособлено (анонімно), розшифровці не підлягають;

16^{-1}) перенесення абонентського номера, користування персональним номером та отримання послуг національного роумінгу;

17) інші права, визначені законодавством України та договором про надання телекомунікаційних послуг.

2. Абонент, який отримує телекомунікаційні послуги без укладення договору в письмовій формі, може зареєструватися в оператора, надавши йому персональні дані відповідно до закону в порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації.

Стаття 33. Обов'язки споживачів телекомунікаційних послуг

1. Споживачі телекомунікаційних послуг зобов'язані дотримуватися Правил надання та отримання телекомунікаційних послуг, що затверджує Кабінет Міністрів України, зокрема:

1) використовувати кінцеве обладнання, що має документ про підтвердження відповідності;

2) не допускати використання кінцевого обладнання споживача для вчинення протиправних дій або дій, що суперечать інтересам національної безпеки, оборони та охорони правопорядку;

3) не допускати дій, що можуть створювати загрозу для безпеки експлуатації мереж телекомунікацій, підтримки цілісності та взаємодії мереж телекомунікацій, захисту інформаційної безпеки мереж телекомунікацій, електромагнітної сумісності радіоелектронних засобів, ускладнювати чи унеможливлювати надання послуг іншим споживачам;

4) не допускати використання на комерційній основі кінцевого обладнання та абонентських ліній для надання телекомунікаційних послуг третім особам;

5) виконувати умови договору про надання телекомунікаційних послуг у разі його укладення, у тому числі своєчасно оплачувати отримані ними телекомунікаційні послуги;

6) виконувати інші обов'язки відповідно до законодавства.

2. У разі використання абонентами лічильників обліку тривалості телекомунікаційних послуг, що встановлюються на кінцевому обладнанні для перевірки правильності нарахування плати за отримані послуги, абоненти зобов'язані:

1) використовувати лічильники, що мають документ про підтвердження відповідності згідно із законодавством України;

2) періодично здійснювати метрологічну повірку лічильників як засобів вимірювальної техніки в порядку, визначеному законодавством України.

3. Споживачі телекомунікаційних послуг зобов'язані виконувати інші обов'язки відповідно до цього Закону та законодавства України.

Стаття 34. Захист інформації про споживача

1. Оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача,

отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

2. Призначені для оприлюднення телефонні довідники, у тому числі електронні версії та бази даних інформаційно-довідкових служб, можуть містити інформацію про прізвище, ім'я, по батькові, найменування, адресу та номер телефону абонента в разі, якщо в договорі про надання телекомунікаційних послуг міститься згода споживача на опублікування такої інформації. Під час автоматизованої обробки інформації про абонентів оператор телекомунікацій забезпечує її захист відповідно до закону. Споживач має право на безоплатне вилучення відомостей про нього повністю або частково з електронних версій баз даних інформаційно-довідкових служб.

3. Інформація про споживача та про телекомунікаційні послуги, що він отримав, може надаватись у випадках і в порядку, визначених законом. В інших випадках зазначена інформація може поширюватися лише за наявності письмової згоди споживача.

Стаття 35. Захист інтересів споживачів у разі припинення діяльності оператором, провайдером телекомунікацій з надання телекомунікаційних послуг

1. Оператор, провайдер телекомунікацій, який припиняє діяльність з надання телекомунікаційних послуг, зобов'язаний попередити споживачів не пізніше ніж за три місяці до припинення надання телекомунікаційних послуг.

2. У разі вилучення номерного та/або радіочастотного ресурсу внаслідок порушення оператором, провайдером телекомунікацій законодавства такий оператор, провайдер зобов'язаний відшкодувати абоненту витрати, пов'язані з припиненням надання телекомунікаційних послуг, у встановленому законом порядку.

Стаття 36. Відповідальність споживачів телекомунікаційних послуг

1. Споживачі телекомунікаційних послуг несуть відповідальність за порушення норм цього Закону, Правил надання та отримання телекомунікаційних послуг відповідно до закону.

2. У разі затримки плати за надані оператором, провайдером телекомунікаційні послуги споживачі сплачують пеню, яка обчислюється від

вартості неоплачених послуг у розмірі облікової ставки Національного банку України, що діяла в період, за який нараховується пеня.

3. Сплата споживачем пені, правомірне припинення чи скорочення оператором, провайдером переліку телекомунікаційних послуг не звільняє споживача від обов'язку оплатити надані йому телекомунікаційні послуги.

4. У разі виявлення пошкодження телекомунікаційної мережі, що сталося з вини споживача, усі витрати оператора телекомунікацій на усунення пошкодження, а також відшкодування інших збитків (у тому числі неотриманий прибуток) покладаються на споживача.

ЗАКОН УКРАЇНИ ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз – показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки – відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого

управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4) кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

5) кібербезпека – 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 та нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості та надійності функціонування комунікаційних, технологічних систем;

8) кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність – сукупність кіберзлочинів;

10) кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) кіберпростір – 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;

12) кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури;

16) критично важливі об'єкти інфраструктури (далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки й оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

17) Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних

захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

18) національні електронні інформаційні ресурси (далі – національні інформаційні ресурси) – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Електронні інформаційні ресурси розуміютья як будь-яку інформацію, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

19) об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

20) система управління технологічними процесами (далі – технологічна система) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі «Інтернет» та/або інших глобальних мереж передачі даних;

21) системи електронних комунікацій (далі – комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, у якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних

ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі «Інтернет» та/або інших глобальних мереж передачі даних.

Терміни «національна безпека», «національні інтереси», «загрози національній безпеці» вживаються в цьому Законі у значенні, визначеному Законом України «Про основи національної безпеки України».

ЗАКОН УКРАЇНИ
ПРО НАЦІОНАЛЬНУ ПОЛІЦІЮ

(Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379)

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 2. Завдання поліції

1. Завданнями поліції є надання поліцейських послуг у сферах:

1) забезпечення публічної безпеки і порядку;

2) охорони прав і свобод людини, а також інтересів суспільства та держави;

3) протидії злочинності;

4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

Розділ IV
ПОВНОВАЖЕННЯ ПОЛІЦІЇ

Стаття 25. Повноваження поліції у сфері інформаційно-аналітичного забезпечення

1. Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених цим Законом.

2. Поліція в межах інформаційно-аналітичної діяльності:

1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;

2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями;

5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів в електронній формі та в обсягах даних, зазначених у статтях 7, 14 Закону України «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів», відомості, необхідні для забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів.

3. Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

4. Діяльність поліції, пов'язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України «Про захист персональних даних», іншими законами України.

5. Поліція зобов'язана письмово інформувати митні органи про виявлення нецільового використання та/або передачі транспортних засобів особистого користування, тимчасово ввезених на митну територію України чи поміщених у митний режим транзиту, у володіння, користування або розпорядження особам, які не ввозили такі транспортні засоби на митну територію України або не поміщували в митний режим транзиту, а також про виявлення розкомплектування таких транспортних засобів.

Стаття 26. Формування інформаційних ресурсів поліцією

1. Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно:

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;

3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;

4) розшуку осіб, зниклих безвісти;

5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;

6) зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;

7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);

8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;

9) зареєстрованих кримінальних та адміністративних правопорушень, пов'язаних з корупцією, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;

10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;

11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;

12) викрадених (втрачених) документів за зверненням громадян;

13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;

14) викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;

15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;

16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;

17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;

18) бази даних, що формуються у процесі здійснення оперативно-розшукової діяльності відповідно до закону.

2. Під час наповнення баз (банків) даних, визначених у пункті 7 частини першої цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК).

3. Поліція забезпечує внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та здійснює підтримання таких відомостей в актуальному стані в межах, визначених законодавством.

Стаття 27. Використання поліцією інформаційних ресурсів

1. Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних».

2. Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.

3. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 цього Закону, фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Стаття 28. Відповідальність за протиправне використання інформаційних ресурсів

1. Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації.

2. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

3. Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних у порядку, визначеному у статтях 26, 27 цього Закону.

Навчальне видання

ОЛЬГА В_____ КОВАЛЬОВА

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ

НАВЧАЛЬНИЙ ПОСІБНИК

Підготовлено до друку ВД «Дакор»
Друкується в авторській редакції

Підписано до друку __.__.2021. Гарнітура BookmanC. Формат 60×84 1/16.
Папір офсетний. Друк офсетний. Ум.-друк. арк. 13,71. Обкл.-вид. арк. 12,75. Наклад ___ прим.

ТОВ «ВД «Дакор»
Свід. ДК № 4349 від 05.07.2012
(044) 461-85-06; vd_dakor@ukr.net www.dakor.kiev.ua
04655, м. Київ, просп. Степана Бандери, 8