В. Я. ПЄВНЄВ
Г. А. ЗЕМЛЯНКО

ОСНОВИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

НАВЧАЛЬНИЙ ПОСІБНИК
З КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Про авторів

Георгій Землянко **(ORCID: 0000-0003-4153-7608)**, Володимир Пєвнєв **(ORCID: 0000-0002-3949-3514)** — викладачі Національного аерокосмічного університету **«ХАІ»**. Їхні наукові дослідження в галузі інформаційних технологій, телекомунікацій та кібербезпеки опубліковані в провідних міжнародних базах **Scopus** та **Web of Science**.

Цей посібник — результат багаторічної викладацької роботи. Він системно висвітлює ключові теми курсу: від класифікації інформації та політик безпеки до кіберзахисту критичної інфраструктури. Викладення ґрунтується на чинних нормативних документах України та враховує актуальні виклики кіберпростору. Видання призначене для студентів, а також буде корисне фахівцям, які прагнуть глибше зрозуміти принципи захисту цифрового середовища.

м. Харків,
Україна

Pevnev V. Ya., Zemlianko H. A.

FUNDAMENTALS OF INFORMATION AND CYBER SECURITY

Textbook

Kharkiv 2026

УДК 518.9(07) / UDC 518.9(07)
П 23

DOI: 10.5281/zenodo.22076953

Рецензенти:
д-р техн. наук, проф. Роман Васильович Олійников (Roman Oliynykov);
д-р техн. наук, проф. Кучук Георгій Анатолійович (Heorhii Kuchuk).

Півнєв В. Я., Землянко Г. А.
П 23 Основи інформаційної та кібернетичної безпеки: навч. посіб. / В. Я. Півнєв, Г. А. Землянко. – Харків: ФОП Бровін О.В., 2026. – 90 с.
ISBN 978-617-8587-71-0

Навчальний посібник складено з розділів, що доповнюють лекційний курс «Основи інформаційної безпеки» і містять додаткову інформацію щодо питань, які розглядаються під час занять. Розглянуто поняття інформації, її класифікацію, властивості та життєвий цикл; визначено інформаційну безпеку, її моделі (загроз, порушника, концептуальну), політику безпеки, канали витоку та методи забезпечення конфіденційності, цілісності, доступності та спостережності. Окрему увагу приділено кібербезпеці: принципам, організаційно-технічній моделі, національній системі кібербезпеки, сучасним загрозам (шкідливе ПЗ, соціальна інженерія, DDoS-атаки, інсайдерські загрози, використання штучного інтелекту) та кібергігієні. Розглянуто заходи кіберзахисту об’єктів критичної інфраструктури, зокрема ідентифікацію ризиків, рівні впровадження та розроблення профілю кіберзахисту.

Для студентів вищих навчальних закладів різних спеціальностей, а також фахівців у галузі інформаційних технологій.

Pevnev V. Ya., Zemlianko H. A.
П 23 Fundamentals of Information and Cyber Security: textbook / V. Ya. Pevnev, H. A. Zemlianko. – Kharkiv: FOP Brovin O.V., 2026. – 90 p.
ISBN 978-617-8587-71-0

The textbook consists of chapters that supplement the lecture course «Fundamentals of Information Security» and provide additional information on the topics covered during classes. The concepts of information, its classification, properties and life cycle are considered; information security is defined, its models (threat, offender, conceptual), security policy, leakage channels and methods of ensuring confidentiality, integrity, availability and observability are outlined. Special attention is paid to cyber security: principles, organizational and technical model, national cyber security system, modern threats (malware, social engineering, DDoS attacks, insider threats, use of artificial intelligence) and cyber hygiene. Measures for cyber protection of critical infrastructure objects, including risk identification, implementation levels and development of a cyber protection profile, are examined.

For students of various specialties of higher educational institutions, as well as for specialists in the field of information technology.

ISBN 978-617-8587-71-0

ЗМІСТ

ВСТУП

Розвиток інформаційних технологій є визначальним у формуванні сучасного суспільства. Інформація стає дедалі ціннішим ресурсом. Володіння таким ресурсом дає змогу управління державами, розвитку суспільних взаємин і створення матеріальних благ. Дедалі актуальнішим стає завдання захисту інформаційних ресурсів. З появою обчислювальних машин з практично необмеженими можливостями штучного інтелекту виникає висока ймовірність несанкціонованого доступу до таких ресурсів.

Таке їх використання може призвести до витоку конфіденційної інформації, аварій на транспорті та промислових об'єктах і техногенних катастроф. Блокуванням таких можливостей потенційних порушників покликані правила, методи та засоби забезпечення інформаційної та кібернетичної безпеки.

Останнім часом у нашій державі велика увага приділяється кібербезпеки. Про це свідчить ухвалення ЗУ «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», численних нормативних документів уряду та різних відомств. Ці документи створили нормативно-правову базу для забезпечення захисту держави та її громадян від можливого атаки в кіберпросторі.

У першому розділі розглянуто поняття інформації, її класифікація та визначення, способи доступу до інформації та її основні властивості. Цей розділ дозволяє виробити у слухачів понятійний апарат, необхідний подальшого вивчення курсу, тому що інформація є основним об'єктом захисту.

У другому розділі розглядаються питання, пов'язані з інформаційною безпекою. Насамперед це концептуальна модель, за допомогою якої показані взаємозв'язки між усіма складовими інформаційної безпеки. Розглянуто моделі другого рівня (загроз та порушника), на підставі яких розробляється політика безпеки інформації. З цих даних грунтується вся система інформаційної безпеки інформаційно-комунікаційних систем. Забезпечення інформаційної безпеки будується на гарантії конфіденційності, цілісності, доступності та спостережності. Ці властивості систем ретельно надано у цьому розділі. Розгляд навчальних питань грунтується на нормативних документах Держспецзв'язку, який регулює питання інформаційної безпеки.

У третьому розділі розглядаються питання, пов'язані із кібернетичною безпекою. Це принципи забезпечення кібербезпеки, організаційно-технічна модель, методи кіберзахисту. Під час вивчення організаційно-технічної моделі розглянуто принципи її функціонування, засоби кіберзахисту, склад систем забезпечення організаційно-керуючій інфраструктури кіберзахисту, технологічна та базисна інфраструктура кіберзахисту. При розгляді національної системи кібербезпеки

визначаються основні суб’єкти та їх основні завдання, принципи функціонування та шляхи їх досягнення. Багато уваги у розділі приділено загрозам кібербезпеки. Розгляд цих загроз дозволяє планувати дії щодо побудови систем кіберзахисту від шкідливого програмного забезпечення, атак з використанням соціальної інженерії та штучного інтелекту, інсайдерских загроз. Окремим підрозділом виділено кібергігієну. Це поради та інструкції користувачам, які можуть допомогти в організації захищеного простору в електронному світі.

У четвертому розділі розглядається кібербезпека об'єктів критичної інфраструктури. Особлива увага приділяється розгляду заходів кіберзахисту об'єктів критичної інфраструктури, розробці та впровадженню профілю кіберзахисту об’єктів критичної інфраструктури інформації. Розгляд навчальних питань грунтується на нормативних документах Держспецзв'язку, який регулює питання інформаційної безпеки об'єктів критичної інфраструктури.

ПЕРЕЛІК СКОРОЧЕНЬ

АРМ	-	Автоматизоване робоче місце
ВР України	-	Верховна Рада України
ДЗС	-	Допоміжні засоби та системи
ДСТУ	-	Державний стандарт України
ЕМІ	-	Електромагнітний імпульс
ЕП	-	Електронний підпис
ІБ	-	Інформаційна безпека
ІЗ	-	Інсайдерська загроза
ІоТ	-	Інтернет речей
ІКС	-	Інформаційно-телекомунікаційна система
КВІ	-	Канал відтоку інформації
ПБ	-	Політика безпеки інформації
ПЗ	-	Програмне забезпечення
ПЗП	-	Постійний запам’ятовуючий пристрій
ПЕВ	-	Побічні електромагнітні випромінювання
ПРД	-	Правила розмежування доступу
ЗІ	-	Захист інформації
ЗПО	-	Засоби прийому, обробки та зберігання інформації
ЗСУ	-	Збройні Сили України
ЗУ	-	Закон України
КМ	-	Концептуальна модель
КЗЗ	-	Комплекс засобів захисту;
КС	-	Комп’ютерна система
КСЗІ	-	Комплексна система захисту інформації
ЛОМ	-	Локальна обчислювальна мережа
НД ТЗІ	-	Нормативний документ системи технічного захисту інформації
НСД	-	Несанкціонований доступ
ОКІ	-	Об’єкти критичної інфраструктури
ОКІІ	-	Об’єкти критичної інфраструктури інформації
ОС	-	Операційна система
СЗІ	-	Система захисту інформації
РЕЗ	-	Радіоелектронні засоби
СУБД	-	Система управління базами даних
ТЗ	-	Технічні засоби
ЦІ	-	Цілісність інформації
ШІ	-	Штучний інтелект
ШПЗ	-	Шкідливе програмне забезпечення

РОЗДІЛ 1 ІНФОРМАЦІЯ

1.1 Поняття та визначення терміну «інформація»

Інформація — абстрактне поняття, що має різні значення від контексту покладу. Походити від латинського слова «informatio», яку має декілька значень:

- роз'яснення; виклад фактів, подій;
- витлумачення;
- представлення, поняття;
- ознайомлення, просвіта.

У сучасній науці розглядаються два види інформації :

Об'єктивна (первинна) інформація — властивість матеріальних об'єктів і явищ(процесів) породжувати різноманіття станів, які за допомогою взаємодій (фундаментальні взаємодії) передаються іншим об'єктам і відображаються в їх структурі.

Суб'єктивна (семантична, смислова, вторинна) інформація - смисловий зміст об'єктивної інформації про об'єкти і процеси матеріального світу, сформоване свідомістю людини за допомогою смислових образів (слів, образів і відчуттів) і зафіксоване на якому-небудь матеріальному носії.

У побутовому сенсі інформація — відомості про навколишній світ і процеси, що протікають в нім, сприймані людиною або спеціальним пристроєм.

Нині не існує єдиного визначення інформації як наукового терміну. З точки зору різних областей знання, це поняття описується своїм специфічним набором ознак. Згідно концепції К. Шенона, інформація — це знята невизначеності, тобто відомості, які повинні зняти в тому або іншому ступені існуючу у споживача до їх отримання невизначеність, розширити його розуміння об'єкту корисними відомостями.

Згідно з атрибутивної концепцією інформація розглядається як властивість матерії та воно грунтується на твердженні, що інформацію містять будь-які повідомлення, що сприймаються людиною або приладами. При цьому інформація визначається як міра неоднорідності розподілу матерії та енергії в просторі і в часі

Функціональна концепція інформації представлена двома різновидами: кібернетичною, яка вважає, що інформація (інформаційні процеси) є у всіх самоврядних (технічних, біологічних, соціальних) системах, і антропоцентристською, у рамках якої інформація інтерпретується як особливість живих, самоврядних систем або ж свідомих істот, як основна передумова і умова оптимального управління.

З точки зору інформатики, інформація має ряд фундаментальних властивостей: новизна, актуальність, достовірність, об'єктивність, повнота, цінність та ін.

Закон України «Про інформацію» визначає що, інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Закон України «Про телекомунікації» визначає що, інформація відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи іншим способом.

Згідно з ДСТУ 3396.2- 97 інформація – відомості про суб’єкти, об’єкти, явища та процеси.

В залежності від галузі використання термін «інформація» має безліч визначень, зокрема:

- відомості або повідомлення про щось(побутове);
- роз'яснення, виклад;
- оригінальність, новизна;
- комунікація та зв'язок, в процесі якого усувається невизначеність;
- міра неоднорідності розподілу матерії та енергії у просторі та у часі, міра змін, якими супроводжуються всі процеси, що протікають у світі;
- позначення змісту, отриманого із зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів;
- заперечення ентропії, міра хаосу в системі;
- передача різноманітності;
- міра складності структур;
- ймовірність вибору;
- відображена різноманітність;
- властивості матеріальних об'єктів породжувати та зберігати певний стан, який в різних матеріально-енергетичних формах може передаватись між об'єктами;
- результат інтелектуальної (аналітико - синтетичної чи евристичної) діяльності певної людини щодо подання відомостей, повідомлень, сигналів, кодів, образів;

ЮНЕСКО визначає інформацію як універсальну субстанцію, що пронизує усі сфери людської діяльності, яка слугує провідником знань та відомостей, інструментом спілкування, взаєморозуміння та співробітництва, утвердження стереотипів мислення та поведінки.

Як бачимо, визначення терміну інформація істотно відрізняються один від одного, що значно ускладнює проведення інформаційного аудиту та визначення суми збитків завданих правопорушниками.

Існують також й інші, переважно несумісні між собою визначення поняття «інформація». Але практично всі чисельні погляди на сутність інформації групуються навколо двох концепцій — атрибутивної та функціональної.

Інформація - це будь-які відомості, які цікавлять конкретну людину в конкретній ситуації. Серіал - це теж інформація, причому часом дуже

актуальна. Іноді об'єктом інформації може стати телефон нового салону краси, в якому зараз знижки.

Інформація в електронній сфері – це двійкове число, яке завжди фіксоване. Статична форма електронної інформації характерна для зберігання в ПЗП комп'ютера.

Інформація - це відомості про об'єкти або явища довкілля, які ми використовуємо у разі виникнення необхідності в них. Інформація може бути новою - це відомості, яких ми ще не знаємо, і застарілою - тобто відомою, переробленою. Інформація поширюється на носіях, її актуальність для індивіда носить суб'єктивний характер

Інформація - стан (або зміна стану) зовнішнього середовища, що призводить до зміни внутрішнього стану системи.

Інформація - це генералізаційний безпочатково-нескінченний єдиний законопроцес мікро- та макромірних відносин, взаємозв'язків та взаємозбереження енергії, руху та маси на основі резонансно-стільникової, частотно-квантової та хвильової природи світла, тепла, звуку та інших властивостей та форм у мікро- та макроструктурах Всесвіту.

1.2 Класифікація інформації

Інформацію можливо класифікувати за:

- змістом;
- способом сприйняття;
- формою представлення;
- призначенням;
- з порядком доступу до інформації.

Згідно за Законом України «Про інформацію» 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;
- критична технологічна інформація;
- інші види інформації.

Інформація про фізичну особу

Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

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.

Інформація довідково-енциклопедичного характеру

Інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

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-комунікаційними системами.

Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана ВР України.

Інформація про стан довкілля (екологічна інформація)

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.

Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана ВР України.

Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Інформація про товар (роботу, послугу)

Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

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 ВР України.

Науково-технічна інформація

Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Правовий режим науково-технічної інформації визначається Законом України "Про науково-технічну інформацію", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана ВР України. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Податкова інформація

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.

Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами.

Правова інформація

Правова інформація - будь-які відомості 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 і підзаконні нормативно-правові акти, міжнародні договори та

угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення медіа, публічні виступи, інші джерела інформації з правових питань.

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.

Статистична інформація

Статистична інформація - документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом.

Правовий режим офіційної державної статистичної інформації визначається Законом України "Про офіційну статистику", іншими законами України та міжнародними договорами України, згода на обов’язковість яких надана ВР України.

Соціологічна інформація

Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана ВР України.

Критична технологічна інформація

Критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури.

Правовий режим критичної технологічної інформації визначається законами України та міжнародними договорами України, згода на обов’язковість яких надана ВР України.

Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.

За способом сприйняття:

- візуальна — сприймана органами зору;
- звукова — сприймана органами слуху;
- тактильна — сприймана тактильними рецепторами;

– нюхова — сприймана нюховими рецепторами;
– смакова — сприймана смаковими рецепторами.

За формою представлення:
– текстова — передана у вигляді символів, призначених означати лексеми мови;
– числова — у вигляді цифр і знаків, що означають математичні дії;
– графічна — у вигляді зображень, предметів, графіків;
– звукова — усна або у вигляді запису передача лексем мови аудіальним шляхом.

За призначенням:
– масова — містить тривіальні відомості і оперує набором понять, зрозумілим більшій частині соціуму;
– спеціальна — містить специфічний набір понять, при використанні відбувається передача відомостей, які можуть бути не зрозумілі основній масі соціуму, але потрібні і зрозумілі у рамках вузької соціальної групи, де використовується ця інформація;
– секретна — передана вузькому колу осіб і по закритих(захищеним) каналах;
– особиста(приватна) — набір відомостей про яку-небудь особу, що визначає соціальне положення і типи соціальних взаємодій усередині популяції.

1.3 Доступ до інформації

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформація з обмеженим доступом

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:
– виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

– розголошення інформації може завдати істотної шкоди цим інтересам;

– шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами. Віднесення інформації до державної таємниці - процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обгрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до «Зводу відомостей, що становлять державну таємницю» (ЗВДТ). До державної таємниці, згідно з Законом України «Про державну таємницю» відноситься інформація:

1) у сфері оборони:

– про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення ЗСУ та інших військових формувань;

– про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв'язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об'єктів національної економіки у воєнний час;

– про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

– про застосування систем озброєння, підготовку та проведення військових операцій;

– про винаходи, дослідження і розробку нових зразків озброєння в інтересах забезпечення національної безпеки і оборони та про результати таких досліджень і розробок;

– про заходи та показники розвитку ЗСУ та їх спроможносте;

– про склад, завдання та матеріально-технічне забезпечення розвідувального органу Міністерства оборони України та зібрану і створену ним інформацію в результаті його діяльності;

– про особовий склад Сил спеціальних операцій ЗСУ, а також осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі із Силами спеціальних операцій ЗСУ, фінансування та матеріально-технічне забезпечення руху опору, засоби, зміст, плани, організацію, завдання, форми, методи і результати ведення руху опору, оперативний резерв та мережу осередків руху опору;

2) у сфері економіки, науки і техніки:

– про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також відомості про номенклатуру та норми накопичення, загальні обсяги поставок, закладення, зберігання, освіження та відпуску, а також фактичні запаси матеріальних цінностей державних резервів;

– про використання транспорту, зв'язку, потужносте інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;

– про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

– про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

– про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, предметом яких є створення новітніх складних зразків озброєння, військової або спеціальної техніки та інші роботи, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

– про найменування, загальну кількість, вартість озброєння, військової техніки, боєприпасів, запасних частин та матеріалів до них, що закуповуються для потреб військових формувань (правоохоронних органів);

– про кількість, строки поставок військовим формуванням чи правоохоронним органам, спеціальним формуванням Міністерства внутрішніх справ України для забезпечення їх боєздатності основних видів пального (мастильних матеріалів), речового майна та продовольства;

– про факт та предмет закупівлі товарів, робіт і послуг оборонного призначення для забезпечення ЗСУ та інших військових формувань та правоохоронних органів (крім випадків, якщо окрема інформація про закупівлю таких товарів, робіт і послуг оборонного призначення, що закуповуються відповідно до Закону України "Про оборонні закупівлі", становить державну таємницю. У такому разі окрема інформація розміщується у додатку до тендерної документації). Інформація не може бути повторно віднесена до державної таємниці після розсекречення та оприлюднення;

3) у сфері зовнішніх відносин:

– про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

– про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

– про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

– про зміст секретної інформації, що отримується від іноземної держави чи міжнародної організації;

4) у сфері державної безпеки та охорони правопорядку:

– про особовий склад органів, що здійснюють оперативно-розшукову діяльність або розвідувальну чи контррозвідувальну;

– про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

– про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України "Про державну охорону органів державної влади України та посадових осіб";

– про систему урядового та спеціального зв'язку;

– про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;

– про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;

– про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

– про організацію режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

– про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;

– про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

– про організацію, стан, планування та здійснення заходів із захисту та забезпечення безпеки і стійкості об’єктів критичної інфраструктури з I та II категорій критичності, включаючи створення резервів необхідних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків на об’єктах критичної інфраструктури (крім інформації про використання коштів на закупівлі товарів, робіт та послуг, про ціну товарів, робіт, послуг, проектної документації, кошторисів, матеріальних ресурсів, необхідних для ремонту, будівництва об’єктів критичної інфраструктури), а також інформація про здійснення закупівель за закритими закупівлями;

– про інші засоби, форми і методи охорони державної таємниці.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності "особливої важливості", "цілком таємно" та "таємно". Підставою для цього є ЗВДТ, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю.

Доступ до державної таємниці виконується на підставі допуску до державної таємниці (оформлення права громадянина на доступ до секретної інформації), який надає повноважна посадова особа громадянину на ознайомлення з конкретною інформацією та провадження діяльності, пов'язаної з державною таємницею або ознайомлення з конкретною інформацією пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

До службової може належати така інформація:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами

державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

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

– про стан довкілля, якість харчових продуктів і предметів побуту;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

– 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;

– 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 особами, які брали участь або сприяли реалізації російської імперської політики, представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

– про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

– 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;

– інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана ВР України.

1.4 Ознаки та властивості інформації

До основних *ознак* інформації відносять:

– невичерпність. Інформація є невичерпною, тиражується, але не витрачається, може поширюватися в необмеженій кількості екземплярів практично без зміни її змісту і втрати якості, може належати багатьом особам, може бути використана необмежену кількість разів;

– вимірність. Інформація може бути кількісно виміряна (кількість символів, знаків);

– двоєдинство інформації та її носія. Інформація передається і поширюється в більшості випадків на матеріальному носії і за допомогою матеріального носія;

– фізична невідчужуваність інформації від її творця, власника, споживача;

– наявність організаційної форми, структури у вигляді інформаційних систем, документів, бібліотек тощо;

– цінність. Інформація має певну цінність (може продаватися);

– поширюваність. Інформація не локалізована в просторі, може легко розповсюджуватися;

– джерела інформації. Передбачені або встановлені законом носії інформації: документи, інші носії інформації, які являють собою матеріальні об’єкти, що зберігають інформацію, повідомлення ЗМІ, публічні виступи..

Цінність є найбільш повною характеристикою інформації. Цінність інформації визначається ступенем її корисності до прийняття рішення. Будучи комплексним показником, вона безпосередньо або опосередковано об'єднує практично всі властивості інформації. Цінність інформації змінюється у часі. Найчастіше вона зменшується. Проте цінність деякої інформації зростає. Прикладом такого збільшення є стародавні рукописи.

Якість інформації — міра її відповідності потребам споживачів. Ця властивість є відносною, оскільки залежить від потреб споживача інформації.

Об'єктивність інформації характеризує її незалежність від чиєї-небудь думки або свідомості, а також від методів отримання. Об'єктивніша та інформація, в яку методи отримання і обробки вносять менший елемент суб'єктивності. Відображаючись у свідомості людини, інформація може спотворюватися залежно від думки, судження, досвіду, знань конкретного суб'єкта, і, таким чином, перестати бути об'єктивною.

Достовірність - вірність інформації, вона відповідає реальності та не викликає сумнівів. Об'єктивна інформація завжди достовірна, але достовірна інформація може бути як об'єктивною, так і суб'єктивною. Причинами недостовірності можуть бути:

– умисне спотворення(дезінформація);

– неумисне спотворення суб'єктивної властивості;

– спотворення в результаті дії перешкод;

– помилки фіксації інформації.

У загальному випадку достовірність інформації досягається: вказівкою часу звершення подій, відомості про яких передаються; зіставленням даних, отриманих з різних джерел; своєчасним розкриттям дезінформації; виключенням перекрученої інформації та ін.

Захищеність – властивість, що характеризує неможливість несанкціонованого ознайомлення з інформацією, її використання чи зміни.

Адекватність — це ступінь відповідності реальному об'єктивному стану справи. Слід визначити, що завжди існує певна ступінь невизначеності. Від ступеня адекватності інформації реальному стану об’єкта або процесу залежить правильність прийняття рішень людиною. Адекватність інформації може виражатися у трьох формах: синтаксичній, семантичній, прагматичній. Синтаксична адекватність відображає формальні структурні характеристики інформації і не зачіпає її сутнісного змісту. Семантична адекватність визначає ступінь відповідності образа об’єкта та самого об’єкта. Семантичний аспект передбачає врахування сутнісного змісту повідомлення. Прагматична адекватність відображає відношення інформації та її користувачів, відповідність інформації тій меті, заради якої ця інформація отримується і яка на її основі реалізується.

Доступність означає, що інформація однозначно та зрозуміло відображає дійсність, є зрозумілою для цілком ясного й однозначного її усвідомлення тим, для кого призначається. Найбільш простим прикладом доступності для більшості наших здобувачів є отримана інформація, яка написана китайською мовою. Хоча більш мільярду людей на планеті абсолютно однозначно зрозуміють подану інформацію.

Повнота означає, що інформації достатньо для розуміння ситуації та прийняття рішення. Інформацію можна вважати повною, коли вона містить мінімальний, але достатній для ухвалення правильного рішення набір показників. Як неповна, так і надмірна інформація знижує ефективність рішень, що приймаються на підставі інформації.

Актуальність — відповідності отриманої інформації теперішньому моменту часу. Ця властивість пов’язана з тим, що будь-яка інформація з часом старіє, втрачає адекватність.

Корисність — практична цінність інформації. Корисність інформації оцінюється по тим завданням, які можливо вирішити з її допомогою.

Ергономічність – властивість, що характеризує зручність форми й обсягу інформації з погляду даного споживача

Емоційність — властивість інформації викликати різні емоції у людей. Цю властивість інформації використовують виробники медіа інформації. Чим емоції, що сильніше викликаються, тим більше вірогідності звернення уваги і запам'ятовування інформації.

1.5 Життєвий цикл інформації

Будь-яка інформація має власний життєвий цикл. Найчастіше необхідно вести розмову про створення інформації, її поширення зберігання, обробку, старіння та утилізацію. Слід зазначити, що на будь-якому етапі інформація може зазнавати деструктивних впливів.

У процесі створення інформації необхідно провести збір даних, їх пошук і перевірку, обробку та аналіз. При використанні неповних та/або неправдивих даних під час створення інформації можна отримати

інформацію, що не відповідає дійсності. Адекватність прийнятого рішення, що базується на такій інформації, викликає сумніви.

При обробці інформації внаслідок технічних несправностей, алгоритмічних та програмних помилок, помилок та деструктивних дій обслуговуючого персоналу, зовнішнього втручання, дії руйнівних та шкідливих програм (вірусів, експлойтів, черв'яків, логічних бомб) також можливе спотворення інформації.

У процесі передавання на інформацію можуть впливати різноманітні перешкоди як природного, і штучного походження. При цьому можливе її спотворення чи стирання (знищення). Крім цього, можливе перехоплення інформації з метою її модифікації та подальшого нав'язування.

У процесі зберігання основними загрозами є несанкціонований доступ для модифікації (аж до знищення) інформації, шкідливі програми (віруси, трояни, черв'яки, логічні бомби) і технічні несправності. Процес зберігання інформації багато в чому залежить від її категорії. При зберіганні носіїв інформації, яка відноситься до конфіденційної, використовують спеціально виділені приміщення, сейфи. Доступ до таких сховищ обмежений.

У процесі старіння зменшується цінність, актуальність та адекватність інформації. Основними загрозами інформації, поряд із загрозами при зберіганні, можна вважати втрату технологій, здатних відтворити ту чи іншу інформацію, та фізичне старіння носіїв інформації.

Слід зазначити те що, що у перелічених періодів життєвого циклу інформація може уточнюватися. Проведення цих змін має бути регламентовано та здійснюватися особами, які мають на це повноваження. Прикладом таких змін може бути зміна місця проживання чи права власності у базах даних відповідних структур.

У процесі знищення основними загрозами інформації є витік конфіденційної інформації. Особливо це стосується обчислювальної техніки. Для гарантованого видалення інформації з електронних носіїв необхідно багаторазовий запис та стирання нулів та одиниць. Якщо йдеться про секретну інформацію, то необхідне фізичне знищення носія. Це стосується як друкованих видань, так і електронних носіїв (флешок, вінчестерів, дисків).

РОЗДІЛ 2 ІНФОРМАЦІЙНА БЕЗПЕКА

2.1 Визначення інформаційної безпеки

Зупинимося на терміні інформаційної безпеки. .На жаль Україна не має закону про ІБ та однозначного тлумачення терміну ІБ в інших законах. Існує велика кількість означень, що пояснюють значення ІБ, але всі вони є досить специфічними або характеризують цю область досить у вузькому діапазоні. Розглянемо означення ІБ, яке надано у ЗУ «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»: інформаційна безпека - 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 розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Це означення має глибоке внутрішнє протиріччя, яке дискредитує саме означення. Відповімо на запитання «Що таке несанкціоноване розповсюдження інформації?» Це означає, що будь-яка інформація повинна отримати дозволу на поширення. Це означає наявність органу, який дає цей дозвіл, тобто цензора, який обмежує доступність інформації. Зрозумілою є наявність цього органу, коли йдеться про конфіденційну інформацію, але в цьому фрагменті означення мається на увазі вся інформація, оскільки про конфіденційну інформацію йдеться нижче. Про те Конституція Україні (ст. 15) та ЗУ «Про інформацію» забороняють будь-яку цензуру.

Розглянемо наступний фрагмент «запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується». Це говорить про те, що повна, своєчасна і достовірна інформація не може завдати шкоди, а наступною частиною «негативний інформаційний вплив », виключається така можливість. Слід зазначити, що перший розглянутий фрагмент в цьому абзаці є не що інше, як порушення цілісності інформації, про яку йдеться наприкінці визначення.

Абсолютно незрозуміло, які можуть бути «негативні наслідки застосування інформаційних технологій», якщо дотримується цілісність, конфіденційність і доступність інформації. Негативні наслідки можуть настати при використанні достовірної інформації, яка несе потенційну загрозу. При цьому інформація залишається відкритою і доступною. Тут може йтися про безпечну інформацію.

Деякими авторами ІБ описується, як захищеність установлених законом правил, з якими відбуваються інформаційні процесі в державі, що забезпечують гарантовані Конституцію умови існування і розвитку людини, усього суспільства і держави. Це тлумачення ототожнює ІБ та ІБ держави, тобто звужує саме поняття ІБ.

У роботах дається наступне тлумачення ІБ: стан, що забезпечує захищеність інформаційних ресурсів і каналів, а також доступу до джерел інформації або як захищеність інформації на будь-яких носіях від випадкових і навмисних несанкціонованих впливів природного чи штучного характеру, спрямованих на знищення, руйнування, видозміни тих або інших даних, змінення ступеня доступності цінних відомостей. Ці визначення є дуже близьким до поняттям ІБ інформаційних систем та прирівнюється до безпеки інформації.

Визначення ІБ як стану захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), при якому сторонні інформаційні впливи не завдають їм суттєвої шкоди, є найбільш оптимальним тому, що об'єднує пасивну (стан захищеності) та активну (стан інформаційного розвитку) складові, а також є лаконічним, і передбачається поділ ІБ на різновиди та дається чітке визначення, але в цьому визначенні проходить заміна поняття ІБ на безпечну інформацію.

Історично поняття ІБ виникла, як калька англійського терміну *information security*. Рівнозначним його перекладом є захист інформації (ЗІ). У НД ТЗІ 1.1-003-99 *information security* має переклад «безпека інформації» та означає стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Слід розглянути ті особливості ІБ, грунтуючись на які можна дати означення цьому терміну. Коли говорять про ІБ, то повинно йтися про якусь систему, наприклад державу, корпорацію, телекомунікаційну мережу або щось інше.

Філософський енциклопедичний словник трактує систему як сукупність визначених елементів, між якими існує закономірний зв’язок чи взаємодія. Якісні характеристики цих елементів становлять зміст системи, сукупність закономірних зв’язків між елементами - внутрішню форму, або структуру системи. Кожна система має кілька властивостей і може перебувати в тому чи іншому стані.

Стан системи – це характеристика системи на певний момент її функціонування. Поняття стану характеризує миттєву «фотографію», тимчасовий «зріз» системи. Стан системи в певний момент часу - це безліч її істотних властивостей у цей момент часу.

Поняття ІБ завжди має бути логічно прив'язане до інформації, засобів її оброблення, зберігання, доставки, впливу на об'єкт. У життєвому циклі інформацію можна піддати різним видам впливів, спрямованим на порушення конфіденційності, цілісності та доступу до інформації. Слід сказати, що в багатьох нормативних документах як ІБ, так і ІБ держави розглядаються в певний конкретний момент часу, наприклад говориться, що «Доктрина інформаційної безпеки України спрямована на забезпечення необхідного рівня інформаційної безпеки України до конкретних умов цього

історичного періоду», тобто ІБ має бути забезпеченою деякий час. Залежно від системи цей час може бути різним.

Виходячи з викладеного вище, пропонується таке означення ІБ: інформаційна безпека - властивість системи протягом заданого часу протистояти несанкціонованому зняттю та модифікації інформації.

Під несанкціонованим зняттям розуміється отримання інформації, до якої в абонента немає доступу, тобто порушення правил доступу. Під несанкціонованою модифікацією розуміється змінення інформації, яке призводить до порушення її цілісності. Слід зазначити, що цілісність у загальному випадку це не тільки отримана інформація в початковому вигляді, але і її повнота.

Розглянувши детально всі аспекти терміну «інформаційна безпека», логічно буде навести і її складові. ІБ являє собою комплекс заходів, основним завданням якого є забезпечення таких властивостей інформаційних систем:

– конфіденційність - можливість ознайомитися з інформацією (саме з даними або відомостями, що несуть смислове навантаження, а не з послідовністю символів) мають у своєму розпорядженні тільки ті особи, які мають відповідні повноваження;

– цілісність - можливість змінити інформацію повинні мати тільки ті особи, яких на це уповноважено;

– доступність - можливість отримання авторизованого доступу до інформації з боку уповноважених осіб у відповідний санкціонований для роботи період часу.

Згідно з керівними документами та стандартами (НД ТЗІ 2.5-004-99, ДСТУ ISO/IEC 27000:2019) до цього списку може бути додано такі властивості:

– неспростовність - можливість засвідчувати подію, яка мала місце, або дію і їх суб'єкти так, щоб ця подія або дія і суб'єкти, які мають до нього відношення, не могли бути поставлені під сумнів;

– апелювання – не можливість особи, яка направила інформацію іншій особі, відректися від факту направлення інформації, а особа, що отримала інформацію, не може відректися від факту її отримання;

– спостереженість – можливість провести ідентифікацію та контроль з діями користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки та/або забезпечення відповідальності з певні дії.

Допоміжні фактори, які допомагають конкретизувати ІБ:

– облік, тобто всі значимі дії особи, виконувані ним в рамках, контрольованих системою безпеки (навіть якщо вони не виходять з рамки визначених для цієї особи правил), повинні бути зафіксованій й проаналізовані;

– автентифікація - перевірка достовірності користувача інформаційної системи через порівняння введеного ним пароля з паролем, збереженим у базі даних користувачів.

Слід відзначити, що існують и інші визначення наведених термінів.

Наприклад, згідно з НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»:

– конфіденційність інформації— властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;

– цілісність інформації— властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом;

– цілісність системи — властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;

– доступність — властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;

– спостереженість — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Слід зазначити той факт, що з точки зору теорії, інформація не має властивостей конфіденційності та цілісності. У цих визначеннях безпосередньо бере участь поняття комп'ютерної системи. І це необхідно враховувати під час використання даних визначень.

2.2 Модель інформаційної безпеки

2.2.1 Концептуальна модель інформаційної безпеки

Побудова концептуальної моделі (КМ) дає змогу подивитися на проблему ІБ ніби то з боку. Завдяки чому можна абстрагуватися від незалежних від дослідника впливів, при цьому залишається можливість їх нейтралізації. Існує велика кількість КМ ІБ. Однак більшість КМ ІБ є однорангові графи, де як вузлова вершина подається інформація, інші вершини не пов'язані одна з одною Один з таких варіантів показано на рис. 2.1.

Рисунок 2.1 – Концептуальна схема інформаційної безпеки

У деяких моделях гілка може складатися з двох або трьох вершин, які можуть гілкуватися, але вони теж не пов'язані з іншими гілками.

Концептуальна модель інформаційної безпеки зображена на рис. 2.2.

Рисунок 2.2 – Концептуальна схема інформаційної безпеки

Вона включає наступні елементи:

– носії інформації (особи, що обізнані з таємницею, документальні матеріали, машинні носії, фізичні поля);

– джерела загроз інформації (конкуренти, зловмисники, спеціальні служби);

- цілі порушників (здобуття цінної інформації науково-технічного характери, інформації у сфері безпеки та оборони, нанесення збитків, отримання переваг, корисні мотиви тощо);
- методи доступу (агентурні, технічні);
- загрози інформації (конфіденційності, цілісності, доступності);
- об’єкти загроз (відомості економічного, науково-технічного, оборонного характеру тощо);
- методи захисту (правові, організаційні, інженерно-технічні, технічний, криптографічний та стеганографічний захист);
- засоби захисту (технічні, апаратні та програмні в комп’ютерних системах).

Головний недолік подібних моделей полягає в тому, що на них дуже докладно наведено складові елементи, в яких важко розібратися. Однією з основних вимог до КМ є високий рівень абстракції.

При будуванні подібних моделей необхідно відповісти на найбільш загальні питання забезпечення ІБ того чи іншого об'єкта, причому його складність не повинна впливати на КМ. Необхідний високий рівень абстракції дає змогу вирішити завдання, які поставлено вище. Концептуальна модель ІБ ІКС зображено на рис. 2.3

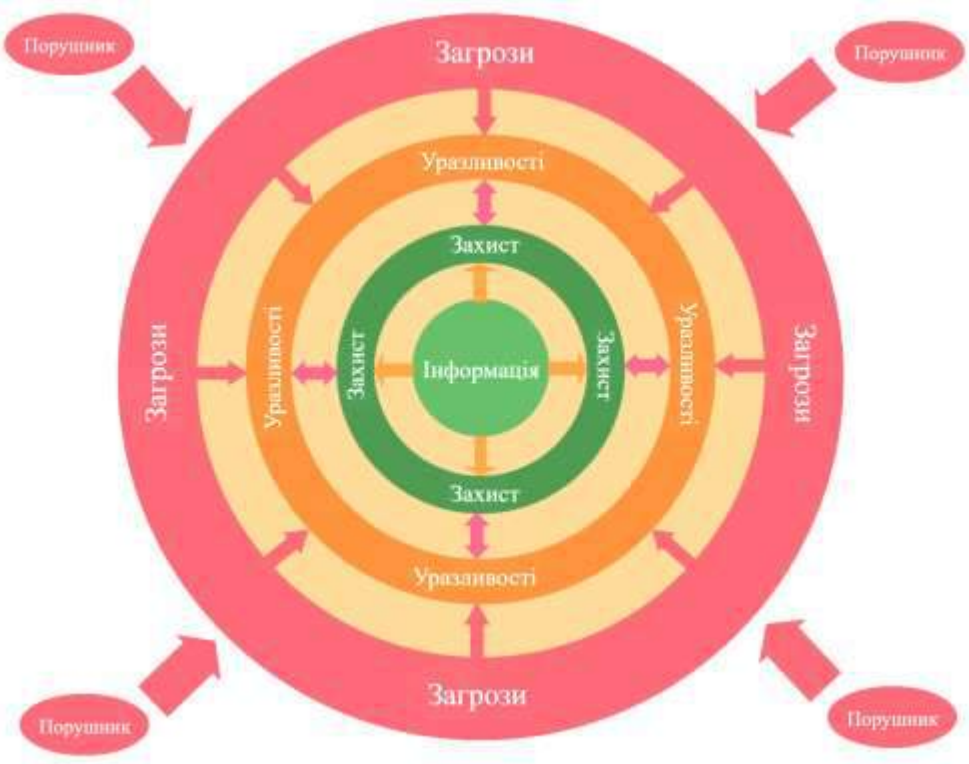

Рисунок 2.3 – Концептуальна схема інформаційної безпеки.

У запропонованій моделі ключовим елементом є інформація. З цінності цієї інформації будується система захисту. Система захисту безпосередньо пов'язана з можливими уразливостями, перебуваючи з

ними в тісному діалектичному зв'язку. Система захисту має змінюватися залежно від виникнення нових уразливостей. Прикладом таких змін можуть бути поновлення, які регулярно приходять кожному користувачеві мобільного телефону або персонального комп'ютера. Суть таких оновлень полягає в перебудові внутрішньої системи захисту від нововиявлених можливостей втручання в роботу цього пристрою. Загрози ІБ грунтуються на уразливостях, які ще не усунуто організатором захисту. Порушник здійснює вплив на інформацію через загрози та уразливості, долаючи захист. Слід зазначити той факт, що порушники можуть діяти як поодинці, так і вступаючи в попередній злочинний зговір.

Перевагою наведеної моделі є, по-перше, високий рівень абстракції, тому що ця модель годиться для будь-якої системи, по-друге, на ній наведено всі діалектичні зв'язки між інформацією, яку необхідно захищати, системою захисту, можливими уразливими, яких не було враховано під час створення або виникли під час експлуатації, загрозами, які можуть використовувати наявні уразливості, і самими порушниками, які можуть використовувати наявні уразливості через погрози, для впливу на інформацію.

До основних елементів системи інформаційної безпеки слід віднести цінності, інтереси та цілі.

Цінність – властивість того чи іншого предмета, явища задовольняти потреби, бажання, інтереси соціального суб'єкта (індивіда, групи людей суспільства).

Інтереси – це усвідомлені потреби, сформовані фахівцями в даній предметній області. Потреби ІБ – це необхідність її підтримки на належному рівні, тобто – необхідність забезпечення ІБ.

Однак більш важливим елементом формування процесу щодо забезпечення ІБ, ніж цінності та інтереси, виступають цілі в інформаційній сфері. Цілі в інформаційній сфері – це суть мотиваційних установок, орієнтованих на досягнення необхідної ІБ.

Важливим елементом (підсистемою) системи ІБ виступає також система небезпек і загроз (джерела загроз і загрози ІБ), що представляє собою сукупність факторів обстановки, здатних негативно впливати на ІБ в цілому.

2.2.2 Модель загроз

Моделі загроз є моделями другого рівня. Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків ІКС.

Ключовими в цьому визначенні є слова: «умова», «фактор» і «небезпека».

Умова – те, від чого залежить щось інше. Найчастіше умови розглядаються як щось зовнішнє для явища, на відміну від більш широкого поняття причини, що включає як зовнішні, так і внутрішні чинники.

Фактор – причина, рушійна сила будь-якого процесу, явища, визначає його характер або окремі його риси.

Небезпека – здатність заподіяти якоїсь шкоди; можливість чого-небудь небезпечного.

У змістовному плані поняття небезпека – це сукупність умов і факторів, що викликають порушення нормального функціонування і розвитку будь-якої системи (інформаційної системи). Для того щоб розкрити зміст будь-якої небезпеки, необхідно знати конкретний перелік таких умов і факторів.

Головні цілі забезпечення ІБ – запобігання, локалізація і нейтралізація загроз в інформаційній сфері.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в ІКС:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в ІКС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІКС і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів ІКС;

– наслідки помилок під час проектування та розробки компонентів ІКС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) ІКС під час експлуатації;

– навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості ІКС.

Практично усі шляхи порушення конфіденційності так чи інакше зводяться до втрати контролю над СЗІ та виникнення КВІ. Втрата керування СЗІ може бути реалізована внаслідок різних причин та джерел порушень безпеки. Зрозуміло, що в реальному житті слід розглядати їх комбінації. Вони можуть бути також причиною виникнення прихованих каналів витоку інформації.

Прихований КВІ – це спосіб отримання інформації за рахунок використання шляхів передачі інформації, які присутні в ІКС, але не керуються або не спостерігаються СЗІ. КВІ характеризують ситуацію, коли або проектувальники не змогли попередити НСД, або СЗІ не в змозі розглядати такий доступ як заборонений.

Загалом КВІ в ІКС вважатимуться несприятливі доступи користувача U_i до об'єкта O через ланцюжок доступів $a_k \in \mathbf{A}$, k=1,…K наступного виду

$$U_i \xrightarrow{a_k} *O, \quad U_j \xrightarrow{a_l} *O, \quad i \neq j, k \neq l$$

Будемо також вважати, що якщо $O \in \boldsymbol{R}_t^*$, де $R_t^* = \bigcup_i D_t(U_i)$, а

$$D_t(U_i) = \left\{ O_j \mid U_i \xrightarrow{a} *O_j, a \in \mathbf{A}, t \in \mathbf{N}_0 \right\},$$

то ніякі доступи $\forall a_k \in \mathbf{A}$, не можуть створити КВІ.

Відповідно до структури множини доступів і ІКС, можна записати вираз для КВІ або, іншими словами, загрози конфіденційності:

$$\exists t \in \boldsymbol{N}_0, \exists a \in \mathbf{A}_1, \exists U_i \in \boldsymbol{U}_t, \exists O \in \boldsymbol{O}_t, \; U_i \xrightarrow{a} *O,$$
$$O \in O_t(U_j), \; i \neq j; \; i, j = 1, \ldots, n_U,$$

змістовний сенс якого у тому, що у певний час існує деякий несприятливий вид доступу певного користувача до об'єкту, створеному іншим користувачем.

З метою протидії загрозам конфіденційності в ІКС запроваджується низка послуг:

– довірча конфіденційність – це управління доступом, у якому засоби захисту дозволяють звичайним користувачам управляти (передають управління) потоками інформації між іншими користувачами та об'єктами свого домену (наприклад, виходячи з права власності об'єкта), тобто. призначення та передача повноважень не потребують адміністративного втручання;

– адміністративна конфіденційність – таке управління, у якому засоби захисту дозволяють керувати потоками інформації між

користувачами та об'єктами лише спеціально авторизованим користувачам;

– повторне використання об'єктів - якщо перед наданням об'єкта користувачеві або процесу в ньому не залишається інформації, яку він містив, та скасовуються попередні права доступу до цього об'єкта;

– аналіз прихованих каналів – проводиться з метою виявлення та перекриття існуючих потоків інформації, які не контролюються іншими послугами;

– конфіденційність при обміні – дозволяє забезпечити безпеку обміну інформацією між захищеними об'єктами у незахищеному середовищі.

Мова опису загроз цілісності інформації є аналогічною мові опису загроз конфіденційності. Однак між загрозами цим властивостям є принципова різниця. Так, для конфіденційності основна загроза – це незаконне ознайомлення з інформацією, тобто на саму інформацію активна дія відсутня. Виявилося, що для опису такої загрози достатньо поняття КВІ. Для цілісності ж основна загроза – це незаконна модифікація інформації, тобто активна дія на інформацію з боку порушника.

Отже, замість звичайного КВІ зручно ввести поняття каналу дії на цілісність. Формально це зводиться до заміни доступу на читання (r) доступом на запис (w). Тоді, скориставшись представленому вище формалізмом, запишемо наступний вираз для визначення каналу дії на цілісність

$$\exists t \in \boldsymbol{N}_0,\ \exists \boldsymbol{a} \in \mathbf{R}_i,\ \exists U_i \in \boldsymbol{U}_t,\ \exists O \in \boldsymbol{O}_t,\ U_i \xrightarrow{a} {}^*O,$$

$$O \in O_t(U_j),\ i \neq j;\ i, j = 1,\ldots,n_U$$

де R_i - підмножина доступів, за якими можлива модифікація інформації. Отже, в деякий момент часу існують певні види доступу до інших об’єктів, що можливі для деякого користувача. Такі доступи вважаються несприятливими.

Прикладом виникнення каналу дії на цілісність є використання програми «троянський кінь». Така програма, крім документованих функцій, може здійснювати приховані дії від того, хто її активізує, на користь розробника програми (зловмисника). Як правило, «троянський кінь» використовується для модифікації захищеної інформації.

Порушення цілісності може виникнути внаслідок створення випадкових або навмисних критичних ситуацій, зараження вірусами тощо. Серед механізмів захисту від порушень цілісності виділяються наступні:

– своєчасне регулярне копіювання цінної інформації;

– введення надмірності в саму інформацію, тобто застосування завадостійкого кодування інформації, що дозволяє забезпечити її цілісність;

– введення надмірності в процес обробки інформації, тобто використання автентифікації, що дозволяє контролювати цілісність файлів, повідомлень і програм;

– введення системної надмірності, тобто, за військовою термінологією, підвищення «живучості» системи.

Порушення доступності може виникнути внаслідок різних причин порушень безпеки та їх джерел. Відповідно до визначення доступності, особа, використовуючи ресурси ІКС за правилами політики безпеки, повинна отримати інформацію в необхідному їй вигляді, місці і вчасно.

Доступність в ІКС забезпечується правильним використанням ресурсів, стійкістю до відмов окремих компонент, можливістю їх ефективної заміни («гаряча» заміна), здатністю до відновлення після збоїв.

В більшості випадків доступність в ІКС інформації визначається працездатністю самої ІКС, тобто її відсутність слід вважати основною загрозою. Можна виділити наступні напрямки повсякденної діяльності в ІКС для підтримки її працездатності:

– підтримка користувачів, тобто консультації і різного роду допомоги користувачам;

– конфігураційне керування, яке дозволяє контролювати зміни в програмній конфігурації;

– резервне копіювання;

– керування носіями, що забезпечує фізичний захист носіїв;

– документування;

– регламентні роботи.

Оскільки результатом дії будь-якої загрози доступності є її відсутність або відсутність будь-яких каналів доступу, то формально це можна виразити наступним чином

$$\exists t \in \boldsymbol{N}_0,\ \neg\exists a_k \in \mathbf{A}_1 \cup \mathbf{A}_2,\ \exists U_i \in \boldsymbol{U}_t,\ \exists O \in \boldsymbol{O}_t,\ \exists i,\ \exists k,\ U_i \xrightarrow{a_k} {}^*O,\ O \in O_t(U_i),$$

а також

$$\exists t \in \boldsymbol{N}_0,\ (\neg\exists a \in \mathbf{A}_1) \vee (\neg\exists a \in \mathbf{A}_2),\ \exists U_i \in \boldsymbol{U}_t,\ \exists O \in \boldsymbol{O}_t,\ \exists i,\ U_i \xrightarrow{a} {}^*O,\ O \notin O_t(U_i).$$

Послуги доступні такі:

– використання ресурсів – дозволяє користувачам керувати використанням послуг та ресурсів;

– стійкість до відмови – покликана гарантувати доступність ІКС (можливість використання інформації, окремих функцій або ІКС загалом) після відмови її компонента;

– гаряча заміна – дозволяє гарантувати доступність ІКС у процесі заміни окремих компонентів;

– відновлення після збоїв – забезпечує повернення ІКС до відомого захищеного стану після відмови в обговоренні.

На відміну від конфіденційності або цілісності, де наявність каналів витоку є негативною обставиною, спостереженість зобов'язує мати канали спостереження. Тобто канали, за допомогою яких можна отримати доступ на читання до певної множини процесів та об'єктів, якщо вважати, що доступ на читання з об'єкта забезпечує можливість його спостерігати. Формально це можна зобразити наступним чином

$$U \xrightarrow{r,\,act} P \xrightarrow{r} \{P_k, O_l\},\ k=1,\ldots,K;\ l=1,\ldots,L,$$

тобто користувач U_1 активізує процес P, який може отримати доступ на читання (r) до певної множини процесів та об'єктів $\{P_k, O_l\}$. Термін певна множина має на увазі обраний і фіксований перелік подій, які мають відношення до безпеки інформації в ІКС. Слід також звернути увагу на те, що доступ на читання (r) є досить сильною вимогою, оскільки для спостереженості достатньо більш слабкого доступу (який, наприклад, дозволяв би тільки визначати – була подія чи ні). Загроза спостереження полягає в тому, що користувач, який має відповідні повноваження, не може отримати доступ з A_3 до інформації, що формально виражається наступним чином

$$\exists t \in \boldsymbol{N}_0,\ \overline{\exists a \in \mathbf{A}_3},\ \exists U_i \in \boldsymbol{U}_t,\ \exists O \in \boldsymbol{O}_t,\ \exists i,\ U_i \xrightarrow{a} {}^*O, O \in O_t(U_j), \forall j.$$

Очевидно, що загрози спостереження зводяться до пошкодження каналів спостереження, а головне завдання спостереження в ІКС – підтримувати їх. Вона реалізується за допомогою послуг:

– реєстрація (аудит) – дозволяє контролювати несприятливі для ІКС дії;

– ідентифікація та аутентифікація – дозволяють СЗІ визначити та перевірити особу користувача, який намагається отримати доступ до ІКС;

– достовірний канал – дозволяє гарантувати, що користувач взаємодіє безпосередньо із СЗІ і жодний інший користувач чи процес не може включитися у взаємодію;

– розмежування обов'язків – дозволяє знизити ймовірність навмисних чи помилкових дій користувача та величину потенційних збитків від таких дій;

– цілісність КСЗІ – визначає міру готовності КСЗІ захищати себе та гарантувати безперебійність управління захищеними об'єктами;

– самотестування – дозволяє перевірити, і на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ІКС;

– ідентифікація та аутентифікація при обміні – дозволяє одному об'єкту ідентифікувати інший та забезпечити іншому ідентифікувати перший, перш ніж розпочати взаємодію;

– автентифікація відправника – дозволяє забезпечити захист від відмови від авторства та однозначно встановити належність об'єкта певному користувачеві;

– аутентифікація одержувача – дозволяє забезпечити захист від відмови від отримання та однозначно встановити факт отримання об'єкта певним користувачем.

Випадковими загрозами суб’єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови ІКС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи ІКС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

– неумисне зараження ПЗ комп’ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в ІКС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

– наслідки некомпетентного застосування засобів захисту;

– інші.

Навмисними загрозами суб’єктивної природи, спрямованими на дезорганізацію роботи ІКС або виведення її з ладу, проникнення в систему і одержання можливості НСД до її ресурсів, можуть бути:

– порушення фізичної цілісності ІКС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІКС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);

– порушення режимів функціонування ІКС (обладнання і ПЗ);

– впровадження і використання комп’ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу ІКС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам’яті ЕОМ, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача (“маскарад”);

– неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;

– впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

– інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

– на порушення яких властивостей інформації або ІКС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості ІКС);

– джерела виникнення (які суб’єкти ІКС або суб’єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

– можливі способи здійснення загроз.

2.2.3 Модель порушника

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної ІКС. Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії т. ін. По відношенню до ІКС порушники можуть бути:

– внутрішніми – з числа співробітників, користувачів системи

– зовнішніми – сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони.

Таксономію порушників зображено на рис.2.4

Модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для ІКС;

– категорії осіб, з числа яких може бути порушник.;
– припущення про кваліфікацію порушника;
– припущення про характер його дій.

Рисунок 2.4 - Таксономія порушників

Метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами ІКС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– перший рівень визначає найнижчий рівень можливостей ведення діалогу з ІКС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням ІКС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення ІКС, аж до включення до складу ІКС власних засобів з новими функціями обробки інформації.

За рівнем знань про ІКС усіх порушників можна класифікувати як таких, що володіють:

– інформацією про функціональні особливості ІКС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації ІКС;

– інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що використовують:

– виключно агентурні методи одержання відомостей;

– пасивні технічні засоби перехоплення інформаційних сигналів;

– виключно штатні засоби ІКС або недоліки проектування КС ЗІ для реалізації спроб НСД;

– способи і засоби активного впливу на ІКС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

– без одержання доступу на контрольовану територію організації (ІКС);

– з одержанням доступу на контрольовану територію, але без доступу до технічних засобів ІКС;

– з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів ІКС;

– з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

– з одержанням доступу до засобів адміністрування ІКС і засобів керування КСЗІ.

Таксономії, подібні зображеної на рис. 2.4, також можна визначити для інших специфікацій порушників, що класифікуються за :

– мотивами здійснення порушень;

– метою здійснення порушень;
– за рівнем кваліфікації та обізнаності щодо ІКС;
– за можливостями використання засобів і методів подолання систем захисту;
– за часом дії;
– за місцем дії.

Онтологічна модель порушника зображена на рис.2.5

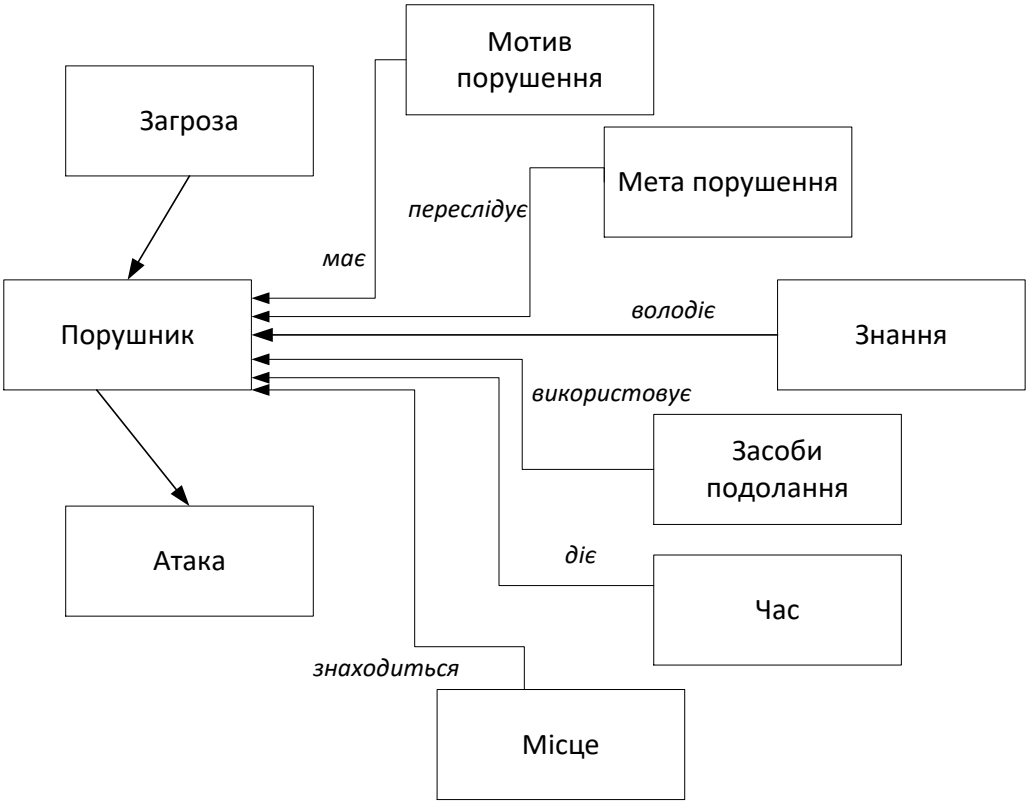

Рисунок 2.5 - Онтологічна модель порушника

2.2.4 Політика безпеки інформації в ІКС

Під політикою безпеки інформації (далі - політика безпеки) слід розуміти набір вимог, правил, обмежень, рекомендацій т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо ІКС, окремого її компонента, послуги захисту, що реалізується системою т. ін. Політика безпеки інформації в ІКС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В ІКС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в ІКС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів ІКС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів ІКС політика безпеки стосується, а яких – ні).

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в ІКС кожного з цих видів.

Політика безпеки повинна базуватися на наступних основних принципах:

– системності;
– комплексності;
– неперервності захисту;
– достатності механізмів і заходів захисту та їхньої адекватності загрозам;
– гнучкості керування системою захисту, простоти і зручності її використання;
– відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки повинна доказово давати гарантії того, що:

– в ІКС (в кожній окремій складовій частині, в кожному функціональному завданні т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;
– реалізація заходів захисту інформації є рентабельною;
– в будь-якому середовищі функціонування ІКС забезпечується оцінюваність і перевіряємість захищеності інформації;
– забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів ІКС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування ІКС;
– персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;

– всі критичні з точки зору безпеки інформації технології (функції) ІКС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;

– враховані вимоги всіх документів, які регламентують порядок захисту інформації в ІКС, та забезпечується їхнє суворе дотримання.

Політика безпеки розробляється на підготовчому етапі (НД ТЗІ 3.7-001-99) створення КСЗІ. Методологія розроблення політики безпеки включає в себе наступні роботи:

– розробка концепції безпеки інформації в ІКС;

– аналіз ризиків;

– визначення вимог до заходів, методів та засобів захисту;

– вибір основних рішень з забезпечення безпеки інформації;

– організація виконання відновлювальних робіт і забезпечення неперервного функціонування ІКС;

– документальне оформлення політики безпеки.

Концепція безпеки інформації в ІКС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної ІКС і виконується на підставі аналізу наступних чинників:

– правових і (або) договірних засад;

– вимог до забезпечення безпеки інформації згідно з завданнями і функціями ІКС;

– загроз, яким зазнають впливу ресурси ІКС, що підлягають захисту.

За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в ІКС:

– мета і пріоритети, яких необхідно дотримуватись в ІКС під час забезпечення безпеки інформації;

– загальні напрями діяльності, необхідні для досягнення цієї мети;

– аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;

– відповідальність посадових осіб та інших суб’єктів взаємовідносин в ІКС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

2.2.5 Аналіз ризиків

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в ІКС. Під час проведення аналізу ризиків необхідним є виконання наступних робіт:

– визначення компонентів і ресурсів ІКС, які необхідно враховувати при аналізі;
– ідентифікація загроз з об’єктами захисту;
– оцінка ризиків;
– оцінювання величини можливих збитків, пов'язаних з реалізацією загроз;
– вибір варіанту побудови КСЗІ;
– оцінювання витрат на КСЗІ.

Визначення компонентів і ресурсів ІКС, які необхідно враховувати при аналізі. Повинні бути визначені критичні з точки зору безпеки компоненти і ресурси ІКС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об’єкти захисту). Для цього використовуються відомості, одержані в результаті обстеження середовищ функціонування ІКС.

Ідентифікація загроз з об’єктами захисту. Встановлюється відповідність моделі загроз і об’єктів захисту, тобто складається матриця загрози/компоненти (ресурси) ІКС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс ІКС. У процесі упорядкування матриці може уточнювати список загроз і об’єктів захисту, внаслідок чого коригуватись модель загроз.

Оцінка ризиків. Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На практиці для більшості загроз неможливо одержати достатньо об’єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз. Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені ІКС (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості ІКС внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків - відсутня, низька, середня, висока, неприпустимо висока).

Вибір варіанту побудови КСЗІ. В залежності від конфіденційності інформації, яка обробляється в ІКС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника ІКС, а також інших чинників обгрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ. Можливі наступні варіанти:

– досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІКС;

– досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в ІКС;

– досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в ІКС.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

Оцінювання витрат на КСЗІ. Здійснюється первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів. На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм “ефективність/вартість”), вибирається найбільш оптимальна серед них і первинна оцінка уточняється.

Якщо залишковий ризик перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийнятного результату.

2.2.6 Визначення вимог до заходів, методів та засобів захисту

Вихідними даними для розробки є:

– завдання і функції ІКС;

– результати аналізу середовищ функціонування ІКС;

- модель загроз, модель порушників;
- результати аналізу ризиків.

На підставі цих даних визначаються компоненти ІКС (наприклад, окрема ЛОМ, спеціалізований АРМ, Internet-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІКС.

Для кожного компонента та (або) ІКС в цілому формується перелік необхідних функціональних послуг захисту від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг (згідно з НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99). Визначені вимоги складають профіль захищеності інформації в ІКС (компоненті).

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи ІКС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній ІКС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред’являються.

Для стандартних функціональних профілів захищеності не вимагається ні зв’язаної з ними політики безпеки, ні рівня гарантій, хоч їх наявність і допускається в разі необхідності. Політика безпеки КС, що реалізує певний стандартний профіль, має бути «успадкована» з відповідних документів, що встановлюють вимоги до порядку обробки певної інформації в ІКС.

Так, один і той же профіль захищеності може використовуватись для опису функціональних вимог з захисту оброблюваної інформації і для ОС, і для СУБД, в той час, як їх політика безпеки, зокрема визначення об’єктів, буде різною.

Для кожного компонента та (або) ІКС в цілому визначаються загальні підходи та вимоги з захисту інформації від витоку технічними каналами.

На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами.

2.2.7 Вибір основних рішень з забезпечення безпеки інформації

Комплекс заходів з забезпечення безпеки інформації розглядається на трьох рівнях:

- правовому;
- організаційному;
- технічному.

На правовому рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

– системи нормативно-правового забезпечення робіт з захисту інформації в ІКС (організації);

– підтримки керівництвом організації заходів з забезпечення безпеки інформації в ІКС (організації), виконання правових та (або) договірних вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників СЗІ;

– процедур доведення до персоналу і користувачів ІКС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;

– системи контролю за своєчасністю, ефективністю і повнотою реалізації в ІКС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

– застосування режимних заходів на об’єктах ІКС;

– забезпечення фізичного захисту обладнання ІКС, носіїв інформації, інших ресурсів;

– організації проведення обстеження середовищ функціонування ІКС;

– порядку виконання робіт з захисту інформації, взаємодії з цих питань з іншими суб’єктами системи ТЗІ в Україні;

– виконання робіт з модернізації ІКС (окремих компонентів);

– регламентації доступу сторонніх користувачів до ресурсів ІКС;

– регламентації доступу власних користувачів і персоналу до ресурсів ІКС;

– здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів та ін.);

– реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до ІКС, використання мереж передачі даних загального користування, зокрема Internet, використання несертифікованого ПЗ та ін.).

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації.

Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

– інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти ІКС, експлуатація і супроводження засобів блокування технічних каналів витоку інформації;

– реєстрація санкціонованих користувачів ІКС, авторизація користувачів в системі;

– керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;

– виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

– перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в ІКС;

– забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;

– резервне копіювання критичних даних, супроводження архівів даних і ПЗ;

– відновлення роботи ІКС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;

– захист ПЗ, окремих компонентів і ІКС в цілому від внесення несанкціонованих доповнень і змін;

– забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

2.2.8 Організація проведення відновлювальних робіт і забезпечення неперервного функціонування ІКС

Повинні бути вироблені підходи щодо планування і порядку виконання відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування ІКС в захищеному режимі. Під час планування цих робіт рекомендується враховувати наступні питання:

– виявлення критичних з точки зору безпеки процесів у роботі ІКС;

– визначення можливого негативного впливу надзвичайних ситуацій на роботу ІКС;

– визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;

– підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

План проведення відновлювальних робіт і забезпечення неперервного функціонування ІКС повинен описувати дії щодо улагодження інциденту, дії щодо резервування, дії щодо відновлення. Він включає в себе:

– опис типових надзвичайних ситуацій, які потенційно найбільш можливі в ІКС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;

– опис процедур реагування на надзвичайні ситуації, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;

– опис процедур тимчасового переводу ІКС або окремих її компонентів на аварійний режим роботи;

– опис процедур поновлення нормальної виробничої діяльності ІКС або окремих її компонентів;

– порядок тестування плану, тобто проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

План проведення відновлювальних робіт і забезпечення неперервного функціонування ІКС підлягає перегляду у разі виникнення істотних змін в ІКС.

Такими змінами можуть бути:

– встановлення нового обладнання або модернізація існуючого, включення до складу ІКС нових компонентів;

– встановлення нових систем життєзабезпечення ІКС;

– проведення будівельно-ремонтних робіт;

– організаційні зміни у структурі ІКС, виробничих процесах, процедурах обслуговування ІКС;

– зміни у технології обробки інформації;

– зміни у програмному забезпеченні;

– будь-які зміни у складі і функціях КСЗІ.

2.2.9 Правила розмежування доступу

Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів ІКС, складають ПРД. ПРД - є певним абстрактним механізмом, який виступає посередником при будь-яких взаємодіях об’єктів ІКС і є найбільш суттєвим елементом політики безпеки.

Як приклад, загальні ПРД можуть бути наступними (за припущення, що в ІКС визначено такі ієрархічні ролі – адміністратор безпеки ІКС, адміністратор, користувач):

– кожне робоче місце повинно мати свого адміністратора, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов’язаних з обробкою інформації та її захистом. Таку роль може виконувати уповноважений користувач. Цей користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

– для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів ІКС, керування механізмами захисту здійснюється адміністратором безпеки ІКС;

– для попередження поширення комп’ютерних вірусів відповідальність за дотримання правил використання ПЗ несуть: на АРМ –

користувачі, адміністратор, в ІКС - адміністратор безпеки ІКС. Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки;

– за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки ІКС. Такі роботи виконуються за його дозволом;

– кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки ІКС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

– користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІКС;

– атрибути користувачів періодично змінюються, а невикористовувані і скомпрометовані – видаляються;

– процедури використання активного мережевого обладнання, а також окремих видів ПЗ, яке може суттєво впливати на безпеку (аналізатори трафіку, аналізатори безпеки мереж, засоби адміністрування та ін.), авторизовані і здійснюються під контролем адміністратора безпеки ІКС;

– усі користувачі повинні знати “Інструкцію користувача” (пройти відповідний курс навчання, скласти іспит);

– адміністратор безпеки ІКС і адміністратори повсякденно здійснюють перевірку працездатності засобів захисту інформації, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

2.2.10 Документальне оформлення політики безпеки

Результати робіт з розроблення політики безпеки оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в ІКС. Структурно до політики безпеки (документів, що її складають) повинні входити наступні розділи:

– загальний, у якому визначається відношення керівництва ІКС (організації) до проблеми безпеки інформації;

– організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу;

– класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є у наявності в ІКС, та необхідний рівень їхнього захисту;

– розділ, у якому визначаються ПРД до інформації;

– розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;

– розділ, у якому висвітлюються питання фізичного захисту;

– розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;

– розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;

– розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування ІКС;

– юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

2.3 Канали відтоку інформації

2.3.1 Загальна характеристика каналів відтоку інформації

Згідно з ДСТУ 3396.2 під поняттям відтік інформації мається неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання. КВІ це сукупність носіїв інформації та середовища її поширення. Частіше використається поняття технічний КВІ з наступним тлумаченням - сукупність носіїв інформації, середовища її поширення та засобів технічної розвідки. Слід визначити те, що поняття КВІ поширюється лише на неконтрольовану зону. Існує велика кількість КВІ, серед котрих слід визначити акустичний, віброакустичний, електричний, електромагнітний, оптичний, оптоелектронний, параметричний та інші КВІ. Класифікація КВІ наведено на рис. 2.6

2.3.2 Канали відтоку інформації під час її обробки

Електричні КВІ. КВІ цього типу утворюються завдяки :

- наведень електромагнітних випромінювань ЗПО на з'єднувальні лінії ДЗС і сторонні провідники, що виходять за межі контрольованої зони;
- просочування інформаційних сигналів в ланцюзі електроживлення ЗПО;
- просочування інформаційних сигналів в ланцюзі заземлення ЗПО.

Наведення виникають при випромінюванні елементами ЗПО (у тому числі і їх з'єднувальними лініями) інформаційних сигналів, а також при наявності гальванічного зв'язку з'єднувальних ліній ЗПО і сторонніх провідників або ліній ДЗС. Рівень сигналів, що наводяться, значною мірою залежить від потужності випромінюваних сигналів, відстані до провідників, а також довжини з'єднувальних ліній ЗПО і сторонніх провідників.

Просочування інформаційних сигналів в ланцюзі електроживлення ЗПО можливо за наявності взаємноіндуктивного зв'язку між вихідним трансформатором підсилювача і трансформатором випрямлювального пристрою. Крім того, струми посилюваних інформаційних сигналів замикаються через джерело електроживлення, створюючи на його

внутрішньому опорі падіння напруги, яке при недостатньому згасанні у фільтрі випрямлювального пристрою може бути виявлено в лінії електроживлення.

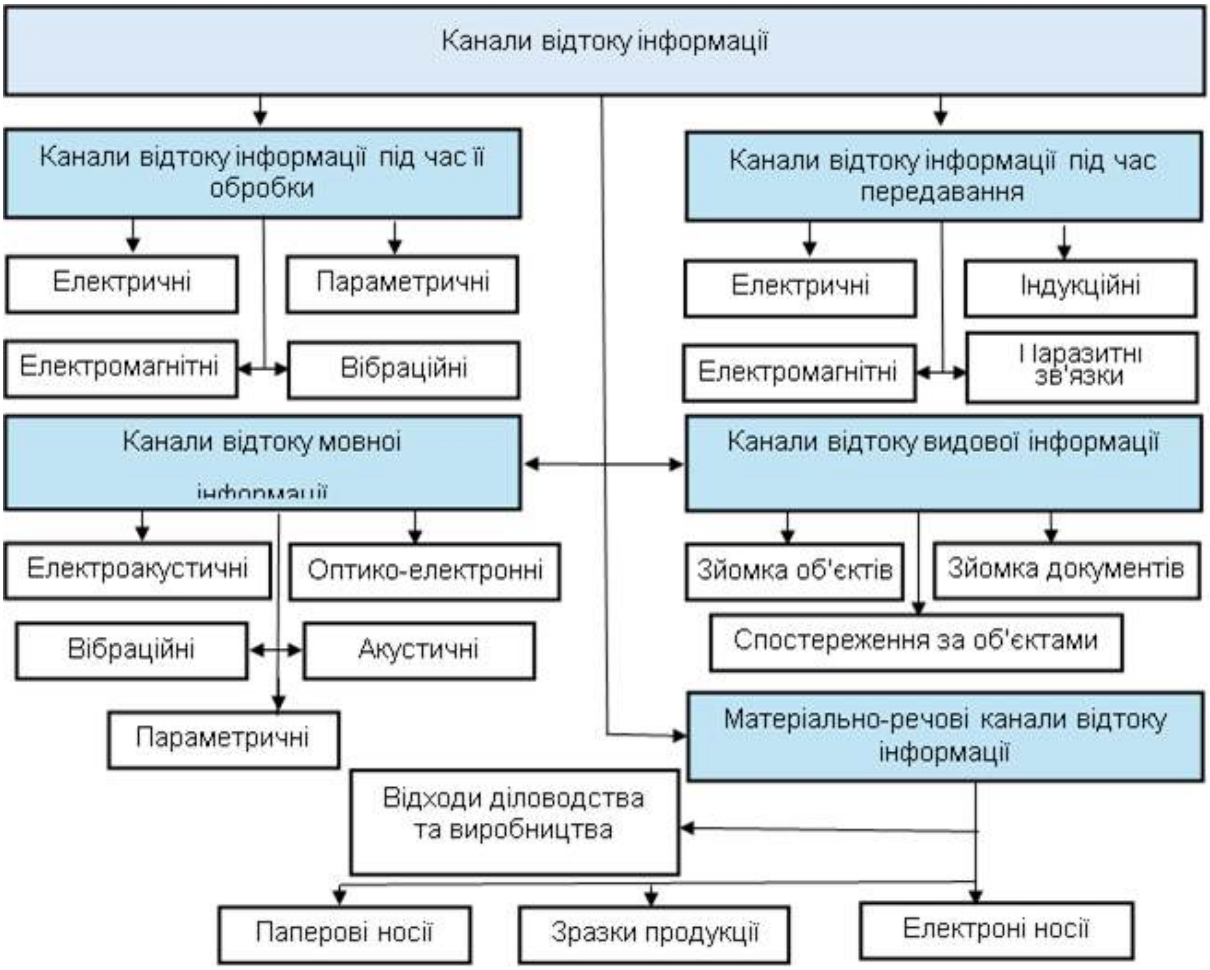

Рисунок 2.6 - Класифікація каналів витоку інформації

Інформаційний сигнал може проникнути в ланцюги електроживлення також в результаті того, що середнє значення споживаного струму в крайових каскадах підсилювачів більшою чи меншою мірою залежить від амплітуди інформаційного сигналу, що створює нерівномірне навантаження на випрямляч і призводить до зміни споживаного струму за законом зміни інформаційного сигналу.

Просочування інформаційних сигналів в ланцюзі заземлення ЗПО. Окрім заземлюючих провідників, що служать для безпосереднього з'єднання ЗПО з контуром заземлення, гальванічний зв'язок із землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий провід мережі електроживлення, екрани(металеві оболонки) сполучних кабелів, металеві труби систем опалювання та водопостачання, металева арматура залізобетонних конструкцій тощо. Всі ці провідники спільно із заземлюючим пристроєм утворюють розгалужену систему заземлення, де можуть наводитися

інформаційні сигнали. Крім того, в грунті навколо заземлювального пристрою виникає електромагнітне поле, яке також є джерелом інформації.

Електромагнітні КВІ. Основним каналом витоку інформації під час її обробки ЗПО є електромагнітний канал, зумовлений побічними інформативними електромагнітними випромінюваними основних засобів обробки інформації.

До електромагнітних відносяться КВІ, що виникають з допомогою різного виду ПЕМВ ЗПО. ПЕМВ – це паразитні електромагнітні випромінювання радіодіапазону, створювані в навколишньому просторі пристроями, які спеціально для цього не призначені.

До ПЕМВ ЗПО відносяться:

– випромінювання елементів ЗПО;

– випромінювання на частотах роботи високочастотних генераторів ЗПО;

– випромінювання на частотах самозбудження підсилювачів низької частоти ЗПО.

При зовнішніх впливах інформаційного сигналу на елементах високочастотних генераторів індукуються електричні сигнали. Приймальними антенами для магнітного поля можуть служити котушки індуктивності коливальних контурів, згладжуючі дроселі в ланцюгах електроживлення і т.д. Приймачами електричного поля є дроти високочастотних ланцюгів та інші елементи. Індуковані електричні сигнали можуть викликати модуляцію власних високочастотних коливань генераторів і випромінювання їх в простір.

Особливу увагу слід звернути на персональні комп'ютери. Сучасне обладнання передбачає перехоплення майже 100% даних, що обробляються ПК. Проте, якщо розглядати цінність отриманої інформації, її частка становить 1-2%. Ця частка в основному включають дані, що вводяться з клавіатури або відображаються на моніторі. Крім цього, ПК та з'єднувальні кабелі утворюють резонансні контури, що випромінюють електромагнітні хвилі, які модулюються сигналами даних.

Електромагнітні випромінювання на частотах самозбудження підсилювачів низької частоти можливе завдяки перетворення негативних зворотних зв'язків (індуктивних або ємнісних) в позитивні паразитні в результаті фазового зсуву сигналу зворотного зв'язку на певних частотах, що призводить до переведення підсилювача з режиму посилення в режим автогенерації сигналів.

Частота самозбудження знаходиться в межах робочих частот елементів підсилювачів низької частоти, що переходять у нелінійний режим роботи при навантаженні завдяки дії позитивного зворотного зв'язку. Сигнал на частотах самозбудження, як правило, виявляється промодульованим інформаційним сигналом.

Параметричний КВІ. Даний КВІ використовується для перехоплення інформації, що обробляється в технічних засобах шляхом їх високочастотного опромінення. При дії опромінюючого електромагнітного поля на елементи ЗПО відбувається перевипромінювання електромагнітного поля. У ряді випадків можлива модуляція вторинного випромінюючого поля інформаційним сигналом.

Вібраційний КВІ. У процесі обробки інформації в ЗПО виникають різноманітні вібрації. Джерелами цих вібрацій є струми в котушках індуктивності, трансформаторах і конденсаторах, системи охолодження, жорсткі диски, клавіатури, частини устаткування, що рухаються. В результаті таких вібрацій виникають мікровібрації, які генерують ПЕМВ.

2.3.3 Канали відтоку інформації під час передавання

Для передачі інформації використовують в основному короткохвильові, ультракороткохвильові, радіорелейні, тропосферні, лазерні, метеорні та супутникові канали зв'язку, а також кабельні та волоконно-оптичні лінії зв'язку.

Електричні КВІ. Даний КВІ при її передачі лініями зв'язку може бути утворений шляхом безпосереднього контактного підключення до кабельних ліній апаратури перехоплення. Цей канал найчастіше використовується для перехоплення низькочастотних телефонних сигналів в лініях зв'язку в місцях вільного доступу.

Для прослуховування телефонних розмов може бути використане послідовне та паралельне підключення до лінії зв'язку. Можливості КВІ не обмежуються перехопленням телефонних розмов. Існує можливість прослуховування приміщень через мікрофон телефону. Невелика схема, поставлена в апарат, дозволяє знімати інформацію за покладеної трубки.

Електромагнітні КВІ. Електромагнітні випромінювання передавачів зв'язку, модульовані інформаційним сигналом, можуть перехоплюватися з використанням як стандартними технічними засобами радіорозвідки, так і приймачами, аналогічними тим, що використовуються в даній мережі. Даний канал широко використовується для прослуховування телефонних розмов, що ведуть по радіотелефонах, радіорелейних та супутникових лініях зв'язку, стільникові системи зв'язку та канали на основі технологій Bluetooth та WiFi.

Індукційні КВІ. Індукційний канал, де використовується ефект виникнення навколо високочастотного кабелю електромагнітного поля під час проходження інформаційних сигналів. Індукційні датчики використовуються в основному для знімання інформації з високочастотних симетричних кабелів. Сучасні індукційні датчики здатні знімати інформацію з броньованих кабелів, що знаходяться на поверхні, під землею та під водою на глибинах понад 1 км.

Паразитні зв'язки КВІ. Паразитні зв'язки, що реалізуються за рахунок паразитних ємнісних, індуктивних та резистивних зв'язків та наведень

близько розташованих один від одного ліній передачі інформації. Паразитний зв'язок обумовлений не передбаченою конструкцією взаємодією між елементами пристрою, пристроями або лініями зв'язку, що призводить до витоку інформаційного сигналу.

Будь-який паразитний зв'язок – це передача енергії між об'єктами, що взаємодіють. У більшості випадків це взаємна операція, але при цьому кожен з об'єктів втрачає енергію. Фізична основа цього процесу - виникнення електромагнітного поля при передачі інформації по лінії зв'язку. При цьому найбільший ефект з погляду зняття інформації виходить при прийомі високочастотних гармонік.

2.3.4 Канали відтоку мовної інформації

Електроакустичні КВІ виникають з допомогою електроакустичних перетворень акустичних сигналів у електричні. Перехоплення акустичних коливань здійснюється через допоміжні технічні засоби та системи, що мають "мікрофонний ефект", а також шляхом "високочастотного нав'язування".

Вібраційний КВІ. У вібраційних (структурних) КВІ середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалення, каналізації та інші тверді тіла. Для перехоплення акустичних коливань використовуються контактні мікрофони (стетоскопи).

Оптико-електронний (лазерний) КВІ утворюється при опроміненні лазерним променем тонких поверхонь, що вібрують в акустичному полі (скла, вікон, картин, дзеркал тощо). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється по амплітуді та фазі (за законом вібрації поверхні) і приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Акустичний КВІ. У даних КВІ середовищем поширення акустичних сигналів є повітря, а їх перехоплення використовуються мікрофони і спеціальні спрямовані мікрофони. При використанні параболічних мікрофонів можливе зняття інформації в міській смузі на відстані до 150 – 200 метрів, а на відкритій місцевості до 1 км. Ще один канал витоку акустичної інформації утворюють системи повітряної вентиляції приміщень, різні витяжні системи та системи подачі чистого повітря. Можливості утворення таких каналів визначаються конструктивними особливостями повітроводів та акустичними характеристиками їх елементів: засувок, переходів, розподільників та ін.

Параметричний КВІ виникає завдяки незначній зміні взаємного розташування елементів електронних схем. Внаслідок зміни міжвиткової відстані в котушках індуктивності або відстані між пластинами в конденсаторах відбувається зміна частоти випромінювання генератора. Що призводить до частотної модуляції високочастотного сигналу.

2.3.5 Канали відтоку видової інформації

Візуальне спостереження є найбільш відомим, досить простим, широко поширеним добре оснащеним найсучаснішими оптичними приладами різного класу - бінoклями, стереотрубами, приладами нічного бачення, ТБ камерами, волоконно-оптичними системами і тощо.

Цей вид дій має:

- достовірність і точність інформації, що видобувається;
- високою оперативність отримання інформації;
- доступність реалізації;
- документальність отриманих відомостей (фото, кіно, TV).

Ці особливості визначають небезпеку цього виду каналів витоку інформації

Зйомка об'єктів проводиться для документування результатів спостереження та детальнішого вивчення об'єктів. Для зйомки об'єктів використовуються телевізійні та фотографічні засоби. Для зйомки об'єктів вдень з близької відстані застосовуються мініатюрні або портативні камери, що камуфлюються та відеокамери.

Зйомка (зняття копії) документів здійснюється за допомогою спеціальних портативних фотоапаратів для зйомки документів. При необхідності можна використовувати і звичайний фотоапарат або смартфон, але для досягнення прийнятних результатів фотограф повинен мати відповідні знання та навички в області фотографії

Спостереження за об'єктами із застосуванням оптичних приладів (монокуляри, оптичні труби, бінoклі, телескопи тощо) та телевізійних камер. Для спостереження вночі є прилади нічного бачення, тепловізори, телевізійні камери. Для спостереження з великої відстані використовуються засоби аеро- і космічної кіно- фотозйомки, довгофокусні оптичні системи, а для спостереження з близької відстані - камуфльовані потай встановлені телевізійні камери.

2.3.6 Матеріально-речові канали відтоку інформації

Особливість цього каналу викликана специфікою джерел та носіїв інформації, порівняно з іншими каналами. Джерелами та носіями інформації в ньому є суб'єкти (люди) та матеріальні об'єкти (макро- та мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Витік інформації в цих каналах супроводжується фізичним переміщенням людей та матеріальних тіл з інформацією за межами контрольованої зони.

Основні джерела матеріально-речового КВІ:

- чернетки різних документів та макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних та дослідно-конструкторських робіт, що ведуть на підприємстві (організації); відходи

діловодства та видавничої діяльності на підприємстві (організації), у тому числі використаний копіювальний папір, забраковані листи при оформленні документів;

- дискети, що не читаються через їх фізичні дефекти та спотворень завантажувальних чи інших кодів;
- бракована продукція та її елементи;
- відходи виробництва в газоподібному, рідкому та твердому вигляді;
- радіоактивні матеріали.

Перенесення інформації в цьому каналі за межі контрольованої зони можливе такими суб'єктами та об'єктами:

- співробітниками організації та підприємства;
- повітряними масами атмосфери;
- рідким середовищем;
- випромінювання радіоактивних речовин.

Для підприємств хімічної, парфумерної, фармацевтичної та інших сфер розробки та виробництва продукції, технологічні процеси яких супроводжуються використанням або одержанням різних газоподібних або рідких речовин, можливе утворення КВІ через викиди в атмосферу газоподібних або злив у водоймища рідких демаскуючих речовин. Подібні канали утворюються у разі можливості добування демаскуючих речовин внаслідок взяття зловмисниками проб повітря, води, землі, снігу, пилу на листі чагарників та дерев, траві та квітах на околицях підприємства.

2.3.7 Методи захисту від каналів відтоку інформації

Ефективний захист інформаційних ресурсів від каналів відтоку є невід'ємною частиною комплексної системи забезпечення інформаційної безпеки та сприяє оптимізації фінансових витрат на організацію захисту інформації.

Захист від ПЕМВ. Ефективність системи захисту від витоку інформації каналами ПЕМВ оцінюється за різними критеріями, які визначаються фізичною природою інформаційного сигналу, але найчастіше за співвідношенням «сигнал/шум». Захист здійснюється із застосуванням пасивних та активних методів та засобів.

Мета пасивних та активних методів захисту – зменшення відношення сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення інформаційного сигналу. У пасивних методах захисту зменшення відносин С/Ш досягається шляхом зменшення рівня інформаційного сигналу, в активних методах – шляхом збільшення рівня шуму.

Пасивні методи захисту спрямовані на:

– ослаблення ПЕМВ на межі контрольованої зони;

– ослаблення наведень ПЕМВ у сторонніх провідниках, сполучних лініях, ланцюгах електроживлення та заземлення, що виходять за межі контрольованої зони;

– виключення або ослаблення просочування інформаційних сигналів у ланцюзі електроживлення та заземлення, що виходять за межі контрольованої зони.

Ослаблення небезпечного сигналу необхідно проводити до величин, що забезпечують неможливість його виділення і натомість природних шумів.

До пасивних методів захисту відносяться:

– застосування розділових трансформаторів та завадопригнічувальних фільтрів;

– екранування;

– заземлення всіх пристроїв як необхідна умова ефективного захисту інформації;

– доопрацювання пристроїв ВТ з метою мінімізації рівня випромінювання.

Активні методи захисту спрямовані на:

– створення маскуючих просторових електромагнітних перешкод;

– створення маскуючих електромагнітних перешкод у сторонніх провідниках, сполучних лініях, ланцюгах електроживлення та заземлення.

До активних методів захисту відносяться просторове та лінійне зашумлення.

Екранування електромагнітних хвиль. Теоретичне вирішення задачі екранування та визначення значень напруженості полів у загальному випадку надзвичайно важко. Тому в залежності від типу розв'язуваної задачі є зручним розглядати окремі види екранування: електричне, магнітостатичне та електромагнітне:

– електростатичне екранування – пригнічення паразитних ємнісних зв'язків;

– магнітостатичне екранування - пригнічення паразитних індуктивних зв'язків;

– електромагнітне екранування – пригнічення електромагнітного поля.

При реалізації електромагнітного екранування необхідне заземлення екрана джерела ПЕМВ, під яким розуміється навмисне електричне з’єднання екрана із заземлювальним пристроєм. Крім того, правильне заземлення пристроїв є однією з важливих умов захисту інформації від витоку по колах заземлення.

Захисна дія заземлення грунтується на двох принципах:

– зменшення до безпечного значення різниці потенціалів між заземлюваним провідним предметом та іншими провідними предметами, що мають природне заземлення;

– відведення струму витоку при контакті заземлюваного провідного предмета з фазним проводом.

Ключовою характеристикою заземлення є електричний опір кола заземлення. Чим нижчий опір, тим ефективніше заземлення ($R_p \leq 4$ Ом).

Розділові трансформатори та завадопригнічувальні фільтри. Фільтрація є основним і ефективним засобом пригнічення ПЕМВ у колах електроживлення, у сигнальних колах інтерфейсу, на друкованих платах та у дротах заземлення.

Завадопригнічувальні фільтри — це пристрій, що обмежує поширення ПЕМВ дротами, які є спільними для джерела та приймача наводки. Вони дозволяють знизити ПЕМВ як від зовнішніх, так і від внутрішніх джерел.

Розділові трансформатори забезпечують розв’язку первинного та вторинного кіл за сигналами наводки. Інакше кажучи, наводки первинної обмотки трансформатора не повинні потрапляти у вторинну.

Засоби активного захисту застосовуються, коли відношення сигнал/шум перевищує встановлений допустимий рівень після застосування пасивних засобів або є технічно та/або економічно неефективними.

Просторове зашумлення передбачає створення маскуючих перешкод в навколишньому просторі і використовується для унеможливлення перехоплення ПЕМВ по електромагнітному каналу. Воно є ефективним не тільки для закриття електромагнітного, але і електричного каналів витоку інформації, оскільки перешкодовий сигнал при випромінюванні наводиться в сполучних лініях ДЗС та сторонніх провідниках, що виходять за межі контрольованої зони.

Системи лінійного шуму застосовуються для маскування наведених сигналів в лініях, якщо вони мають вихід за межі контрольованої зони. У найпростішому випадку система являє собою генератор шумового сигналу, що формує шумову маскувальну напругу із заданими спектральними, тимчасовими та енергетичними характеристиками. Генератор гальванічно підключається в лінію, яку необхідно зашуміти. На практиці найчастіше подібні системи використовуються для зашумлення ліній електроживлення.

Захист мовної інформації. Для захисту мовної інформації використовуються пасивні та активні методи та засоби.

Звукоізоляція приміщень спрямована на локалізацію джерел акустичних сигналів усередині них і проводиться з метою виключення перехоплення мовної інформації по прямому акустичному (через щілини, вікна, двері, технологічні отвори, вентиляційні канали тощо) і вібраційному ((через огороджувальні конструкції, труби водо-, тепло- та газопостачання, каналізації тощо)) каналів.

Основна вимога до звукоізоляції приміщень полягає в тому, щоб за його межами відношення акустичний с/ш не перевищувало деякого допустимого значення, що виключає виділення мовного сигналу на тлі природних шумів.

В основі активних методів захисту акустичної інформації лежить використання різного типу генераторів завад, а також застосування інших спеціальних технічних засобів.

Акустичне маскування - активна міра захисту, полягає у створенні акустичних перешкод, що маскують. Віброакустичне маскування ефективно використовується для захисту мовної інформації від витоку по прямому акустичному, вібраційному та оптико-електронному КВІ. Для формування акустичних завад застосовують спеціальні генератори, до виходів яких підключені звукові колонки або вібраційні випромінювачі.

Захист видовою інформації. Для захисту від зняття видової інформації найчастіше використовуються два способи. Це маскування та візуальна зміна профілю об'єкта. Маскування передбачає застосування маскуючих сіток, фарб, укриттів, аерозольних завіс, створення штучних об'єктів (макетів).

Візуальна зміна профілю об'єкта передбачає встановлення різноманітних відбивних конструкцій, в яких елементи, що відбивають, встановлюються під різними кутами і з різною відбивною здатністю. Крім цього використовуються покриття антивідблиску та світлові завади.

Захист від відтоку інформації по матеріально-речовому каналу спрямований на запобігання несанкціонованому винесенню, викраденню або копіюванню фізичних носіїв інформації (документів, дисків, флешок, виробів). Цей канал пов'язаний із безпосереднім доступом людини до матеріальних носіїв.

Фізичне знищення носія. Для паперових носіїв, чернеток, копірки, стрічки принтерів та термоплівок – використовується подрібнення або спалювання. Для магнітних носіїв – подрібнення дисків та вінчестерів.

Збирання та зберігання використаних носіїв здійснюється у спеціальних закритих контейнерах з подальшим централізованим вивезенням для утилізації. Утилізація проводиться у присутності спеціальної комісії зі складанням акту.

Для відходів виробництва у газоподібному та рідкому стані використовуються відповідні фільтри. Тверді відходи повинні перероблятися або переміщуватися в місця зберігання, що охороняються.https://www.google.com/search?q=%D0%97%D0%BD%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D1%8F+%D0%BD%D0%BE%D1%81%D1%96%D1%97%D0%B2&rlz=1C1CHBD_ruUA970UA970&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDE2MzZqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8&fbs=ADc_l-ZhZwqRfIRNTFz1njGTSUZt-oZYyuWjrWfVSrNYC75inD-_Me3mpmMgdLqScuUG0Bb5IHxQ2olWR8TTZ5VN63dhwuCehNPbeLGLELd09P8aWAAxPC3AdGC5kCjRnqM_zbxMqmNvGTS84IPhLjhBZQGf1LEB1jfcWRGUKpPZsxiOyUYzlTHnf3wPfio9QtqHr2UwBiKDMN-

2.4 Забезпечення інформаційної безпеки

2.4.1 Забезпечення конфіденціальності

Перш ніж говорити про методи забезпечення конфіденційності, необхідно відзначити той факт, що під конфіденційною інформацією в ІБ в першу чергу розуміється НСД до інформації. І тут слід виділити два основні напрямки. Це шифрування та організаційні методи. Останнім часом все більше уваги приділяється і стеганографічним методам.

Шифрування. Даний метод слід застосовувати у процесі передачі та зберігання інформації. Шифрування забезпечується криптологічними системами.

Криптологія з'явилася ще до нашої ери. Якісний стрибок у її розвитку стався з появою першої ЕОМ "Колосс". Це була перша реально працююча ЕОМ, яка вирішувала прикладну задачу криптоаналізу. Власне, саме потреба в цьому і спонукало до побудови першої обчислювальної машини. Зараз криптологія включає дві гілки – криптографію та криптоаналіз. Криптографія займається розробкою криптоалгоритмів, що використовуються для шифрування та розшифрування текстів з використанням секретних ключів. Криптоаналіз розробляє алгоритми прочитання зашифрованих повідомлень без знання ключів.

Залежно від ключів, що використовуються, існує два види криптосистем. Це системи з одним секретним ключем (симетричні) та системи з відкритим ключем. У системах з відкритим ключем використовуються два ключі - відкритий і закритий. Інформація шифрується за допомогою відкритого ключа, який доступний всім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення. Найбільш відомими в даний час є симетричні алгоритми - AES (американський стандарт шифрування), ChaCha20 (алгоритм потокового шифрування), Калина (ДСТУ 7624:2014), Струмок (ДСТУ 8845:2019), асиметричні - RSA (факторизації великих чисел), DSA (обчислення дискретних логарифмів), ECC (еліптичні криві).

Шифрування даних — процес перетворення відкритого тексту в шифртекст. Розшифрування даних — процес перетворення шифртексту у відкритий текст. Секретним елементом будь-якого алгоритму шифрування є ключ.

Ключ — конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

Імітовставка — блок інформації фіксованої довжини, що одержується із відкритого тексту і ключа, однозначно відповідний даному відкритому тексту. Імітовставка це засіб забезпечення імітозахисту в протоколах автентифікації повідомлень з учасниками, що довіряють один одному, — спеціальний набір символів, який додається до повідомлення і призначений для контролю його цілісності та автентифікації джерела даних. Використовуються симетричні алгоритми.

Цифровий підпис — дані, одержані в результаті криптографічного перетворення блоку даних і/або його параметрів (хеш функції, довжини, дати утворення, ідентифікатора відправника та ін.), що дозволяють приймальнику даних впевнитись в цілісності блоку і справжності джерела даних й забезпечити захист від підробки та підлогу. Застосовуються системи з відкритим ключем із шифруванням за допомогою закритого ключа. Застосовується для контролю цілісності.

Забезпечення конфіденційності під час передавання даних може здійснюватися шляхом:

– керування маршрутом передачі пасивних об'єктів з метою унеможливлення несанкціонованого ознайомлення з їх умістом;

– приховування семантики (вмісту) переданих пасивних об'єктів з використанням шифрування;

– заповнення трафіка методом доповнення хибних даних;

– заповнення трафіка методом генерації хибних повідомлень;

– використання змінного надання даних;

– розподілу каналів для передачі різних частин повідомлення (розподілу спектра);

– організації прихованого каналу передачі усередині іншого відкритого каналу.

Стеганографія. Стеганографічні методи використовуються для приховування факту передачі інформації. Для передачі потрібен контейнер, в якому розміщується повідомлення, що передається. Як контейнер може бути використане текстове повідомлення, малюнок, ауді- або відеофайли.

Крім захисту інформації від несанкціонованого доступу стеганографію можливо використовувати для:

– захисту авторських прав на деякі види інтелектуальної власності;

– подолання систем моніторингу та керування мережними ресурсами;

– камуфляжу деяких видів програмного забезпечення;

– забезпечення цілісності інформації;

– створення прихованих від законного користувача каналів витоку інформації.

Методи комп'ютерної стеганографії використовують для приховування факту передавання повідомлення текстові, графічні, аудіо- або відеофайли, у які вбудовується інформація, що необхідно передати. Ці методи грунтуються на:

– використання властивостей комп'ютерних форматів, які спеціально призначено для зберігання та передавання даних;

– надмірність аудіо-, візуальної або текстової інформації з позиції психофізіологічних особливостей сприйняття людини.

Сьогодні існує велика різноманітність стегографічних алгоритмів. Методи комп'ютерної стеганографії поділяються на три основні групи, у кожній з яких є кілька реалізацій, що використовують різні механізми приховування інформації:

а) методи приховування інформації в аудіоконтейнерах:

1) метод приховування в найменших значущих бітах;
2) метод приховування на основі розподілу за спектром;
3) метод приховування на основі використання луна-сигналу;
4) метод приховування у фазі сигналу;

б) методи приховування інформації в текстових контейнерах:

1) метод приховування на основі прогалин;
2) метод приховування на основі синтаксичних особливостей тексту;
3) метод приховування на основі синонімів;
4) метод приховування на основі використання помилок;
5) метод приховування на основі генерації квазітексту;
6) метод приховування на основі використання особливостей шрифту;
7) метод приховування на основі використання коду документа і файлу;
8) метод приховування на основі використання чергування довжини слів;
9) метод приховування на основі використання перших букв;

в) методи приховування інформації в графічних контейнерах:

1) метод приховування в найменших значущих бітах;
2) метод приховування на основі модифікації індексного формату подання;
3) метод приховування на основі використання автокореляційної функції;
4) метод приховування на основі використання нелінійної модуляції вбудованого повідомлення;
5) метод приховування на основі використання знакової модуляції вбудованого повідомлення;
6) метод приховування на основі вейвлет-перетворення;

7) метод приховування на основі використання дискретного косинусного перетворення.

Найбільшого розвитку і застосування сьогодні набувають методи приховування інформації в графічних контейнерах. Це зумовлено великим розміром графічних файлів, великим обсягом інформації, яку можна помістити в таких контейнерах без помітного спотворення зображення, існуванням у більшості реальних зображень областей, що мають шумову структуру і добре підходять для вбудовування інформації, різноманітністю методів оброблення зображень і цифрових форматів подання зображень, які використовуються в стеганографії. Класифікацію методів стеганографії, у яких використовуються графічні контейнери показано на рисунку 2.7.

Одним з найбільш поширених є метод приховування в найменших значущих бітах (LSB). Суть цього методу полягає в заміні останніх значущих бітів у контейнері на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами буде невідчутною для органів сприйняття людини. Існує велика кількість реалізацій цього методу.

Недоліком же методу LSB є його нестійкість до оброблення файлу-контейнера, що робить неможливим його використання в приховуванні даних у файлі, який у подальшому піддається стисненню.

Більш стійкими до спотворень, у тому числі й компресії, є методи, у яких застосовується розподіл за спектром для приховування інформації, тому що в них використовуються дані, які вже перетворено з допомогою каналів зв’язку.

Існує кілька способів подання зображення в частотній області. При цьому певна декомпозиція зображення використовується як контейнер. Наприклад, існують методи на основі дискретно-косинусного перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення, перетворення Карунена - Лоєва та ін. Подібні перетворення можуть застосовуватися як до окремих частин зображення, так і до зображення в цілому.

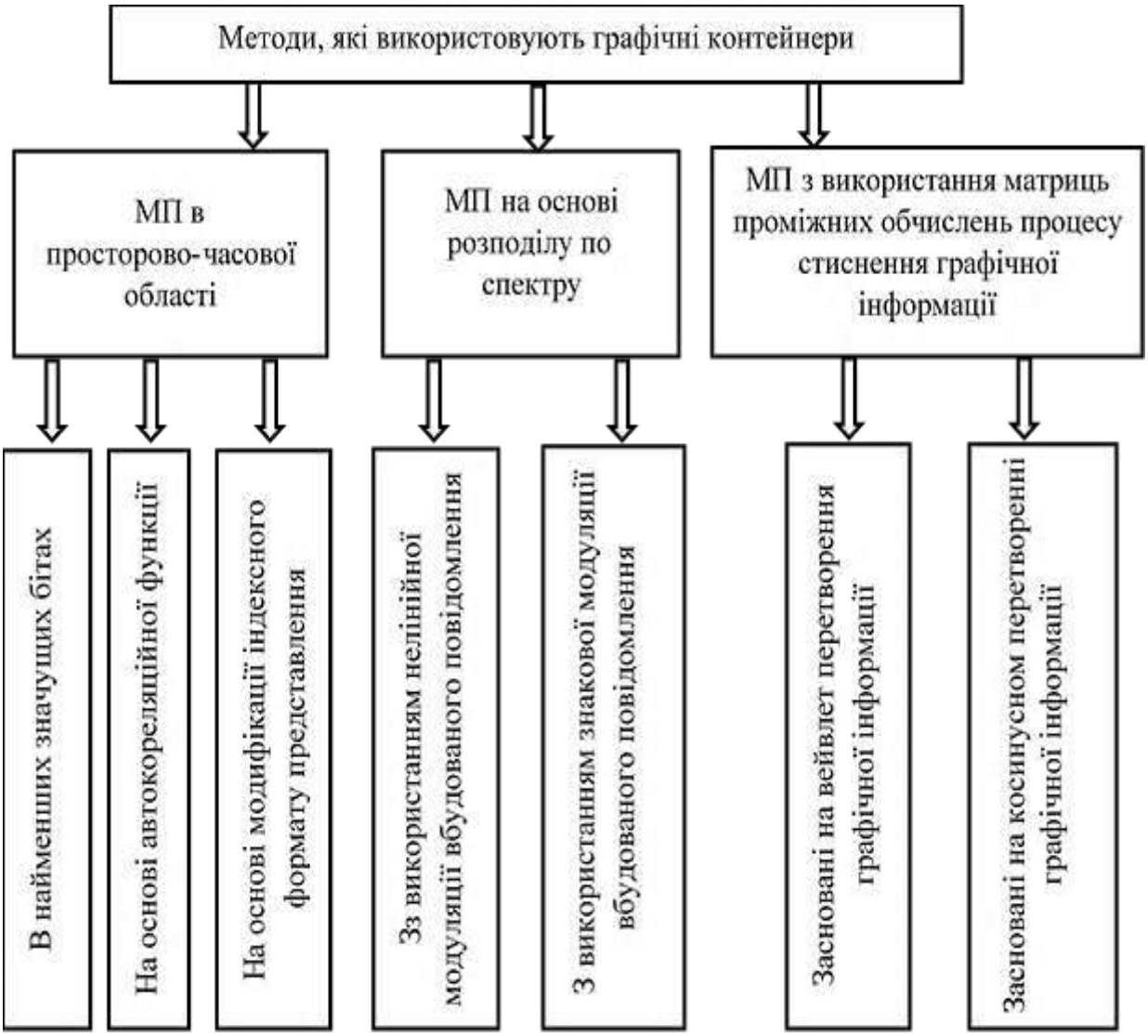

Рисунок 2.7 – Класифікація методів стеганографії,
у яких використовуються графічні контейнери

Найбільшого поширення серед всіх ортогональних перетворень у стеганографії набули вейвлет-перетворення і ДКП. Це пояснюється значним поширенням їх використання при компресії зображень. Крім того, для приховування даних доцільно застосовувати саме те перетворення контейнера, якому цього будуть піддавати у відомих алгоритмах компресії. Наприклад, алгоритм ДКП є базовим у стандарті JPEG, а вейвлет-перетворення - у стандарті JPEG2000.

Одним з найвідоміших стегографічних методів є метод Коха і Жао - метод відносної заміни величин коефіцієнтів ДКП. У цьому алгоритмі впроваджується біт водяних знаків у блоки зображення розміром 8 х 8 пікселів (1 біт на блок). При цьому як повідомлення може використовуватися монохромне зображення або якась послідовність {0, 1}, що складається з довільної кількості чисел.

При застосуванні цього алгоритму передбачається, що одержувачу

мають бути відомі крім контейнера з вбудованими даними та його розмірності алгоритм приховування даних, розмірність сегментів, на які розбивався контейнер, і матричні координати коефіцієнтів косинусних функцій, які використовувалися для приховування. При отриманні даних із зображення проводиться повторне ДКП і порівняння вибраних коефіцієнтів за правилом, що використовувався при приховуванні даних.

Таким чином, оригінальне зображення спотворюється з допомогою внесення змін у коефіцієнти ДКП, якщо їх відносна величина *P* не відповідає біту, який приховується. Чим більше значення *P*, тим приховування є більш стійким до стиснення, однак якість зображення при цьому значно погіршується. І навпаки, чим менше *P*, тим менше помітна наявність інформації у контейнері, але тим більша кількість помилок у витягнутій інформації.

Іншим стегографічним методом є метод Фрідріх. На відміну від попереднього алгоритму Коха і Жао, у якому ДКП проводиться по блоках, в алгоритмі Фрідріх ДКП відбувається для всього зображення, яке захищається. Приховуване повідомлення являє собою послідовність {-1, 1}. У цьому алгоритмі дані вбудовуються в зображення двома різними способами залежно від того, у яких коефіцієнтах ДКП відбувається приховування - у середньочастотних або у низькочастотних. У цьому алгоритмі має місце той же недолік: стійкість алгоритму до стиснення зменшується зі збільшенням місткості контейнера.

Аналогічний недолік є характерним і для інших алгоритмів, у яких використовується приховування в коефіцієнтах спектральних перетворень.

Слід також зазначити властиве описаним вище алгоритмам значне погіршення точності відновлених даних при збільшенні ступеня стиснення.

2.4.2 Забезпечення цілісності

Методи забезпечення ЦІ можна розділити на дві великі групи. До першої групи будуть належати методи, які безпосередньо забезпечують ЦІ. До другої групи - методи, які дають змогу контролювати ЦІ і в разі необхідності відновлювати повідомлення (рис. 2.8).

2.4.2.1 Методи забезпечення цілісності

Організаційні заходи. Досить поширеним та ефективним методом забезпечення ЦІ є організація доступу до інформації та обладнання, що використовується. Цей метод належить до організаційних, при якому передбачається доволі великий перелік заходів, починаючи від підбору співробітників і закінчуючи роботою з технікою і документами. Серед них можна виокремити технології захисту, оброблення та зберігання документів, атестацію приміщень і робочих зон, порядок ЗІ від випадкових та/або несанкціонованих дій персоналу і т. д.

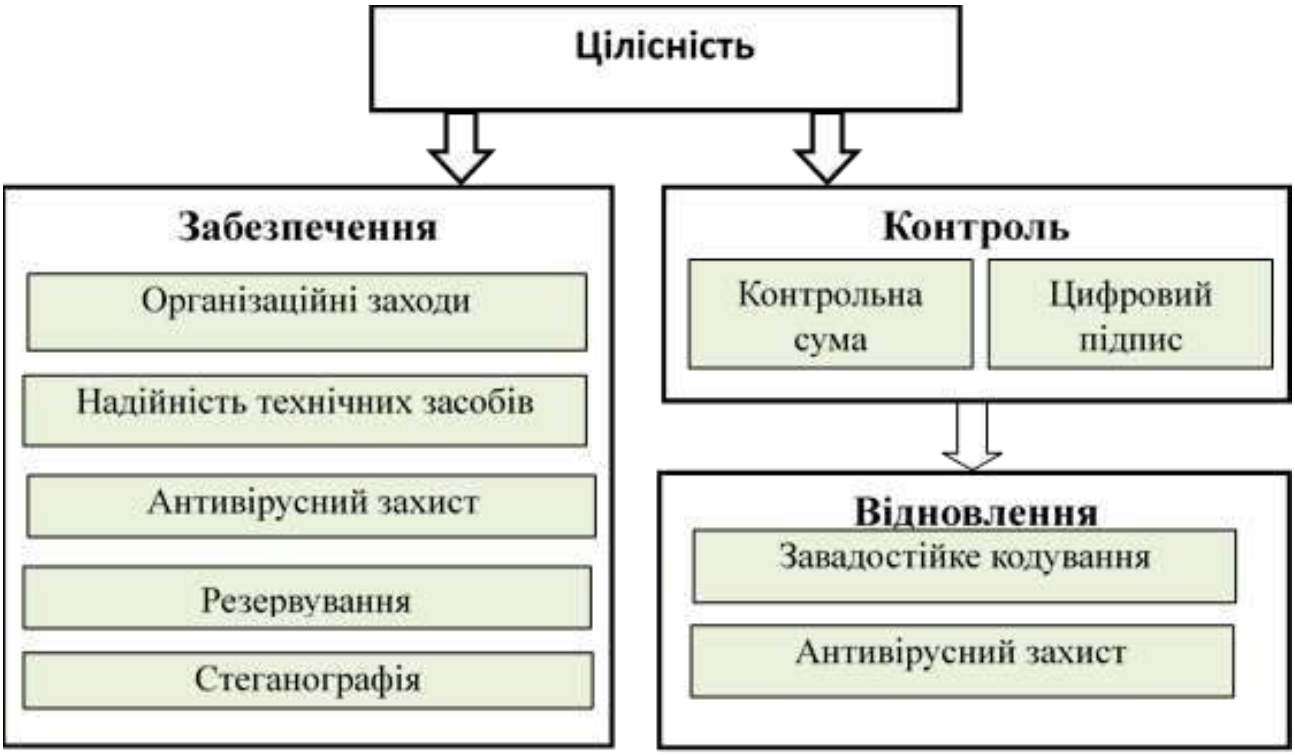

Рисунок 2.8 – Методи забезпечення ЦІ

Для забезпечення ЦІ в ІКС особливу увагу слід приділити захисту ОС, що забезпечують функціонування майже всіх складових системи. Найбільш дієвим механізмом розмежування доступу для ОС є ізольоване програмне середовище. Воно підвищує стійкість ІКС до різних шкідливих і руйнівних програм, що дають змогу забезпечити ЦІ.

Надійність технічних засобів. Необхідною умовою забезпечення ЦІ є наявність високонадійних ТЗ, які містять в себе як апаратну, так та/або програмну складові. Таке обладнання має забезпечувати як високу відмовостійкість, так і ЗІ від можливих загроз.

Одним з найбільш поширених засобів підвищення надійності ТЗ є резервування. Якщо розглядати ТЗ з огляду на інформаційні складові, то підвищення надійності досягається завдяки послідовному з'єднанню елементів системи, що відповідають з цю складову. Якщо послідовно з'єднати два комп'ютери, поставивши на кожен з них свій антивірус, то ймовірність проникнення шкідливої програми зменшується. Однак при цьому зменшується ймовірність безвідмовної роботи ТЗ, що складається з двох комп'ютерів, які послідовно з'єднано.

Для забезпечення заданої надійності такого інформаційно-технічного комплексу необхідно застосовувати послідовно-паралельну архітектуру будування систем ТЗ. При застосуванні ТЗ припускається й можливість використання виділених та/або фізично захищених ліній зв'язку, наприклад броньованих кабелів з контролем цілісності оболонки.

До ТС забезпечення ЦІ слід віднести й засоби захисту від ЕМІ. Вражаючими факторами ЕМІ є високоінтенсивні електромагнітні поля, які

або безпосередньо впливають на РЕЗ, або трансформуються в небезпечних трактах цих засобів у наведені струми та напруги. Найбільш ефективним методом зменшення інтенсивності ЕМІ є екранування - розміщення обладнання в електропровідному корпусі, який перешкоджає проникненню електромагнітного поля від джерела до обладнання, що захищається. Однак, у більшості випадків, обладнання, яке захищають, має зовнішні комунікації, що призводить до проникнення в екранований простір наведених завадових струмів і напруги, що спричиняють пошкодження елементної бази РЕЗ.

Слід зазначити, що часткове екранування мікросхем не впливає на рівень стійкості до імпульсних електромагнітних випромінювань, причому напруга, яка виникає на мікро структурних елементах, формується виводами мікросхеми.

Рішенням є методи обмеження наведених напруг і струмів з амплітудою і спектра в зовнішніх трактах РЕЗ та електромагнітна розв'язка зовнішніх ланцюгів РЕЗ від екранованих пристроїв. Для обмеження наведень за амплітудою і спектром використовуються іскрові й газорозрядні розрядники, напівпровідникові обмежувальні пристрої, варистори й спеціальні нелінійні опори. До обмежувача спектра належать прохідні конденсатори, дроселі та фільтри.

Електромагнітна розв'язка досягається з допомогою ізолювальних трансформаторів, дроселів, оптронів, елементів оптоелектроніки. Застосування оптоелектронних схем дає змогу зменшити кількість замкнутих контурів і забезпечити електричну розв'язку кола. Крім того, системи на базі оптоелектроніки є некритичними до впливу перешкоджальних електромагнітних полів унаслідок того, що носіями інформації в цих системах є електрично нейтральні фотони. Ще однією перевагою оптоелектронних систем є обмеження смуги пропускання, особливо на високих частотах, і тим самим є бездротовими обмежувачами високочастотних завадових наведень на вхідні кола РЕЗ, які властиві ЕМІ.

Одночасно із захистом від ЕМІ, ТЗ необхідно вирішувати проблему електромагнітної сумісності, яка є однією з найбільш пріоритетних в сучасній безпроводовій техніці зв’язку. Збільшення кількості користувачів, використання технологій IoT приводить до необхідності уніфікації персональних засобів комунікації, що означає можливість використання одного термінала для з’єднання з інформаційними службами в різноманітних середовищах. Зі свого боку це викликає потребу в отриманні високошвидкісних безпроводових систем зв’язку, що потрібує ефективного використання електромагнітного спектра.

Стеганографія. Цей термін знають усі, хто займається питаннями ЗІ. Сьогодні можна виокремити три тісно пов'язаних між собою напрями цифрової стеганографії: приховування даних, цифрові водяні знаки і заголовки. При прихованому передавання інформації одночасно із забезпеченням конфіденційності вирішується і питання забезпечення ЦІ.

Не можна змінити того, чого не бачиш - головний аргумент використання стеганографії для забезпечення цілісності інформації.

Одним з найпростіших способів прихованого передавання є відправлення повідомлення всередині іншого повідомлення. Це може бути якийсь контейнер, наприклад, в об'єкті, який є згрупованим, на другому плані знаходиться текстове повідомлення, написане білим по білому. Це - найбільш простий приклад реалізації стеганографічного методу. При цьому функціональність файлів ні змінюється.

Сьогодні використовують як контейнери графічні, текстові, аудіо- й відеофайли, де різними засобами розташовують потрібну інформацію. Можливо приховувати інформацію за допомогою спеціальних знаків. До цього методу можна віднести й використання спеціальних сигналів, наприклад широкосмугових шумоподібних або ортогональних. Широкосмужність сигналу визначає не абсолютна величина ширини використаної смуги частот, а співвідношення спектра повідомлення, яке визначено швидкістю отримання інформації, та шириною спектра сигналу.

Головним недоліком використання стеганографії для забезпечення ЦІ є значно більший обсяг контейнера порівняно з обсягом повідомлення. Однак цей недолік можна нівелювати, передаючи як контейнер корисну інформацію, не критичну до ЦІ.

Про використання методів стеганографії з метою забезпечення ЦІ не прийнято говорити, хоча вони є найбільш ефективними для досягнення поставленої мети.

Антивірусний захист. Однією із загроз ІБ є шкідливі програми, у яких окремим класом виокремлюються віруси. Їх безліч видів і типів, вони різняться між собою способами впливу на різні файли, розміщенням у пам'яті ЕОМ або програмах, об'єктами впливу. Однак головна властивість вірусів - здатність до розмноження. Ця властивість виокремлює їх серед безлічі шкідливих програм і робить найбільш небезпечними.

Одним з найбільш дієвих способів забезпечення ЦІ є добре продуманий і надійний захист від вірусів. Найбільш поширеним способом захисту від вірусів є використання антивірусних програм, яких сьогодні є достатня кількість. Однак необхідно пам'ятати, що жодна програма не гарантує виявлення невідомого вірусу.

Евристичні сканери, що застосовуються, теоретично можуть виявити невідомі віруси з непрямими ознаками, не завжди дають правильний діагноз. Прикладом подібних помилок можуть бути дві антивірусні програми, запущені на одному комп'ютері. Майже будь-який користувач стикався з ситуацією, коли файли одного антивірусу (бази вірусів) приймалися з шкідливу програму іншим антивірусом.

Найкращим засобом захисту від вірусів є використання локальних мереж, які не мають зв'язку з інтернетом. При цьому необхідно жорстко контролювати різні носії інформації з прикладними програмами, з допомогою яких можна занести вірус, однак і це не гарантує від зараження

мережі. Крім того застосування локальних мереж призводить до досить відчутного зниження ефективності використання комп`ютерної техніки.

Резервування. Під резервуванням в цьому контексті розуміється можливість програмних засобів створювати свої копії під час виконання програм. Створюються так звані точки відкату, до яких програма працювала правильно. Якщо внаслідок збоїв або інших причин сталося порушення ходу виконання програми, то вона відкочується до заздалегідь визначеної точки і продовжує своє виконання. Найчастіше точки відкоту створюються користувачем шляхом вибору часу створення такої точки.

2.4.2.2 Методи контролю цілісності

Перевірку цілісності повідомлення можна проводити двома методами. До першого методу належать контрольна сума (КоС), у якій виділяються безпосередньо контрольна сума, і хеш-сума. До другого методу -цифровий підпис.

Контрольна сума. Під терміном «контрольна сума» розуміється метод перевірки цілісності прийнятої інформації на приймальній стороні. Суть контрольної суми полягає в діленні повідомлення на деяку заздалегідь визначену константу, де сумою є залишок від ділення. Найбільш проста контрольна сума - перевірка на парність, яка відповідає діленню на два. Зазвичай як дільник використовують поліноми 8, 16 або 32 ступеня.

Контрольною суми може бути перевірка на парність різних комбінацій переданих бітів. У цьому випадку можна казати не тільки про виявлення помилок, а й про їх виправлення. Цей принцип є основою систем завадостійкого кодування, що дає змогу відновлювати як одиничні, так і кратні помилки в прийнятих повідомленнях. У цьому випадку можна казати не тільки про контроль цілісності, а й про її забезпечення.

Подальшим розвитком контрольної суми стало використання хеш-функцій, які мають деякі відмінності від перевірки на парність. Найголовніша відмінність - це наявність лавинного ефекту, коли результат застосування хеш функції залежить від кожного біта повідомлення. Окрім того, ці функції мають постійний розмір, незалежно від довжини повідомлення, обчислюванням неможливо згенерувати два різних повідомлення з однаковими хешами, обчислювальне неможливо відновити повідомлення зі значення хешу.

У деяких випадках як хеш-функції використовуються алгоритми блокового шифрування, при цьому значення хешу залежить не лише від самого повідомлення, але й від секретного ключа, використовуваного в алгоритмі шифрування.

Електронний підпис. ЕП є механізмом перевірки ЦІ, яка приймається. ЕП – це електронні дані, які додаються підпісувачем до інших електронних даних або логічно з ними пов'язуються і використовують ним

як підпис. Документ, який підписується, подається у відкритому вигляді, тобто незашифрованим.

На стороні відправника обчислюється хеш документа, який необхідно передати. Отриманий хеш шифрується з допомогою особистого ключа відправника й відсилається разом з документом, що передається.

На приймальній стороні обчислюється хеш документа, розшифровується отриманий разом з документом хеш з допомогою відкритого ключа, і порівнюються два отриманих хеші. Якщо вони збігаються, то документ під час передавання не був спотвореним, в іншому випадку він відкидається.

Головною проблемою отримання пари ключів є знаходження простих чисел великої розмірності, на яких грунтується будування асиметричної системи шифрування. Сьогодні розміри ключів становить чотири кілобіти, що відповідає десятковим числам розміром приблизно в 1300D. Це означає, що прості числа, які використовуються як основа системи мають мати розмір не менше 650D. Будування простих чисел таких розмірів є складною обчислювальною задачею.

2.4.2 3 Методи відновлення цілісності

Завадостійке кодування. Найуразливішою інформація буває під час її передавання. Це можна пояснити тим, що така міра забезпечення ЦІ, як розмежування доступу, знімає багато загроз, але вона є неможливою при використанні в каналі зв'язку бездротових ліній. Інформація є найбільш вразливою саме на таких ділянках ІКС. Очевидно, що при навмисному впливі на сигнал, який передається, забезпечити ЦІ неможливо. Для виправлення помилок, що виникли внаслідок природних явищ, технічних збоїв, використовується завадостійке кодування інформації

Головною ідеєю виправлення помилок, що виникають під час передавання, є введення надмірності в повідомлення, що передається. Чим більше необхідно виправити помилок, тим більшою має бути надмірність.

Класичним прикладом завадостійкого кодування є алгоритм Хеммінгу. Надмірність , що вноситься у повідомлення пропорційна log n, де n – число інформаційних розрядів. Код Хеммінга працює лише з однією помилкою. Подальшим розвитком таких алгоритмів стали циклічні коди (БЧХ) (використовуються для виявлення та виправлення групових помилок) та коди Ріда-Соломона (ефективні для боротьби з пачками помилок).

Сьогодні все більшої популярності набуває «м'яке» декодування, яке грунтується на спільному конструюванні коду й багатьох сигнальних точок. Така сигнальна кодова конструкція забезпечує більш високу ефективність і більший енергетичний виграш від кодування, ніж послідовне застосування ЗКІ і модуляції. Однак, при використанні запропонованого методу надмірність повідомлення, що передається значно зростає.

Резервування. Цей метод забезпечення ЦІ використовується в основному при передаванні й зберіганні інформації. Під час передавання можливим є багатократне повторення повідомлення в один напрямок або розсилання повідомлень в усі можливі напрямки. Цей підхід можна розглядати як один з методів завадостійкого кодування. Недолік такого підходу очевидний - велике завантаження каналів передачі інформації.

При зберіганні ідея резервування є досить простою - створення копій отриманих файлів і їх зберігання окремо від первинних документів. Найчастіше такі сховища створюються в географічно рознесених місцях. Як приклад можна розглянути сучасні хмарні технології.

Як один із прикладів резервування можна привести резервування операційної системи в комп'ютерах, коли у випадку збою система сама себе відновлює грунтується на спільному конструюванні коду й багатьох сигнальних точок.

Одним з головних недоліків резервування інформації є підвищення можливості її несанкціонованого зняття або модифікації, тому що інформація, яка розташовується на зовнішніх пристроях зберігання, найчастіше буває незахищеною увесь період збереження..

Антивірусний захист. На відміну від застосування антивірусного захисту при забезпеченні ЦІ, при якому антивірусна програма виявляє вірус до моменту зараження й нейтралізує його дію, у цьому випадку ці засоби є засобами відновлення інформації. Якщо під час сканування виявляється файл, пошкоджений вірусом, то в багатьох випадках такі файли відновлюються. Це визначається механізмом зараження файлів.

Відновлення відбувається шляхом знищення коду вірусу, який було впроваджено в тіло файлу і на його місце переписується оригінальний код. У деяких випадках файл відновленню не підлягає, і його поміщають в карантин. Так як при виявленні вірусу заражений файл переміщається в приховану директорію на диску, існує можливість відновлення таких файлів. Файл у карантині зберігається у зашифрованому вигляді або зі зміненим розширенням.

Відновлення відбувається за допомогою переміщення відновленого файлу збереженим шляхом. Слід зазначити, що файли в карантині зберігаються обмежений час, після чого остаточно видаляються. Таких файли можна відновити тільки шляхом резервування.

2.4.3 Забезпечення доступності

Доступність —властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Доступність системи в загальному випадку досягається шляхом застосування трьох груп заходів, спрямованих на підвищення:

– безвідмовності (під цим розуміється мінімізація ймовірності виникнення якої-небудь відмови; це елемент пасивної безпеки, що далі розглядатися не буде);

– відмовостійкості;

– обслуговування.

Головне при розробці й реалізації заходів забезпечення високої доступності - повнота й систематичність. У цьому зв'язку уявляється доцільним скласти карту інформаційної системи організації, у якій фігурували б усі об'єкти ІС, їхній стан, зв'язки між ними, процеси, асоційовані з об'єктами й зв'язками. За допомогою подібної карти зручно формулювати намічені заходи, контролювати їхнє виконання, аналізувати стан ІС.

Відмовостійкість. Під терміном відмовостійкості розуміється здатності до нейтралізації відмов, "живучості", тобто здатності зберігати необхідну ефективність, незважаючи на відмови окремих компонентів. Основним засобом підвищення "живучості" є внесення надмірності в конфігурацію апаратних і програмних засобів, підтримуючої інфраструктури й персоналу, резервування технічних засобів і тиражування інформаційних ресурсів (програм і даних). Заходи щодо забезпечення відмовостійкості можна розділити на локальні й розподілені.

Локальні заходи спрямовані на досягнення "живучості" окремих комп'ютерних систем або їх апаратних і програмних компонентів (у першу чергу з метою нейтралізації внутрішніх відмов ІС). Типові приклади подібних заходів - використання кластерних конфігурацій як платформа критичних серверів або "гаряче" резервування активного мережевого устаткування з автоматичним перемиканням на резерв.

Резервування програм і даних може виконуватися багатьма способами - шляхом віддзеркалювання дисків, резервного копіювання й відновлення, реплікації баз даних і т. п.

За допомогою ПЗ проміжного шару можна для довільних прикладних сервісів домогтися високої "живучості" з повністю прозорим для користувачів перемиканням на резервні потужності. Основні достоїнства даного ПЗ:

– зменшує складність створення розподілених систем. Подібне ПЗ покладає на себе частину функцій, які в локальному випадку виконують операційні системи;

– покладає на себе маршрутизацію запитів, дозволяючи тим самим забезпечити "живучість" прозорим для користувачів чином;

– здійснює балансування завантаження обчислювальних потужностей, що також сприяє підвищенню доступності даних;

– у стані здійснювати тиражування будь-якої інформації, а не тільки вмісту баз даних. Отже, будь-який додаток можна зробити стійким до відмов серверів;

– у стані відслідковувати стан додатків і при необхідності тиражувати й перезапускати програми, що гарантує "живучість" програмних систем;

– дає можливість прозорим для користувачів чином виконувати переконфігурування (і, зокрема, нарощування) серверних компонентів, що дозволяє масштабувати систему, зберігаючи інвестиції в прикладних системах.

Обслуговування. Під обслуговуванням розуміється мінімізація часу простою компонентів, що відмовили, а також негативного впливу ремонтних робіт на ефективність інформаційних сервісів, тобто швидке й безпечне відновлення після відмов. Заходи щодо забезпечення обслуговування спрямовані на зниження строків діагностування й усунення відмов та їхніх наслідків.

Для забезпечення обслуговування рекомендується дотримуватися наступних архітектурних принципів:

– орієнтація на побудову інформаційної системи з уніфікованих компонентів з метою спрощення заміни частин, що відмовили;

– орієнтація на рішення модульної структури з можливістю автоматичного виявлення відмов, динамічного переконфігурування апаратних і програмних засобів і заміни компонентів, що відмовили, в "гарячому" режимі.

Динамічне переконфігурування переслідує дві основні цілі:

– ізоляція компонентів, що відмовили;

– збереження працездатності сервісів.

Ізольовані компоненти утворять зону поразки реалізованої загрози. Чим менше відповідна зона ризику, тим вищим є обслуговування сервісів. Так. при відмовах блоків живлення, вентиляторів й/або дисків у сучасних серверах зона ризику обмежується компонентом, що відмовив; при відмовах процесорних модулів весь сервер може зажадати перезавантаження (що здатне викликати подальше розширення зони ризику). Очевидно, в ідеальному випадку зони поразки й ризику збігаються, і сучасні сервери й активне мережеве устаткування, а також програмне забезпечення провідних виробників досить близькі до цього ідеалу.

Можливість передбачення реакції на відмову також підвищує якість обслуговування систем. Кожна організація може вибрати свою стратегію реагування на відмови тих або інших апаратних і програмних компонентів й автоматизувати цю реакцію. Так, у найпростішому випадку можливе відправлення повідомлення системному адміністратору, щоб прискорити початок ремонтних робіт; у більш складному випадку може бути

реалізована процедура "м'якого" вимикання (перемикання) сервісу, щоб спростити обслуговування.

Можливість вилученого виконання адміністративних дій - важливий напрямок підвищення обслуговування, оскільки при цьому прискорюється початок відбудовних заходів, а в ідеалі всі роботи (зазвичай пов'язані з обслуговуванням програмних компонентів) виконуються у вилученому режимі, без переміщення кваліфікованого персоналу, тобто з високою якістю та в найкоротший термін. Для сучасних систем можливість вилученого адміністрування - стандартна властивість, але важливо подбати про його практичну реалізацію в умовах різнорідності конфігурацій (у першу чергу клієнтських).

Централізоване поширення й конфігурування програмного забезпечення, керування компонентами інформаційної системи й діагностування - надійний фундамент технічних заходів підвищення обслуговування.

Істотний аспект підвищення обслуговування - організація консультаційної служби для користувачів (обслуговування користувачів), впровадження програмних систем для роботи цієї служби, забезпечення достатньої пропускної здатності каналів зв'язку з користувачами, у тому числі в режимі пікових навантажень.

2.4.4 Забезпечення спостережності

Спостереженість — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії. Спостереженість забезпечується в КС такими послугами:

- реєстрація (аудит);
- ідентифікація і автентифікація;
- достовірний канал;
- розподіл обов'язків; цілісність КЗЗ;
- самотестування;
- ідентифікація і автентифікація при обміні;
- автентифікація відправника;
- автентифікація отримувача.

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності виявлення потенційних порушень.

Реєстрація — це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів, а особливо засобів

налагодження механізмів фіксування подій, має бути прерогативою спеціально авторизованих користувачів.

Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку.

Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації. Для жодного з рівнів послуги не встановлюється ніякого фіксованого набору контрольованих подій, оскільки для кожної системи їх перелік може бути специфічним.

Критична для безпеки подія визначається як подія, пов'язана з звертанням до якої-небудь послуги безпеки або результатів виконання якої-небудь функції КЗЗ, або як будь-яка інша подія, яка хоч прямо і не пов'язана з функціонуванням механізмів, які реалізують послуги безпеки, але може призвести до порушення політики безпеки. Остання група подій визначається як така, що має непряме відношення до безпеки. Для визначення ступеню небезпеки таких подій часто необхідним має бути їх аналіз у контексті інших подій, що відбулися.

Для реалізації найбільш високих рівнів даної послуги необхідна наявність засобів аналізу журналу реєстрації. Засоби аналізу — це засоби, що виконують більш складну, ніж перегляд, оцінку журналу реєстрації з метою виявлення можливих порушень політики безпеки.

Ці засоби повинні надавати адміністратору можливість виконання сортування, фільтрації за певними критеріями та інших подібних операцій. КЗЗ повинен надавати адміністратору можливість вибирати події, що реєструються. Це може бути досягнето або через "передвибірки", або "поствибірки".

Передвиборка подій, що реєструються, дозволяє виділити під час ініціалізації системи з всієї множини доступних для реєстрації подій підмножину тих, що необхідно реєструвати в журналі. Використовуючи передвибірку, адміністратор може зменшити кількість реально реєстрованих подій і, отже, розмір остаточного журнального файла. Недоліком предвибірки є те, що ті події, які не були вибрані, не можуть уже пізніше бути проаналізовані, навіть, якщо постає така необхідність. Перевага поствибірки полягає в гнучкості можливості аналізу "пост-фактум", проте така організація ведення журнального файла вимагає виділення значного обсягу пам'яті для даних реєстрації.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація

відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем.

За результатами ідентифікації і автентифікації користувача система (КЗЗ), по-перше, приймає рішення про те, чи дозволено даному користувачеві ввійти в систему, і, по-друге, використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації Відомі три основних типу автентифікації:

- щось, відоме користувачеві;
- щось, чим володіє користувач;
- щось, властиве користувачеві.

Пароль, персональний номер або інша подібна інформація є прикладом того, що називається "дещо, відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена простотою його повторення: достатньо просто обчислити або вгадати інформацію автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.

Такі фізичні об'єкти як смарт-карта, магнітна картка, генератор запитів відповідей, електронний ключ або фізично прошитий криптографічний ключ є прикладами того, що називається "дещо, чим володіє користувач". Основною перевагою даного типу автентифікації є складність або висока вартість дублювання інформації автентифікації. З іншого боку, втрата пристрою автентифікації може стати причиною потенційної компрометації. Проте, в більшості випадків достатньо просто установити факт втрати такого пристрою і попередити адміністратора безпеки про необхідність зміни інформації автентифікації.

Результати таких біометричних вимірювань, як відбитки пальців, параметри райдужної оболонки ока або геометрія руки служать прикладами того, що називають "дещо, що властиве користувачеві". Реалізація даного типу автентифікації повинна забезпечувати значно сильнішу автентифікацію, ніж два попередніх типи. Основною перешкодою для використання даного механізму є висока вартість пристроїв автентифікації. Крім того, використання цих достатньо дорогих засобів автентифікації не гарантує безпомилкової роботи. Рівень (ймовірність) помилок першого і другого роду для таких пристроїв може стати непридатним для деяких застосувань.

Для підвищення ефективності захисту від специфічних загроз несанкціонованого доступу вимагається використання комбінації мінімум двох різних типів автентифікації, наприклад, введеного з клавіатури пароля і носимого ідентифікатора.

Достовірний канал. Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається).

Розподіл обов'язків. Дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій. Система повинна передусім забезпечувати існування ролей для адміністратора і звичайного користувача.

Одна з цих ролей повинна бути роллю адміністратора безпеки (ця роль може бути поділена на ролі адміністратора реєстрації (аудиту) і адміністратора каталогів або облікових карток користувачів). Роль адміністратора безпеки повинна бути визначена так, щоб обов'язки, що мають відношення до безпеки, могли бути виконані тільки в цій ролі. Ролі не обов’язково мають бути абсолютно взаємовиключаючими, оскільки деякі функції або команди можуть знадобитись і адміністратору, і користувачу, або різним адміністраторам тощо.

Цілісність комплексу засобів захисту. Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Жодна КС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів за ініціативою користувача, в процесі запуску або штатної роботи.

Ідентифікація і автентифікація при обміні. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація відправника. Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Найширше для реалізації даної послуги, як і послуги автентифікації одержувача, використовується цифровий підпис, оскільки використання несиметричних криптоалгоритмів (на відміну від симетричних) дозволяє забезпечити захист від внутрішнього шахрайства і автентифікацію за взаємної недовіри сторін.

Автентифікація одержувача. Ця послуга дає можливість забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

РОЗДІЛ 3 КІБЕРБЕЗПЕКА

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 і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Це визначення наведено в ЗУ «Про основні засади забезпечення кібербезпеки України».

У середньостроковій перспективі (до п’яти років) індустрія кібербезпеки продовжуватиме прискорене зростання та глибоку модернізацію. Це зумовлено трьома взаємопов’язаними чинниками.

По-перше, невпинне розширення світової ІТ-екосистеми завдяки цифровізації охоплює практично всі сфери людської діяльності – включно з критично важливими. Це ускладнює структуру глобального кіберсередовища, створює нові загрози, багаторазово збільшує вектори атак і вимагає інноваційних рішень. Галузь кібербезпеки залишається надзвичайно привабливою для інвестицій та венчурного капіталу, особливо в передових (cutting-edge) секторах.

По-друге, галузь розвивається на тлі ескалації глобальної воєнно-політичної та фінансово-економічної турбулентності й стратегічної невизначеності. Це актуалізує питання власної безпеки – як індивідуальної, так і корпоративної, – додатково стимулюючи сталий попит на кіберзахист.

По-третє, індустрія переживає черговий якісний технологічний перехід – синергію бурхливого розвитку штучного інтелекту, хмарних обчислень та квантових технологій, що кардинально змінює як методи атак, так і арсенал захисту.

3.1 Основні положення

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони, Конвенція про кіберзлочинність, інші міжнародні договори, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Згідно ЗУ «Про основні засади забезпечення кібербезпеки України». об’єктами кібербезпеки є:

- конституційні права і свободи людини і громадянина;
- суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
- національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

– об’єкти критичної інфраструктури.

Суб’єкти забезпечення кібербезпеки:

а) координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України;

б) національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України;

в) Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури (крім об’єктів критичної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг);

г) суб’єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури;

8) суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Об’єктами кіберзахисту є:

– комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого

самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

– об’єкти критичної інформаційної інфраструктури;

– комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

– здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

– здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

– здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

– розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

– забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

– здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

3.2 Принципи забезпечення кібербезпеки

Забезпечення кібербезпеки в Україні грунтується на принципах:

– верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

– державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід’ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

– міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

– забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

3.3 Організаційно-технічна модель кіберзахисту

Організаційно-технічна модель кіберзахисту є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливостей комунікаційних систем.

Організаційно-технічна модель кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури та впроваджується для забезпечення функціонування національної системи кібербезпеки.

3.3.1 Базова термінологія

Слід визначити наступні терміни, які вживаються у такому значенні:

– базисна інфраструктура кіберзахисту - організована сукупність об’єктів кіберзахисту операторів критичної інфраструктури, а також суб’єктів господарювання, громадян та їх об’єднань, інших осіб, які провадять діяльність та/або надають послуги у сферах електронних комунікацій, електронної комерції, розвитку національних електронних інформаційних ресурсів, захисту інформації та кібербезпеки;

– кібергігієна - уміння, навички користування інформаційними технологіями, спрямовані на здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз;

– команди реагування на комп’ютерні надзвичайні події - групи фахівців з кібербезпеки, які утворюються з метою забезпечення кіберзахисту об’єктів кіберзахисту;

– організаційно-керуюча інфраструктура кіберзахисту - організована сукупність суб’єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки, визначають процедури та механізми кіберзахисту, організаційно-правові засади взаємодії між силами кіберзахисту та іншими суб’єктами забезпечення кібербезпеки;

– технологічна інфраструктура кіберзахисту - організована сукупність сил та засобів кіберзахисту, інфраструктурних об’єктів, що забезпечують функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту;

– сили кіберзахисту - урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA, інші команди реагування на комп’ютерні надзвичайні події, підрозділи (групи, команди, служби) захисту інформації, підприємства, установи та організації незалежно від форми власності, які провадять діяльність та/або надають послуги з кіберзахисту.

3.3.2 Функціонування організаційно-технічної моделі

Функціонування організаційно-технічної моделі кіберзахисту забезпечується шляхом:

– формування та реалізації державної політики у сфері кібербезпеки, зокрема з урахуванням досвіду держав - членів ЄС та НАТО;

– координації суб’єктів забезпечення кібербезпеки під час здійснення заходів з кіберзахисту об’єктів кіберзахисту та національних електронних інформаційних ресурсів;

– кіберзахисту інформаційно-комунікаційних систем, що обробляють національні електронні інформаційні ресурси, інших об’єктів кіберзахисту, забезпечення їх стійкості, здійснення постійного моніторингу стану їх кіберзахисту;

– розвитку системи реагування на кіберзагрози;

– розвитку сил кіберзахисту та системи їх координації;

– створення систем управління ризиками інформаційної безпеки на об’єктах критичної інфраструктури;

– формування та розвитку спроможносте суб’єктів забезпечення кібербезпеки;

– створення умов для безпечного функціонування інформаційної інфраструктури державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до закону, підприємств, установ та організацій незалежно від форми власності;

– створення умов для розвитку державно-приватної взаємодії в сфері кібербезпеки;

– розвитку системи кадрового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту;

– розвитку та вдосконалення систем кіберзахисту за результатами оцінки повноти, адекватності, результативності та ефективності здійснення заходів з кіберзахисту.

3.3.3 Засоби кіберзахисту

Засобами кіберзахисту, які використовуються для впровадження організаційно-технічної моделі кіберзахисту, є системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, інформаційні технології, технічні і програмні засоби (пристрої, обладнання, комплекси), які використовуються з метою забезпечення кіберзахисту національних електронних інформаційних ресурсів та об'єктів кіберзахисту.

Заходами з кіберзахисту, які здійснюються у процесі впровадження організаційно-технічної моделі кіберзахисту, є організаційні, правові, інженерно-технічні заходи, заходи з криптографічного та технічного захисту інформації, які проводяться силами кіберзахисту та базуються на принципах персональної відповідальності за власні дії та колективної відповідальності за безпеку кожного, забезпечення пропорційності та/або співрозмірності заходів реальним та потенційним ризикам.

У рамках впровадження організаційно-технічної моделі кіберзахисту сили кіберзахисту у межах своєї компетенції здійснюють базові заходи з кіберзахисту, в тому числі щодо проведення аналізу ефективності та корегування здійснених заходів з кіберзахисту, затвердження планів кіберзахисту та планів реагування на кіберінциденти/кібератаки.

Базовими заходами з кіберзахисту є заходи з:

– управління - визначення стратегій, політик, ролей та обов'язків, здійснення моніторингу щодо управління ризиками у сфері кібербезпеки;

– ідентифікації - оцінка реальних та потенційних ризиків у сфері кібербезпеки для запобігання та нейтралізації кіберзагроз;

– забезпечення захисту - розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталого та надійного функціонування об'єктів кіберзахисту, удосконалення систем реагування на кіберінциденти та кібератаки з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам;

– виявлення - проведення ідентифікації, збору та обробки кіберінцидентів/кібератак;

– реагування - запобігання кіберінцидентам та кібератакам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення;

– відновлення - поновлення штатного режиму функціонування об'єктів кіберзахисту після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки та кіберінциденту.

Базові заходи з кіберзахисту, а також методичні рекомендації щодо їх здійснення затверджуються Адміністрацією Держспецзв'язку.

Порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки для банків, інших осіб, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю

яких здійснює Національний банк, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг затверджуються Національним банком.

3.3.4 Сектора та суб'єкти забезпечення організаційно-керуючій інфраструктури кіберзахисту

Організаційно-керуюча інфраструктура кіберзахисту складається з таких секторів:

– загальнодержавний, до складу якого входять основні суб'єкти національної системи кібербезпеки, сили безпеки і оборони та Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України;

– галузевий, до складу якого входять центральні органи виконавчої влади, інші державні органи, які забезпечують формування та/або реалізацію державної політики в одній чи кількох сферах, або безпосередньо проводять відповідно до компетенції заходи із забезпечення кібербезпеки, секторальні органи у сфері захисту критичної інфраструктури, оператори критичної інфраструктури;

– регіональний (місцевий), до складу якого входять місцеві органи виконавчої влади, органи місцевого самоврядування, підприємства, установи та організації незалежно від форми власності, що провадять діяльність у сфері захисту інформації та кіберзахисту;

– освіти та науки, до складу якого входять науково-дослідні установи, заклади вищої освіти у сфері захисту інформації та кібербезпеки, що беруть участь у підготовці, підвищенні кваліфікації та перепідготовці професійних кадрів;

– приватний, до складу якого входять підприємства недержавної форми власності, організації та установи, що провадять діяльність у сфері захисту інформації та кіберзахисту (крім операторів критичної інфраструктури);

– громадський, до складу якого входять громадські організації, об'єднання, асоціації, спілки та фахівці у сфері кібербезпеки, а також міжнародні та міжурядові організації, що провадять свою діяльність у сфері кібербезпеки.

Під час функціонування організаційно-керуючої інфраструктури кіберзахисту суб'єкти забезпечення кібербезпеки:

– здійснюють в межах компетенції законодавче та нормативно-правове регулювання питань забезпечення кіберзахисту інформаційно-комунікаційних систем, що обробляють національні електронні інформаційні ресурси, інших об'єктів кіберзахисту;

– забезпечують гармонізацію законодавства у сфері захисту інформації, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та кібербезпеки з відповідним законодавством ЄС;

– забезпечують розвиток сил кіберзахисту, системи кадрового, фінансового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту;

– організовують здійснення базових заходів з кіберзахисту;

– залучають наукові установи, професійні та громадські об’єднання до підготовки проектів законодавчих та інших нормативно-правових актів у сфері кіберзахисту;

– організовують і проводять огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

– створюють умови для розвитку спроможности сил кіберзахисту, спрямованих на виявлення кібератак та захист від них, для ліквідації їх наслідків, відновлення сталості і надійності функціонування об’єктів кіберзахисту;

– забезпечують впровадження сучасних принципів, методів, підходів та механізмів публічного управління в сфері кібербезпеки;

– здійснюють співробітництво з питань кібербезпеки з органами інших держав, міжнародними, міжурядовими організаціями відповідно до компетенції та законодавства і міжнародних договорів України;

– координують дії з розроблення протоколів та регламентів взаємодії, карт технологічних процесів, регламентів робіт, планів реагування на кіберінциденти, планів відновлення та інших документів, що регламентують взаємодію між силами кіберзахисту;

– організовують та проводять кібернавчання, розробляють програми та методики їх проведення, сценарії реагування на кібератаки та кіберінциденти, рекомендації щодо відновлення після кібератак та кіберінцидентів, а також заходи з кібергігієни.

3.3.5 Технологічна інфраструктура кіберзахисту

Технологічна інфраструктура кіберзахисту складається з таких рівнів:

– національного - на базі сил кіберзахисту основних суб’єктів національної системи кібербезпеки та Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України;

– галузевого (регіонального, місцевого) - на базі сил кіберзахисту секторальних органів у сфері захисту критичної інфраструктури, інших суб’єктів забезпечення кібербезпеки галузевого (регіонального) рівня;

– об’єктового - на базі сил кіберзахисту інших суб’єктів забезпечення кібербезпеки, операторів критичної інфраструктури.

Суб’єкти, що діють у технологічній інфраструктурі кіберзахисту, забезпечують оперативне (кризове) реагування на кібератаки та кіберінциденти та здійснюють обмін інформацією про загрози та ризики у сфері кібербезпеки, а також про кіберінциденти, кібератаки на:

– національному рівні - між собою та відповідними підрозділами інших суб’єктів забезпечення кібербезпеки;

– галузевому (регіональному, місцевому) рівні - з відповідними суб’єктами національного та галузевого (регіонального, місцевого) рівня технологічної інфраструктури кіберзахисту;

– об’єктовому рівні - з відповідними суб’єктами всіх рівнів технологічної інфраструктури кіберзахисту.

Під час функціонування технологічної інфраструктури кіберзахисту сили кіберзахисту:

– здійснюють заходи з оперативного та ефективного захисту кіберпростору щодо зменшення ризиків у сфері кібербезпеки, протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, а також забезпечення кібероборони та кіберрозвідки шляхом збору, аналізу, оцінювання, узагальнення та поширення інформації про ризики у сфері кібербезпеки, кіберінциденти, кібератаки;

– здійснюють заходи з оперативного (кризового) реагування на кібератаки та кіберінциденти, зокрема за допомогою системи інформаційного обміну щодо таких подій, контрзаходи, спрямовані на усунення вразливостей об’єктів кіберзахисту;

– здійснюють заходи з кіберзахисту об’єктів кіберзахисту, в яких обробляються національні електронні інформаційні ресурси та/або які використовуються державними органами, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до закону;

– забезпечують функціонування систем реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту;

– розвивають об’єднання (мережі) команд реагування на комп’ютерні надзвичайні події, взаємодіють з командами реагування на комп’ютерні надзвичайні події, а також підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки у кіберпросторі;

– здійснюють взаємодію між собою відповідно до рішень суб’єктів забезпечення кібербезпеки;

– інформують про кібератаки/кіберінциденти та потенційні ризики у сфері кібербезпеки інші сили кіберзахисту та суб’єктів забезпечення кібербезпеки, опрацьовують отриману від них, зокрема від громадян, інформацію про кіберінциденти та щодо об’єктів кіберзахисту, надають консультативну та практичну допомогу з питань реагування на кібератаки;

– сприяють державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам у вирішенні питань щодо кіберзахисту та протидії кіберзагрозам;

– створюють та забезпечують функціонування основних складових частин системи захищеного доступу державних органів до Інтернету, системи антивірусного захисту національних електронних інформаційних ресурсів;

– беруть участь у проведенні кібернавчань, розробленні програм та методик їх проведення, сценаріїв реагування на кіберзагрози та проводять заходи щодо протидії кіберзагрозам, з кібергігієни;

– отримують і надають послуги з кіберзахисту.

3.3.6 Базисна інфраструктура кіберзахисту

Під час забезпечення функціонування базисної інфраструктури кіберзахисту забезпечується:

– захист у кіберпросторі національних електронних інформаційних ресурсів, що обробляються на об’єктах кіберзахисту;

– захист об’єктів кіберзахисту, у тому числі шляхом здійснення базових заходів з кіберзахисту;

– захист інтересів громадянина та суспільства у кіберпросторі;

– розроблення програм розвитку основ кібергігієни на національному, галузевому (регіональному, місцевому), об’єктовому рівні;

– здійснення заходів з формування культури кібербезпеки суб’єктами забезпечення кібербезпеки;

– інформування громадян про кіберінциденти.

Базисна інфраструктура кіберзахисту функціонує для забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів у кіберпросторі.

3.4 Національна система кібербезпеки

Національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури.

Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб ЗСУ, розвідувальні органи, Національний банк України.

Державна служба спеціального зв’язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, кіберзахисту об’єктів критичної інформаційної інфраструктури, координує

діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі та деякі інші завдання.

Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності.

Міністерство оборони України, Генеральний штаб ЗСУ відповідно до компетенції здійснюють заходи з підготовки держави до кібероборони, здійснюють військову співпрацю з НАТО, міжнародними організаціями та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз.

Розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, забезпечує функціонування системи кіберзахисту для банків

Функціонування національної системи кібербезпеки забезпечується шляхом:

– вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

– створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

– встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури;

– формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

– залучення експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

– функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розвитку мережі команд реагування на комп’ютерні надзвичайні події;

– розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

– забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

– створення та забезпечення функціонування Національної телекомунікаційної мережі;

– обміну інформацією про інциденти кібербезпеки між суб’єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

– впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов’язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об’єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

– впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

– встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

– державно-приватної взаємодії у запобіганні кіберзагрозам об’єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

– періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

– стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

– розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

– здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

– здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

– обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб’єктів господарювання, які перебувають під контролем держави, визнаної ВР України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб’єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

– розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

– проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об’єктів критичної інформаційної інфраструктури.

Органи державної влади, військові формування, утворені відповідно до законів України, державні підприємства, установи та організації з метою усунення можливих наслідків кіберінцидентів та кібератак створюють резервні копії національних електронних інформаційних ресурсів, що перебувають у їх володінні або розпорядженні та є критичними для їх сталого функціонування, та передають їх на зберігання до Національного центру резервування державних інформаційних ресурсів, крім тих, передача яких обмежена законодавством. Порядок передачі, збереження і доступу до зазначених копій визначається Кабінетом Міністрів України.

Національний центр резервування державних інформаційних ресурсів забезпечує:

– безперервність роботи відповідного національного електронного інформаційного ресурсу, резервного копіювання інформації та відомостей національного електронного інформаційного ресурсу через єдині основний та резервний захищені центри обробки даних (дата-центри), призначені для обробки національних електронних інформаційних ресурсів, резервного копіювання національних електронних інформаційних ресурсів;

– надійне функціонування серверного обладнання, системи зберігання даних, активного мережевого обладнання, архітектурно-технічних рішень щодо резервного копіювання й дублювання інформаційних систем, постійно працюючої інженерної інфраструктури;

– здійснення обов’язкового контролю за статистичними даними роботи з фізичного захисту об’єктів, системи управління та моніторингу інформаційних систем, комплексу організаційних заходів;

– розроблення, створення (побудову), модернізацію, розвиток, впровадження та супроводження програмного забезпечення інформаційної системи (платформи) для побудови та ведення реєстрів.

3.5 Загрози кібербезпеки

Сучасні загрози кіберсистемам дуже різноманітні. Але їх поєднує одна мета – порушення інформаційної безпеки у кіберпросторі. Реалізація цієї мети досягається різними методами та засобами, починаючи зі звичайного блокування систем та крадіжки даних, та закінчення високотехнологічними атаками на комп'ютерні системи..

3.5.1 Шкідливе програмне забезпечення

ШПЗ - це тип програмного забезпечення, призначеного для пошкодження або порушення роботи комп'ютерних систем. Воно може мати різні форми, включаючи віруси, хробаки та трояни. За умови запуску ШПЗ може завдати шкоди різними способами, зокрема:

- призвести до блокування пристрою та його непридатності для використання;
- крадіжки, видалення або шифрування даних;
- використовувати ваші пристрої для атак на інші організації;
- отримання облікових даних, які дозволяють отримати доступ до систем або служб якими ви користуєтесь;
- майнинг криптовалюти;
- використання платних послуг на основі ваших даних (наприклад, телефонні дзвінки преміум-класу).

Існує безліч типів шкідливих програм. Ось деякі з найпоширеніших.

Програми-здирники - це тип ШПЗ, яке шифрує файли компанії та вимагає оплату в обмін на ключ для розшифрування. Атаки вірусів-здирників можуть бути руйнівними для малого бізнесу, спричиняючи значні фінансові збитки та потенційно навіть призводячи до закриття підприємства.

Програма для показу реклами встановлюється на пристрій без згоди власника для відображення або завантаження реклами, часто у вигляді спливаючих вікон, з метою отримання прибутку за кліки. Така реклама часто уповільнює роботу пристрою. Більш небезпечні програми для показу реклами можуть встановлювати додаткове програмне забезпечення, змінювати параметри браузера і збільшувати вразливість пристрою до інших шкідливих атак.

Криптоджекінг – це ШПЗ, яке передбачає захоплення обчислювальної потужності пристрою для майнінгу криптовалют без відома власника, що сповільнює роботу зараженої системи.

Викрадач інформації – це ШПЗ, яке збирає інформацію на комп'ютері жертви і, як правило, відправляє її зловмисникові. Як приклад можна привести програми, що збирають хеші паролів, перехоплювачі і кейлогери. Дане ШПЗ зазвичай використовується для отримання доступу до облікових записів інтернет-додатків, таких як електронна пошта або інтернет-банкінг.

Бекдор - це шкідливий програмний код, який встановлюється в систему, щоб надати зловмиснику віддалений доступ. Бекдори зазвичай дозволяють підключитися до комп'ютера з мінімальною аутентифікацією або зовсім без такої і виконувати команди в локальній системі.

Руткіт . Це ШПЗ, що приховує існування іншого коду. Руткіти зазвичай застосовуються в поєднанні з іншим ШПЗ, таким як бекдор, що дозволяє їм відкрити зловмисникові доступ до системи і ускладнити виявлення коду.

Кейлогер -це ШПЗ, що реєструє кожну дію користувача, наприклад з пристроїв вводу (рух комп’ютерної миші, натиснення кнопок клавіатури).

Дозволяє заволодіти даними користувача, що були введені після його встановлення.

Програма для розсилки спаму - це ШПЗ, яке заражає комп'ютер користувача і потім з його допомогою розсилає спам. Цей тип програм генерує дохід для зловмисників, дозволяючи їм продавати послуги з розсилки спаму.

3.5.2 Соціальна інженерія

Соціальна інженерія стала однією з найбільших загроз у сфері кібербезпеки. Ця маніпулятивна тактика використовує людську психологію, щоб змусити людей розкривати конфіденційну інформацію або виконувати дії, які підривають безпеку. У той час як організації посилюють свої технічні засоби захисту, кіберзлочинці все більше звертаються до соціальної інженерії як основного вектора атаки.

Загроза, яку представляє соціальна інженерія, значна і зростає. Згідно з Звітом Verizon 2023 про порушення даних, 74% порушень включають людський фактор, зокрема соціальну інженерію. Згідно з даними Verizon DBIR за 2025 рік, 62% порушень були пов'язані з людським фактором, соціальна інженерія становила 16% порушень, а середній рівень успіху був на 40% вищим для фішингових атак, орієнтованих на мобільні пристрої, ніж через електронну пошту. Ця статистика підкреслює вразливість як компаній, так і окремих осіб до цих психологічних тактик. Цій вид атаки може привести до таких наслідків:

- витік даних;
- фінансові втрати;
- репутаційні збитки;
- порушення роботи;
- юридичні та регуляторні наслідки.

Соціальна інженерія як вид кібератаки існує у різних формах, кожна з яких спрямована на експлуатацію певних людських слабкостей і вразливостей. Знання цих типів є ключовим для розробки ефективних стратегій захисту. До найбільш поширених типів належать:

- *фішинг* , зміст якого полягає в тому, що зловмисники надсилають електронні листи або повідомлення, що виглядають як офіційні, наприклад, від банку або компанії. У них містяться посилання на фальшиві веб-сайти, де жертва вводить свої паролі, номери кредитних карток або іншу конфіденційну інформацію;
- *смішинг* – варіант фішингу через SMS. Зокрема, жертва отримує повідомлення з проханням перейти за посиланням або зателефонувати на номер для підтвердження даних, що призводить до втрат її приватної інформації або грошей;
- *вішинг* – це телефонні шахрайства, коли зловмисники видають себе за представників компанії або служби підтримки. Вони можуть

просити надати конфіденційну інформацію або змусити жертву виконати дії, що відкриють доступ до системи;

– *клонування сайтів*. Зловмисник створює копію реального сайту (зокрема, веб-сайт банку) та спонукає жертву відвідати його та ввести свої дані;

– *захоплення профілю*. Зловмисник видає себе за довірену особу в онлайн-спілкуванні або соціальних мережах, щоб обманом отримати від жертви інформацію або змусити її виконати певні дії;

– *атаки через соціальні мережі*, коли шахраї використовують соціальні мережі для збору інформації про цільову жертву або надсилають фальшиві запити про дружбу від імені знайомих для отримання доступу до особистих даних.

3.5.3 DoS та DDoS-атаки

DoS-атака (відмова в обслуговуванні) — це тип кібератаки, під час якої зловмисник виводить з ладу роботу комп’ютера, мережі або онлайн-сервісу завдяки атаці з одного комп'ютера. Існує два способи виконання DoS-атак: затоплення та збій. Атаки затоплення відбуваються, коли сервер отримує занадто багато даних у буфер, що призводить до зупинки його роботи. Атаки зі збоями використовують вразливості системи жертви аби покласти її.

DDoS-атаки (розподілена відмова в обслуговуванні) - це тип кібератаки, який полягає в перевантаженні сервера трафіком, що призводить до його виходу з ладу. DDoS-атаки можуть бути використані для виведення з ладу веб-сайту або мережі компанії, що спричиняє значні перебої в роботі бізнесу.

DDoS-атаки застосовуються зловмисниками частіше, адже мають наступні переваги:

– такі атаки можуть використовувати більшу кількість машин, щоб розпочати досить потужну атаку;

– оскільки атакуючі системи розподілені випадковим чином — інколи навіть по всьому світу — важко зрозуміти, звідки походить атака;

– ідентифікувати справжніх зловмисників важко, оскільки вони ховаються за багатьма системами;

– зі збільшенням кількості пристроїв IoT у світі зростатиме й кількість атак, адже зловмисники можуть робити їх частиною ботнетів.

Також існують й інші відмінності, які дозволяють ідентифікувати той чи інший вид атаки.

Простота виявлення. Оскільки DoS надходить з одного місця, легше виявити його походження та розірвати з’єднання. З іншого боку, DDoS-атака відбувається з кількох віддалених місць, приховуючи своє походження.

Швидкість атаки. Враховуючи, що DDoS-атака відбувається з кількох місць, її можна розгорнути набагато швидше, ніж DoS-атаку, яка походить з одного місця. Збільшена швидкість атаки ускладнює її виявлення, що означає збільшення шкоди.

Обсяг трафіку. DDoS-атака використовує кілька віддалених машин (зомбі або ботів), одночасно. Це означає, що вона здатна надсилати значно більші обсяги трафіку з різних місць та швидко перевантажувати сервер.

Спосіб виконання. DDoS-атака координує кілька хостів, заражених шкідливим програмним забезпеченням (ботами). В результаті вона створює ботнет, який керується командно-контрольним (C&C) сервером. Водночас DoS-атаку зловмисники зазвичай здійснюють з однієї машини.

3.5.4 Атаки на паролі

Атаки на паролі - це тип кібератак, коли хакери намагаються отримати доступ до систем або даних, вгадуючи або зламуючи паролі. Атаки на паролі можуть бути дуже ефективними, особливо якщо користувачі використовують слабкі або легко вгадуванні паролі. Якщо кіберзлочинець отримає доступ лише до одного з облікових записів, він може отримати доступ до наступної інформації:

- банківської інформації;
- даних кредитної картки;
- домашній адреси;
- номеру соціального страхування та ін.

Атака з розпорошенням паролів відбувається, коли зловмисник використовує загальнопоширені паролі, щоб спробувати отримати доступ до кількох облікових записів в одному домені. Використовуючи список поширених ненадійних паролів, таких як 123456 або password1, зловмисник може отримати доступ до сотень облікових записів за одну атаку.

При атаці з підстановкою облікових даних використовується той факт, що багато людей використовують одні й самі облікові дані для входу в кілька облікових записів. Зазвичай це повністю підтверджені облікові дані (ім'я користувача та пароль), які часто розкриваються внаслідок витоку даних.

На відміну від підстановки облікових даних, атаки з розпорошенням паролів зазвичай здійснюються за допомогою спеціального набору інструментів (набору програмних інструментів або однієї програми) після збирання імен користувачів з каталогу або відкритого вихідного коду. За допомогою цього інструментарію спочатку добуваються імена користувачів, потім перебираються паролі зі списку загальнопоширених паролів у спробі злому облікових записів.

Розпорошення паролів та підстановка облікових даних. Основна відмінність між розпорошенням паролів та підстановкою облікових даних полягає в тому, що при розпорошенні паролів використовується список загальнопоширених паролів для доступу до кількох облікових записів в одному домені, тоді як при підстановці облікових даних використовується лише один набір облікових даних у спробі доступу до різних облікових записів у кількох доменах.

Повний перебір (*атаки з використанням грубої сили*) відноситься до практики спроби підбору всіх можливих комбінацій букв і цифр, поки не підбереться той, який відповідає паролю. Найкращий спосіб пом'якшити атаки з використанням грубої сили - це зробити так, щоб паролі були довгими (вісім символів часто пропонуються як мінімум, але найкраще зробити пароль до можливої допустимої довжини) і не використовували слова або фрази. Чим довше пароль, тим більше кількість можливих комбінацій, які атакуючий повинен спробувати, щоб підібрати цій пароль.

Щоб запобігти парольним атакам, важливо впроваджувати надійну політику використання паролів, зокрема вимагати від користувачів використовувати складні паролі та регулярно їх змінювати. Крім того, впровадження багатофакторної автентифікації може забезпечити додатковий рівень безпеки.

Спуфінг (підробка) – це кібератака, яка відбувається, коли шахрай маскується під надійне джерело для отримання доступу до важливих даних або інформації. Спуфінг може відбуватися через веб-сайти, електронні листи, телефонні дзвінки, текстові повідомлення, IP-адреси та сервери.)

Якщо користувач вводить свою реєстраційну інформацію на підроблену сторінку, зловмисник отримає дані користувача. Атаки за допомогою спуфінгу простіше виконати, ніж може здатися на перший погляд. Будь-хто, хто контролює налаштування конфігурації мережі, може легко перенаправити відвідувачів на підроблену версію будь-якого сайту, який він забажає, змінивши конфігурацію DNS.

Атака за словником – це кібератака, яка передбачає, що в якості паролю використовується загальновживані слова. Перебираючи загальновживані словникові терміни, якщо ваш пароль складається з одного або двох стандартних слів, він буде скомпрометованим.

3.5.5 Інсайдерська загроза

Інсайдерська загроза (ІЗ) – ризик заподіяння шкоди організації людьми, які знаходяться всередині контуру організації. До таких людей – їх називають інсайдерами – можуть бути як колишні, так і нинішні співробітники самої компанії, і фахівці підрядників або партнерів, тобто кожен, хто має доступ до конфіденційної інформації і критичної інфраструктури компанії.

Інсайдер - особа, яка має або мав уповноважений доступ до критичних активів організації, де вони працюють та мають законний доступ до мережі компанії, які використовують їх доступ, зловмисно, або ненавмисно, діяв таким чином, щоб негативно вплинути на організацію. Ресурси можуть бути як загальнодоступні, так і не загальнодоступні. Інсайдерами можуть бути наступні категорії користувачів:

- користувачі, якім організація довіряє, включаючи співробітників, членів організації та тих, кому організація надала конфіденційну інформацію, таку як фінансові дані, бізнес-стратегія, а також сильні та слабкі сторони організації. У контексті державних функцій це також може включати секретну інформацію. Ці користувачі також могутть мати як фізичний, так і цифровий доступ до конфіденційної інформації;
- користувачі, які мають бейдж або інший пристрій, що надає їм можливість безперервного доступу до фізичної власності компанії, наприклад до центру обробки даних або головного офісу компанії;
- користувачі, які мають корпоративний комп’ютер із доступом до мережі;
- користувачі, які мають доступ до корпоративної мережі компанії, хмарних ресурсів, програм або даних;
- користувачі, яким відома стратегія компанії та її фінансові показники.
- користувачі, які мають глибокі знання про продукти та послуги організації та, можливо, допомагає їх розвивати. Ця група включає тих, хто знає секрети продуктів, що надають цінності організації працюють над створенням продуктів або послуг компанії.

Інсайдери можуть діяти усвідомлено та неусвідомлено. Зазвичай їх виділяють на три категорії:

Зловмісні інсайдери - ті, хто навмисно зловживає обліковими даними для крадіжки інформації у фінансових чи особистих цілях. Наприклад, це може бути людина, яка незадоволена роботодавцем і тому дає секретну конкуренту. Інсайдери мають перевагу перед іншими зловмисниками, тому що вони знайомі з політикою та процедурою організації та їх вразливістю.

Інсайдери «з необережності» - невинні жертви, які ненавмисно наражають компанію на ризик. Це найпоширеніші типи внутрішніх загроз. Наприклад, співробітник може перейти за незабезпеченими посиланнями та заразити системними шкідливими програмними забезпеченнями.

"Кріт" - шахрай, яким отримано інсайдерський доступ до привілейованої мережі.

Найбільш типові внутрішні загрози.

Випадковість. Іноді користувачі припускаються помилок, які можуть призвести до потенційних інцидентів із безпекою. Наприклад, бізнес-партнер надсилає документ із даними клієнтів колезі, не усвідомлюючи, що той не має дозволу на перегляд цієї інформації. Або працівник реагує на фішингову кампанію та випадково встановлює зловмисну програму.

Наявність наміру заподіяти шкоду. У інциденті з безпекою з наявним наміром заподіяти шкоду, спричиненому інсайдером, працівник або довірена особа навмисно робить те, що, на його думку, має негативно вплинути на компанію. Такі особи можуть керуватися особистими образами або іншими особистими причинами. Вони також можуть розраховувати на фінансовий або інший прибуток в результаті своїх дій.

Недбалість схожа на випадковість в тому, що особа не має на меті спричинити інцидент із безпекою даних. Різниця полягає в тому, що вони можуть свідомо порушувати політику безпеки. Типовий приклад недбалості – працівник дозволяє комусь увійти в будівлю без перепустки. Цифровим еквівалентом подібної поведінки буде відмова політики безпеки заради швидкості та зручності без урахування можливих наслідків, або вхід у ресурси компанії з використанням незахищеного безпровідного підключення.

Змова. Деякі інциденти із безпекою, спричинені інсайдерами, є результатом того, що довірена особа співпрацює з кіберзлочинною організацією, допомагаючи їй у шпигунській діяльності або у скоєнні крадіжки. Це також тип інциденту з безпекою з наявним наміром заподіяти шкоду.

3.5.6. Використання штучного інтелекту

Різні моделі ШІ та методи машинного навчання також допомагають зловмисникам здійснювати більш масштабні та складні атаки, дають змогу обходити засоби контролю безпеки та можливість пошуку нових вразливостей з безпрецедентною швидкістю та руйнівними наслідками для IT-інфраструктур різних компаній. За даними щорічного опитування зловмисників Bugcrowd, опублікованого в жовтні 2024 року, 77 % зловмисників використовують ШІ для злому, а 86 % стверджують, що він докорінно змінив їхній підхід до злому. Сьогодні 71 % вважають, що технології штучного інтелекту корисні для злому, тоді як у 2023 році таких було лише 21 %.

Експерти попереджають про потенційні проблеми поширення штучного інтелекту. Зокрема, нещодавній звіт Національного центру кібербезпеки Великої Британії (NCSC) наголошує, що протягом найближчих двох років технології ШІ майже напевно збільшать динаміку кібератак та посилять їхній вплив. За оцінками Центру, машинне навчання відкриває широкі можливості у цьому напрямі навіть для тих злочинців, що не мають відповідних технічних навичок. Інакше кажучи, хакерство ще ніколи не було таким доступним. Це занепокоєння поділяють і в бізнесі.

Опитування SecurityMagazine 2023 року показало, що 75 % фахівців з безпеки відзначили збільшення кількості кібератак за минулі 12 місяців. 85 % опитаних пов’язують це зростання з використанням зловмисниками генеративного ШІ.

Також згідно з жовтневим звітом компанії Keeper Security, 51 % керівників ІТ-відділів і служббезпеки вважають, що атаки з використанням ШІ є найсерйознішою загрозою, з якою стикаються їхні організації. Зловмисники можуть використовувати штучний інтелект для найрізноманітніших злочинів: від автоматизованих DDoS-атак до складного фішингу і соціальної інженерії. Наприклад, у 2021 році дослідники McAfee викрили кампанію кібершпигунства під назвою Operation Dianxun.

Злочинці використовували ШІ для створення фішингових електронних листів, націлених на телекомунікаційні компанії у всьому світу. Зловмисники застосували генерацію природної мови, аби створювати переконливі повідомлення, схожі на типові листи рекрутерів або галузевих експертів. Однак ці листи містили вкладення та посилання із шкідливим ПЗ.

У 2023 році зловмисники застосували ШІ, щоб обійти систему біометричної автентифікації криптобіржі Bitfinex, яка вимагала від користувачів підтверджувати свою особу за допомогою обличчя та голосу. Злочинці застосували Deepfake, аби генерувати реалістичні зображення облич, а також голосу і поведінки жертв. У результаті зловмисники привласнили цифрові активи на $150 млн. У лютому 2024 року фінансовий фахівець міжнародної інженерної компанії Arup був уведений в оману злочинцями та перевів їм понад $25 млн. Аби подолати сумніви менеджера щодо дивної транзакції, шахраї у режимі реального часу згенерували за допомогою технологій Deepfake відеодзвінок з фінансовим директором та деякими іншими співробітниками Arup.

Як описано у вищенаведеному прикладі, можливість генерувати адаптивні фішингові листи зловмисники використовують для автоматизації вчинення злочинів у кіберпросторі. Експерти з кібербезпеки з SoSafe, станом на 23 квітня 2023 року, провідного європейського постачальника обізнаності та навчання з питань безпеки давно попереджають про можливість того, що генеративний штучний інтелект може писати фішингові електронні листи краще, ніж люди. Початкові дослідження SoSafe показують, що це попередження про загрозу виправдане: дані показали, що фішингові електронні листи, написані штучним інтелектом, відкривали 78% людей, а 21% продовжували натискати на шкідливий контент всередині наприклад, посилання або вкладення. У проведеному дослідженні фішингові електронні листи, створені людиною, отримали трохи більше кліків - 27 %, тоді як показники відкриття були однаковими як для штучного інтелекту, так і для фішингових листів, створених людиною. Дані демонструють, що люди не можуть відрізнити фішингові електронні листи, створені штучним інтелектом, від фішингових атак, написаних вручну

Як бачимо, хакери опанували технології ШІ дуже швидко й активно використовують їх для кібератак за низкою напрямків:

- автоматизація процесів зламу (пошук вразливостей, подолання засобів захисту);
- спрощення та автоматизація цільового фішингу для викрадення особистих даних;
- виготовлення дипфейків для шахрайства та соціальної інженерії;
- “отруєння даних” для виведення ладу ШІ-моделям для будь-яких завдань;
- спрощення розробки шкідливого софту.

Одним із найбільш очевидних застосувань ШІ в кібербезпеці є сфера фішингу: тоді як жертви атак колись могли покладатися на друкарські помилки та граматичні помилки, щоб відсіяти підозрілі повідомлення, цей шлях захисту значною мірою був відрізаний із появою загальнодоступних генеративних LLM, які пропонують ідеальну граматику та орфографію безкоштовно або за низькою ціною. У свою чергу, навчання з питань обізнаності в галузі безпеки бореться з меншою ефективністю, ніж будь-коли раніше. Моделі ШІ також підсилюють неповедінкові шляхи атак, оскільки вони здатні ефективно створювати та редагувати шкідливий код.

Приклади використання ШІ:

– автоматичний збір даних із відкритих джерел - OSINT, аналіз трафіку для виявлення вразливих точок, використання ШІ для обробки великих обсягів інформації про жертву;

– генерація переконливих фішингових листів, створення deepfake-контенту: аудіо, відео, зображення, автоматизація створення підроблених профілів користувачів;

– використання фішингових листів, створених ШІ, персоналізованих для жертв, обхід біометричної автентифікації за допомогою deepfake-технологій;

– розгортання шкідливого програмного забезпечення, створеного ШІ, з функціями самонавчання та адаптації для обходу засобів безпеки;

– створення динамічних бекдорів за допомогою ШІ, які змінюють поведінку залежно від середовища;

– використання ШІ для аналізу та експлуатації відомих вразливостей у системах, адаптація атак у режимі реального часу;

– мутація шкідливого коду під час виконання, імітація легітимного трафіку або файлів за допомогою генеративних моделей;

– атаки на паролі з використанням алгоритмів машинного навчання, які адаптуються до кожної невдалої спроби, автоматизоване добування даних із витоків;

– аналіз мережевого трафіку для виявлення доступних пристроїв, вивчення системних конфігурацій і політик безпеки з використанням алгоритмів ШІ;

– автоматизація пошуку слабких місць у внутрішніх мережах і переміщення між системами за допомогою розподілених атак;

– швидкий аналіз даних, зібраних із компрометованих систем, оптимізація їх ексфільтрації на основі аналізу ризиків виявлення;

– створення стелс-каналів зв’язку, які імітують звичайний трафік, або використання генеративних моделей для адаптивного управління мережею ботів;

– застосування ШІ для маскування виведених даних як звичайних файлів, оптимізація шляхів ексфільтрації залежно від структури мережі жертви ;

– оптимізація атак типу DDoS, створення шкідливого коду, здатного адаптуватися для максимального руйнування, атаки на системи за допомогою deepfake-контенту для маніпуляцій запобігти чотирьом поширеним інсайдерським загрозам.

Шкідливе програмне забезпечення, кероване штучним інтелектом: DeepLocker представляє нове покоління атак на основі штучного інтелекту, які можуть уникати традиційних методів виявлення. Компанія IBM його розробила як тестовий зразок, DeepLocker перебуває в сплячому режимі доти, доки не визначить свою конкретну ціль, використовуючи машинне навчання для розпізнавання рис обличчя, геолокації або навіть голосових даних. Як тільки ціль підтверджено, шкідливе програмне забезпечення активується, доставляючи своє корисне навантаження у такий спосіб, що його майже неможливо виявити, поки не стане надто пізно. Традиційне шкідливе програмне забезпечення програмується з єдиною метою, але машинне навчання дає змогу шкідливим застосункам вчитися у свого оточення і коригувати свою поведінку. Наприклад, якщо виявлено антивірусне програмне забезпечення, зловмисник може змінити метод атаки, щоб уникнути виявлення. Наприклад, як у випадку з DeepLocker – застосунок може маскуватися під легітимні програми.

Соціальна інженерія з використанням рішень машинного навчання, згідно з дослідженнями компанії Microsoft, вважається однією з поширених атак у 2024 році. Зокрема, такі інструменти, як EvilProxy, використовують ШІ для створення персоналізованих електронних листів. EvilProxy автоматизує процес вилучення даних із соціальних мереж, даючи змогу зловмисникам створювати фішингові електронні листи, пристосовані до конкретних цілей на основі їхньої поведінки в інтернеті. Від традиційних методів фішинг з використанням штучного інтелекту відрізняє його здатність адаптуватися. ШІ може аналізувати звички та інтереси користувача, автоматично змінюючи вміст листа, щоб підвищити його правдоподібність. Наприклад, в електронному листі, створеному штучним інтелектом, можуть міститися посилання на нещодавні публікації в соціальних мережах, поточні проекти або навіть особисті інтереси, що робить його майже неможливим виявити як фішинговий на перший погляд. Розробка і впровадження систем для автоматизованого виявлення фішингових атак є важливою складовою сучасних оборонних

кібероперацій. Використання таких алгоритмів, як випадкові ліси, логістична регресія та метод опорних векторів, дає змогу комплексно оцінювати ознаки фішингу, зокрема наявність IP-адрес у посиланні, валідність SSL-сертифікатів та кількість субдоменів.

Атаки грубої сили за допомогою PassGAN використовує машинне навчання для прогнозування ймовірних паролів на основі шаблонів, знайдених у витоку наборів даних паролів. Традиційні атаки грубої сили просто перебирають всі можливі комбінації, але підхід PassGAN з використанням машинного навчання робить цей процес набагато ефективнішим, надаючи пріоритет найбільш вірогідним комбінаціям. На відміну від традиційних інструментів для атак грубої сили, які були обмежені необхідністю послідовно перебирати паролі, PassGAN здатний навчатись на попередньо отриманих позитивних результатах. Інструмент генерує потенційні паролі на основі реальних даних. Таке рішення може передбачити типи паролів, які користувачі, ймовірно, створять, наприклад, на основі особистої інформації, загальних фраз або передбачуваних шаблонів.

Технологія Deepfake дала змогу зловмисникам створювати реалістичні відео та аудіозаписи, які неможливо відрізнити від справжніх. Такі інструменти, як FaceSwap і Respeecher, зазвичай використовуються для того, щоб видавати себе за керівників, знаменитостей або навіть членів сім'ї, що призводить до шахрайства, шантажу або інших зловмисних дій. Ці інструменти штучного інтелекту можуть генерувати переконливий контент, що імітує голос або зовнішність практично будь-якої людини, що полегшує шахраям завдання обманом змусити жертв передати конфіденційну інформацію або великі суми грошей. Діпфейки особливо небезпечні, оскільки підривають довіру до цифрової комунікації. Оскільки зловмисники вдосконалюють ці інструменти, навіть відеодзвінки або голосова автентифікація можуть стати ненадійними.

Чат-боти на основі ШІ зробили обслуговування клієнтів більш ефективним, але зловмисники також використовують цю технологію в зловмисних цілях. SNAP_R - це чат-бот зі штучним інтелектом, розроблений спеціально для фішингових кампаній, що дає змогу зловмисникам автоматизувати персоналізовані фішингові атаки через електронну пошту та соціальні мережі. На відміну від традиційних фішингових листів, які часто є шаблонними і їх легко роз пізнати, SNAP_R може вступати в реалістичні розмови зі своїми цілями, коригуючи свої відповіді на основі даних жертви, щоб зробити атаку більш правдоподібною. Окрім уже згаданих інструментів, сучасні зловмисники мають у своєму розпорядженні ще більше можливостей завдяки спеціалізованим чат-ботам та програмам, які базуються на великих мовних моделях (LLM). Одним із таких інструментів є Worm GPT. Цей чат-бот, створений на основі GPT-J з відкритим вихідним кодом, призначений для підтримки зловмисників у програмуванні та кіберзлочинній діяльності.

Відсутність обмежень і фільтрів безпеки дає змогу використовувати Worm GPT для створення шкідливого коду, аналізу вразливостей та автоматизації атак. Ще одним прикладом використання машинного навчання зловмисниками є Auto GPT - експериментальна програма, що працює на основі GPT-4. Вона здатна самостійно виконувати завдання, генеруючи необхідні підказки та дії з мінімальним втручанням людини. Auto GPT може стати інструментом у руках кіберзлочинців для автоматизації складних процесів, таких як сканування систем на вразливості чи розробка зловмисного ПЗ.

DAN Prompt (“Do Anything Now”) дає змогу знімати обмеження з Chat GPT і розкривати його повний потенціал. Цей інструмент дає змогу створювати контент на заборонені теми, зокрема наркотики, злочини чи насильство, що робить його особливо привабливим для зловмисників. Інший інструмент, Fraud GPT, спеціалізується на створенні текстів для фішингових атак, шахрайських схем та написання шкідливого коду. Його функції дають змогу створювати переконливі повідомлення, які обманом змушують жертв розголошувати конфіденційну інформацію або виконувати небажані дії. Нарешті, Poison GPT демонструє, як можна використати великі мовні моделі для поширення неправдивої інформації та створення шкідливих програм. Його потенціал відкриває нові горизонти для атак із використанням соціальної інженерії.

Всі ці інструменти, від Worm GPT до Poison GPT, є прикладом того, як штучний інтелект може бути використаний не лише для інновацій, а й для створення значних кіберзагроз. Це підкреслює важливість розробки захисних механізмів, які зможуть протистояти цим новим викликам.

3.6 Кібергігієна

Згідно з «Положенням про організаційно-технічну модель кіберзахисту» кібергігієна - уміння, навички користування інформаційними технологіями, спрямовані на здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз.

Кібергігієна – це комплекс заходів та звичок, спрямованих на захист особистих даних, пристроїв та цифрової ідентичності від кіберзагроз. У сучасному світі, де цифрові технології стали невід'ємною частиною нашого повсякденного життя, поняття кібергігієни набуває критичної важливості.

Основи кібергігієни включають створення надійних унікальних паролів, використання багатофакторної автентифікації, обережність із підозрілими повідомленнями та регулярне оновлення програмного забезпечення

3.6.1 Паролі. Створення та зберігання.

Пароль - це секретний набір символів, призначений для підтвердження справжності користувача (автентифікації) та надання йому санкціонованого доступу до даних, систем або пристроїв.

Тут виникає два питання. Як створити пароль та як його зберігати.

Для створення пароля потрібне виконання деяких принципів:

– логін і пароль не повинен бути ідентичним;

– пароль не повинен складатися з особистої інформації (дата народження, телефон тощо);

– пароль повинен складатися виключно з довільними комбінаціями літер верхнього та нижнього регістру, цифр та спеціальних символів;

– створювати новий пароль для кожного окремого сервісу;

– не вводити паролі на сайтах без протоколу HTTPS (за його допомогою шифруються всі дані між клієнтом і сервером, що створює повну конфіденційність інформації користувача, наприклад паролі або банківські реквізити);

– враховувати довжину паролю – бажано не менше 12 символів;

– міняти пароль щоразу, коли здається, що його могли вкрасти. В інших випадках змінювати пароль не рідше ніж раз на 6 місяців.

3.6.1.1 Методи створення стійких паролів

При створенні стійких паролів виникають дві задачі – вигадати складний пароль та запам’ятати його. Паролі створюються за шаблонами власного мислення. Дослідження та аналіз паролів показали, що більш 40% із них можна підібрати, використовуючи програмні методи. Часто людина, яка складає пароль, вказує в ньому те, що має безпосереднє відношення до неї та/або її оточення

Найбільш стійкими є паролі, які створені за допомогою «генераторів паролей». Ідея таких генераторів полягає у виборі випадкових символів (літер на верхньому та нижньому регістрах, цифр, спеціальних знаків) із заданою кількістю. Ця кількість збільшується з часом і на сьогодні становить 10-12 символів і більше. Такі паролі досить стійкі до компрометоції, але мають істотний недолік. Їх майже неможливо запам'ятати.

Велике значення під час створення паролів надається його довжині. Пароль з 6 - 8 символів, складений генератором паролів, буде менш надійним ніж пароль, що представляє набір з 12 цифр.

Однією з найпрактичніших рекомендацій при створенні пароля є використання будь-якої парадоксальної фрази, яка дуже легко запам'ятовується. Наприклад «Спекотним травневим днем діти у пісочниці вбирали новорічну ялинку». Якщо в якості пароля взяти перші літери цього речення, записати їх на англійській розкладці зі зміною регістру і поставити між ними спеціальні символи, то отриманий пароль C_n-l_l-e#g#d#y#z буде досить надійним.

3.6.1.2 Зберігання паролів

Перш ніж говорити про способи зберігання пароля, слід відзначити два важливі моменти. Перший. Нам необхідно створений пароль надіслати комп'ютеру для зберігання та його використання для ідентифікації. Другий. Нам потрібно просто зберігати пароль, щоб мати можливість повторно увійти в комп'ютер або, іншими словами, згадати цей пароль.

Перший момент. Сам процес доступу до комп'ютера передбачає введення пароля і після збігу зі збереженим у машині цей доступ дозволяється. Очевидно, що зберігати у відкритому вигляді пароль у комп'ютері не можна. У разі доступу до комп'ютера сторонніх осіб такий пароль легко компрометується. Розв'язанням цього завдання може бути шифрування пароля. Однак для цієї процедури необхідна система шифрування та ключ, за допомогою якого можна буде зробити саме шифрування. У цьому випадку ключ повинен зберігатися безпосередньо на комп'ютері у відкритому вигляді. Це вразливість, якою легко може скористатися зловмисник. Рішенням є застосування функції хешування.

Сама функція хешування є математичне перетворення тексту, що надходить на її вхід. На виході цього перетворення виходить повідомлення стандартної довжини, що не залежить від розміру входу, сильно залежить від зміни навіть одного елемента входу і неможливості відновити вхідну послідовність по вихідний. Комп'ютер зберігає тільки результати хешування паролів, що виключає відновлення паролів. При введенні пароля проводиться його хешування та порівняння з хеш, який зберігається в комп'ютері. Якщо обидва хеша збігаються, дозволяється доступ.

Вимога створювання нового паролю для кожного окремого сервісу є досить проста. Але запам’ятовувати усі ці паролі дуже проблематично. Для надійного зберігання великої кількості сильних паролів, які важко запам’ятати, доцільно використовувати менеджери (диспетчери) паролів – спеціалізовані програмні продукти для роботи з паролями, PIN-кодами. Менеджер паролів може бути реалізовано як онлайн-сервіс, бути вбудованим до браузеру чи інстальований в операційну систему пристрою. Менеджер використовує досить потужне шифрування AES, яке практично не піддається зламу з довжиною ключа у 256 біт. Таку базу можна розблокувати тільки за допомогою використання правильного майстер-паролю, отже, користувачу необхідно запам’ятати лише один надійний пароль.

Другий момент. Процес зберігання паролю поза комп’ютера. Якщо з певних причин пароль необхідно записати, уникайте наступних сценаріїв:

- ніколи не записуйте паролі на наліпках з подальшим розміщенням на моніторі або у блокноті, який зберігається прямо на робочому місці у відкритому доступі;
- не залишайте паролі в інших місцях, де з ними можуть ознайомитися сторонні люди;
- не зберігайте паролі в електронному вигляді у комп'ютері або смартфоні.

3.6.2 Двофакторна автентифікація

Двофакторна автентифікація є процесом, що вимагає від користувача подання двох різних форм ідентифікації для отримання доступу до облікового запису. Це часто використовується як додатковий захисний етап для захисту ваших облікових записів і онлайн-сервісів. Двофакторна автентифікація є важливою, оскільки вона додає додатковий рівень безпеки до вашого облікового запису, що ускладнює процес незаконного доступу. Навіть якщо зловмисник знає ваш пароль, він все одно не зможе увійти в систему, оскільки він потребує другого фактору автентифікації.

Двофакторна автентифікація працює шляхом використання двох з трьох можливих "факторів": щось, що ви знаєте (наприклад, пароль), щось, що ви маєте (наприклад, смартфон), або щось, що ви є (наприклад, ваш відбиток пальця). Деякі поширені приклади двофакторної автентифікації включають SMS-повідомлення з кодом, яке відправляється на ваш телефон після введення пароля, мобільні додатки, що генерують коди, та біометричні фактори, такі як відбитки пальців або розпізнавання обличчя.

Двофакторна автентифікація забезпечує:

- збільшення безпеки шляхом додавання ще одного рівня автентифікації, що значно знижує ризик несанкціонованого доступу до облікового запису;
- захист ваших персональних даних та фінансової інформації;
- захист доступу до облікових записів при компрометації паролю без другого фактора автентифікації.

3.6.3 Обережність із підозрілими повідомленнями та в соціальних мережах

Мережа Інтернет надає безліч можливостей, але разом з тим, є місцем, де користувач ризикує зіштовхнутися з безліччю кіберзагроз. Можливі кіберзагрози розглянуті у попередньому розділі. Для захисту від злочинців потрібно бути уважним та дотримуватися кращих практик безпечної роботи в Інтернеті.

При отриманні різних повідомлень не поспішайте переходити на посилання з них. До таких повідомлень можуть належати різноманітні конкурси, пропозиції недорогого відпочинку, участь у розіграшах тощо. Одним із головних елементів у них буде реєстрація з отриманням персональних даних. Особливо обережно необхідно розміщувати свою інформацію у соціальних мережах. Подібні електронні знайомства можуть стати збором відомостей, які можуть бути використані для фальсифікації пригод або шантажу.

При діалогах у мережах необхідно пам'ятати, що розмова ведеться з незнайомою людиною, яка може представитися будь-ким. Найчастіше співрозмовником може виявитися досвідчений психолог, який досить

швидко увійде в довіру, непомітно вам отримає велику кількість інформації, складе ваш психологічний портрет і знайде вразливості, за допомогою яких можна буде керувати вами.

3.6.4 Оновлення програмного забезпечення

У процесі експлуатації у програмному забезпеченні виявляються вразливості. Після їх виявлення необхідно здійснити оновлення ПЗ. Для цього можливе використання автоматичного поновлення операційної системи, браузерів.

Аналогічні дії слід здійснити з антивірусами. Суть таких оновлень полягає в завантаженні в базу вірусів нових сигнатур, які використовуються для сигнатурного аналізу програм, що завантажуються.

Розділ 4 Кібербезпека об’єктів критичної інфраструктури

4.1 Об’єкти критичної інфраструктури

Віднесення об’єктів до об’єктів критичної інфраструктури (ОКІ) та формування Реєстру ОКІ здійснюються відповідно до ЗУ "Про критичну інфраструктуру". Критерії та порядок віднесення об’єктів до ОКІ, перелік таких об’єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а щодо банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг - Національним банком України.

До секторів критичної інфраструктури відносяться наступні:

- паливно-енергетичний сектор;
- цифрові технології;
- захист інформації ;
- харчова промисловість та агропромисловий комплекс;
- державний матеріальний резерв;
- охорона здоров'я ;
- ринки капіталу та організовані товарні ринки;
- фінансовий сектор;
- транспорт і пошта ;
- системи життєзабезпечення ;
- місцеве самоврядування;
- промисловість;
- сектор громадської безпеки;
- цивільний захист населення і територій ;
- охорона навколишнього природного середовища;
- сектор оборони;
- оборонно- промисловий комплекс
- правосуддя;
- виконання кримінальних покарань, тримання під вартою та утримання військовополонених;
- державна реєстрація;
- наукові дослідження та розробки;
- фінансова та банківська діяльність;
- вибори та референдуми;
- соціальний захист;
- інформаційний сектор;
- державна влада та місцеве самоврядування.

До паливно-енергетичного сектору відносяться:

- електроенергетика;
- вугільно-промисловий комплекс;
- торфодобування;
- нафтова промисловість
- газова промисловість;
- ядерна енергетика;
- енергетичне машинобудування.

До сектору цифрових технологій відносяться:

- електронні довірчі послуги та електронна ідентифікація;
- електронні комунікації;
- електронне урядування;
- цифрова інфраструктура.

До сектору захисту інформації відносяться:

- криптографічний захист інформації;
- технічний захист інформації;
- спеціальний та конфіденційний зв’язок;
- кіберзахист.

До сектору харчової промисловості та агропромислового комплексу відносяться виробництво та переробка сільськогосподарської та/або харчової продукції та ветеринарних препаратів, експлуатація елеваторів та зрошувальних систем і каналів.

До сектору державного матеріального резерву відноситься забезпечення зберігання запасів державного матеріального резерву.

До сектору охорони здоров'я відносяться:

- медична допомога;
- громадське здоров'я;
- судово-медична експертиза;
- інформаційні технології у сфері охорони здоров'я;
- фармацевтична промисловість.

До сектору ринків капіталу та організованих товарних ринків відносяться забезпечення функціонування ринків капіталів та організованих товарних ринків.

Фінансовий сектор забезпечує організацію планування, обслуговування, моніторинг виконання бюджетів, запобіганню та протидії легалізації доходів, одержаних злочинним шляхом.

До сектору транспорту і пошти відносяться:

- авіаційний транспорт
- автомобільний та міський електричний транспорт
- метрополітен
- залізничний транспорт
- морський та внутрішній водний транспорт

– поштовий зв'язок

Системи життєзабезпечення включають до себе комунальні послуги.

До сектору місцевого самоврядування відносяться виконання функцій місцевого самоврядування

До сектору промисловості відносяться:

– хімічна промисловість;

– металургійна промисловість.

До сектору громадської безпеки відносяться:

– громадська безпека;

– екстрена допомога населенню за єдиним телефонним номером 112;

– експертна служба МВС.

До сектору цивільного захисту населення і територій відносяться атестовані аварійно-рятувальні служби

До сектору охорони навколишнього природного середовища відносяться:

– управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства;

– поводження з радіоактивними відходами;

– охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду.

До сектору оборони та оборонно- промислового комплексу відносяться:

– зберігання ракет, боєприпасів та вибухових речовин;

– оборонна промисловість;

– космічна промисловість;

– авіаційна промисловість;

– суднобудівна промисловість.

До сектору правосуддя відносяться питання здійснення правосуддя.

Сектор виконання кримінальних покарань, тримання під вартою та утримання військовополонених забезпечує тримання засуджених, осіб, узятих під варту, а також утримання військовополонених.

Сектор державної реєстрації забезпечує функціонування інформаційних технологій у сфері державної реєстрації.

До сектору наукових дослідження та розробки відносяться дослідницька інфраструктура наукових установ та закладів вищої освіти.

До сектору фінансової та банківської діяльності відносяться:

– банківська система;

– ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків) ;

– ринок платіжних послуг.

Сектор виборів та референдумів забезпечує організація підготовки та проведення виборів та референдумів за допомогою інформаційних

(автоматизованих), інформаційно-комунікаційних систем та електронних реєстрів.

До сектору соціального захисту відносяться:

- пенсійне забезпечення;
- соціальне страхування;
- соціальна допомога і соціальні послуги;
- інформаційна система соціальної сфери;
- реабілітація.

Інформаційний сектор забезпечує надання послуг в:

- сфері телебачення та радіомовлення;
- інформаційній та видавничій сфері.

Сектор державної влади забезпечує виконання функцій держави.

Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на ОКІ встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на ОКІ здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

4.2 Система заходів кіберзахисту об'єктів критичної інфраструктури

Система заходів кіберзахисту базується на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом з технологіями забезпечення кібербезпеки. Це забезпечує ефективність реалізації заходів кіберзахисту та можливість підтримки нових технологій і методів забезпечення кібербезпеки. Систему заходів кіберзахисту не слід розглядати як вичерпний перелік заходів.

Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з наступних функцій кібербезпеки (рис. 4.1):

- ідентифікація ризиків;
- кіберзахист;
- виявлення кіберінцидентів;
- реагування;
- відновлення поточного стану кібербезпеки.

Функції кібербезпеки забезпечують:

- прийняття рішення з управління ризиками кібербезпеки на ОКІ;

– вибір та впровадження заходів кіберзахисту;
– реагування на загрози кібербезпеки;
– удосконалення кіберзахисту, враховуючи набутий досвід.

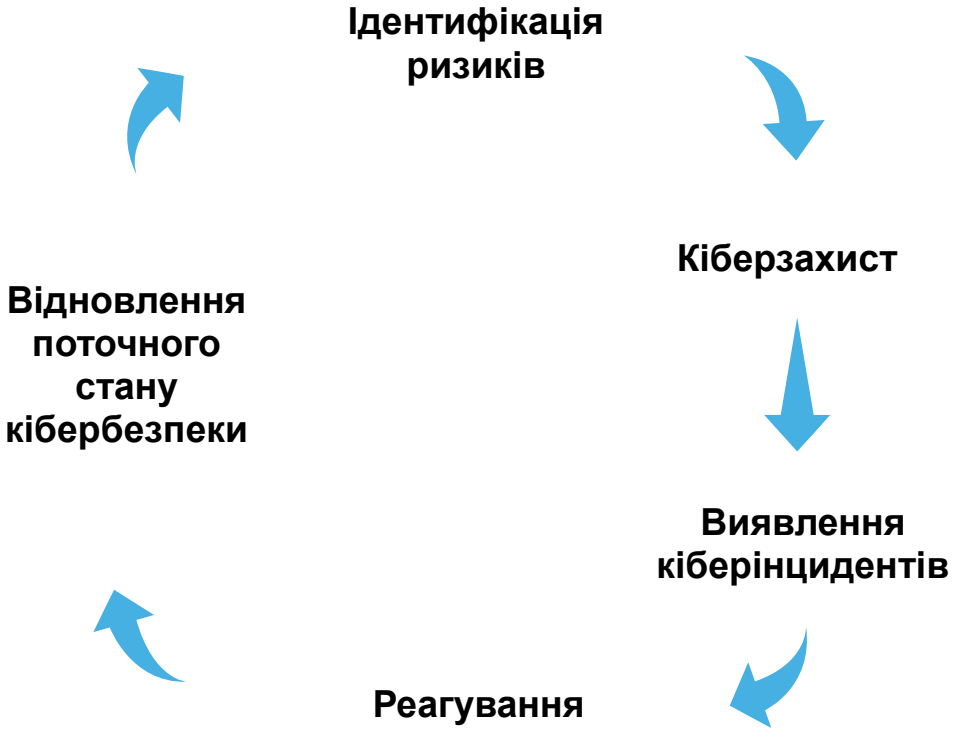

Рисунок 4.1 - Цикл управління кібербезпекою

Функції кібербезпеки узгоджуються з чинними підходами щодо управління ризиками кібербезпеки та допомагають продемонструвати ефективність інвестицій в кібербезпеку.

Таксономія заходів кіберзахисту складається з наступних елементів:

– клас заходів кіберзахисту;
– категорія заходів кіберзахисту;
– підкатегорія заходів кіберзахисту;
– інформаційні посилання.

4.3 Заходи кіберзахисту об’єктів критичної інфраструктури

Клас заходів кіберзахисту організовує заходи кіберзахисту на системному рівні та визначає зміст циклу управління кібербезпекою. Серед цього класу можна виділити наступні:

– ідентифікація ризиків;
– кіберзахист;
– виявлення кіберінцидентів;
– реагування на кіберінциденти;
– відновлення поточного стану кібербезпеки.

4.3.1 Ідентифікація ризиків кібербезпеки

Клас заходів кіберзахисту «Ідентифікація ризиків кібербезпеки» передбачає заходи, реалізація яких спрямована на поглиблення знань керівництва та персоналу ОКІІ щодо наявних ризиків, способів управління ризиками кібербезпеки для інформаційних систем, активів, даних, що використовуються для надання життєво важливих послуг та функцій. Реалізація заходів кіберзахисту класу «Ідентифікація ризиків» є чинником для ефективного використання Рекомендацій, розуміння умов, ресурсів, що підтримують надання життєво важливих послуг та функцій, а також пов'язаних ризиків кібербезпеки, обгрунтованого вибору конкретних заходів для впровадження. Це дозволяє визначити пріоритетність ризиків кібербезпеки потребами надання життєво важливих послуг та функцій, а також розподіляти ресурси і зусилля відповідно до встановлених пріоритетів.

Категорія заходів кіберзахисту являє собою складові елементи класу заходів кіберзахисту, упорядковані за групою цільових результатів забезпечення кібербезпеки та тісно пов'язані із завданнями забезпечення кібербезпеки та конкретними групами заходів кіберзахисту:

- управління активами;
- середовище надання життєво важливих послуг та функцій;
- управління безпекою;
- оцінка ризиків;
- стратегія управління ризиками організації;
- управління ризиками системи постачання.

У процесі управління ризиками системи постачання описуються дані, персонал, пристрої та носії інформації, інформаційні системи, що дозволяють забезпечити надання життєво важливих послуг та функцій до рівня важливості для організації відносно життєво важливих послуг та функцій, а також описується політика управління ризиками.

Середовище надання життєво важливих послуг та функцій забезпечує формування обов'язків персоналу щодо забезпечення кібербезпеки, а також рішень з управління ризиками у сфері кібербезпеки.

Управління безпекою забезпечує формування правил, процедур і процесів для управління й моніторингу впроваджених нормативних, екологічних та експлуатаційних вимог, а також вимог щодо забезпечення кібербезпеки.

Оцінка ризиків забезпечує визначення ризиків у сфері кібербезпеки для процесів надання життєво важливих послуг та функцій, а також активів організації.

Стратегія управління ризиками організації забезпечує визначення пріоритетів, обмежень, допустимого рівня ризику для підтримки рішень щодо зниження ризиків кібербезпеки.

Управління ризиками системи постачання забезпечує визначення пріоритетів, обмежень, допустимого рівня ризику щодо системи постачання для підтримки рішень щодо ризиків, пов’язаних із системою постачання послуг третіми особами.

4.3.2 Кіберзахист

Клас заходів кіберзахисту «Кіберзахист» визначає діяльність із розробки та впровадження відповідних методів, засобів, процедур кіберзахисту для забезпечення стійкого, безперервного та безпечного надання життєво важливих послуг та функцій ОКІ. Ці заходи дозволяють обмежити або стримати вплив кіберінцидентів. До цього класу відносяться:

– управління ідентифікацією, автентифікацією та контроль доступу;
– обізнаність та навчання;
– безпека даних;
– технічне обслуговування;
– процеси та процедури кіберзахисту;
– технології кіберзахисту.

Управління ідентифікацією, автентифікацією та контроль доступу припускає забезпечення доступу до фізичних і логічних ресурсів ОКІ та пов'язаних з ними об'єктів тільки для авторизованих користувачів, адміністраторів або процесів. Управління здійснюється з урахуванням встановленого допусти-мого рівня ризику несанкціонованого доступу.

Обізнаність та навчання забезпечують інформування та обізнаність організації та партнерів організації щодо питань кібербезпеки. Співробітники мають освіту або пройшли спеціалізовану підготовку для покращення інформованості з питань кібербезпеки, пройшли належну підготовку для виконання своїх обов'язків щодо забезпечення кібербезпеки відповідно до встановлених політик, правил, процедур та угод.

Безпека даних забезпечує управління інформацією та документацією, з метою захисту конфіденційності, цілісності та доступності інформації.

Технічне обслуговування гарантує як технічне обслуговування так і ремонт компонентів системи управління виробничими процесами, компонентів інформаційно-телекомунікаційних систем, який виконуються з дотриманням правил та процедур безпеки.

Процеси та процедури кіберзахисту забезпечує підтримання та управління політикою (правилами) безпеки, процесами та процедурами, які використовуються для управління захистом інформаційних систем і активів організації.

Технології кіберзахисту гарантує управління технічними рішеннями (технологіями) кіберзахисту з метою забезпечення безпеки та стійкості систем і активів організації з дотриманням правил, процедур з безпеки.

4.3.3 Виявлення кіберінцидентів

Клас заходів кіберзахисту «Виявлення кіберінцидентів» містить заходи своєчасного виявлення кіберінцидентів:

- аномалії та кіберінциденти;
- безперервний моніторинг кібербезпеки;
- процеси виявлення кіберінцидентів.

Аномалії та кіберінциденти забезпечує своєчасне виявлення аномальної активності та передбачення потенційного впливу кіберінцидентів.

Безперервний моніторинг кібербезпеки забезпечує відстеження безпеки інформаційних систем та активів організації через дискретні інтервали для виявлення кіберінцидентів та перевірки ефективності заходів кібербезпеки.

Процеси виявлення кіберінцидентів забезпечує підтримання і тестування процесів й процедур виявлення кіберінцидентів для забезпечення своєчасного та адекватного оповіщення про аномальні кіберінциденти.

4.3.4 Реагування на кіберінциденти

Клас заходів кіберзахисту «Реагування на кіберінцидентів» містить заходи реагування на кіберінциденти та кібератаки. Реалізація заходів спрямована на зниження потенційного негативного впливу кіберінциденту (кібератаки) на надання життєво важливих послуг та функцій. До цього класу відносяться:

- планування реагування ;
- комунікації
- аналіз
- мінімізація наслідків
- удосконалення

Планування реагування припускає, що процеси та процедури реагування на кіберінциденти виконуються та підтримуються з метою забезпечення своєчасного реагування на виявлені кіберінциденти.

Комунікації забезпечують координацію заходів з реагування між внутрішніми та зовнішніми партнерами організації (у разі доцільності).

Аналіз кіберінцидентів використовується для забезпечення адекватних заходів реагування та підтримки відновлення.

Мінімізація наслідків забезпечує виконання заходів з метою запобігання розширенню кіберінциденту, мінімізації його наслідків та унеможливлення його повторення.

Удосконалення заходів припускає реагування шляхом врахування досвіду з поточних або виконаних заходів виявлення/реагування.

4.3.5 Відновлення поточного стану кібербезпеки

Клас заходів кіберзахисту «Відновлення стану кібербезпеки» визначає діяльність щодо забезпечення спроможности ОКІІ щодо стійкого, надійного та безперервного надання життєво важливих послуг та функцій, які були порушені внаслідок кіберінциденту (кібератаки). Ці заходи забезпечують своєчасне відновлення штатної роботи ОКІІ та зменшення негативного впливу кіберінциденту (кібератаки). До цього класу відносяться:

- планування відновлення;
- удосконалення;
- комунікації.

Планування відновлення це використання процесів і процедур відновлення, які виконуються та підтримуються з метою своєчасного відновлення систем або активів, постраждалих від кіберінцидентів.

Удосконалення припускає планування відновлення та процеси відновлення удосконалюються шляхом урахування отриманого досвіду.

Комунікації забезпечують координацію заходів з відновлення з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, оператори, провайдери телекомунікацій, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою, та постачальники.

4.3.5 Відновлення поточного стану кібербезпеки

Інформаційне посилання являє собою елемент системи заходів кіберзахисту, який містить посилання на стандарти, нормативні документи, рекомендації та загальноприйняті практики, поширені у галузях (секторах) критичної інфраструктури для забезпечення безпеки ОКІІ. Ці посилання ілюструють методи, способи та технології досягнення цільових результатів (показників) для кожної підкатегорії заходів кіберзахисту. Інформаційні посилання, наведені в Рекомендаціях Держспецзв’язку, є довідковими та не є вичерпними.

Нормативні посилання базуються на національних стандартах, нормативних документах, прийнятих в Україні. Довідкові посилання базуються на міжнародних і регіональних стандартах, нормативних документах інших країн.

4.4 Рівні впровадження заходів з кіберзахисту

Рівні впровадження заходів кіберзахисту характеризують ступінь практичного впровадження організацією заходів із кіберзахисту, здатність організації досягти запланованих результатів кіберзахисту та надають інструментарій оцінювання ступеня впровадження процесів управління кібербезпекою.

Визначаються чотири рівні впровадження заходів кіберзахисту:

- рівень – частковий;
- рівень – ризик-орієнтований;
- рівень – повторюваний;
- рівень – адаптивний.

Під час вибору рівня впровадження, організації доцільно розглянути свою поточну практику управління ризиками, навколишнє середовище загроз, юридичні та нормативні вимоги, цілі бізнесу/місії та організаційні обмеження.

Частковий рівень. Практика кіберзахисту існує, але вона не є формалізованою, обмежене розуміння ризиків, власник ОКІ не розуміє місце та роль ОКІ у системі забезпечення кібербезпеки сектору інфраструктури.

Ризик-орієнтований рівень. Практика кіберзахисту впроваджується, але не є інституціональною, ризики кібербезпеки розуміються, але немає формалізованого процесу управління ризиками, оператор ОКІ взаємодіє з іншими об'єктами, але процеси взаємодії не є формалізованими.

Повторюваний рівень. Практика кіберзахисту інституціоналізована, впроваджено загально-організаційний підхід до управління ризиками кібербезпеки, взаємодія з іншими ОКІ формалізована та інституціоналізована.

Адаптивний рівень. Практика кіберзахисту адаптується на основі практичного досвіду та прогнозованих показників безпеки. Управління ризиками кібербезпеки є частиною організаційної культури та розвивається на основі усвідомлення попередньої діяльності з управління ризиками та постійної обізнаності про діяльність із забезпечення кібербезпеки. Взаємодія здійснюється на постійній основі, інформація про стан кібербезпеки використовується в реальному часі.

Процес вибору рівня впровадження враховує поточну практику щодо реалізації заходів кіберзахисту та управління ризиками кібербезпеки на ОКІІ, характеристики загроз кібербезпеки, законодавчі та нормативні вимоги, комерційні та стратегічні цілі ОКІ, вимоги до кібербезпеки в ланцюзі поставок програмного/апаратного забезпечення та організаційні обмеження, а також інші наявні обмеження.

Рекомендовано визначати цільовий рівень впровадження, переконавшись, що вибраний рівень зменшує ризик кібербезпеки до критично важливих активів і ресурсів, прийнятних для організації. Рекомендується враховувати вимоги галузевих (секторальних) нормативних актів, нормативно-правових актів у сфері кібербезпеки та захисту інформації, рекомендації урядової або секторальної/міжсекторальної команди реагування на комп’ютерні інциденти (CERT-UA/CERT)/інциденти комп’ютерної безпеки (CSIRT) або галузевих (секторальних) центрів управління безпекою (SOC), існуючі

моделі зрілості або інші джерела, які допоможуть визначити бажаний рівень ризику кібербезпеки.

ОКІІ, що досягли певного рівня впровадження, рекомендується розглянути можливість просування до наступного або більшого рівня. Рівні призначено для підтримки прийняття організаційних рішень про те, як керувати ризиком кібербезпеки, які заходи для ОКІІ мають вищий пріоритет та на які заходи можуть виділятися додаткові ресурси.

Успішність упровадження заходів з кіберзахисту базується на досягненні результатів, описаних у цільовому профілі організації, а не на визначеному рівні впровадження.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Adriaans P. Information [Електронний ресурс] / Pieter Adriaans // The stanford encyclopedia of philosophy / ред.: E. N. Zalta, U. Nodelman. – [Б. м.]. – URL: https://plato.stanford.edu/archives/sum2024/entries/ information/.

2. Alnatheer M. A. A conceptual model to understand information security culture [Електронний ресурс] / Mohammed A. Alnatheer // International journal of social science and humanity. – 2014. – Т. 4, № 2. – С. 104–107. – URL: https://doi.org/10.7763/ijssh.2014.v4.327 (дата звернення: 14.08.2025).

3. Analysis of cyber attacks using machine learning on the information security management systems / A. V. Habrylchuk [et al.] // Computer systems and network. – 2025. – Vol. 7, no. 1. – P. 68–78. – Mode of access: https://doi.org/10.23939/csn2025.01.068 (дата звернення: 14.08.2025).

4. An evaluation strategy of state security level from the risk of external cyber influence [Електронний ресурс]. В. Л/ Бурячок [та ін.] // Ukrainian information security research journal. – 2013. – Т. 15, № 1. – URL: https://doi.org/10.18372/2410-7840.15.4207 (дата звернення: 04.09.2025).

5. Conceptual model of information security [Електронний ресурс] / Vladimir Pevnev [та ін.] // Lecture notes in networks and systems. – Cham, 2021. – С. 158–168. – URL: https://doi.org/10.1007/978-3-030-66717-7_14 (дата звернення: 24.08.2025).

6. Goldenberg N. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems [Electronic resource] / Niv Goldenberg, Avishai Wool // International journal of critical infrastructure protection. – 2013. – Vol. 6, no. 2. – P. 63–75. – Mode of access: https://doi.org/10.1016/j.ijcip.2013.05.001 (дата звернення: 11.08.2025).

7. Handbook of metaphysics and ontology / ред.: H. Burkhardt [та ін.]. – [Б. м.] : Philosophia, 1991. – URL: https://doi.org/10.2307/j.ctv2x8v8nc.

8. Hjørland B. Information: objective or subjective/situational? [Електронний ресурс] / Birger Hjørland // Journal of the american society for information science and technology. – 2007. – Т. 58, № 10. – С. 1448–1456. – URL: https://doi.org/10.1002/asi.20620 (дата звернення: 16.07.2025).

9. Oleshchenko, V., & Pevnev, V. (2017). Development of digital steganography techniques for copyright protection, based on the watermark. *Advanced Information Systems*, *1*(1), 57–60. https://doi.org/10.20998/2522-9052.2017.1.10

10. Pevnev, V.; Frolov, A.; Tsuranov, M.; Zemlianko, H. Ensuring the Data Integrity in Infocommunication Systems. *IJC* **2022**, *21*, 228-233. https://doi.org/10.47839/ijc.21.2.2591

11. Pevnev, V., & Voikov, Y. (2020). RESEARCH AND PROTOTYPING METHODS OF STEGANOGRAPHY USING MOSAIC. *Advanced Information Systems*, *4*(2), 137–141. https://doi.org/10.20998/2522-9052.2020.2.20

12. V. Pevnev, S. Kapchynskyi. Database Security: Threats and Preventive Measures, AIS. 2(1) (2018) 69–72. https://doi.org/10.20998/2522-9052.2018.1.13

13. Verizon DBIR 2026: Vulnerability Exploitation Overtakes Credential Theft as Top Breach Vector URL:https://www.securityweek.com/verizon-dbir-2026-vulnerability-exploitation-overtakes-credential-theft-as-top-breach-vector/

14. Yudin, Oles & Kharchenko, Vyacheslav & Pevnev, Vladimir. (2023). Scanning of Web-Applications: Algorithms and Software for Search of Vulnerabilities “Code Injection” and “Insecure Design”. 1005-1010. https://doi.org/10.1109/IDAACS58523.2023.10348918.

15. X.805 : Security architecture for systems providing end-to-end communications [Електронний ресурс] // Connecting the world and beyond. – URL: https://www.itu.int/rec/T-REC-X.805-200310-I/en. (дата звернення: 18.07.2025).

16. Антонюк А. О. Теоретичні основи моделювання та аналізу систем захисту інформації / А. О. Антонюк, В. В. Жора. – [Б. м.] : Держ. податк. адмін. України, Нац. ун-т держ. податк. служби України, 2010.

17. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдин. – Київ : К-Прес, 2005. – 432 с.

18. Василенко В. Теорія інформації та кодування : монографія / В. Василенко, О. Я. Матов. – 300-те вид. – Київ : Ін-т проблем реєстрації інформації НАН України, 2014. – 439 с.

19. Горбенко І. Д., Горбенко Ю. І., Інфраструктура відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. Харків: Форт, 2010. 608 с.

20. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. – Чинний від 1997-01-01. – Вид. офіц. – Україна : Держ. служба спец. зв’язку та зах. інформації України, 1996. – 6 с.

21. ДСТУ 3396.2-97. Захист інформації. технічний захист інформації. терміни та визначення. – Чинний від 1998-01-01. – Вид. офіц. – Україна : Держ. служба спец. зв’язку та зах. інформації України, 1997. – 11 с.

22. ДСТУ EN ISO/IEC 27000:2022. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. – На заміну EN ISO/IEC 27000:2020; ДСТУ ISO/IEC 27000:2019; ISO/IEC 27000:2018 ; чинний від 2023-12-31. – Вид. офіц. – Україна : ДП «Укр. н.-д. і навч. центр проблем стандартизації, сертифікації та якості», 2022.

23. ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Базова модель. – На заміну ISO/IEC 7498-1:1994 ; чинний від 2006-01-01. – Вид. офіц. – Україна : Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20). – 67 с.

24. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1.

Концепції й моделі безпеки ІТ. – На заміну ISO/IEC TR 13335-1:1996 ; чинний від 2004-10-01. – Вид. офіц. – Україна : [б. в.], 2003.нформаційна безпека.

25. Дудикевич В. Б. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б.,Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.

26. Терміни і визначення : довідник / В. Я. Пєвнєв, Т. В. Лавровська ; М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харк. авіац. ін-т". - Харків. - Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харк. авіац. ін-т", 2016. - 84 с . - http://library.khai.edu/library/fulltexts/metod/

27. Жора В. В. Дослідження застосовності онтологічного підходу до побудови комплексних систем захисту інформації / В. В. Жора // Технологічний аудит і резерви виробництва. – 2016 - № 2/2(28). С. 21-24.

28. Інформаційна та кібербезпека: соціотехнічний аспект [Електронний ресурс] : підручник / В. Л. Бурячок [та ін.] ; ред. В. Б. Толубко. – К. : ДУТ, 2015. – 288 с. – URL: https://duikt.edu.ua/uploads /p_303_79299367.pdf.

29. Климчик О.О. Кримінально-правова кваліфікація використання комп’ютерних технологій для вчинення терористичних актів / О.О. Климчик, Р.М. Кравченко // Інформаційна безпека людини, суспільства, держави — №1 (3), 2010. — С. 26-30.

30. Конституція України [Електронний ресурс] : від 28.06.1996 № 254к/96- Р : станом на 1 січ. 2020 р. –
URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 14.08.2025).

31. Концепція інформаційної безпеки Основні концептуальні положення системи захисту інформації [Електронний ресурс] // StudFiles. – URL: https://studfile.net/preview/3904693 (дата звернення: 10.09.2025).

32. Кормич Б. Інформаційна безпека: організаційно-правові основи [Електронний ресурс]: навч. посіб. / Б. Кормич. – Київ: Кондор, 2004. – 384 с. –
URL: https://lib.univer.km.ua/sites/default/files/Право/Кормич% 20Б%20А%20 Інформаційна%20безпека%20організаційно%20правові%20основи.pdf.

33. Кушнір О. І., Тимочко О .І, Сєвєрінов О. В. Аналіз методів завадостійкого кодування у цифрових системах зв’язку**.** *Системи обробки інформації*. 2007. Вип. 9 (67). С. 63-65.

34. Методи та засоби захисту інформації: Конспект лекцій / Укладач В. І. Стаценко. Друге навч. вид. Дніпро :Репозиторій ФТФ ДНУ, 2022. – 132 с. URL: https://files.fti.dp.ua › uploads › tainacan-items.

35. НД ТЗІ 1.1-003-99 Термінологія в галузі захиту інформації в комп'ютерних системах від несанкціонованого доступу: НОРМ. ДОК. СИСТЕМИ ТЕХН. ЗАХ. ІНФОРМАЦІЇ від 28.04.1997 ДСТСЗІ СБУ від 28.04.99 № 22. – URL:доступу: https://tzi.ua/assets/files/1.1_003_99.pdf.

36. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс] : НОРМ. ДОК. СИСТЕМИ ТЕХН. ЗАХ. ІНФОРМАЦІЇ від 28.04.1999 № 22 (Зміна № 1 наказ № 806) : станом на 28 груд. 2012 р. – URL: https://tzi.com.ua/downloads/2.5-004-99.pdf.

37. НД ТЗІ 2.5-005-99, Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] : НОРМ. ДОК. СИСТЕМИ ТЕХН. ЗАХ. ІНФОРМАЦІЇ від 28.04.1999 № 22 (Зміна № 1 наказ № 172) : станом на 15 жовт. 2008 р. – URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf.

38. НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці: НОРМ. ДОК. СИСТЕМИ ТЕХН. ЗАХ. ІНФОРМАЦІЇ.

39. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс] : НОРМ. ДОК. СИСТЕМИ ТЕХН. ЗАХ. ІНФОРМАЦІЇ від 28.04.1999 № 22 (Зміна № 2 наказ № 806) : станом на 28 груд. 2012 р. – URL: https://tzi.com.ua/downloads/3.7-001-99.pdf.

40. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі : НОРМ. ДОК. СИСТЕМИ ТЕХН. ЗАХ. ІНФОРМАЦІЇ від 08.11.2005 № № 924 : станом на 28 жовт. 2023 р.

41. Остроухов В. В. Інформаційна безпека (соціально-правові аспекти) : підручник / В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк ; ред. Є. Д. Скулиш. – Київ : КНТ, 2010. – 776 с.

42. Пєвнєв В.Я. Моделі загроз і забезпечення цілісності інформації. Системи та технології, 2018, № 2. С. 79-94.

43. Політична енциклопедія [Електронний ресурс] / ред.: Ю. Левенець [та ін.]. – Київ : Парлам. вид-во, 2011. – 808 с. – URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/2011_Politychna_ entsyklopediia.pdf.

44. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу [Електронний ресурс] : Адмін. Держспецзв'язку від 30.08.2023 № № 773 (v0773519-23). – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0773519-23#Text.

45. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. – URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 14.09.2025).

46. Про захист персональних даних [Електронний ресурс] : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. – URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 14.09.2025).

47. Про інформацію [Електронний ресурс] : Закон України від 02.10.1992 № 2657- II : станом на 14 черв. 2025 р. – URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 14.09.2025).

48. Про критичну інфраструктуру [Електронний ресурс] : Закон України від 16.11.2021 № 1882- IX : станом на 21 верес. 2024 р. – URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 14.10.2025).

49. Про національну безпеку України [Електронний ресурс] : Закон України від 21.06.2018 № 2469- VIII : станом на 30 серп. 2025 р. – URL: https://zakon.rada.gov.ua/ laws/show/2469-19#Text (дата звернення: 14.09.2025).

50. Про Національну програму інформатизації [Електронний ресурс] : Закон України від 01.12.2022 № 2807-IX. – URL: https://zakon.rada.gov.ua/ laws/show/2807-20#Text (дата звернення: 14.09.2025).

51. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. – URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.09.2025).

52. Фурашев В.М., Сутність та визначення понять “інформаційна безпека” і “безпека інформації” | Інститут інформації, безпеки і права Національної академії правових наук України [Електронний ресурс] // Інститут інформації, безпеки і права Національної академії правових наук України. – URL: https://ippi.org.ua/furashev-vm-sutnist-ta-viznachennya-ponyat-“informatsiina-bezpeka”-i-“bezpeka-informatsii” (дата звернення: 14.08.2025).

53. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційної сфері: навчальний посібник / М.В.Цуранов, В.М.Струков, В.Я.Пєвнєв. –Х.: ХНУВС, 2015. – 256 с

54. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2012. - № 2. - С. 299-309. – URL: http://nbuv.gov.ua/UJRN/boz_2012_2_36.

Г. А. Землянко, В.Я. Пєвнєв
H. A. Zemlianko, V.Y. Pevnev

ОСНОВИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

FUNDAMENTALS OF INFORMATION AND CYBER SECURITY

Відповідальний за випуск Г. А. Землянко
Responsible for Publication: Heorhii Zemlianko

Видавець ФОП Бровін О.В.
Свідоцтво про внесення субєкта до Державного реєстру
видавців та виготовників видавничої продукції серія ДК 3587 від 23.09.09 р.
Формат 60x84/16. Ум. друк. арк. 7.21. Тир. 100 прим. Зам. 887.

Надруковано з макету замовника ФОП Бровіна І.П.
61022, м. Харків, вул. Трінклера, 2, корп.1, к.19. Т. (066) 822-71-30

СТИЛЬ-ІЗДАТ®
друкарня
www.stil-izdat.com