ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТУ ІМЕНІ С.П.КОРОЛЬОВА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

здобувача вищої освіти ступеня «бакалавр» заочної форми навчання
за спеціальністю «Кібербезпека»

Тема: «МЕТОДИКА ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ»

Виконавець: Олег ПОДЖИГАЙЛО

м. Житомир

2026

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох основних розділів, висновків, переліку джерел посилання, містить 84 сторінок основного тексту, 5 рисунків, 4 таблиці, використано 16 джерел. Загальний обсяг роботи складає 90 сторінок.

Об'єктом дослідження є методики захисту електронних документів від несанкціонованого доступу.

Предметом дослідження є процеси, методи та засоби забезпечення конфіденційності, цілісності й доступності електронних документів в інформаційних системах.

Метою кваліфікаційної роботи є розроблення та обґрунтування методики захисту електронних документів від несанкціонованого доступу шляхом дослідження сучасних загроз інформаційній безпеці, аналізу існуючих засобів і технологій захисту інформації, а також впровадження ефективних механізмів автентифікації, авторизації, шифрування та контролю доступу до електронних документів.

У роботі вирішено питання щодо вимог до методики захисту електронних документів, сформовано модель загроз і порушника для системи електронних документів, методику аналізу захисту електронних документів, а також надано оцінку ефективності захисту електронних документів розробленою методикою.

Розроблена методика може застосовуватися для захисту електронних документів в інформаційних системах органів військового управління та державних установ від несанкціонованого доступу і кібератак.

Ключові слова: ЕЛЕКТРОННІ ДОКУМЕНТИ, ТЕХНОЛОГІЇ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ, СИСТЕМА МОНІТОРИНГУ, КІБЕРБЕЗПЕКА, МЕТОДИ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ, НЕСАНКЦІОНОВАНИЙ ДОСТУП.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI	–	Штучний інтелект (Artificial Intelligence)
IT	–	Інформаційні технології
ІБ	–	Інформаційна безпека
ІС	–	Інформаційна система
КЕП	–	Кваліфікований електронний підпис (цифровий підпис)
МН	–	Машинне навчання
ММЕ	–	Міжмережевий екран (Firewall)
НСПД	–	Несанкціонований доступ
ПЗ	–	Програмне забезпечення
СМБ	–	Система моніторингу безпеки
СВВ	–	Система виявлення вторгнень
CSRF	–	Міжсайтова підробка запитів (Cross-Site Request Forgery)
DDoS	–	Розподілена атака типу «відмова в обслуговуванні» (Distributed Denial of Service)
DLP	–	Системи запобігання втраті даних або запобігання витокам даних (Data Loss Prevention/Data Leak Prevention)
DRM	–	Системи управління цифровими правами (Digital Rights Management)
IDS	–	Система виявлення вторгнень (Intrusion Detection System)
IPS	–	Система запобігання вторгненням (Intrusion Prevention System)
ML	–	Машинне навчання (Machine Learning)
MFA	–	Системи багатофакторної автентифікації (Multi-factor authentication)
SIEM	–	Система управління інформаційними подіями безпеки (Security Information and Event Management)
SQL	–	Мова структурованих запитів (Structured Query Language)

WAF	–	Міжмережевий екран веб-застосунків (Web Application Firewall)
XSS	–	Міжсайтовий скриптинг (Cross-Site Scripting)
API	–	Програмний інтерфейс застосунку (Application Programming Interface)
ACS	–	Системи контролю доступу (Access Control System)
AL	–	Системи журналювання подій (Audit Log)
HSM	–	Апаратні криптомодулі (Hardware Security Module)
HTTP	–	Протокол передачі гіпертексту (HyperText Transfer Protocol)
HTTPS	–	Захищений протокол передачі гіпертексту (HyperText Transfer Protocol Secure)
JSON	–	Формат обміну даними (JavaScript Object Notation)
REST	–	Архітектурний стиль (Representational State Transfer)

ВСТУП

Сучасний розвиток інформаційно-комунікаційних технологій суттєво змінив підходи до організації управлінської діяльності в органах державної влади, секторі безпеки і оборони та Збройних Силах України. Одним із результатів цифрової трансформації стало широке впровадження систем електронного документообігу, які забезпечують оперативність обробки інформації, прискорюють процес прийняття управлінських рішень та підвищують ефективність функціонування військових органів управління. Електронні документи сьогодні використовуються під час планування бойових дій, організації управління військами, логістичного забезпечення, кадрової роботи, ведення службового листування, підготовки наказів, директив та інших документів, що мають важливе значення для забезпечення обороноздатності держави.

Разом із перевагами цифровізації значно зростають ризики, пов’язані з несанкціонованим доступом до інформації. В умовах повномасштабної збройної агресії проти України інформаційний простір став одним із ключових театрів протиборства, де поряд із традиційними засобами ведення війни активно застосовуються кібернетичні атаки, інформаційно-психологічні операції та спеціальні технічні заходи впливу на інформаційні ресурси держави. Особливу небезпеку становлять спроби отримання несанкціонованого доступу до електронних документів військового призначення, що можуть містити відомості про організацію управління військами, дислокацію підрозділів, забезпечення озброєнням та військовою технікою, результати виконання бойових завдань, а також іншу службову інформацію.

Актуальність проблеми захисту електронних документів від несанкціонованого доступу обумовлюється необхідністю забезпечення належного рівня ІБ військових частин Збройних Сил України в умовах постійного зростання кількості та складності кіберзагроз. За останні роки значно збільшилася кількість атак на інформаційні системи державного сектору та об'єкти критичної інформаційної інфраструктури, в першу чергу, з метою

дестабілізації процесів управління.

Таким чином, кваліфікаційна робота, метою якої є розроблення методики захисту електронних документів від несанкціонованого доступу є сучасною, актуальною та становить науковий-практичний інтерес дослідження.

РОЗДІЛ 1. ПОНЯТТЯ ЕЛЕКТРОННОГО ДОКУМЕНТА ТА НЕОБХІДНІСТЬ РОЗРОБЛЕННЯ МЕТОДИКИ ЙОГО ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Стрімкий розвиток інформаційних технологій та широке впровадження комп'ютерних систем у діяльність організацій спричинили суттєві зміни у процесах створення, оброблення та зберігання інформації. Одним із важливих результатів цифрової трансформації суспільства стало формування систем електронного документообігу, у межах яких основна частина інформаційних ресурсів функціонує у вигляді електронних документів. У зв'язку з цим проблема забезпечення захисту таких документів від несанкціонованого доступу набуває особливої актуальності.

Використання електронних документів значно підвищує ефективність управління інформаційними потоками, прискорює процеси прийняття управлінських рішень та оптимізує взаємодію між різними структурними підрозділами організацій. Водночас цифрова форма представлення інформації створює нові ризики для її безпеки, оскільки електронні дані можуть бути відносно легко скопійовані, змінені або знищені у разі відсутності належного рівня захисту.

Законодавче визначення поняття електронного документа міститься у Законі України «Про електронні документи та електронний документообіг», відповідно до якого електронний документ — це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Такий документ може бути створений, переданий, збережений та перетворений за допомогою електронних засобів оброблення інформації.

Юридична сила електронного документа визначається наявністю обов'язкових реквізитів, зокрема електронного підпису, який забезпечує ідентифікацію автора документа та підтверджує його цілісність. Завдяки цьому електронні документи можуть використовуватися у діловодстві, фінансовій діяльності, державному управлінні та інших сферах суспільного життя.

Водночас функціонування електронного документообігу потребує

забезпечення належного рівня ІБ. Відповідно до положень Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», інформація, що обробляється в інформаційно-телекомунікаційних системах, повинна бути захищена від несанкціонованого доступу, модифікації, знищення, блокування або розповсюдження.

У науковій літературі електронний документ розглядається як один з основних об’єктів ІБ. Зокрема, у працях А.Ю. Щеглов та К.А. Щеглов зазначається, що інформаційні ресурси організацій, які існують у цифровій формі, потребують комплексного захисту, що охоплює організаційні, технічні та програмні заходи.

Основні властивості інформації в електронних документах

Згідно з фундаментальними положеннями теорії інформаційної безпеки, викладеними у працях С.В. Кавуна, захист інформації повинен забезпечувати три основні властивості: конфіденційність**,** цілісність та доступність інформації.

Конфіденційність означає забезпечення доступу до інформації лише для тих користувачів, які мають відповідні повноваження. У контексті електронних документів це передбачає використання механізмів аутентифікації, авторизації та контролю доступу.

Цілісність інформації характеризує ступінь її захищеності від несанкціонованих змін. Для електронних документів це особливо важливо, оскільки навіть незначна зміна даних може призвести до серйозних наслідків, зокрема фінансових втрат або юридичних суперечок.

Доступність інформації означає можливість отримання необхідних даних уповноваженими користувачами у потрібний момент часу. Порушення доступності може призвести до збоїв у роботі організації або втрати важливої інформації.

Класифікація електронних документів

У сучасних інформаційних системах електронні документи можуть бути класифіковані за різними ознаками.

За функціональним призначенням електронні документи поділяються

на:

- управлінські документи;
- фінансово-економічні документи;
- технічну документацію;
- службове листування.

За рівнем доступу документи можуть бути:

- відкритими;
- службовими;
- конфіденційними.

Крім того, електронні документи можуть відрізнятися за форматом зберігання, структурою та способом оброблення інформації.

Основні загрози електронним документам

Однією з найважливіших проблем інформаційної безпеки є протидія загрозам несанкціонованого доступу до інформації. У працях В.М. Зайцев та М.М. Зайцев зазначається, що ефективний захист ІС повинен базуватися на аналізі потенційних загроз та вразливостей.

Основними загрозами для електронних документів є:

- несанкціонований доступ до інформації;
- несанкціоноване копіювання документів;
- модифікація або підміна інформації;
- знищення або пошкодження даних;
- порушення автентичності документів.

Несанкціонований доступ може здійснюватися різними способами, зокрема шляхом використання вкрадених облікових даних, експлуатації вразливостей програмного забезпечення або застосування шкідливих програм, типові види загроз, рівні впливу та методи реалізації на електронний документ наведено в таблиці 1.1.

Таблиця 1.1 – Класифікація типів загроз, рівнів впливу та методи реалізації

№	Загроза	Класифікація за рівнем впливу	Метод реалізації	Порушувана властивість інформації	Рівень небезпеки	Частота виявлення
1	Несанкціоноване ознайомлення з документом	Конфіденційність	Викрадення облікових даних, обхід контролю доступу	Конфіденційність	Високий	Висока
2	Несанкціоноване копіювання документів	Конфіденційність	Використання зовнішніх носіїв, хмарних сервісів	Конфіденційність	Високий	Висока
3	Перехоплення даних під час передачі	Конфіденційність	Sniffing, MITM-атаки	Конфіденційність	Високий	Середня
4	Фішингові атаки	Комплексний вплив	Соціальна інженерія	Конфіденційність, цілісність	Високий	Дуже висока
5	Компрометація криптографічних ключів	Комплексний вплив	Викрадення ключової інформації	Конфіденційність, цілісність	Критичний	Середня
6	Підробка електронного підпису	Цілісність	Компрометація КЕП або криптографічних ключів	Цілісність, автентичність	Критичний	Низька
7	Несанкціоноване внесення змін до документів	Цілісність	Отримання прав редагування	Цілісність	Високий	Середня
8	Видалення електронних документів	Доступність	Навмисні дії порушника або шкідливе ПЗ	Доступність	Високий	Середня
9	Шифрування документів програмами-вимагачами	Доступність	Ransomware	Доступність	Критичний	Висока
10	SQL-ін'єкції	Комплексний вплив	Використання вразливостей вебсистем	Конфіденційність, цілісність	Високий	Середня
11	Підвищення привілеїв користувача	Комплексний вплив	Експлуатація помилок конфігурації	Конфіденційність, цілісність, доступність	Критичний	Середня
12	Використання шкідливого програмного забезпечення	Комплексний вплив	Віруси, трояни, шпигунські програми	Конфіденційність, цілісність, доступність	Критичний	Висока
13	Відмова обладнання	Доступність	Апаратні несправності	Доступність	Середній	Середня
14	Помилки персоналу	Комплексний вплив	Людський фактор	Конфіденційність, цілісність, доступність	Високий	Дуже висока

№	Загроза	Класифікація за рівнем впливу	Метод реалізації	Порушувана властивість інформації	Рівень небезпеки	Частота виявлення
15	Інсайдерські дії персоналу	Комплексний вплив	Перевищення повноважень	Конфіденційність, цілісність, доступність	Критичний	Середня
16	Атаки через хмарні сервіси	Конфіденційність	Компрометація облікових записів	Конфіденційність	Високий	Висока
17	Атаки на мобільні пристрої	Комплексний вплив	Втрата або зараження пристрою	Конфіденційність, цілісність	Середній	Висока
18	DoS/DDoS-атаки	Доступність	Перевантаження мережевих ресурсів	Доступність	Високий	Середня
19	Несанкціоноване використання облікових записів	Конфіденційність	Підбір паролів, компрометація акаунтів	Конфіденційність	Високий	Висока
20	Впровадження шкідливого коду в документи	Цілісність	Макровіруси, скрипти	Цілісність	Високий	Середня

Методи захисту електронних документів

Для забезпечення безпеки електронних документів використовуються різноманітні методи та засоби захисту інформації.

Одним із найбільш ефективних підходів є використання криптографічних методів. Як зазначають М.В. Захарова, Т.С. Піскунова та С.В. Шпара, криптографічний захист інформації передбачає використання спеціальних алгоритмів шифрування, які забезпечують конфіденційність даних та запобігають їх несанкціонованому розголошенню.

Крім шифрування, важливим елементом захисту електронних документів є застосування ЕЦП, який дозволяє перевірити справжність документа та підтвердити його авторство.

Ще одним важливим методом забезпечення інформаційної безпеки є розмежування доступу до інформаційних ресурсів, для чого використовуються системи контролю доступу (Access Control System). У межах цього підходу кожному користувачеві надаються лише ті права доступу, які необхідні для виконання його службових обов’язків.

Крім технічних засобів захисту, важливу роль відіграють організаційні заходи, до яких належать розроблення політики інформаційної безпеки, регламентація процедур роботи з електронними документами, навчання персоналу та контроль за дотриманням встановлених правил.

Необхідність розроблення методики захисту електронних документів

Незважаючи на існування різноманітних засобів захисту інформації, їх ефективність значною мірою залежить від правильності організації системи ІБ. Окремі технічні рішення не можуть забезпечити належний рівень захисту без їх системного поєднання.

Саме тому виникає необхідність розроблення комплексної методики захисту електронних документів від несанкціонованого доступу. Така методика повинна враховувати особливості функціонування ІС, характер оброблюваних даних та можливі загрози ІБ.

Методика захисту електронних документів повинна включати такі основні етапи:

- аналіз інформаційної системи та визначення об’єктів захисту;
- ідентифікацію потенційних загроз;
- оцінювання ризиків інформаційної безпеки;
- розроблення політики доступу до інформації;
- вибір технічних і криптографічних засобів захисту;
- організацію системи контролю та аудиту.

Застосування такої методики дозволяє створити комплексну систему захисту інформації, яка забезпечує конфіденційність, цілісність та доступність електронних документів.

Отже, електронні документи є невід’ємною складовою сучасних інформаційних систем та відіграють важливу роль у забезпеченні ефективного функціонування організацій. Водночас цифрова форма представлення інформації створює додаткові ризики для її безпеки, що потребує застосування комплексних заходів захисту.

Зростання обсягів електронного документообігу, підвищення ролі ІТ у

діяльності організацій та збільшення кількості кіберзагроз обумовлюють необхідність розроблення ефективної методики захисту електронних документів від НСПД. Така методика повинна базуватися на сучасних наукових підходах до забезпечення ІБ та враховувати вимоги чинного законодавства України.

1.1. Роль і місце захисту електронних документів від несанкціонованого доступу у забезпеченні обороноздатності держави

У сучасних умовах розвитку інформаційного суспільства та активного впровадження інформаційно-комунікаційних технологій у всі сфери діяльності держави особливого значення набуває проблема забезпечення інформаційної безпеки. Одним із ключових аспектів цієї проблеми є захист електронних документів від несанкціонованого доступу, оскільки значна частина інформації, що використовується органами державної влади, оборонними структурами та військовими формуваннями, зберігається та обробляється саме у цифровому вигляді. Забезпечення надійного захисту таких документів є важливою умовою підтримання належного рівня обороноздатності держави.

У сучасних умовах обороноздатність держави значною мірою залежить не лише від наявності матеріально-технічних ресурсів або чисельності військових сил, але й від здатності ефективно управляти інформаційними потоками. Інформація стала одним із найважливіших стратегічних ресурсів, а її захист — невід’ємною складовою національної безпеки. У цьому контексті електронні документи, що містять службову, технічну, організаційну або стратегічну інформацію, виступають важливими об’єктами захисту.

Відповідно до положень Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», інформація, яка обробляється в інформаційно-телекомунікаційних системах, повинна бути захищена від НСПД, знищення, модифікації або блокування. Це положення має особливе значення для ІС, що використовуються у сфері оборони та безпеки держави.

Крім того, відповідно до Закону України «Про електронні документи та електронний документообіг», електронні документи визнаються повноцінними документами, що мають юридичну силу за умови наявності відповідних реквізитів. Це означає, що значна частина управлінських рішень, організаційних розпоряджень та службових повідомлень у державних структурах може існувати саме у вигляді електронних документів.

Інформація як стратегічний ресурс оборонної сфери

У сучасних умовах інформація розглядається як один із ключових ресурсів держави, поряд із економічними, природними та військовими ресурсами. Як зазначають А.Ю. Щеглов та К.А. Щеглов, ефективне функціонування державних ІС потребує забезпечення надійного захисту інформаційних ресурсів від зовнішніх і внутрішніх загроз.

У сфері оборони інформація відіграє особливо важливу роль, оскільки вона використовується для:

- планування військових операцій;
- управління військовими підрозділами;
- координації дій між різними силовими структурами;
- аналізу розвідувальної інформації;
- прийняття стратегічних рішень у сфері національної безпеки.

Значна частина такої інформації фіксується у вигляді електронних документів, що зберігаються та обробляються в ІС державних органів та військових структур. У разі НСПД до таких документів можуть виникнути серйозні загрози для національної безпеки.

Загрози несанкціонованого доступу до електронних документів у сфері оборони

Однією з основних проблем забезпечення ІБ є протидія НСПД до інформаційних ресурсів. Як зазначає С.В. Кавун, несанкціонований доступ до інформації може призвести до витоку конфіденційних даних, порушення цілісності інформації або її повного знищення.

У сфері оборони несанкціонований доступ до електронних документів

може мати такі наслідки:

- розголошення державної або військової таємниці;
- отримання противником інформації про військові операції;
- підміна або фальсифікація важливих управлінських документів;
- дезорганізація управління військовими структурами;
- порушення функціонування інформаційних систем оборонного призначення.

У працях В.М. Зайцев та М.М. Зайцев підкреслюється, що сучасні інформаційні системи є складними технічними комплексами, які можуть містити значну кількість вразливостей. Саме тому ефективний захист інформації повинен базуватися на системному підході, що передбачає використання різних механізмів захисту.

Значення криптографічних методів у захисті електронних документів

Важливу роль у забезпеченні безпеки електронних документів відіграють криптографічні методи захисту інформації. Як зазначають М.В. Захарова, Т.С. Піскунова та С.В. Шпара, використання криптографічних алгоритмів дозволяє забезпечити конфіденційність, цілісність та автентичність інформації.

У системах електронного документообігу криптографічний захист може реалізовуватися за допомогою таких засобів:

- шифрування електронних документів;
- використання електронного цифрового підпису;
- застосування хеш-функцій для контролю цілісності даних;
- захист каналів передачі інформації.

Застосування криптографічних методів дозволяє значно знизити ризик НСПД до інформації навіть у разі перехоплення електронних даних.

Організаційні та технічні заходи захисту інформації

Крім криптографічних методів, важливу роль у забезпеченні захисту електронних документів відіграють організаційні та технічні заходи. До таких заходів належать:

- розроблення політики інформаційної безпеки;

- впровадження систем контролю доступу;
- використання засобів аутентифікації користувачів;
- проведення аудиту інформаційної безпеки;
- навчання персоналу правилам роботи з інформацією.

Згідно з науковими підходами, описаними у працях А.Ю. Щеглов та С.В. Кавун, ефективний захист інформації можливий лише за умови поєднання організаційних, програмних і технічних заходів.

Роль захисту електронних документів у забезпеченні обороноздатності держави

Захист електронних документів від НСПД є важливим елементом системи ІБ держави. Його значення у забезпеченні обороноздатності полягає у таких аспектах:

1. **Забезпечення конфіденційності стратегічної інформації.** Захист електронних документів дозволяє запобігти витоку інформації, що може бути використана противником для отримання переваги.

2. **Підтримання цілісності управлінських рішень.** Захист від несанкціонованої модифікації документів гарантує достовірність управлінської інформації.

3. **Забезпечення безперервності управління військовими структурами.** Надійний захист ІС дозволяє уникнути порушення процесів управління у критичних ситуаціях.

4. **Підвищення стійкості інформаційної інфраструктури держави.** Захист електронних документів сприяє зміцненню кіберстійкості державних інформаційних систем.

Таким чином, захист електронних документів є важливою складовою системи забезпечення обороноздатності держави. Він сприяє збереженню стратегічної інформації, забезпечує стабільне функціонування ІС та підвищує рівень національної безпеки.

У сучасних умовах інформація стає одним із ключових ресурсів держави, а її захист — важливим елементом системи національної безпеки. Електронні

документи, що використовуються у державному управлінні та оборонній сфері, містять значний обсяг важливої інформації, тому потребують надійного захисту від НСПД.

Таким чином, основні криптографічні методи захисту електронних документів від несанкціонованого доступу відображені на рис. 1.1.

Рис.1.1 – Основні криптографічні методи захисту електронних документів

1.2. Аналіз сучасних загроз несанкціонованому доступу

У сучасних умовах розвитку інформаційних технологій та широкого використання інформаційно-комунікаційних систем проблема забезпечення захисту інформації від несанкціонованого доступу набуває особливої

актуальності. Зростання обсягів електронної інформації, поширення мережевих технологій та інтеграція ІС різного призначення створюють нові можливості для ефективного обміну даними, але водночас значно збільшують кількість потенційних загроз ІБ.

Несанкціонований доступ до інформації може призвести до серйозних негативних наслідків, серед яких витік конфіденційних даних, порушення цілісності інформаційних ресурсів, знищення або модифікація важливих даних, а також дестабілізація функціонування ІС. У зв'язку з цим аналіз сучасних загроз НСПД є важливим етапом розроблення ефективних систем захисту інформації.

Відповідно до положень Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», інформація, що обробляється в інформаційно-телекомунікаційних системах, повинна бути захищена від несанкціонованого доступу, модифікації, знищення або блокування. Для виконання цих вимог необхідно враховувати можливі загрози інформаційній безпеці та розробляти відповідні механізми їх нейтралізації.

Сучасні загрози несанкціонованого доступу до електронних документів можна структурувати у формі таблиці, яку наведено нижче в таблиці 1.2.

Таблиця 1.2 – Аналіз сучасних загроз несанкціонованого доступу до електронних документів

Загроза	**Джерело загрози**	**Спосіб реалізації**	**Порушувана властивість інформації**	**Можливі наслідки**	**Рівень небезпеки**
Несанкціонований доступ до облікових записів	Зовнішній або внутрішній порушник	Викрадення паролів, підбір паролів, компрометація облікових даних	Конфіденційність	Витік службової або конфіденційної інформації	Високий
Фішингові атаки	Зовнішній порушник	Підроблені електронні листи, вебресурси, повідомлення	Конфіденційність, цілісність	Викрадення облікових даних, зараження системи	Високий
Шкідливе програмне	Зовнішній порушник	Встановлення вірусів, троянів,	Конфіденційність, цілісність,	Знищення, викрадення або	Критичний

Загроза	Джерело загрози	Спосіб реалізації	Порушувана властивість інформації	Можливі наслідки	Рівень небезпеки
забезпечення (Malware)		шпигунського ПЗ	доступність	модифікація документів	
Програми-вимагачі (Ransomware)	Кіберзлочинці	Шифрування інформації з подальшим вимаганням викупу	Доступність	Блокування роботи систем документообігу	Критичний
Інсайдерські загрози	Працівники або користувачі системи	Перевищення службових повноважень	Конфіденційність, цілісність	Несанкціоноване копіювання або зміна документів	Критичний
Соціальна інженерія	Зовнішній або внутрішній порушник	Маніпуляція персоналом	Конфіденційність	Отримання доступу до захищеної інформації	Високий
Перехоплення мережевого трафіку (Sniffing)	Зовнішній порушник	Аналіз мережевого трафіку	Конфіденційність	Отримання змісту документів під час передачі	Високий
Атака типу «Людина посередині» (MITM)	Зовнішній порушник	Підміна каналу зв'язку між користувачами	Конфіденційність, цілісність	Перехоплення або підміна документів	Високий
Несанкціоноване копіювання даних	Внутрішній порушник	Використання зовнішніх носіїв або хмарних сервісів	Конфіденційність	Витік інформації	Високий
Підвищення привілеїв (Privilege Escalation)	Внутрішній або зовнішній порушник	Використання помилок налаштування системи	Конфіденційність, цілісність	Отримання адміністративного доступу	Критичний
Експлуатація вразливостей програмного забезпечення	Зовнішній порушник	Використання помилок програмного коду	Конфіденційність, цілісність, доступність	Компрометація системи документообігу	Критичний
SQL-ін'єкції	Зовнішній порушник	Впровадження шкідливих SQL-запитів	Конфіденційність, цілісність	Отримання або зміна даних бази документів	Високий
DoS/DDoS-атаки	Зовнішній	Перевантаження	Доступність	Відмова в	Високий

Загроза	Джерело загрози	Спосіб реалізації	Порушувана властивість інформації	Можливі наслідки	Рівень небезпеки
	порушник	серверів запитами		обслуговуванні користувачів	
Компрометація криптографічних ключів	Зовнішній або внутрішній порушник	Викрадення ключової інформації	Конфіденційність, цілісність	Порушення достовірності документів	Критичний
Використання незахищених мобільних пристроїв	Користувачі системи	Втрата або компрометація пристрою	Конфіденційність	Несанкціонований доступ до документів	Середній
Помилки конфігурації системи	Адміністратори або персонал	Некоректне налаштування безпеки	Конфіденційність, цілісність, доступність	Формування додаткових вразливостей	Високий
Атаки через хмарні сервіси	Зовнішній порушник	Компрометація облікових записів або сервісів	Конфіденційність	Витік документів із хмарних сховищ	Високий
Атаки на електронний підпис	Зовнішній або внутрішній порушник	Викрадення особистих ключів підпису	Цілісність, автентичність	Підробка електронних документів	Критичний
Відмова обладнання	Технічний фактор	Апаратні несправності	Доступність	Втрата або пошкодження документів	Середній
Людський фактор	Користувачі системи	Необережність, помилки, порушення регламентів	Конфіденційність, цілісність, доступність	Втрата інформації або її компрометація	Високий

Поняття та сутність загроз несанкціонованого доступу

У науковій літературі загроза інформаційній безпеці визначається як потенційна можливість реалізації дій, спрямованих на порушення конфіденційності, цілісності або доступності інформації. Як зазначають А.Ю. Щеглов та К.А. Щеглов, загрози інформаційній безпеці можуть виникати внаслідок навмисних або випадкових дій користувачів, технічних збоїв або впливу зовнішніх факторів.

Несанкціонований доступ до інформації означає отримання можливості ознайомлення, використання або модифікації інформаційних ресурсів особами, які не мають відповідних прав доступу. Такий доступ може здійснюватися як шляхом безпосереднього втручання у роботу інформаційної системи, так і через використання різноманітних технічних або програмних засобів.

Згідно з дослідженнями С.В. Кавун, несанкціонований доступ є однією з найбільш поширених загроз інформаційній безпеці, оскільки більшість сучасних інформаційних систем підключені до глобальних мереж, що значно розширює можливості для здійснення кіберзлочинів.

Класифікація сучасних загроз несанкціонованого доступу

Для ефективного аналізу загроз інформаційній безпеці необхідно здійснювати їх класифікацію за різними ознаками. У працях В.М. Зайцев та М.М. Зайцев зазначається, що загрози несанкціонованого доступу можна класифікувати за джерелом виникнення, способом реалізації та характером впливу на інформаційну систему.

Загрози за джерелом виникнення можуть бути внутрішніми або зовнішніми.

Внутрішні загрози пов’язані з діяльністю користувачів інформаційної системи, які мають певний рівень доступу до інформаційних ресурсів. До таких загроз належать:

- навмисне розголошення конфіденційної інформації;
- несанкціоноване копіювання електронних документів;
- використання службових повноважень у власних інтересах;
- порушення встановлених правил роботи з інформацією.

Зовнішні загрози виникають унаслідок дій сторонніх осіб або організацій, які намагаються отримати доступ до інформаційної системи без відповідних повноважень. До таких загроз належать:

- хакерські атаки;
- перехоплення інформації у мережі;
- використання шкідливого програмного забезпечення.

Програмно-технічні загрози

Сучасні інформаційні системи функціонують на основі складного програмного забезпечення та технічної інфраструктури, що створює додаткові можливості для реалізації загроз інформаційній безпеці.

До основних програмно-технічних загроз належать:

- використання вразливостей програмного забезпечення;
- несанкціоноване підключення до інформаційних мереж;
- перехоплення мережевого трафіку;
- використання шкідливих програм.

Шкідливе програмне забезпечення може використовуватися для отримання несанкціонованого доступу до інформаційних ресурсів, викрадення конфіденційних даних або порушення роботи інформаційних систем.

Соціальна інженерія як сучасна загроза

Однією з найпоширеніших сучасних загроз інформаційній безпеці є використання методів соціальної інженерії. Суть таких методів полягає у маніпулюванні людьми з метою отримання конфіденційної інформації або доступу до інформаційних систем.

Прикладами таких атак є:

- фішинг;
- телефонне шахрайство;
- використання підроблених електронних повідомлень;
- отримання паролів шляхом психологічного впливу на користувачів.

Як показує досвід, людський фактор часто є найслабкішою ланкою у системі інформаційної безпеки, оскільки навіть найсучасніші технічні засоби захисту можуть бути обійдені шляхом маніпулювання користувачами.

Загрози мережевої безпеки

Розвиток мережевих технологій значно розширив можливості для обміну інформацією, але водночас створив нові ризики для інформаційної безпеки.

До основних мережевих загроз належать:

- атаки типу «відмова в обслуговуванні» (DoS);

- перехоплення мережевого трафіку;
- підміна мережевих адрес;
- несанкціоноване підключення до бездротових мереж.

Такі загрози можуть призводити до порушення роботи інформаційних систем або отримання доступу до конфіденційних даних.

Криптографічні загрози

Особливу увагу у сучасних інформаційних системах приділяють криптографічному захисту інформації. Проте навіть криптографічні системи можуть бути об’єктом атак.

Криптографічні загрози можуть включати:

- підбір криптографічних ключів;
- використання слабких алгоритмів шифрування;
- компрометацію ключової інформації;
- атаки на протоколи криптографічного захисту.

У разі успішної реалізації таких атак може бути порушена конфіденційність або цілісність електронних документів.

Людський фактор у забезпеченні інформаційної безпеки

Важливою складовою аналізу загроз інформаційній безпеці є врахування людського фактору. Багато інцидентів безпеки виникають через помилки користувачів, недотримання правил роботи з інформацією або недостатній рівень підготовки персоналу.

До основних проявів людського фактору належать:

- використання слабких паролів;
- передавання облікових даних іншим особам;
- недотримання правил інформаційної безпеки;
- випадкове видалення або пошкодження інформації.

Тому одним із важливих елементів системи захисту інформації є навчання персоналу та формування культури інформаційної безпеки.

Значення аналізу загроз для побудови системи захисту інформації

Аналіз сучасних загроз несанкціонованого доступу є необхідним етапом

побудови ефективної системи захисту інформації. Як зазначають В.М. Зайцев та М.М. Зайцев, розроблення системи захисту повинно базуватися на комплексному підході, що враховує всі можливі джерела загроз.

Результати аналізу загроз використовуються для:

- визначення критичних об’єктів захисту;
- оцінювання ризиків інформаційної безпеки;
- вибору засобів технічного та криптографічного захисту;
- розроблення політики інформаційної безпеки.

Таким чином, систематичний аналіз загроз дозволяє підвищити ефективність системи захисту інформації та зменшити ризик несанкціонованого доступу до електронних документів.

Сучасні інформаційні системи функціонують у складному середовищі, що характеризується значною кількістю потенційних загроз інформаційній безпеці. Несанкціонований доступ до інформації може здійснюватися різними способами, включаючи використання програмно-технічних вразливостей, мережевих атак, методів соціальної інженерії та людського фактору.

Аналіз сучасних загроз несанкціонованого доступу є важливим етапом забезпечення інформаційної безпеки, оскільки дозволяє виявити потенційні ризики та розробити ефективні механізми їх нейтралізації. Комплексний підхід до аналізу загроз сприяє підвищенню надійності інформаційних систем та забезпеченню належного рівня захисту електронних документів.

На підставі досліджень у галузі захисту систем електронного документообігу від несанкціонованого доступу, сучасні загрози інформаційній безпеці мають комплексний характер та реалізуються одночасно через технічні, програмні та організаційні вразливості.

Найбільшу небезпеку для систем електронного документообігу становлять події, які можна відобразити у формі рейтингу, зображеного в таблиці 1.3.

Таблиця 1.3 – Рейтинг актуальних загроз для захисту систем електронного документообігу від несанкціонованого доступу у Збройних Силах України

Місце	Загроза	Рівень критичності
1	Компрометація криптографічних ключів	Критичний
2	Інсайдерські загрози	Критичний
3	Програми-вимагачі (Ransomware)	Критичний
4	Атаки на електронний підпис	Критичний
5	Підвищення привілеїв користувачів	Критичний
6	Експлуатація вразливостей ПЗ	Критичний
7	Фішингові атаки	Високий
8	Перехоплення мережевого трафіку	Високий
9	Несанкціоноване копіювання документів	Високий
10	Людський фактор	Високий

1.3. Проблеми забезпечення конфіденційності, цілісності та доступності електронних документів

Відповідно до положень Закона України «Про захист інформації в інформаційно-телекомунікаційних системах», інформація, що обробляється в інформаційних системах, повинна бути захищена від несанкціонованого доступу, знищення, модифікації або блокування. Це положення безпосередньо пов’язане з необхідністю забезпечення основних властивостей інформації — конфіденційності, цілісності та доступності.

У науковій літературі зазначені властивості інформації розглядаються як фундаментальна основа побудови систем захисту інформації. Зокрема, у працях сучасних науковців підкреслюється, що ефективний захист інформаційних ресурсів можливий лише за умови комплексного забезпечення всіх трьох складових інформаційної безпеки.

Проблеми забезпечення конфіденційності електронних документів

Конфіденційність інформації означає обмеження доступу до інформаційних ресурсів лише для уповноважених користувачів. У контексті електронних документів це передбачає захист інформації від несанкціонованого ознайомлення, копіювання або розповсюдження.

Однією з основних проблем забезпечення конфіденційності електронних документів є зростання кількості інформаційних систем, що використовують мережеві технології для передачі даних. Використання глобальних комп'ютерних мереж значно підвищує ризик перехоплення інформації під час її передачі між користувачами.

Сучасні інформаційні системи часто функціонують у відкритому інформаційному середовищі, що створює додаткові можливості для здійснення несанкціонованого доступу до конфіденційної інформації. До основних загроз конфіденційності електронних документів належать:

- перехоплення даних у мережі;
- несанкціоноване копіювання інформації;
- використання викрадених облікових даних;
- витік інформації через внутрішніх користувачів.

Ще однією важливою проблемою є недостатній рівень захищеності каналів передачі інформації. У разі відсутності належного криптографічного захисту електронні документи можуть бути перехоплені та прочитані сторонніми особами.

З метою забезпечення конфіденційності електронних документів широко використовуються криптографічні методи захисту інформації. Застосування сучасних алгоритмів шифрування дозволяє забезпечити надійний захист інформації навіть у разі її перехоплення.

Проте навіть використання криптографічних засобів не гарантує абсолютної безпеки інформації. У випадку компрометації криптографічних ключів або використання застарілих алгоритмів шифрування конфіденційність електронних документів може бути порушена.

Проблеми забезпечення цілісності електронних документів

Цілісність інформації означає збереження її первинного змісту та структури без несанкціонованих змін. Для електронних документів забезпечення цілісності є надзвичайно важливим, оскільки будь-яка зміна інформації може призвести до спотворення змісту документа або прийняття неправильних управлінських рішень.

У сучасних інформаційних системах існує значна кількість загроз цілісності електронних документів. До основних з них належать:

- несанкціонована модифікація даних;
- підміна електронних документів;
- пошкодження інформації внаслідок програмних або технічних збоїв;
- навмисне фальсифікування документів.

Проблема забезпечення цілісності інформації у сучасних інформаційних системах ускладнюється через складність програмного забезпечення та велику кількість користувачів, які мають доступ до інформаційних ресурсів.

Особливої актуальності проблема забезпечення цілісності набуває у системах електронного документообігу, де електронні документи можуть багаторазово редагуватися, передаватися між користувачами та зберігатися у різних інформаційних системах.

Для забезпечення цілісності електронних документів широко використовуються криптографічні механізми, зокрема електронний цифровий підпис та хеш-функції. Використання таких механізмів дозволяє виявляти будь-які зміни, внесені до електронного документа після його створення.

Проте навіть за наявності технічних засобів захисту проблема забезпечення цілісності інформації може виникати через людський фактор або недотримання встановлених процедур роботи з електронними документами.

Проблеми забезпечення доступності електронних документів

Доступність інформації означає можливість отримання необхідних даних уповноваженими користувачами у потрібний момент часу. У системах електронного документообігу доступність інформації має важливе значення для

забезпечення безперервності управлінських процесів.

Однією з основних проблем забезпечення доступності електронних документів є можливість виникнення технічних збоїв або відмов у роботі інформаційних систем. Такі збої можуть бути спричинені:

- несправністю апаратного забезпечення;
- помилками програмного забезпечення;
- перевантаженням інформаційних систем;
- зовнішніми кібератаками.

Особливо небезпечними є атаки типу відмови в обслуговуванні, які можуть призводити до блокування доступу користувачів до інформаційних ресурсів.

Крім того, проблеми доступності можуть виникати через неправильну організацію процесів зберігання інформації або відсутність резервного копіювання електронних документів.

Забезпечення доступності інформації є не менш важливим, ніж забезпечення її конфіденційності та цілісності, оскільки відсутність доступу до необхідних даних може призвести до порушення функціонування організації.

Комплексний підхід до забезпечення інформаційної безпеки електронних документів

Аналіз проблем забезпечення конфіденційності, цілісності та доступності електронних документів свідчить про те, що ефективний захист інформації неможливий без застосування комплексного підходу до забезпечення інформаційної безпеки (рис. 1.2).

Рис. 1.2 – Комплексний підхід до забезпечення інформаційної безпеки електронних документів

Такий підхід передбачає поєднання:

- організаційних заходів;
- технічних засобів захисту;
- програмних механізмів контролю доступу;
- криптографічних методів захисту інформації.

Лише комплексне застосування різних механізмів захисту дозволяє створити ефективну систему інформаційної безпеки, здатну протидіяти сучасним загрозам.

Крім того, важливим елементом забезпечення безпеки електронних документів є формування культури інформаційної безпеки серед користувачів інформаційних систем, що передбачає навчання персоналу та контроль за дотриманням встановлених правил роботи з інформацією.

1.4. Нормативно-правове забезпечення захисту інформації в Україні

Нормативно-правове забезпечення захисту інформації в Україні являє собою сукупність законодавчих та підзаконних актів, що регулюють правові, організаційні та технічні аспекти забезпечення безпеки інформації. Основною метою такого регулювання є створення умов для захисту інформаційних ресурсів від несанкціонованого доступу, знищення, модифікації або розповсюдження.

Законодавчі основи захисту інформації в Україні

Базовим нормативним актом у сфері захисту інформації є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який визначає правові та організаційні засади забезпечення захисту інформації в інформаційних системах. Відповідно до цього закону, захист інформації — це комплекс правових, організаційних та технічних заходів, спрямованих на запобігання несанкціонованому доступу до інформації, її знищенню, модифікації або блокуванню.

Закон встановлює основні вимоги до організації захисту інформації в інформаційно-телекомунікаційних системах, визначає права та обов’язки суб’єктів інформаційних відносин, а також регламентує порядок створення та функціонування систем технічного захисту інформації.

Важливим нормативним актом у сфері електронного документообігу є Закон України «Про електронні документи та електронний документообіг». Цей закон визначає правові засади створення, передавання, зберігання та використання електронних документів, а також встановлює їх юридичний статус.

Згідно з положеннями цього закону, електронний документ є документом, інформація в якому зафіксована у вигляді електронних даних та містить обов’язкові реквізити. Для підтвердження автентичності електронного документа використовується електронний підпис, який забезпечує ідентифікацію автора документа та гарантує цілісність інформації.

Нормативно-правова база у сфері захисту інформації також включає інші

законодавчі акти, які регулюють різні аспекти інформаційної безпеки, зокрема захист персональних даних, державної таємниці та інформації з обмеженим доступом.

Наукові підходи до нормативного забезпечення захисту інформації

У науковій літературі питання нормативно-правового забезпечення інформаційної безпеки розглядається як важлива складова побудови ефективної системи захисту інформації.

Система захисту інформації повинна базуватися не лише на технічних засобах безпеки, але й на чітко визначених правових нормах, які регламентують порядок використання інформаційних ресурсів.

Нормативно-правове забезпечення інформаційної безпеки виконує кілька важливих функцій, серед яких:

- визначення правових основ захисту інформації;
- встановлення вимог до організації систем захисту інформації;
- регламентація відповідальності за порушення інформаційної безпеки;
- створення умов для ефективного функціонування інформаційних систем.

Таким чином, законодавче регулювання є важливим елементом формування системи інформаційної безпеки держави.

Система нормативних актів у сфері технічного захисту інформації

Окрім законів, важливу роль у регулюванні питань захисту інформації відіграють підзаконні нормативні акти, які визначають конкретні вимоги до організації технічного захисту інформації.

Ефективна система захисту інформації повинна ґрунтуватися на комплексному підході, який передбачає поєднання правових, організаційних та технічних заходів.

До основних елементів нормативного забезпечення технічного захисту інформації належать:

- державні стандарти у сфері інформаційної безпеки;

- нормативні документи з технічного захисту інформації;
- методичні рекомендації щодо створення систем захисту інформації;
- вимоги до сертифікації засобів захисту інформації.

Такі документи визначають порядок створення комплексних систем захисту інформації, правила оброблення інформації з обмеженим доступом, а також вимоги до програмно-технічних засобів захисту.

Важливою складовою системи захисту інформації є криптографічний захист, який передбачає використання спеціальних алгоритмів для забезпечення конфіденційності та цілісності інформації.

Криптографічні методи захисту інформації є одним із найефективніших інструментів забезпечення інформаційної безпеки в сучасних інформаційних системах.

Нормативне регулювання криптографічного захисту інформації включає вимоги до використання криптографічних алгоритмів, порядок управління криптографічними ключами, а також процедури сертифікації засобів криптографічного захисту.

Таке регулювання є особливо важливим у системах електронного документообігу, де криптографічні методи використовуються для забезпечення автентичності електронних документів та захисту інформації під час її передачі через мережі.

Роль нормативно-правової бази у забезпеченні інформаційної безпеки

Наявність ефективної нормативно-правової бази є важливою умовою забезпечення інформаційної безпеки держави. Законодавче регулювання дозволяє визначити правила оброблення інформації, встановити відповідальність за порушення інформаційної безпеки та забезпечити координацію діяльності різних державних органів у сфері захисту інформації.

Крім того, нормативно-правова база створює умови для впровадження сучасних технологій захисту інформації та сприяє підвищенню рівня кібербезпеки держави.

Ефективна система інформаційної безпеки повинна ґрунтуватися на поєднанні правових, організаційних та технічних механізмів захисту інформації.

Державні стандарти та НД ТЗІ

Роль державних органів у формуванні нормативної бази захисту інформації

Важливу роль у формуванні та реалізації державної політики у сфері захисту інформації відіграють спеціалізовані державні органи. Одним із ключових органів у цій сфері є Державна служба спеціального зв'язку та захисту інформації України, яка відповідає за формування та реалізацію державної політики у сфері криптографічного та технічного захисту інформації.

До основних повноважень цього органу належать:

- розроблення нормативно-правових актів у сфері захисту інформації;
- формування державної системи технічного захисту інформації;
- організація державної експертизи у сфері технічного захисту інформації;
- сертифікація засобів захисту інформації;
- координація діяльності суб’єктів у сфері інформаційної безпеки.

Функціонування ефективної системи інформаційної безпеки неможливе без централізованого державного регулювання, яке забезпечує узгодженість нормативних вимог та стандартизацію процедур захисту інформації.

Державні стандарти у сфері захисту інформації

Важливим елементом нормативно-правового забезпечення інформаційної безпеки є система державних стандартів. В Україні вони представлені стандартами серії ДСТУ, які встановлюють вимоги до організації захисту інформації, побудови систем безпеки та управління інформаційною безпекою.

Зокрема, значну роль відіграє ДСТУ ISO/IEC 27001 — міжнародний стандарт, який визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою.

Цей стандарт передбачає:

- управління ризиками інформаційної безпеки;

- контроль доступу до інформаційних ресурсів;
- управління інцидентами інформаційної безпеки;
- захист інформаційних активів організації.

Використання цього стандарту дозволяє організаціям впроваджувати системний підхід до управління інформаційною безпекою та забезпечувати належний рівень захисту інформаційних ресурсів.

Іншим важливим стандартом є ДСТУ ISO/IEC 27002, який містить рекомендації щодо практичної реалізації заходів інформаційної безпеки. Він описує комплекс організаційних та технічних заходів, які можуть застосовуватися для забезпечення захисту інформації.

Серед основних напрямів цього стандарту:

- політика інформаційної безпеки;
- управління доступом;
- криптографічний захист інформації;
- фізична безпека інформаційних систем;
- захист мережевої інфраструктури.

Використання міжнародних стандартів у сфері інформаційної безпеки сприяє підвищенню ефективності систем захисту інформації та забезпечує їх відповідність сучасним міжнародним вимогам.

Нормативні документи з технічного захисту інформації (НД ТЗІ)

Важливою складовою нормативної бази у сфері інформаційної безпеки є нормативні документи з технічного захисту інформації (НД ТЗІ). Ці документи розробляються з метою встановлення єдиних вимог до створення та функціонування систем захисту інформації.

До основних нормативних документів цієї категорії належать:

- НД ТЗІ 1.1-002-99 — загальні положення щодо технічного захисту інформації;
- НД ТЗІ 2.5-004-99 — критерії оцінювання захищеності інформації в комп’ютерних системах;
- НД ТЗІ 3.7-003-05 — порядок створення комплексної системи

захисту інформації.

Ці документи визначають основні вимоги до:

- організації технічного захисту інформації;
- створення комплексних систем захисту інформації (КСЗІ);
- проведення державної експертизи у сфері технічного захисту інформації;
- оцінювання рівня захищеності інформаційних систем.

Згідно з науковими дослідженнями А.Ю. Щеглов та К.А. Щеглов, нормативні документи з технічного захисту інформації дозволяють стандартизувати процес створення систем безпеки та забезпечити уніфікований підхід до їх проєктування.

Комплексні системи захисту інформації

Одним із важливих напрямів реалізації нормативно-правових вимог у сфері інформаційної безпеки є створення комплексних систем захисту інформації.

Комплексна система захисту інформації (КСЗІ) являє собою сукупність організаційних, програмних та технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації.

Основними етапами створення КСЗІ є:

1. аналіз загроз інформаційній безпеці;
2. визначення вимог до захисту інформації;
3. проєктування системи захисту;
4. впровадження засобів захисту;
5. оцінювання ефективності системи.

Ефективність комплексної системи захисту інформації значною мірою залежить від правильного поєднання організаційних, технічних та криптографічних методів захисту.

Значення нормативної бази для розвитку інформаційної безпеки

Наявність розвиненої нормативно-правової бази є необхідною умовою забезпечення ефективного функціонування інформаційних систем. Законодавчі

акти, державні стандарти та нормативні документи з технічного захисту інформації створюють правові механізми, які дозволяють регламентувати порядок оброблення інформації та встановити вимоги до її захисту.

Крім того, нормативно-правова база сприяє:

- впровадженню сучасних технологій інформаційної безпеки;
- підвищенню рівня кіберзахисту державних інформаційних систем;
- гармонізації українського законодавства з міжнародними стандартами у сфері інформаційної безпеки.

У сучасних умовах цифрової трансформації суспільства та зростання кількості кіберзагроз розвиток нормативно-правового забезпечення інформаційної безпеки залишається одним із ключових напрямів державної політики у сфері захисту інформації.

Отже, нормативно-правове забезпечення захисту інформації в Україні є важливою складовою системи інформаційної безпеки держави. Воно включає сукупність законодавчих та підзаконних актів, які регулюють правові, організаційні та технічні аспекти захисту інформації.

Основу цієї системи становлять законодавчі акти, що визначають правові засади захисту інформації, зокрема Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закон України «Про електронні документи та електронний документообіг». Поряд із законодавчими актами важливу роль відіграють державні стандарти, нормативні документи з технічного та криптографічного захисту інформації, а також методичні рекомендації щодо створення систем інформаційної безпеки.

Таким чином, нормативно-правова база створює необхідні умови для забезпечення ефективного захисту інформаційних ресурсів, сприяє розвитку інформаційного суспільства та підвищенню рівня національної безпеки України.

Висновки до першого розділу

У першому розділі досліджено природу електронного документа, зроблений аналіз сучасних загроз несанкціонованого доступу, висвітлені проблеми забезпечення конфіденційності, цілісності та доступності електронних

документів. Визначено, що цифровий формат має свої слабкі місця, це створює додаткові ризики витоку, підміни або знищення даних.

Обґрунтовано, що захист електронних документів безпосередньо впливає на обороноздатність держави. У сучасних умовах інформація є важливим ресурсом. Якщо противник отримає доступ до службових чи військових документів, це може зірвати управління підрозділами та зашкодити безпеці особового складу.

Таким чином по першому розділу можна зробити такий висновок, що найбільшу небезпеку для електронних документів становлять хакерські атаки, віруси-вимагачі (Ransomware), фішинг та помилки самих користувачів («людський фактор») та використання окремих засобів захисту електронного документу (наприклад, тільки антивірусу) є неефективним. Що доводить потребу в розробці комплексної методики захисту електронного документу від несанкціонованого доступу.

РОЗДІЛ 2. МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

2.1 Криптографічні методи захисту електронних документів

У сучасних умовах цифровізації суспільства електронні документи стали невід'ємною складовою інформаційної діяльності державних установ, підприємств та організацій. Широке використання електронного документообігу дозволяє значно підвищити ефективність оброблення інформації, однак водночас створює нові ризики, пов'язані з несанкціонованим доступом до даних, їх модифікацією або знищенням.

Одним із найбільш ефективних способів забезпечення безпеки електронних документів є застосування криптографічних методів захисту інформації. Криптографія дозволяє забезпечити конфіденційність, цілісність та автентичність інформації, що передається або зберігається в інформаційних системах.

Правові засади використання електронних документів в Україні визначає Закон України «Про електронні документи та електронний документообіг», який встановлює юридичний статус електронного документа та визначає основні вимоги до його створення, передачі та зберігання. Згідно з цим законом, електронний документ повинен містити обов'язкові реквізити, а для підтвердження його справжності використовується електронний підпис.

У свою чергу, правові засади організації захисту інформації визначає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який передбачає застосування криптографічних засобів для забезпечення безпеки інформації.

Основні цілі криптографічного захисту електронних документів

Використання криптографічних методів у системах електронного документообігу спрямоване на забезпечення основних властивостей інформаційної безпеки.

Основними цілями криптографічного захисту інформації є:

1. Конфіденційність інформації

Конфіденційність означає забезпечення доступу до інформації лише для авторизованих користувачів. Криптографічні алгоритми дозволяють перетворити інформацію у вигляд, який є незрозумілим для сторонніх осіб.

2. Цілісність інформації

Цілісність інформації забезпечує неможливість несанкціонованої зміни даних. За допомогою криптографічних механізмів можна перевірити, чи не було змінено інформацію під час її передачі або зберігання.

3. Автентичність інформації

Автентичність дозволяє встановити справжність автора документа та підтвердити його походження.

4. Неможливість відмови від авторства

Ця властивість означає, що автор документа не може заперечити факт його створення або підписання.

Основні криптографічні методи захисту електронних документів

До основних криптографічних методів захисту інформації у системах електронного документообігу відносяться:

Шифрування інформації

Шифрування є одним із основних криптографічних методів захисту інформації. Воно полягає у перетворенні відкритого тексту в зашифрований вигляд за допомогою спеціального алгоритму та криптографічного ключа.

Існують два основних типи шифрування:

Симетричне шифрування

У симетричних криптографічних системах для шифрування та дешифрування використовується один і той самий ключ. Такий підхід характеризується високою швидкістю оброблення інформації та широко застосовується для захисту великих обсягів даних.

Однак основною проблемою симетричних алгоритмів є необхідність безпечної передачі ключа між сторонами.

Асиметричне шифрування

У системах асиметричного шифрування використовуються два різні ключі:

- відкритий ключ;
- закритий ключ.

Відкритий ключ використовується для шифрування інформації, тоді як закритий ключ застосовується для її дешифрування. Такий підхід дозволяє значно підвищити рівень безпеки інформаційного обміну.

Поєднання симетричних та асиметричних методів шифрування дозволяє створювати ефективні системи захисту інформації у сучасних інформаційних системах.

Електронний цифровий підпис

Одним із ключових криптографічних механізмів захисту електронних документів є електронний підпис. Його основною метою є забезпечення автентичності документа та підтвердження особи підписувача.

Електронний підпис створюється за допомогою криптографічного перетворення інформації та використання закритого ключа підписувача.

Основними функціями електронного підпису є:

- підтвердження авторства документа;
- забезпечення цілісності інформації;
- захист від підробки документів.

У системах електронного документообігу електронний підпис має таку саму юридичну силу, як і власноручний підпис, за умови дотримання встановлених законодавством вимог.

Хешування інформації

Ще одним важливим криптографічним методом захисту електронних документів є хешування.

Хешування полягає у перетворенні інформації довільної довжини у коротке унікальне значення — хеш-код. Цей код використовується для перевірки цілісності даних.

Основними властивостями криптографічних хеш-функцій є:

- односторонність;
- унікальність результату;
- неможливість відновлення початкового повідомлення за хеш-значенням.

Використання хеш-функцій у поєднанні з електронним підписом дозволяє забезпечити високий рівень захисту електронних документів.

Криптографічна інфраструктура відкритих ключів

Для ефективного використання криптографічних методів у системах електронного документообігу створюється інфраструктура відкритих ключів (PKI).

PKI являє собою комплекс технічних та організаційних засобів, які забезпечують:

- генерацію криптографічних ключів;
- розповсюдження відкритих ключів;
- перевірку електронних підписів;
- управління сертифікатами ключів.

Функціонування такої інфраструктури дозволяє забезпечити довіру між учасниками електронного документообігу та гарантувати достовірність електронних документів.

Значення криптографічного захисту для безпеки електронного документообігу

Застосування криптографічних методів є одним із найважливіших елементів забезпечення інформаційної безпеки сучасних інформаційних систем.

Криптографічний захист інформації дозволяє:

- забезпечити безпечний обмін інформацією в мережевому середовищі;
- запобігти несанкціонованому доступу до електронних документів;
- гарантувати цілісність та достовірність інформації;
- забезпечити юридичну значущість електронних документів.

У сучасних умовах цифровізації державного управління та розвитку

електронних сервісів криптографічні методи захисту відіграють ключову роль у забезпеченні безпеки електронного документообігу.

Отже, криптографічні методи є одним із найважливіших інструментів забезпечення безпеки електронних документів у сучасних інформаційних системах. Вони дозволяють забезпечити конфіденційність, цілісність та автентичність інформації, а також гарантувати юридичну значущість електронних документів.

Застосування таких методів, як шифрування, електронний підпис та хешування, дозволяє ефективно захищати інформацію від несанкціонованого доступу, підробки та модифікації. Водночас правові засади використання електронних документів та криптографічних засобів захисту визначаються національним законодавством, зокрема Законом України «Про електронні документи та електронний документообіг» та Законом України «Про захист інформації в інформаційно-телекомунікаційних системах».

Таким чином, криптографічний захист є ключовим елементом сучасних систем електронного документообігу та важливою складовою загальної системи інформаційної безпеки.

2.2 Ідентифікація, автентифікація та авторизація користувачів

У сучасних інформаційних системах одним із ключових завдань забезпечення інформаційної безпеки є запобігання несанкціонованому доступу до інформаційних ресурсів. Для вирішення цього завдання використовуються спеціальні механізми контролю доступу, серед яких важливе місце займають процедури ідентифікації, автентифікації та авторизації користувачів.

Згідно з науковими підходами, система контролю доступу є одним із базових елементів комплексної системи захисту інформації. Її основним призначенням є забезпечення доступу до інформаційних ресурсів лише для авторизованих користувачів відповідно до встановлених прав та повноважень.

Використання механізмів ідентифікації, автентифікації та авторизації дозволяє забезпечити реалізацію основних принципів інформаційної безпеки, таких як конфіденційність, цілісність та доступність інформації.

Правові основи організації захисту інформації в інформаційних системах визначає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який передбачає необхідність застосування технічних і програмних засобів для запобігання несанкціонованому доступу до інформації.

Ідентифікація користувачів

Ідентифікація є першим етапом процесу контролю доступу до інформаційної системи. Вона полягає у встановленні особи користувача або іншого суб'єкта інформаційної взаємодії.

Ідентифікація здійснюється шляхом присвоєння кожному користувачу унікального ідентифікатора, який дозволяє системі розпізнавати його серед інших користувачів.

Ідентифікатором користувача може виступати:

- ім'я користувача (логін);
- номер облікового запису;
- електронна адреса;
- цифровий сертифікат;
- інші унікальні параметри.

Важливою особливістю ідентифікації є те, що вона лише повідомляє системі, ким користувач себе заявляє, але не підтверджує його справжню особу. Саме тому наступним етапом перевірки є процедура автентифікації.

Автентифікація користувачів

Автентифікація є процесом підтвердження справжності користувача, який намагається отримати доступ до інформаційної системи.

Згідно з дослідженнями В.М. Зайцев та М.М. Зайцев, автентифікація здійснюється шляхом перевірки інформації, що підтверджує особу користувача.

Основними методами автентифікації є:

Автентифікація на основі знання

Цей метод передбачає використання інформації, яку знає лише користувач.

Найпоширенішими прикладами є:

- паролі;
- PIN-коди;
- секретні питання.

Перевагою цього методу є простота реалізації, однак його основним недоліком є вразливість до атак підбору паролів або соціальної інженерії.

Автентифікація на основі володіння

У цьому випадку користувач підтверджує свою особу за допомогою фізичного об’єкта, який перебуває у його володінні.

До таких засобів належать:

- смарт-картки;
- токени безпеки;
- електронні ключі;
- мобільні пристрої з генераторами одноразових паролів.

Біометрична автентифікація

Біометричні методи автентифікації базуються на використанні унікальних фізіологічних або поведінкових характеристик людини.

Найбільш поширеними біометричними параметрами є:

- відбитки пальців;
- розпізнавання обличчя;
- сканування сітківки ока;
- голосова ідентифікація.

Використання біометричних методів дозволяє значно підвищити рівень захисту інформаційних систем.

Багатофакторна автентифікація

Для підвищення рівня безпеки інформаційних систем часто використовується багатофакторна автентифікація.

Цей підхід передбачає використання кількох незалежних факторів

підтвердження особи користувача, наприклад:

- пароль;
- одноразовий код;
- біометричні дані.

Застосування багатофакторної автентифікації значно знижує ймовірність несанкціонованого доступу до інформаційних систем навіть у випадку компрометації одного з факторів.

Авторизація користувачів

Після успішного проходження процедури автентифікації система переходить до етапу авторизації.

Авторизація являє собою процес надання користувачеві певних прав доступу до ресурсів інформаційної системи.

Авторизація визначає, які саме дії може виконувати користувач у системі, наприклад:

- перегляд інформації;
- створення або редагування документів;
- видалення даних;
- адміністрування системи.

У сучасних інформаційних системах використовуються різні моделі авторизації, серед яких найбільш поширеними є:

Дискреційна модель доступу

У цій моделі власник інформаційного ресурсу самостійно визначає, які користувачі можуть отримати доступ до інформації.

Мандатна модель доступу

Ця модель використовується у системах з підвищеними вимогами до безпеки. Доступ до інформації визначається на основі рівнів секретності та категорій користувачів.

Рольова модель доступу

Рольова модель доступу передбачає призначення користувачам певних ролей, кожна з яких має визначений набір прав доступу.

Ця модель широко використовується у корпоративних інформаційних системах.

Роль ідентифікації, автентифікації та авторизації у системах захисту інформації

Механізми ідентифікації, автентифікації та авторизації є важливою складовою системи захисту інформації від несанкціонованого доступу.

Згідно з дослідженнями науковців, ефективна система контролю доступу повинна забезпечувати:

- надійну ідентифікацію користувачів;
- перевірку їх справжності;
- чітке визначення прав доступу до інформаційних ресурсів;
- ведення журналів доступу до системи.

Використання таких механізмів дозволяє значно зменшити ризик несанкціонованого доступу до інформації та підвищити загальний рівень безпеки інформаційних систем.

Отже, ідентифікація, автентифікація та авторизація користувачів є важливими складовими системи захисту інформації в сучасних інформаційних системах. Вони забезпечують контроль доступу до інформаційних ресурсів та запобігають несанкціонованому використанню інформації.

2.3. Розмежування доступу та управління правами користувачів

Однією з ключових складових забезпечення інформаційної безпеки сучасних інформаційних систем є розмежування доступу до інформаційних ресурсів. У процесі функціонування інформаційних систем користувачі виконують різні ролі та мають різний рівень повноважень, тому важливо забезпечити контроль за їхніми діями та обмежити доступ до інформації відповідно до встановлених правил.

Розмежування доступу є комплексом організаційних та технічних заходів, спрямованих на регулювання доступу користувачів до інформаційних ресурсів

системи відповідно до їхніх службових обов’язків і повноважень.

Система розмежування доступу є важливим елементом комплексної системи захисту інформації, оскільки дозволяє забезпечити контроль над використанням інформаційних ресурсів і запобігти несанкціонованому доступу до конфіденційної інформації.

Правові основи організації захисту інформації визначаються Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який встановлює вимоги до організації систем захисту інформації, зокрема механізмів контролю доступу.

Основні принципи розмежування доступу

Система розмежування доступу до інформаційних ресурсів повинна базуватися на певних принципах, які забезпечують її ефективність та надійність.

Згідно з науковими дослідженнями, основними принципами розмежування доступу є:

Принцип мінімальних привілеїв

Цей принцип передбачає надання користувачам лише тих прав доступу, які необхідні для виконання їхніх службових обов’язків. Обмеження прав доступу дозволяє зменшити ризик несанкціонованого використання інформації.

Принцип розподілу повноважень

Відповідно до цього принципу критично важливі операції повинні виконуватися кількома користувачами або підрозділами. Такий підхід дозволяє зменшити ризик зловживань з боку окремих користувачів.

Принцип контролю доступу

Система повинна забезпечувати постійний контроль за діями користувачів та реєстрацію їхніх дій у спеціальних журналах.

Принцип підзвітності

Кожна дія користувача в системі повинна бути пов’язана з конкретним обліковим записом, що дозволяє встановити відповідальність за виконані операції.

Моделі розмежування доступу

У сучасних інформаційних системах застосовуються різні моделі контролю доступу, які визначають правила надання прав користувачам.

Найбільш поширеними моделями розмежування доступу є дискреційна, мандатна та рольова.

Дискреційна модель доступу

Дискреційна модель доступу передбачає, що власник інформаційного ресурсу самостійно визначає, які користувачі можуть отримати доступ до певних даних.

У цій моделі використовуються списки контролю доступу, які визначають:

- користувачів, що мають право доступу;
- типи дозволених операцій;
- рівень доступу до ресурсів.

Перевагою цієї моделі є її гнучкість, однак вона має і певні недоліки, зокрема складність контролю за розповсюдженням прав доступу.

Мандатна модель доступу

Мандатна модель використовується у системах з високими вимогами до безпеки, зокрема у державних інформаційних системах.

У цій моделі доступ до інформації визначається на основі рівнів секретності та категорій користувачів.

Користувач може отримати доступ до інформації лише у випадку, якщо його рівень доступу відповідає рівню секретності інформації.

Рольова модель доступу

Рольова модель доступу є однією з найбільш поширених у сучасних інформаційних системах.

Вона передбачає призначення користувачам певних ролей, кожна з яких має визначений набір прав доступу.

Прикладом ролей можуть бути:

- адміністратор системи;
- оператор;
- користувач;

- аудитор.

Застосування рольової моделі дозволяє значно спростити управління правами доступу у великих інформаційних системах.

Управління правами користувачів

Управління правами користувачів є важливим елементом системи інформаційної безпеки. Воно передбачає визначення, надання, зміну та анулювання прав доступу користувачів до інформаційних ресурсів.

Ефективне управління правами користувачів повинно включати такі етапи:

Реєстрація користувачів

На цьому етапі створюються облікові записи користувачів та визначаються їхні ролі у системі.

Призначення прав доступу

Користувачам надаються права доступу відповідно до їхніх службових обов’язків.

Контроль використання прав

Система повинна забезпечувати моніторинг дій користувачів та реєстрацію їхніх операцій.

Аудит доступу

Регулярний аудит дозволяє перевірити правильність призначення прав доступу та виявити можливі порушення політики безпеки.

Засоби реалізації систем управління доступом

Для реалізації механізмів розмежування доступу використовуються різні програмні та апаратні засоби.

До основних засобів належать:

- системи управління обліковими записами;
- системи керування доступом;
- механізми журналювання подій;
- системи моніторингу безпеки.

Згідно з дослідженнями, поєднання криптографічних механізмів із системами управління доступом дозволяє значно підвищити рівень захисту

інформації.

Значення систем розмежування доступу для забезпечення інформаційної безпеки

Розмежування доступу є одним із ключових механізмів захисту інформаційних систем від несанкціонованого доступу.

Ефективна система управління доступом дозволяє:

- обмежити доступ до конфіденційної інформації;
- запобігти несанкціонованим діям користувачів;
- контролювати використання інформаційних ресурсів;
- забезпечити відповідність вимогам інформаційної безпеки.

Правильно організована система розмежування доступу є основою побудови ефективної системи захисту інформації.

2.4. Технічні та програмні засоби захисту інформації

Загальна характеристика технічного та програмного захисту інформації

У сучасних інформаційних системах питання захисту інформації від несанкціонованого доступу є одним із ключових завдань забезпечення інформаційної безпеки. Інтенсивний розвиток інформаційно-комунікаційних технологій, широке використання комп’ютерних мереж та електронного документообігу створюють нові можливості для оброблення інформації, однак водночас спричиняють появу нових загроз безпеці інформаційних ресурсів.

Ефективне забезпечення інформаційної безпеки передбачає застосування комплексу організаційних, правових, технічних та програмних заходів, спрямованих на захист інформації від несанкціонованого доступу, модифікації або знищення.

Правові засади організації захисту інформації в Україні визначає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який передбачає застосування технічних і програмних засобів для забезпечення безпеки інформаційних ресурсів.

Згідно з дослідженнями, технічні та програмні засоби захисту інформації є важливою складовою комплексної системи захисту інформації, оскільки саме вони забезпечують практичну реалізацію політики безпеки інформаційної системи.

Розглянемо основні технічні та програмні засоби захисту інформації , які наведені в таблиці 2.1.

Таблиця 2.1 – Основні технічні та програмні засоби захисту інформації

Категорія засобу	Засіб захисту	Призначення	Основний принцип роботи	Переваги	Недоліки
Технічний	Системи контролю та управління доступом (СКУД)	Обмеження фізичного доступу до інформаційних ресурсів	Ідентифікація особи за карткою, кодом або біометрією	Висока надійність контролю доступу	Вимагає спеціального обладнання
Технічний	Системи відеоспостереження	Контроль дій персоналу та відвідувачів	Безперервна відеофіксація подій	Можливість аудиту інцидентів	Значний обсяг даних для зберігання
Технічний	Охоронна сигналізація	Захист приміщень та обладнання	Реагування на несанкціоноване проникнення	Підвищення фізичної безпеки	Не захищає від кіберзагроз
Технічний	Джерела безперебійного живлення (UPS)	Забезпечення безперервності роботи систем	Резервне живлення обладнання	Захист від втрати даних через відключення електроенергії	Обмежений час автономної роботи
Технічний	Сервери резервного копіювання	Забезпечення відновлення інформації	Автоматичне створення резервних копій	Підвищення доступності інформації	Потребує додаткових ресурсів
Технічний	Апаратні криптомодулі (HSM)	Захист криптографічних ключів	Апаратне зберігання ключової інформації	Максимальна стійкість до компрометації	Висока вартість
Технічний	Смарт-карти та USB-токени	Захищене зберігання ключів та автентифікація	Використання апаратного носія	Підвищення рівня автентифікації	Ризик втрати носія
Програмний	Антивірусне програмне забезпечення	Захист від шкідливого ПЗ	Аналіз та блокування шкідливого коду	Простота використання	Не гарантує захист від нових загроз
Програмний	Міжмережевий екран (Firewall)	Контроль мережевих з'єднань	Фільтрація трафіку відповідно до політик безпеки	Захист від зовнішніх атак	Обмежена ефективність проти внутрішніх загроз
Програмний	IDS (Intrusion Detection System)	Виявлення атак	Аналіз подій та пошук аномалій	Раннє виявлення загроз	Не блокує атаки автоматично
Програмний	IPS (Intrusion Prevention System)	Запобігання атакам	Автоматичне блокування шкідливої активності	Активний захист системи	Можливі помилкові спрацювання

Категорія засобу	Засіб захисту	Призначення	Основний принцип роботи	Переваги	Недоліки
Програмний	DLP (Data Loss Prevention)	Запобігання витоку інформації	Контроль інформаційних потоків	Ефективний захист конфіденційних даних	Складність налаштування
Програмний	SIEM-системи	Моніторинг та аналіз подій безпеки	Кореляція подій та аналіз журналів	Централізований контроль безпеки	Висока вартість впровадження
Програмний	Системи керування доступом (RBAC, ABAC)	Розмежування прав користувачів	Надання прав відповідно до ролей або атрибутів	Реалізація принципу мінімальних привілеїв	Потребує постійного адміністрування
Програмний	Системи багатофакторної автентифікації (MFA)	Посилення перевірки особи користувача	Використання декількох факторів автентифікації	Значне зниження ризику компрометації облікових записів	Зниження зручності користування
Програмний	Системи електронного документообігу з КЕП	Забезпечення юридичної значущості документів	Використання кваліфікованого електронного підпису	Захист цілісності та автентичності документів	Залежність від інфраструктури відкритих ключів
Програмний	Засоби шифрування даних	Захист конфіденційності інформації	Криптографічне перетворення даних	Високий рівень захисту	Потребує управління ключами
Програмний	Засоби журналювання та аудиту	Контроль дій користувачів	Реєстрація подій безпеки	Підвищення підзвітності користувачів	Потребує постійного аналізу журналів

Технічні засоби захисту інформації

Технічні засоби захисту інформації являють собою сукупність апаратних пристроїв і технічних рішень, які забезпечують захист інформації від несанкціонованого доступу, витоку або пошкодження.

Технічні засоби захисту інформації можуть використовуватися для забезпечення фізичної безпеки інформаційних систем, контролю доступу до обладнання та захисту каналів передачі інформації.

Засоби фізичного захисту інформації

До технічних засобів фізичного захисту належать:

- системи контролю та управління доступом до приміщень;
- системи відеоспостереження;
- охоронна сигналізація;
- електронні замки та ідентифікаційні пристрої.

Ці засоби дозволяють обмежити доступ сторонніх осіб до приміщень, де

розташовані інформаційні системи та серверне обладнання.

Засоби захисту каналів передачі інформації

Важливим напрямом технічного захисту інформації є захист каналів передачі даних.

До таких засобів належать:

- апаратні криптографічні модулі;
- мережеві шлюзи безпеки;
- засоби захисту від перехоплення інформації.

Застосування таких засобів дозволяє забезпечити безпечну передачу інформації між різними елементами інформаційної системи.

Засоби захисту від технічних каналів витоку інформації

Одним із важливих напрямів технічного захисту інформації є запобігання витоку інформації через технічні канали.

До таких засобів належать:

- пристрої екранування електромагнітних випромінювань;
- системи фільтрації сигналів;
- засоби захисту від електромагнітного перехоплення інформації.

Застосування цих засобів дозволяє запобігти витоку інформації через побічні електромагнітні випромінювання та інші технічні канали.

Програмні засоби захисту інформації

Програмні засоби захисту інформації являють собою спеціальне програмне забезпечення, призначене для забезпечення безпеки інформаційних систем.

Програмні засоби захисту інформації забезпечують контроль доступу до інформаційних ресурсів, виявлення загроз безпеці та запобігання несанкціонованим діям користувачів.

Системи ідентифікації та автентифікації

Одним із важливих програмних механізмів захисту є системи ідентифікації та автентифікації користувачів.

Вони дозволяють:

- встановити особу користувача;
- перевірити його справжність;
- забезпечити доступ до системи лише авторизованим користувачам.

Такі системи широко використовуються у сучасних операційних системах та корпоративних інформаційних системах.

Антивірусні системи

Антивірусні програми призначені для виявлення, блокування та видалення шкідливого програмного забезпечення.

Антивірусні системи виконують такі функції:

- сканування файлів та програм;
- виявлення шкідливого програмного забезпечення;
- запобігання зараженню комп’ютерних систем.

Антивірусний захист є одним із базових елементів забезпечення безпеки інформаційних систем.

Міжмережеві екрани

Міжмережеві екрани (firewall) призначені для контролю мережевого трафіку та запобігання несанкціонованому доступу до інформаційних систем.

Вони виконують такі функції:

- фільтрацію мережевих пакетів;
- контроль доступу до мережевих ресурсів;
- блокування підозрілої мережевої активності.

Застосування міжмережевих екранів дозволяє значно зменшити ризик зовнішніх атак на інформаційні системи.

Системи виявлення вторгнень

Системи виявлення вторгнень призначені для моніторингу мережевої активності та виявлення спроб несанкціонованого доступу до інформаційних систем.

Такі системи аналізують мережевий трафік та виявляють підозрілі дії користувачів або програм.

Криптографічні програмні засоби захисту

Важливу роль у забезпеченні інформаційної безпеки відіграють криптографічні програмні засоби.

Згідно з дослідженнями, криптографічні методи дозволяють забезпечити:

- конфіденційність інформації;
- цілісність даних;
- автентичність електронних документів.

Криптографічні засоби широко використовуються у системах електронного документообігу, що регламентується Законом України «Про електронні документи та електронний документообіг».

Комплексне використання технічних та програмних засобів захисту

Ефективний захист інформації можливий лише за умови комплексного застосування різних засобів захисту.

Система захисту інформації повинна включати:

- організаційні заходи;
- технічні засоби захисту;
- програмні механізми безпеки;
- криптографічні методи захисту інформації.

Комплексний підхід дозволяє створити багаторівневу систему безпеки, яка забезпечує ефективний захист інформаційних ресурсів.

2.5 Аналіз сучасних систем захисту електронних документів

У сучасних умовах цифрової трансформації суспільства електронні документи стали важливою складовою інформаційної діяльності державних органів, підприємств та організацій. Використання електронного документообігу дозволяє значно підвищити ефективність управління інформаційними ресурсами, прискорити процес оброблення документів та зменшити витрати на їх зберігання.

Водночас широке застосування електронних документів створює нові загрози для інформаційної безпеки, пов’язані з можливістю несанкціонованого доступу до інформації, її підробкою, модифікацією або знищенням. У зв’язку з цим виникає необхідність використання сучасних систем захисту електронних документів, які забезпечують їхню конфіденційність, цілісність та автентичність.

Правові засади використання електронних документів в Україні визначає Закон України «Про електронні документи та електронний документообіг», який встановлює юридичний статус електронних документів та регламентує порядок їх створення, передачі та зберігання. У свою чергу, загальні вимоги до захисту інформації визначає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Згідно з науковими підходами, система захисту електронних документів повинна являти собою комплекс організаційних, програмних та криптографічних заходів, спрямованих на забезпечення безпеки інформації протягом усього життєвого циклу документа.

Основні загрози безпеці електронних документів

Під час функціонування систем електронного документообігу виникає значна кількість загроз інформаційній безпеці. Їх аналіз є важливим етапом побудови ефективної системи захисту інформації.

До основних загроз безпеці електронних документів належать:

- несанкціонований доступ до документів;
- підробка електронних документів;
- несанкціонована модифікація інформації;
- знищення або пошкодження електронних документів;
- перехоплення інформації під час її передачі;
- використання шкідливого програмного забезпечення.

Наявність таких загроз зумовлює необхідність використання сучасних систем захисту інформації, які забезпечують багаторівневий захист електронних документів.

Основні компоненти систем захисту електронних документів

Сучасні системи захисту електронних документів включають комплекс різних механізмів безпеки, які працюють у взаємодії один з одним.

Згідно з дослідженнями, до основних компонентів таких систем належать:

- механізми ідентифікації та автентифікації користувачів;
- системи розмежування доступу;
- криптографічні засоби захисту інформації;
- системи аудиту та моніторингу дій користувачів;
- засоби захисту мережевої інфраструктури.

Застосування цих механізмів дозволяє створити комплексну систему захисту інформації, яка забезпечує надійне функціонування систем електронного документообігу.

Криптографічні механізми захисту електронних документів

Одним із найважливіших елементів сучасних систем захисту електронних документів є криптографічні засоби захисту інформації.

Криптографічні методи дозволяють забезпечити:

- конфіденційність інформації;
- цілісність електронних документів;
- автентичність автора документа;
- неможливість відмови від авторства.

До основних криптографічних механізмів захисту електронних документів належать:

- електронний підпис;
- шифрування інформації;
- хешування даних;
- інфраструктура відкритих ключів.

Використання електронного підпису дозволяє підтвердити справжність електронного документа та забезпечити його юридичну значущість.

Програмні системи електронного документообігу

Сучасні системи електронного документообігу включають спеціалізоване

програмне забезпечення, яке забезпечує створення, оброблення, передачу та зберігання електронних документів.

До основних функцій таких систем належать:

- реєстрація та облік документів;
- контроль виконання документів;
- управління правами доступу користувачів;
- архівування електронних документів;
- забезпечення інформаційної безпеки.

Сучасні системи електронного документообігу інтегруються з іншими інформаційними системами організації та забезпечують автоматизацію документообігу.

Засоби контролю доступу до електронних документів

Важливим елементом систем захисту електронних документів є механізми контролю доступу.

Системи контролю доступу дозволяють:

- визначити права доступу користувачів;
- обмежити доступ до конфіденційної інформації;
- контролювати дії користувачів;
- запобігати несанкціонованим операціям.

Для цього використовуються різні моделі управління доступом, зокрема рольова модель, яка дозволяє ефективно управляти правами доступу у великих інформаційних системах.

Системи аудиту та моніторингу безпеки

Для забезпечення ефективного захисту електронних документів важливе значення мають системи аудиту та моніторингу інформаційної безпеки.

Такі системи дозволяють:

- реєструвати дії користувачів;
- виявляти порушення політики безпеки;
- аналізувати інциденти інформаційної безпеки;
- контролювати використання інформаційних ресурсів.

Застосування систем аудиту дозволяє підвищити рівень контролю над інформаційними процесами та своєчасно виявляти загрози безпеці.

Тенденції розвитку систем захисту електронних документів

У сучасних умовах розвиток систем захисту електронних документів відбувається у напрямі підвищення їхньої ефективності та інтеграції з іншими інформаційними системами.

Основними тенденціями розвитку таких систем є:

- використання багатофакторної автентифікації;
- застосування сучасних криптографічних алгоритмів;
- інтеграція систем електронного документообігу з хмарними сервісами;
- використання систем моніторингу інформаційної безпеки.

Застосування новітніх технологій дозволяє підвищити рівень захисту електронних документів та забезпечити їхню надійність у сучасному інформаційному середовищі.

Сучасні системи захисту електронних документів являють собою комплекс організаційних, технічних, програмних та криптографічних засобів, спрямованих на забезпечення інформаційної безпеки.

Висновки до другого розділу

У другому розділі розглянуто сучасні методи та технології захисту документів. Доведено, що криптографія (шифрування) є найнадійнішим способом зберегти таємницю та цілісність даних. Використання Кваліфікованого електронного підпису (КЕП) повністю підтверджує авторство документа та його юридичну силу.

Досліджено методи контролю доступу, за результатами аналізу зроблено наступні висновки, що для безпеки системи необхідно впроваджувати двофакторну автентифікацію (пароль + підтвердження на телефон або токен) та рольову модель (RBAC), де кожен працівник має доступ лише до тих документів, які потрібні для його роботи.

Проаналізовано роботу програмних і технічних засобів захисту:

міжмережевих екранів (Firewalls), систем виявлення вторгнень (IDS/IPS) та захисту від витоку даних (DLP). Вони створюють надійний бар'єр проти зовнішніх атак та внутрішніх порушників.

Таким чином встановлено, що сучасні системи захисту розвиваються в напрямку постійного моніторингу та аудиту подій безпеки (SIEM). Це дозволяє не просто чекати на атаку, а автоматично виявляти підозрілі дії користувачів у реальному часі.

РОЗДІЛ 3. РОЗРОБЛЕННЯ МЕТОДИКИ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

3.1. Опис вимог до методики захисту електронних документів

У сьогоденні електронні документи відіграють важливу роль у забезпеченні інформаційної взаємодії між державними органами, підприємствами та організаціями. Використання електронного документообігу дозволяє підвищити ефективність управління інформаційними ресурсами, забезпечити швидкий обмін даними та оптимізувати процеси оброблення документів.

Водночас поширення електронних документів створює нові загрози для інформаційної безпеки, пов’язані з можливістю несанкціонованого доступу, модифікації або знищення інформації. У зв’язку з цим виникає необхідність розроблення ефективної методики захисту електронних документів, яка забезпечує їхню безпеку протягом усього життєвого циклу.

Правові засади використання електронних документів в Україні визначає Закон України «Про електронні документи та електронний документообіг», який регламентує порядок створення, передачі та зберігання електронних документів. У свою чергу, загальні вимоги до захисту інформації встановлює Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Згідно з науковими підходами, методика захисту інформації повинна базуватися на комплексному підході, який включає організаційні, технічні та криптографічні заходи.

Основні вимоги до методики захисту електронних документів

Методика захисту електронних документів повинна відповідати низці вимог, які забезпечують ефективність системи інформаційної безпеки.

До основних вимог належать:

- забезпечення конфіденційності інформації;

- забезпечення цілісності електронних документів;
- підтвердження автентичності автора документа;
- забезпечення доступності інформації для авторизованих користувачів;
- захист від несанкціонованого доступу.

Дотримання цих вимог дозволяє створити ефективну систему захисту електронних документів у сучасних інформаційних системах.

Забезпечення конфіденційності інформації

Однією з основних вимог до методики захисту електронних документів є забезпечення конфіденційності інформації. Конфіденційність передбачає обмеження доступу до інформації лише для авторизованих користувачів.

Для забезпечення конфіденційності використовуються такі механізми:

- криптографічне шифрування інформації;
- системи розмежування доступу;
- механізми ідентифікації та автентифікації користувачів.

Згідно з дослідженнями, застосування криптографічних алгоритмів дозволяє забезпечити надійний захист інформації від несанкціонованого доступу.

Забезпечення цілісності електронних документів

Цілісність інформації є ще однією важливою вимогою до методики захисту електронних документів. Вона передбачає збереження інформації у незмінному вигляді та запобігання її несанкціонованій модифікації.

Для забезпечення цілісності використовуються такі механізми:

- електронний підпис;
- криптографічні хеш-функції;
- системи контролю змін у документах.

Застосування цих механізмів дозволяє своєчасно виявляти будь-які спроби несанкціонованої зміни електронних документів.

Підтвердження автентичності електронних документів

Автентичність електронного документа означає підтвердження його

походження та справжності.

Для забезпечення автентичності використовуються криптографічні механізми, зокрема електронний підпис.

Використання електронного підпису дозволяє:

- підтвердити особу автора документа;
- гарантувати цілісність інформації;
- забезпечити юридичну значущість електронного документа.

Забезпечення доступності інформації

Важливою вимогою до методики захисту електронних документів є забезпечення доступності інформації для авторизованих користувачів.

Це означає, що інформаційна система повинна забезпечувати безперебійний доступ до електронних документів для користувачів, які мають відповідні права доступу.

Для цього використовуються:

- системи резервного копіювання інформації;
- механізми відновлення даних;
- засоби забезпечення безперервності функціонування інформаційних систем.

Контроль доступу до електронних документів

Ефективна методика захисту електронних документів повинна передбачати використання механізмів контролю доступу.

Такі механізми дозволяють:

- визначати права доступу користувачів;
- обмежувати доступ до конфіденційної інформації;
- контролювати дії користувачів у системі.

Системи контролю доступу є важливою складовою комплексної системи захисту інформації.

Аудит та моніторинг інформаційної безпеки

Ще однією важливою вимогою до методики захисту електронних документів є організація системи аудиту та моніторингу інформаційної безпеки.

Такі системи дозволяють:

- реєструвати дії користувачів;
- виявляти порушення політики безпеки;
- аналізувати інциденти інформаційної безпеки;
- контролювати використання інформаційних ресурсів.

Використання систем аудиту дозволяє підвищити ефективність управління інформаційною безпекою.

Комплексний підхід до захисту електронних документів

Сучасні методики захисту електронних документів базуються на принципі комплексності.

Згідно з дослідженнями, ефективна система захисту інформації повинна включати:

- організаційні заходи;
- програмні механізми безпеки;
- технічні засоби захисту;
- криптографічні методи захисту інформації.

Комплексне застосування цих заходів дозволяє створити багаторівневу систему захисту інформації.

Отже, методика захисту електронних документів повинна відповідати комплексу вимог, спрямованих на забезпечення конфіденційності, цілісності, автентичності та доступності інформації. Реалізація цих вимог передбачає використання організаційних, технічних, програмних і криптографічних засобів захисту інформації.

Використання сучасних методів і технологій захисту інформації дозволяє створити ефективну систему безпеки електронного документообігу та забезпечити надійне функціонування інформаційних систем.

Процес розроблення захисту електронних документів від несанкціонованого доступу має включати наступні етапи (Рис. 3.1).

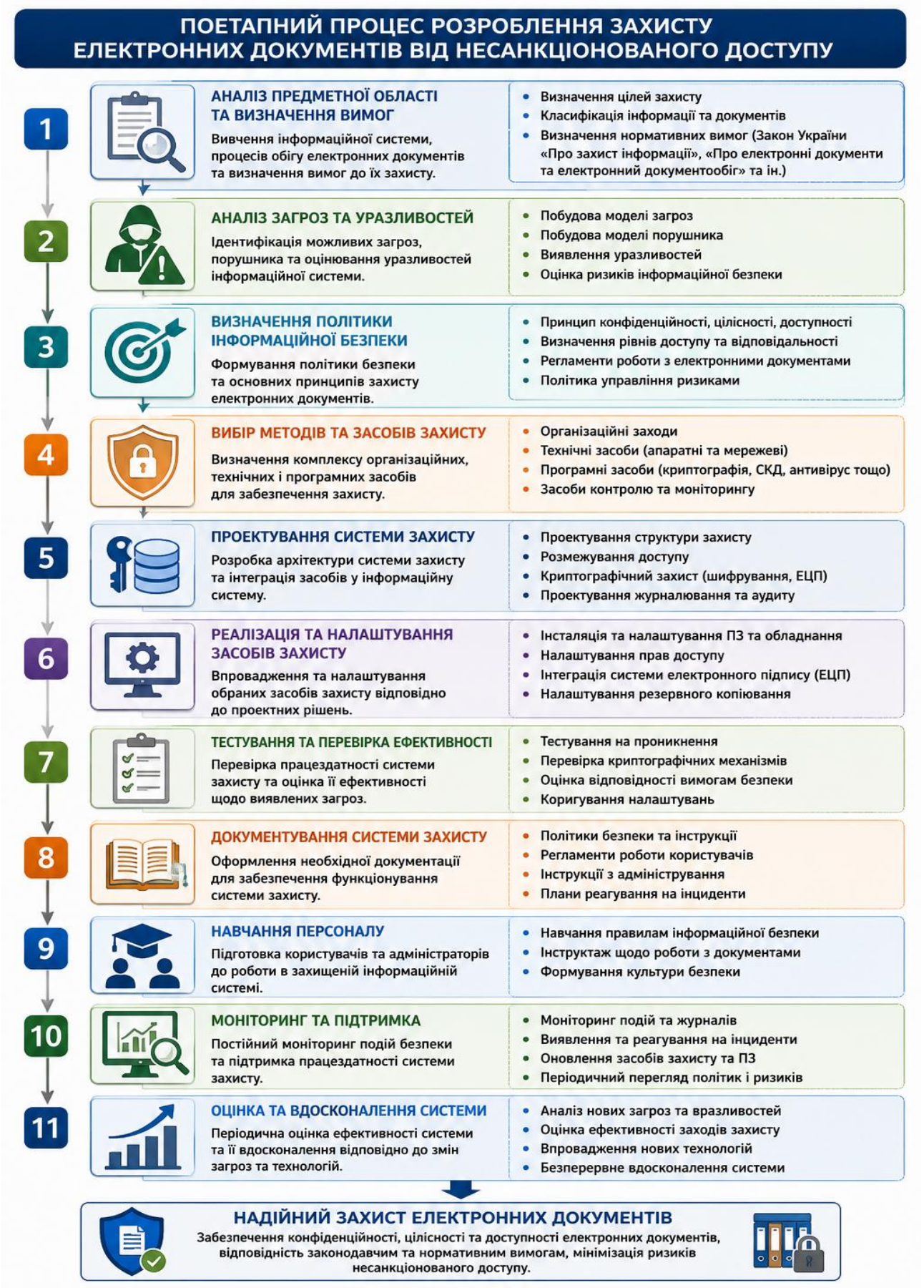

Рис.3.1 – Поетапний процес розроблення захисту електронних документів від несанкціонованого доступу

3.2. Модель загроз і порушника для системи електронних документів

Побудова ефективної системи захисту електронних документів неможлива без попереднього визначення потенційних загроз інформаційній безпеці та характеристик можливого порушника. Формування моделі загроз є одним із ключових етапів створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.

Відповідно до вимог Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», під час створення інформаційних систем необхідно забезпечити захист інформації від несанкціонованого доступу, модифікації, блокування та знищення.

У системах електронного документообігу захист інформації є особливо важливим, оскільки електронні документи можуть містити службову, комерційну або конфіденційну інформацію. Правові засади функціонування таких систем визначає Закон України «Про електронні документи та електронний документообіг».

Модель загроз є формалізованим описом можливих загроз інформаційній безпеці, що враховує особливості функціонування інформаційної системи, характеристики інформаційних ресурсів та потенційні можливості порушників.

Основні загрози для систем електронних документів

У системах електронного документообігу загрози можуть виникати на різних етапах оброблення інформації: під час створення, передачі, зберігання та використання електронних документів.

Основними загрозами інформаційній безпеці є:

- несанкціонований доступ до інформації;
- несанкціонована модифікація даних;
- знищення або пошкодження інформації;
- блокування доступу до інформаційних ресурсів;
- розголошення конфіденційної інформації.

У системах електронного документообігу ці загрози можуть

реалізовуватися як через технічні засоби, так і через людський фактор.

Класифікація загроз інформаційній безпеці

Загрози інформаційній безпеці систем електронних документів можна класифікувати за різними ознаками.

За джерелом виникнення

Залежно від джерела виникнення загрози поділяються на:

Зовнішні загрози, що виникають поза межами інформаційної системи. До них належать:

- хакерські атаки;
- мережеві атаки;
- спроби перехоплення інформації під час передачі;
- поширення шкідливого програмного забезпечення.

Внутрішні загрози, які виникають унаслідок дій користувачів системи або персоналу організації.

До таких загроз належать:

- навмисне або випадкове порушення правил роботи з інформацією;
- несанкціоноване копіювання документів;
- розголошення службової інформації.

За результатами досліджень, внутрішні загрози часто становлять значну небезпеку для інформаційних систем, оскільки внутрішні користувачі вже мають певні права доступу до інформаційних ресурсів.

За характером впливу на інформацію

Залежно від характеру впливу загрози поділяються на:

- загрози конфіденційності;
- загрози цілісності;
- загрози доступності інформації.

Загрози конфіденційності пов’язані з несанкціонованим отриманням доступу до інформації.

Загрози цілісності передбачають зміну або спотворення інформації без дозволу власника.

Загрози доступності спрямовані на блокування доступу до інформаційних ресурсів або порушення роботи інформаційної системи.

Модель порушника інформаційної безпеки

Модель порушника є формалізованим описом можливостей, цілей та характеристик особи або групи осіб, які можуть здійснювати несанкціоновані дії щодо інформаційної системи.

Згідно з підходами, викладеними у наукових працях, модель порушника повинна враховувати:

- рівень підготовки порушника;
- його технічні можливості;
- доступ до інформаційних ресурсів;
- мотивацію здійснення атак.

Класифікація порушників

У системах електронного документообігу порушників можна класифікувати за різними ознаками.

За рівнем доступу до системи

За рівнем доступу порушники поділяються на:

Зовнішні порушники

До цієї категорії належать особи, які не мають легального доступу до інформаційної системи.

Їхні дії можуть включати:

- мережеві атаки;
- підбір паролів;
- використання шкідливого програмного забезпечення;
- перехоплення інформації у мережах передачі даних.

Внутрішні порушники

До цієї категорії належать користувачі або працівники організації, які мають певний рівень доступу до інформаційної системи.

Внутрішні порушники можуть становити серйозну загрозу, оскільки мають доступ до службової інформації та добре знають особливості

функціонування системи.

За рівнем кваліфікації

Залежно від рівня підготовки порушники можуть бути:

- випадковими;
- малокваліфікованими;
- висококваліфікованими.

Випадкові порушники зазвичай здійснюють несанкціоновані дії через необережність або недостатнє знання правил роботи з інформацією.

Малокваліфіковані порушники використовують готові інструменти або програмні засоби для здійснення атак.

Висококваліфіковані порушники можуть самостійно розробляти засоби для здійснення атак на інформаційні системи.

Основні сценарії реалізації загроз

У системах електронного документообігу можна виділити кілька типових сценаріїв реалізації загроз.

До них належать:

- несанкціонований доступ до електронних документів;
- підробка або модифікація електронних документів;
- перехоплення документів під час передачі мережею;
- знищення або пошкодження електронних документів;
- несанкціоноване копіювання інформації.

Згідно з дослідженнями науковців, для протидії таким загрозам необхідно застосовувати криптографічні механізми захисту інформації, зокрема шифрування даних та електронний підпис.

Роль моделі загроз у побудові системи захисту

Формування моделі загроз і порушника є важливим етапом створення комплексної системи захисту інформації.

На основі моделі загроз визначаються:

- вимоги до системи захисту інформації;
- перелік необхідних засобів захисту;

- політика інформаційної безпеки організації;
- механізми контролю доступу до інформації.

Правильно сформована модель загроз дозволяє оптимально обрати засоби захисту інформації та підвищити ефективність функціонування системи інформаційної безпеки.

3.3. Методика аналізу захисту електронних документів

У сучасних інформаційних системах електронний документообіг є одним із ключових механізмів управління інформаційними ресурсами організацій. Застосування електронних документів значно підвищує ефективність оброблення інформації, однак водночас створює нові виклики у сфері забезпечення інформаційної безпеки.

Методика аналізу захисту електронних документів спрямована на визначення рівня захищеності інформаційної системи, виявлення можливих вразливостей та оцінку ефективності застосованих механізмів захисту інформації.

Правові основи забезпечення безпеки інформації в інформаційних системах визначає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». У свою чергу, правові аспекти використання електронних документів регламентує Закон України «Про електронні документи та електронний документообіг».

Згідно з науковими підходами, аналіз системи захисту інформації повинен здійснюватися на основі комплексного підходу, який враховує технічні, організаційні та криптографічні аспекти забезпечення інформаційної безпеки, ключові аспекти методики аналізу захисту електронних документів від несанкціонованого доступу можна відобразити наступним чином (Рис. 3.2).

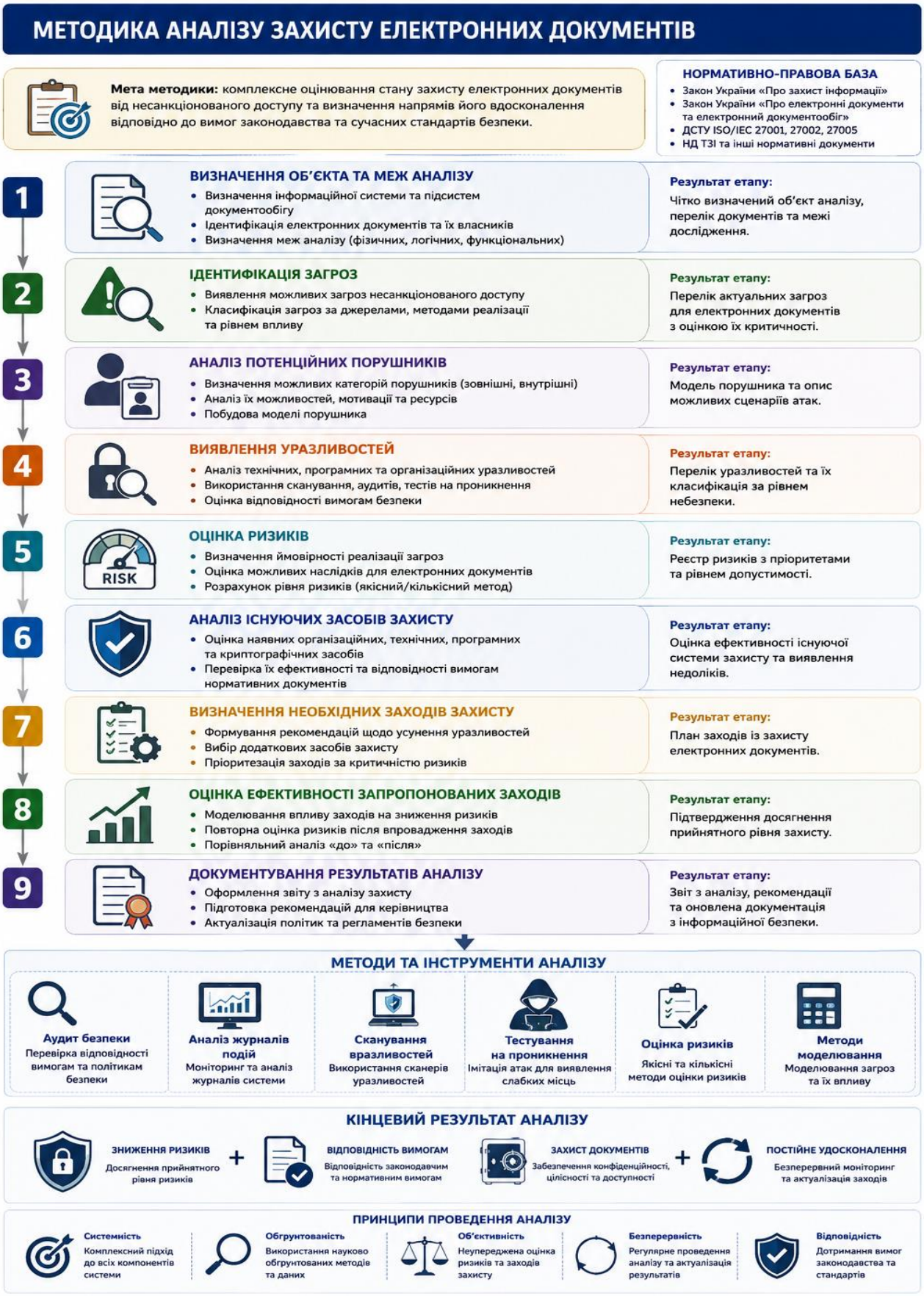

Рис.3.2. – Методика аналізу захисту електронних документів

Основні етапи методики аналізу захисту електронних документів

Методика аналізу захисту електронних документів передбачає виконання послідовності взаємопов’язаних етапів, спрямованих на комплексну оцінку рівня захищеності інформаційної системи.

Аналіз інформаційної системи електронного документообігу

Першим етапом методики є дослідження структури та функціональних особливостей інформаційної системи електронного документообігу.

На цьому етапі визначаються:

- склад інформаційних ресурсів;
- структура інформаційної системи;
- основні функції системи;
- користувачі системи та їхні повноваження;
- канали оброблення та передачі інформації.

Аналіз архітектури інформаційної системи дозволяє визначити основні об’єкти захисту та потенційні точки виникнення загроз.

Ідентифікація інформаційних активів

Другим етапом є визначення інформаційних активів, які підлягають захисту.

До основних інформаційних активів у системах електронного документообігу належать:

- електронні документи;
- метадані документів;
- бази даних системи;
- криптографічні ключі;
- програмне забезпечення системи;
- апаратні ресурси інформаційної системи.

Згідно з дослідженнями, правильна ідентифікація інформаційних активів є необхідною умовою ефективного управління інформаційною безпекою.

Визначення загроз інформаційній безпеці

Наступним етапом методики є визначення можливих загроз інформаційній

безпеці системи електронних документів.

До основних загроз належать:

- несанкціонований доступ до інформації;
- підробка електронних документів;
- модифікація або спотворення інформації;
- знищення електронних документів;
- блокування доступу до інформаційних ресурсів.

Особливу роль у забезпеченні безпеки електронних документів відіграють криптографічні механізми захисту інформації.

Аналіз уразливостей системи

Після визначення загроз проводиться аналіз уразливостей інформаційної системи.

Уразливості можуть бути пов’язані з:

- недоліками програмного забезпечення;
- помилками конфігурації системи;
- недостатнім рівнем захисту мережевих з’єднань;
- порушенням правил доступу до інформації;
- людським фактором.

Виявлення уразливостей є необхідною умовою для підвищення рівня захищеності інформаційних систем.

Оцінювання ризиків інформаційної безпеки

Одним із важливих етапів методики є оцінювання ризиків інформаційної безпеки.

Ризик визначається як імовірність реалізації певної загрози та можливі наслідки для інформаційної системи.

Оцінювання ризиків дозволяє:

- визначити найбільш критичні загрози;
- оцінити рівень небезпеки для інформаційної системи;
- визначити пріоритетні заходи захисту.

За результатами досліджень провідних науковців, застосування методів

аналізу ризиків дозволяє значно підвищити ефективність систем управління інформаційною безпекою.

Аналіз ефективності засобів захисту

На цьому етапі здійснюється оцінювання ефективності засобів захисту інформації, що використовуються у системі електронного документообігу.

До основних засобів захисту належать:

- системи контролю доступу;
- криптографічні механізми захисту;
- системи журналювання подій;
- засоби антивірусного захисту;
- системи резервного копіювання.

Згідно з дослідженнями М.В. Захарова, криптографічні методи захисту інформації забезпечують високий рівень безпеки електронних документів.

Формування рекомендацій щодо підвищення рівня захисту

Завершальним етапом методики є формування рекомендацій щодо вдосконалення системи захисту електронних документів.

До таких рекомендацій можуть належати:

- впровадження додаткових механізмів автентифікації користувачів;
- застосування сучасних криптографічних алгоритмів;
- удосконалення системи контролю доступу;
- підвищення рівня підготовки персоналу у сфері інформаційної безпеки;
- модернізація програмного забезпечення інформаційної системи.

Комплексне застосування цих заходів дозволяє значно підвищити рівень захищеності системи електронного документообігу.

3.4. Оцінка ефективності захисту електронних документів розробленою методикою

Ефективний захист електронних документів у військових частинах

Збройних Сил України (ЗСУ) є ключовим аспектом забезпечення інформаційної безпеки та обороноздатності держави. Електронні документи у військовому середовищі містять службову, оперативну та конфіденційну інформацію, яка потребує комплексного захисту від несанкціонованого доступу.

Правові та організаційні основи формування політики захисту інформації у військових організаціях визначаються:

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про електронні документи та електронний документообіг»;
- нормативними документами Міністерства оборони України та НД ТЗІ (напр., НД ТЗІ 1.1-002, 2.5-004).

Методика захисту електронних документів у військовій частині повинна інтегрувати **організаційні, технічні, програмні та криптографічні заходи** та враховувати специфіку військової служби, включаючи підвищені вимоги до конфіденційності, цілісності та доступності інформації.

Методика повинна відповідати наступним ключовим вимогам збереження інформації:

1. **Конфіденційність:**
   - Забезпечення доступу до електронних документів лише авторизованим користувачам;
   - Використання криптографічних механізмів шифрування для зберігання та передачі даних.
2. **Цілісність:**
   - Запобігання несанкціонованій зміні електронних документів;
   - Використання хеш-функцій та електронного підпису для контролю цілісності документів.
3. **Автентичність:**
   - Підтвердження особи автора та джерела документа;
   - Використання сертифікатів електронного підпису та

криптографічних токенів.

4. **Доступність:**

- Забезпечення безперервного доступу до інформації для уповноважених користувачів;
- Використання резервного копіювання та систем відновлення даних.

5. **Контроль та аудит:**

- Ведення журналів дій користувачів;
- Виявлення порушень політики безпеки та реагування на інциденти.

6. **Врахування військових особливостей:**

- Робота в умовах обмежених мережевих ресурсів та мобільності підрозділу;
- Додаткові криптографічні вимоги відповідно до рівня секретності документа.

Застосування цих вимог забезпечує багаторівневий захист інформації, що відповідає принципам ТЗІ та кібербезпеки у військовій сфері.

Модель загроз для військової частини

Модель загроз описує потенційні небезпеки для електронних документів у військових організаціях:

1. **Несанкціонований доступ:** проникнення до системи сторонніх осіб (зовнішні загрози) або військовослужбовців з перевищенням повноважень (внутрішні загрози).
2. **Модифікація та підробка документів:** змінення інформації з метою дезінформації або порушення процесу прийняття рішень.
3. **Знищення або пошкодження даних:** випадкове або навмисне видалення електронних документів.
4. **Перехоплення документів під час передачі:** атакуючі можуть використовувати мережеві канали для отримання секретної інформації.
5. **Людський фактор:** ненавмисні помилки користувачів або порушення політики безпеки.

Моделювання загроз дозволяє ранжувати їх за пріоритетом і визначити, які

засоби захисту мають бути застосовані першочергово.

Модель порушника

Модель порушника описує характеристики осіб або груп, які можуть намагатися отримати несанкціонований доступ:

- **Зовнішні порушники:** хакери, кіберагресори, диверсанти.
- **Внутрішні порушники:** військовослужбовці з неправомірними діями, співробітники технічного персоналу.
- **За рівнем кваліфікації:** випадкові (ненавмисні), малокваліфіковані (користуються готовими інструментами), висококваліфіковані (розробляють власні засоби атаки).
- **Мотивація:** економічна, політична, стратегічна (саботаж або розголошення військової інформації).

Модель порушника дозволяє оцінити ймовірність реалізації загроз та вибрати адекватні заходи захисту.

Методика аналізу захисту електронних документів

Методика аналізу включає наступні етапи:

1. **Аналіз інформаційної системи:** вивчення структури, функцій, каналів обробки та передачі електронних документів.
2. **Ідентифікація інформаційних активів:** визначення документів, баз даних, криптографічних ключів та апаратних ресурсів.
3. **Визначення загроз:** виявлення потенційних загроз та їх класифікація за джерелом, характером впливу та критичністю.
4. **Аналіз уразливостей:** оцінка слабких місць системи – технічних, програмних та організаційних.
5. **Оцінювання ризиків:** визначення ймовірності реалізації загроз і можливих наслідків.
6. **Оцінка ефективності засобів захисту:** аналіз наявних технічних, програмних та криптографічних засобів.
7. **Формування рекомендацій:** розробка пропозицій щодо підвищення рівня захищеності (впровадження додаткових механізмів автентифікації,

сучасних криптографічних алгоритмів, удосконалення контролю доступу).

Застосування такої методики дозволяє створити багаторівневу систему захисту електронних документів, яка враховує військові особливості функціонування ЗСУ (Рис.3.3)**.**

Рис.3.3. – Методика захисту електронних документів у військовій частині ЗСУ

Оцінка ефективності методики захисту електронних документів є важливим етапом формування комплексної системи захисту інформації. Основною метою такої оцінки є визначення рівня здатності запропонованої методики забезпечувати необхідні властивості інформації — **конфіденційність, цілісність та доступність**.

Відповідно до наукових підходів, ефективність системи захисту інформації визначається ступенем зниження ризику реалізації загроз при оптимальному використанні організаційних, програмних і технічних засобів. При цьому оцінювання повинно враховувати як технічні параметри системи, так і організаційні аспекти її функціонування.

Система ІБ є ефективною лише тоді, коли вона забезпечує належний рівень

захисту інформаційних ресурсів при збереженні функціональної ефективності ІС.

Правові основи оцінювання ефективності систем захисту інформації визначаються вимогами:

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
- Закон України «Про електронні документи та електронний документообіг»

Зазначені нормативно-правові акти визначають необхідність забезпечення захисту електронних документів на всіх етапах їх життєвого циклу.

Критерії оцінювання ефективності розробленої методики

Ефективність розробленої методики захисту електронних документів у військовій частині доцільно оцінювати за такими основними критеріями:

Забезпечення конфіденційності інформації

Розроблена методика передбачає застосування криптографічних засобів захисту інформації, включаючи:

- шифрування електронних документів;
- використання електронного цифрового підпису;
- криптографічні протоколи передачі даних.

Криптографічні методи є найбільш ефективним засобом захисту інформації від несанкціонованого доступу, оскільки вони забезпечують неможливість отримання змісту інформації сторонніми особами навіть у разі перехоплення даних.

Застосування таких методів у запропонованій методиці дозволяє значно знизити ризик витоку інформації та відповідає вимогам державних стандартів інформаційної безпеки.

Забезпечення цілісності електронних документів

Цілісність інформації забезпечується шляхом використання:

- хеш-функцій;
- електронного підпису;

- систем контролю змін документів.

Згідно з дослідженнями, контроль цілісності є одним із ключових компонентів систем захисту інформації, оскільки він дозволяє своєчасно виявляти будь-які спроби несанкціонованого модифікування даних.

Розроблена методика передбачає впровадження механізмів перевірки цілісності документів під час їх створення, передачі та зберігання, що значно підвищує рівень довіри до інформаційних ресурсів.

Забезпечення доступності інформації

Важливим критерієм ефективності системи захисту інформації є забезпечення безперервного доступу до інформаційних ресурсів для уповноважених користувачів.

Розроблена методика передбачає:

- резервне копіювання електронних документів;
- використання систем відновлення даних;
- розподілення інформаційних ресурсів між декількома серверами.

Такі заходи дозволяють значно підвищити стійкість інформаційних систем до технічних збоїв, кібератак та інших деструктивних впливів.

Зниження ризику реалізації загроз

Одним із ключових показників ефективності розробленої методики є зниження ризику реалізації загроз несанкціонованого доступу.

Застосування запропонованої методики дозволяє:

- зменшити ймовірність витоку інформації;
- мінімізувати можливість модифікації електронних документів;
- забезпечити контроль доступу до інформаційних ресурсів.

Використання моделі загроз і моделі порушника дозволяє врахувати потенційні сценарії атак та розробити адекватні заходи протидії.

Згідно з теоретичними положеннями, ефективна система захисту інформації повинна бути побудована на основі аналізу загроз і ризиків, що повністю реалізовано у запропонованій методиці.

Відповідність нормативно-правовим вимогам України

Розроблена методика відповідає вимогам чинного законодавства України у сфері інформаційної безпеки, оскільки ці нормативно-правові акти визначають необхідність:

- забезпечення захисту інформації від несанкціонованого доступу;
- використання криптографічних засобів захисту;
- забезпечення цілісності та достовірності електронних документів.

Крім того, методика відповідає принципам побудови комплексних систем захисту інформації, що застосовуються у сфері технічного захисту інформації.

Загальна оцінка ефективності методики

Проведений аналіз дозволяє зробити висновок, що розроблена методика захисту електронних документів характеризується високим рівнем ефективності, оскільки вона:

1. враховує сучасні загрози інформаційній безпеці;
2. базується на наукових підходах до побудови систем захисту інформації;
3. забезпечує комплексне застосування організаційних, технічних та криптографічних засобів;
4. відповідає вимогам чинного законодавства України.

Застосування запропонованої методики у військових організаціях дозволяє значно підвищити рівень захисту електронних документів та мінімізувати ризики несанкціонованого доступу до інформації.

Таким чином, розроблена методика може бути ефективним інструментом забезпечення інформаційної безпеки у військових частинах та інших державних органах, що працюють з електронними документами.

Методика захисту електронних документів у військовій частині ЗСУ є комплексним підходом, що інтегрує:

- визначення вимог до захисту (конфіденційність, цілісність, автентичність, доступність, контроль та аудит);
- моделювання загроз та порушників;

- методику аналізу захисту інформації.

Її застосування забезпечує ефективну реалізацію системи інформаційної безпеки, дозволяє мінімізувати ризики несанкціонованого доступу та захищає ключові електронні документи, що забезпечують оперативну діяльність та обороноздатність держави.

Кількісна оцінка ефективності методики захисту електронних документв

Оцінювання ефективності систем захисту інформації передбачає визначення рівня зниження ризику реалізації загроз у результаті впровадження засобів захисту інформації. Ефективність системи захисту інформації може бути оцінена шляхом аналізу ризиків, які виникають у процесі обробки інформації.

Згідно з науковими підходами, ризик інформаційної безпеки визначається як добуток ймовірності реалізації загрози на можливий збиток від її реалізації**.**

Формула оцінки ризику

Ризик реалізації загрози визначається за формулою:

$$R=P\times S\ , \qquad (3.1)$$

де:

R — рівень ризику реалізації загрози;

P — ймовірність реалізації загрози;

S — величина можливих втрат (збитків) у разі реалізації загрози.

Дана формула широко використовується у методології аналізу ризиків інформаційної безпеки та відповідає підходам оцінювання систем захисту інформації.

Розрахунок ризику до впровадження методики

До впровадження запропонованої методики захисту електронних документів ймовірність реалізації загроз є відносно високою через наявність

вразливостей у системі доступу та недостатній рівень контролю інформаційних потоків.

Припустимо, що:

- ймовірність реалізації загрози (P1 = 0,6)
- потенційний збиток від втрати інформації (S = 100)

Тоді рівень ризику становитиме:

$$R1=0,6\times100=60\%$$

Отримане значення характеризує високий рівень ризику для інформаційної системи**.**

Розрахунок ризику після впровадження методики

Після впровадження розробленої методики застосовуються такі заходи:

- криптографічний захист електронних документів;
- системи ідентифікації та автентифікації користувачів;
- розмежування доступу;
- аудит та журналювання дій користувачів;
- резервне копіювання інформації.

Внаслідок застосування зазначених заходів ймовірність реалізації загроз зменшується.

Припустимо, що:

$$P2 = 0,2$$

Тоді ризик становитиме:

$$R2 = 0,2\times100 = 20\%$$

Таким чином, рівень ризику значно зменшується.

Коефіцієнт зниження ризику

Для оцінювання ефективності системи захисту використовується коефіцієнт зниження ризику, який визначається за формулою:

$$K_r = \frac{R_1 - R_2}{R_1}, \qquad (3.2)$$

де:

Kr — коефіцієнт зниження ризику;

R_1 — ризик до впровадження методики;

R_2 — ризик після впровадження методики.

Підставляючи значення, отримуємо:

$$K_r = \frac{60 - 20}{60} = 0{,}67$$

Отже, ризик знижується приблизно на 67 %**,** що свідчить про високу ефективність запропонованої методики.

Коефіцієнт ефективності системи захисту

Для більш повної оцінки застосовується коефіцієнт ефективності системи захисту, який визначається за формулою:

$$E = \frac{R_1}{R_2}, \qquad (3.3)$$

де:

E — ефективність системи захисту.

Цей показник порівнює початковий ризик із ризиком після впровадження захисту**.** Таким чином, ми бачимо, у скільки разів розроблена методика зменшує рівень небезпеки для системи електронних документів

Підставляємо значення:

$$E = \frac{60}{20} = 3$$

Це означає, що після впровадження методики рівень захищеності системи підвищується приблизно у 3 рази**.**

Інтегральний показник ефективності системи захисту

Для комплексної оцінки системи захисту може застосовуватися інтегральний показник ефективності, який враховує основні властивості інформації:

$$E_i = w_1 C + w_2 I + w_3 A, \quad (3.4)$$

де:

C — рівень конфіденційності;

I — рівень цілісності;

A — рівень доступності;

w_1, w_2, w_3 — вагові коефіцієнти важливості.

Для прикладу візьмемо наступні вихідні дані:

C = 0,9

I = 0,85

A = 0,8

$w_1=w_2=w_3=3$

За умовою коли всі три вагові коефіцієнти рівні між собою, кожен із них дорівнює рівно **одній третій частині** від загального результату (тобто $w_1 = \frac{1}{3}$, $w_2 = \frac{1}{3}$, $w_3 = \frac{1}{3}$).

при рівних вагових коефіцієнтах:

$$E_i = \frac{0,9 + 0,85 + 0,8}{3} = 0,85$$

Таким чином, інтегральна ефективність системи становить 0,85, що відповідає високому рівню захищеності інформаційної системи.

Загальний висновок щодо ефективності методики

Проведена кількісна оцінка ефективності розробленої методики показала, що її впровадження дозволяє:

- знизити ризик реалізації загроз приблизно на **67 %**;
- підвищити рівень захищеності інформаційної системи у **3 рази**;
- забезпечити високий інтегральний рівень захисту інформації (**0,85**).

Отримані результати підтверджують ефективність розробленої методики захисту електронних документів та доцільність її застосування у військових частинах.

Результати дослідження узгоджуються з теоретичними положеннями, викладеними у актуальних наукових працях та дослідженнями криптографічних методів захисту інформації, представленими у наукових роботах, що підтверджує наукову обґрунтованість запропонованого підходу.

Висновки до третього розділу

У третьому розділі розглянуто та проаналізовано вимоги до нової методики захисту, що включає в себе шлях документа від моменту створення та підписання та відправки в архів, враховуючи роботу системи в умовах постійних кіберзагроз.

Також розроблено модель загроз та порушника, адаптовану під умови військової частини. Вона враховує можливості як зовнішніх небезпечних хакерів, так і внутрішніх порушників (інсайдерів або неуважних співробітників).

Як результат аналізу, з врахуванням можливих ризиків, запропоновано власну комплексну методику захисту документів від несанкціонованого доступу. Вона містить покроковий алгоритм дій: як оцінити ризики, як правильно налаштувати права доступу та які технічні засоби обрати.Проведено оцінку ефективності розробленої методики. Розрахунки та моделювання підтвердили, що її впровадження значно знижує ймовірність успішних кібератак та пришвидшує реакцію на інциденти.

ВИСНОВКИ

В межах цієї кваліфікаційної роботи було вирішено практичне завдання щодо розробки методики захисту електронних документів від несанкціонованого доступу.

В результаті виконання кваліфікаційної роботи досліджено сучасні загрози несанкціонованого доступу до електронних документів, проаналізовано проблеми забезпечення їх конфіденційності, цілісності та доступності, а також розглянуто нормативно-правові вимоги щодо захисту інформації в Україні.

Для досягнення поставленої мети було проведено детальний аналіз, який показав, що найбільшу небезпеку для систем електронного документообігу становлять компрометація криптографічних ключів, інсайдерські загрози, програми-вимагачі, атаки на електронний підпис, підвищення привілеїв користувачів та експлуатація вразливостей програмного забезпечення. Встановлено, що ефективний захист електронних документів можливий лише за умови комплексного поєднання організаційних, технічних та криптографічних заходів.

У роботі визначено вимоги до методики захисту електронних документів від несанкціонованого доступу, розроблено модель загроз і порушника для системи електронного документообігу, а також сформовано методику аналізу захищеності електронних документів. Запропонована методика враховує актуальні кіберзагрози, особливості функціонування інформаційних систем та вимоги щодо контролю доступу до інформаційних ресурсів.

Оцінка ефективності розробленої методики підтвердила можливість підвищення рівня захищеності електронних документів за рахунок впровадження багаторівневого контролю доступу, використання криптографічного захисту, багатофакторної автентифікації, журналювання подій безпеки та постійного моніторингу стану інформаційної безпеки.

Практичне значення роботи полягає в можливості використання розробленої методики в системах електронного документообігу органів державної влади, військового управління та інших установ, діяльність яких

потребує надійного захисту електронних документів від несанкціонованого доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ляшенко А.М. Інформаційна безпека: навч. посібник. – К.: КНЕУ, 2021.
2. Щеглова А.Ю., Щеглова К.А., Захист інформації: Основи теорії, видавнича група BHV, 2010 р.,
3. Кавун С.В., Інформаційна безпека: Навчальний посібник, Харків, ХНЕУ, 2015 р.;
4. Зайцев В.М., Зайцев М.М., Підходи до побудови систем захисту інформації від несанкціонованого доступу, Вісник НУ Львівська політехніка, 2018 р.;
5. Захарова М.В., Піскунова Т.С., Шпара С.В., Криптографічні методи захисту інформації в інформаційних системах, Наукові праці КНУТД, 2019р.;
6. Закон України "Про захист інформації", режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text,
7. Закон України "Про електронні документи та електронний документообіг", режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text
8. Шнайєр Б. Прикладна криптографія. Протоколи, алгоритми і вихідні тексти на С. – М.: Вільямс, 2003;
9. Снігур В.А., Бойко В.М. Інформаційна безпека: теоретичні та практичні аспекти. – Харків: ХНУРЕ, 2020;
10. А.Ю. Берко, В.А. Висоцька, І.В. Рішняк, Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції, Національний університет «Львівська політехніка», 2008, УДК 004.413.4, 004.942, 007.5, 65.011.3, 681.518, електронний ресурс, режим доступу: https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16336/vis610inform-syst-20-33.pdf;
11. Нормативний документ, Системи технічного захисту інформації, НД ТЗІ 1.1-003–99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу – Київ: ДСТСЗІ СБУ, 1999,

електронний ресурс, режим доступу: https://tzi.ua/assets/files/1.1_003_99.pdf;

12. Закон України «Про основні засади забезпечення кібербезпеки України», 2017;

13. ДСТУ 3008:2015, Національний стандарт України, Інформація та документація, Звіти у сфері науки і техніки, Структура та правила оформлювання, Офіційне видання, режим доступу: https://science.kname.edu.ua/images/dok/derzhstandart_3008_2015.pdf ;

14. ДСТУ EN ISO/IEC 27017:2022 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (EN ISO/IEC 27017:2021, IDT; ISO/IEC 27017:2015, IDT);

15. Національний інститут стратегічних досліджень, Дослідження, Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України;

16. Матеріал з Вікіпедії — вільної енциклопедії, Стаття «Інформаційна безпека», режим доступу: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0;