ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Криптографічні методи захисту конфіденційної інформації в організаціях»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Владислав ЛИТВИНЮК
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
ЛИТВИНЮК Владислав
(прізвище, ім'я)

Керівник д. т. н., професор,Кожухівський А.Д.
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. У сучасному цифровому світі конфіденційна інформація — це не просто дані, а стратегічний ресурс, від якого залежить успіх організацій. Її втрата або компрометація може спричинити фінансові збитки, юридичні наслідки та втрату довіри клієнтів. Зростання кіберзагроз, таких як фішинг, шкідливе ПЗ чи соціальна інженерія, робить захист даних не просто важливим, а критично необхідним.

Активне використання хмарних технологій, віддаленої роботи та IoT-пристроїв відкриває нові можливості, але й створює додаткові ризики. Наприклад, один необережний клік у фішинговому листі може запустити ланцюг подій, що призведе до витоку даних. Тому сучасні організації зобов'язані впроваджувати надійні механізми захисту, зокрема криптографічні методи, які відповідають міжнародним стандартам та вимогам національного законодавства.

Об'єкт дослідження. Процеси застосування криптографічних методів захисту інформації в корпоративних інформаційних системах, зокрема механізми їх впровадження та ефективність у реальних умовах експлуатації.

Предмет дослідження. Сучасні криптографічні алгоритми та технології, які можуть бути використані для ефективного захисту конфіденційної інформації в організаціях.

Мета роботи. Дослідити сучасні криптографічні методи захисту даних та розробити практичні рекомендації щодо їх впровадження в організаціях для протидії кіберзагрозам.

Наукові завдання:

виявити ключові загрози для конфіденційної інформації в умовах цифровізації;

дослідити принципи роботи сучасних алгоритмів шифрування;

порівняти симетричні та асиметричні методи шифрування;

оцінити роль хешування, цифрових підписів та PKI у забезпеченні безпеки;

проаналізувати відповідність криптографічних рішень законодавчим вимогам;

запропонувати практичні кроки для впровадження криптографії в організаціях.

Методи дослідження. Використаня та аналіз наукових джерел, порівняльний аналіз алгоритмів, моделювання кіберзагроз, систематизацію практик та аналіз нормативно-правової бази.

Практичне значення одержаних результатів. Отримані результати можуть бути використані фахівцями з інформаційної безпеки для вдосконалення криптографічного захисту даних у корпоративних мережах, оптимізації алгоритмів шифрування під конкретні бізнес-процеси та розробки ефективних механізмів управління криптографічними ключами.

Апробація результатів. Матеріали дослідження обговорювалися з експертами з кібербезпеки, практичні рішення було протестовано в умовах, що моделюють сценарії використання методів захисту. Експерименти підтвердили ефективність запропонованих підходів, що свідчить про їхню придатність для реального використання.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЯХ

1.1 Загрози конфіденційної інформації в сучасних організаціях

У нинішньому цифровому світі інформація стала одним із найважливіших стратегічних активів, що визначає конкурентні переваги, стабільність та довготривалу життєздатність компаній. Особливої ваги набуває конфіденційна інформація — дані, доступ до яких обмежено задля забезпечення безперебійної роботи підприємств, захисту прав фізичних та юридичних осіб. До таких даних належать персональні відомості клієнтів і працівників, фінансові документи, комерційні секрети, внутрішні протоколи, стратегічні плани, результати досліджень, проєктна документація, а також інформація, що підлягає державному захисту або регулюється законодавством [2].

Зовнішні загрози

Організації все частіше стають мішенню зловмисників, які використовують дедалі витонченіші методи несанкціонованого доступу до конфіденційних даних. Мотиви таких атак варіюються від фінансової вигоди до промислового шпигунства, політичного тиску або підриву репутації компанії [4].

Фішингові атаки становлять один із найпоширеніших інструментів соціальної інженерії: зловмисники створюють правдоподібні копії корпоративних листів, вебсайтів або форм введення даних і розповсюджують їх через електронну пошту, SMS, месенджери або рекламу. Особливо небезпечними є персоналізовані повідомлення, що імітують внутрішню корпоративну комунікацію [4];

Уразливості програмного забезпечення також активно експлуатуються, особливо коли системи не отримують своєчасних оновлень безпеки. Наприклад, інциденти, пов’язані з експлойтами EternalBlue чи Log4Shell, мали масштабні наслідки для багатьох організацій у всьому світі [4];

Програми-вимагачі (ransomware) шифрують файли на уражених пристроях і вимагають викуп за їх розблокування. Найчастіше такі атаки здійснюються через фішингові листи або використання вразливостей у протоколах віддаленого доступу, як-от RDP. Часто такі атаки супроводжуються додатковим витоком даних до даркнету з метою подальшого шантажу [4];

Атаки на віддалений доступ стали особливо актуальними в умовах масового переходу на дистанційний режим роботи. Зловмисники дедалі частіше намагаються зламати VPN-з'єднання або служби RDP, особливо в тих випадках, коли працівники використовують незахищені особисті пристрої, не охоплені корпоративною політикою безпеки (BYOD) [8];

Згідно зі звітом Verizon Data Breach Investigations Report 2023, понад 60% витоків даних у приватному секторі мали зовнішнє походження, причому головними векторами атак були соціальна інженерія та компрометація облікових записів через повторне використання паролів [5].

Внутрішні загрози

Не менш серйозну небезпеку становлять внутрішні загрози, джерелом яких можуть бути як звичайні працівники, так і керівники, що мають легітимний доступ до систем.

Ненавмисні порушення безпеки трапляються через неуважність, недостатню обізнаність або ігнорування встановлених процедур. Типовими прикладами є надсилання конфіденційних документів через особисту пошту, використання загальнодоступних месенджерів або незахищених зовнішніх носіїв;

Навмисні дії з боку співробітників — це цілеспрямовані акти саботажу, промислового шпигунства або помсти. Працівник, який має доступ до критичної інформації, може свідомо її викрасти, змінити або знищити, що призводить до суттєвих наслідків для інформаційної безпеки організації;

За дослідженням *IBM 2023*, збитки від внутрішніх інцидентів у середньому на 25% перевищують втрати від зовнішніх атак. Це пояснюється складністю виявлення, збору доказів та масштабністю наслідків [5].

Технічні вразливості

використання застарілих алгоритмів (DES, MD5);

відсутність шифрування трафіку (TLS, HTTPS);

зберігання інформації без шифрування;

незахищені криптографічні ключі;

відсутність журналювання та моніторингу дій.

Недостатня реалізація систем SIEM**,** DLP**,** HSM свідчить про технічну вразливість організації.

Організаційні проблеми

формальність у політиках зберігання й обробки інформації;

нечіткі правила розподілу доступу;

відсутність аудитів і тестів на проникнення;

нехтування стандартами ISO/IEC 27001, GDPR, НД ТЗІ;

недостатнє навчання персоналу;

відсутність перевірки резервного копіювання;

недеактивовані акаунти звільнених працівників;

відсутність реалізації інцидент-менеджменту.

Наслідки

Реалізація загроз конфіденційній інформації має широкомасштабні наслідки, які зачіпають не лише технічну складову, а й стратегічні, фінансові, юридичні та репутаційні аспекти діяльності організації.

На стратегічному рівні витік або втрата критичної інформації може призвести до зриву бізнес-процесів, порушення реалізації проєктів, втрати конкурентних переваг і доступу до ринку. У випадку викрадення ноу-хау або стратегічних планів організація ризикує втратити інвестиційну привабливість та довіру з боку партнерів.

Фінансові наслідки проявляються як у прямій шкоді — витратах на усунення інциденту, сплату штрафів, компенсацій клієнтам, — так і в опосередкованих витратах, пов’язаних із простоєм систем, втратою контрактів або зниженням

вартості компанії [5]. Деякі інциденти можуть спричинити необхідність масштабної модернізації IT-інфраструктури або впровадження нових політик захисту, що вимагає значних ресурсів [8].

Юридичні наслідки охоплюють відповідальність за порушення вимог законодавства щодо захисту персональних даних, таких як GDPR, Закон України «Про захист персональних даних», НД ТЗІ та інші. За неналежний рівень захисту організація може зазнати санкцій з боку регуляторних органів, а також стати об’єктом судових позовів від постраждалих осіб або контрагентів [2].

Репутаційні втрати, хоч і не завжди одразу вимірювані, часто є найбільш руйнівними. Після інцидентів, пов’язаних із витоком інформації, компанії втрачають довіру клієнтів, партнерів і громадськості [5]. Це призводить до зменшення клієнтської бази, складнощів у залученні нових бізнес-партнерів і зниження лояльності персоналу. У випадках, коли інциденти набувають розголосу у ЗМІ, організація змушена витрачати значні ресурси на відновлення свого іміджу.

Таким чином, наслідки реалізованих загроз виходять далеко за межі технічного інциденту і здатні впливати на довгострокову життєздатність та стабільність організації. Саме тому системний і комплексний підхід до захисту конфіденційної інформації є критично необхідним.

1.2 Основні принципи криптографічного захисту

Захист інформації за допомогою криптографічних засобів базується на впровадженні низки ключових принципів, які визначають ефективність і надійність всієї системи інформаційної безпеки [2]. В умовах інтенсивного розвитку цифрового середовища та зростання кіберризиків, криптографічні методи набувають ключового значення для забезпечення безпеки інформаційно-комунікаційних систем як при зберіганні, так і під час передавання даних. Її застосування дозволяє досягти таких критично важливих цілей, як забезпечення

конфіденційності, гарантування цілісності, підтвердження автентичності, запобігання відмовам від здійснених дій та ефективне управління криптографічними ключами. Усе це створює надійну основу для захисту електронної інформації як в особистому, так і в корпоративному та державному середовищі [3].

Криптографічний захист забезпечує низку основних функціональних властивостей, серед яких:

Конфіденційність — гарантує, що доступ до інформації матимуть виключно уповноважені особи;

Цілісність — дозволяє виявляти будь-яке несанкціоноване або випадкове втручання в інформацію;

Автентичність — забезпечує підтвердження справжності джерела даних;

Невідмовність — унеможливлює заперечення факту участі у комунікації або транзакції;

Управління ключами — охоплює всі етапи життєвого циклу криптографічних ключів.

Конфіденційність

Конфіденційність інформації означає, що доступ до неї мають лише ті суб’єкти, яким такий доступ офіційно надано згідно з політиками доступу, внутрішніми регламентами або вимогами законодавства. Вона забезпечується шляхом перетворення зрозумілого (відкритого) тексту у зашифрований формат, який є непридатним для прочитання сторонніми особами без відповідного ключа. Це досягається за допомогою спеціальних криптографічних алгоритмів.

При цьому існує два основні підходи: симетричне шифрування, при якому один і той самий ключ використовується для обох операцій — шифрування та дешифрування, та асиметричне шифрування, де застосовується пара ключів — відкритий і закритий.

Серед методів симетричного шифрування особливо ефективними вважаються алгоритми типу AES або ChaCha20, які демонструють високу

швидкодію та придатні для обробки значного обсягу інформації [6]. Водночас методи, засновані на асиметричному шифруванні — наприклад, RSA або алгоритми на базі еліптичних кривих (ECC), — забезпечують підвищений рівень безпеки при передачі ключової інформації, хоч і потребують значно більше обчислювальних ресурсів для реалізації [10].

У практичних рішеннях найчастіше застосовуються гібридні моделі, де асиметричне шифрування використовується лише для безпечного розповсюдження ключів, після чого сама інформація передається за допомогою симетричних алгоритмів.

Цілісність

Цілісність інформації означає, що дані зберігають свій первинний вигляд і не зазнають несанкціонованих змін у процесі передачі, зберігання чи обробки. Вона підтверджується за допомогою хеш-функцій, які формують унікальний дайджест (контрольну суму) повідомлення. Навіть мінімальні зміни в тексті призводять до істотних змін у результаті хешування. Сучасні хеш-функції — такі як SHA-256, SHA-3, Keccak або BLAKE2 — демонструють високу стійкість до криптографічного аналізу, зокрема до колізій та атак на пошук прообразів [9].

Для підвищення рівня захисту застосовуються також механізми MAC (Message Authentication Code), що використовують криптографічний ключ разом із хеш-функцією, забезпечуючи перевірку цілісності та автентичності водночас [9].

При застосуванні цифрових підписів, дайджест повідомлення шифрується за допомогою приватного ключа відправника, що дозволяє отримувачу перевірити цілісність і походження даних, розшифрувавши його за допомогою публічного ключа [12].

Автентичність

Автентичність гарантує, що повідомлення справді походить від заявленого відправника, а не було підмінене чи створене стороннім суб’єктом. Цей принцип є надзвичайно важливим у відкритих середовищах, де ризики атак типу «людина посередині» або спуфінгу залишаються значними.Найбільш поширеним методом

забезпечення автентичності є використання цифрових підписів на основі асиметричних криптографічних схем [12].

Для встановлення достовірності сторін під час обміну інформацією також використовуються протоколи обміну ключами з автентифікацією, наприклад, розширена схема Диффі — Гелмана або TLS. У таких протоколах передбачається перевірка особи сторони, яка ініціює з'єднання, що унеможливлює доступ до даних з боку неавторизованих суб’єктів [7].

Невідмовність

Невідмовність є важливим правовим і технічним аспектом, який забезпечує неможливість заперечення факту участі сторони у транзакції або комунікації. Це має особливе значення для електронного документообігу, фінансових операцій, надання державних послуг або проведення виборчих процесів в електронній формі.

Досягається цей принцип шляхом застосування цифрових підписів, часового маркування (timestamping), а також ведення журналів подій (audit logging), що разом дозволяють підтвердити факт взаємодії сторін у визначений момент часу [12].

Управління криптографічними ключами

Управління криптографічними ключами є критичним фактором у побудові ефективної криптографічної інфраструктури. Воно охоплює повний життєвий цикл ключів — від їх генерації до остаточного знищення [14]. Генерація ключів має здійснюватися із використанням надійних генераторів випадкових чисел, зокрема апаратних модулів безпеки (HSM), які відповідають вимогам міжнародних стандартів (наприклад, FIPS 140-2 або ISO/IEC 19790). Зберігання ключів повинно здійснюватися у спеціалізованих сховищах, які унеможливлюють несанкціонований доступ [1].

Розповсюдження відкритих ключів часто здійснюється через інфраструктуру відкритих ключів (PKI), яка забезпечує довіру до сертифікатів за допомогою сертифікаційних центрів (CA), списків відкликаних сертифікатів (CRL) та протоколів онлайн-перевірки статусу сертифіката (OCSP) [3]. Ротація ключів,

своєчасне відкликання та заміна скомпрометованих ключів є ключовими умовами підтримання актуальності системи захисту.

Сучасні концепції інформаційної безпеки все частіше впроваджують принцип мінімізації довіри, відомий як Zero Trust. Згідно з цією концепцією, жоден користувач або пристрій не вважається безумовно довіреним, навіть якщо він знаходиться у внутрішній мережі організації [8]. Кожен запит до ресурсу має бути перевірений, автентифікований та дозволений відповідно до політик доступу.

У контексті криптографічного захисту це означає повсюдне застосування шифрування, навіть усередині корпоративної мережі, використання багатофакторної автентифікації (MFA), обмеження прав доступу за принципом найменших привілеїв, а також впровадження контрольованих протоколів обміну ключами.

Такий підхід дозволяє суттєво знизити ризики, пов’язані з внутрішніми загрозами або скомпрометованими вузлами мережі.

Особливу увагу при впровадженні криптографічного захисту слід приділяти нормативно-правовому забезпеченню. Міжнародні стандарти, зокрема ISO/IEC 27001 (система управління інформаційною безпекою), ISO/IEC 19790 (вимоги до криптографічних пристроїв), ISO/IEC 11770 (управління ключами криптографічних засобів захисту інформації), та керівництво Національного інституту стандартів і технологій (NIST), зокрема серія SP 800, є важливими орієнтирами при створенні ефективних криптографічних рішень [1].

В українському контексті слід керуватись вимогами Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», технічними документами НД ТЗІ, зокрема НД ТЗІ 2.5-004-99, та положеннями відповідних ДСТУ, які регламентують порядок впровадження криптографічного захисту на національному рівні [2].

Загалом, криптографічний захист є не просто технічним інструментом, а комплексною системою, що включає технології, процедури, політики, нормативні регламенти та управлінські рішення.

Його ефективність визначається не лише якістю обраних алгоритмів, але і грамотністю реалізації принципів безпеки, рівнем контролю над ключами та відповідністю до встановлених стандартів. Саме завдяки комплексному підходу криптографія здатна гарантувати стійкий рівень захисту в умовах зростаючих викликів цифрового світу.

1.3 Аналіз нормативно-правової бази щодо захисту конфіденційної інформаціїї

Ефективне забезпечення конфіденційності інформації у сучасних умовах цифрової трансформації суспільства неможливе без чіткого нормативно-правового регулювання. Будь-яка система інформаційної безпеки, незалежно від її масштабу чи сфери застосування, повинна ґрунтуватися не лише на технічних рішеннях, а й на суворому дотриманні законодавчих норм, які визначають дозволені механізми обробки, зберігання, передавання, шифрування, архівування та знищення даних з обмеженим доступом [2].

Законодавче підґрунтя виступає каркасом, що забезпечує узгоджене функціонування засобів захисту, попередження загроз, а також юридичну відповідальність за порушення встановлених вимог.

Основні закони України у сфері інформаційної безпеки

Національна нормативна база України у сфері захисту інформації сформована на основі ряду базових законів, кожен з яких відіграє ключову роль у правовому регулюванні відповідних відносин.

Одним з основоположних документів є Закон України «Про інформацію», що визначає класифікацію інформації, вводить поняття інформації з обмеженим доступом, встановлює обов’язки суб’єктів інформаційних відносин та надає

визначення форм захисту таких даних. У свою чергу, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» є спеціалізованим нормативним актом, який регламентує питання побудови комплексної системи захисту в ІТ-середовищі, передбачаючи обов'язковість впровадження як організаційних, так і технічних, включно з криптографічними, засобів захисту [2].

Особливу увагу приділено правовому регулюванню персональної інформації. Закон України «Про захист персональних даних» запроваджує механізми легітимного збирання, обробки, зберігання, передачі та видалення персональних відомостей, встановлюючи принципи мінімізації та цільової обробки даних, вимоги до отримання згоди суб'єкта, а також обов'язки володільця персональних даних.

Важливу роль у правовій інфраструктурі електронного середовища відіграє Закон України «Про електронні довірчі послуги», який регламентує використання електронного підпису, печаток, часових міток, а також визначає вимоги до постачальників таких послуг, забезпечуючи високий рівень довіри у цифрових взаємодіях.

Кримінально-правова відповідальність у сфері інформаційної безпеки

Кримінально-правові механізми гарантують невідворотність відповідальності за порушення у сфері інформаційної безпеки. Кримінальний кодекс України у статтях 361–363 встановлює кримінальну відповідальність за несанкціоноване втручання в роботу комп'ютерних систем, порушення правил захисту інформації та знищення чи модифікацію даних без дозволу. Це забезпечує юридичні важелі реагування на інциденти, пов'язані з компрометацією конфіденційних відомостей або зломом інформаційних систем [2].

Підзаконні акти Держспецзв'язку України

У контексті державної безпеки велике значення мають підзаконні нормативні документи, що затверджуються Державною службою спеціального зв'язку та захисту інформації. Серед нормативних документів, ухвалених Державною

службою спеціального зв'язку та захисту інформації України, ключову роль відіграють такі акти:

НД ТЗІ 2.5-004-99 – встановлює категорії інформації, що не є державною таємницею, але потребує захисту, а також визначає підходи до її класифікації;

НД ТЗІ 2.5-010-2000 – містить основоположні принципи організації криптографічного захисту інформації, зокрема вимоги до сертифікації відповідних засобів;

НД ТЗІ 1.5-003-2005 – окреслює комплекс організаційних заходів у сфері інформаційної безпеки для ІКТ-систем, включаючи багаторівневу модель доступу, облік активностей користувачів і адміністрування систем [2].

Міжнародні стандарти та практики

На міжнародному рівні основу правового регулювання становлять стандарти серії ISO/IEC. Найбільш вагомим серед них є ISO/IEC 27001:2022, який визначає вимоги до створення та вдосконалення систем управління інформаційною безпекою. Цей стандарт інтегрує концепції ризик-менеджменту, безперервного моніторингу і регулярного аудиту безпеки [2].

Додатково використовується ISO/IEC 27002:2022, що надає рекомендації за різними аспектами захисту — навіть починаючи від управління криптографічними ключами, а також призначенням резервних копій, захисту від шкідливого ПЗ та аутентифікації користувачів [14].

У сфері криптографії мають значення ISO/IEC 19790, що встановлює вимоги до безпеки криптографічних модулів, а також рекомендації NIST – SP 800-53 та SP 800-57, які визначають політики управління ключами, обмеження життєвого циклу ключів, вимоги до генерації, зберігання, передачі та знищення ключового матеріалу [14].

Європейське регулювання захисту даних (GDPR)

Особливої уваги заслуговує законодавство Європейського Союзу, зокрема Загальний регламент про захист даних (GDPR), який має екстериторіальну дію та стосується всіх організацій, що працюють з персональними даними громадян ЄС.

Регламент зобов’язує компанії впроваджувати шифрування та псевдонімізацію, вимагає повідомляти про витік даних протягом 72 годин та гарантує користувачам право на видалення їх персональних відомостей [2].

Невиконання вимог GDPR може призвести до значних фінансових санкцій, що робить його важливим інструментом підвищення відповідальності суб’єктів інформаційних відносин.

Регулювання використання криптографічних засобів

У сфері обігу криптографічних засобів встановлено чіткі вимоги як на міжнародному, так і на національному рівнях. В Україні моніторинг, сертифікацію та контроль використання криптографії здійснює Адміністрація Держспецзв’язку. Тільки сертифіковані засоби можуть бути легітимно застосовані в державних структурах. Процедура сертифікації регламентується окремими нормативами, які передбачають перевірку відповідності засобів захисту вимогам до надійності алгоритмів, стійкості до криптоаналізу та рівня інтеграції в IT-інфраструктуру [2].

На глобальному рівні діють угоди на кшталт Вассенаарських домовленостей, які координують контроль за експортом криптографічних технологій і забезпечують збалансованість між безпекою та міжнародним обігом технічних засобів [1].

Внутрішня нормативна база організацій

Окремий рівень регулювання становлять внутрішні нормативні документи, які адаптують загальні вимоги до конкретних умов функціонування установи. Сюди належать:

політики інформаційної безпеки;

інструкції щодо управління ключами;

положення з обробки персональних даних;

внутрішні регламенти шифрування та автентифікації;

протоколи реагування на інциденти.

Ці документи відіграють важливу роль у практичному впровадженні вимог безпеки, стандартизуючи діяльність усіх суб’єктів у межах організації з

урахуванням рівня ризику, структури IT-середовища та застосованих засобів захисту [2].

Таким чином, нормативно-правове регулювання у сфері захисту конфіденційної інформації становить складну ієрархічну систему, що об’єднує закони, підзаконні акти, міжнародні стандарти, а також внутрішню документацію суб’єктів господарювання.

Забезпечення належного рівня відповідності цим вимогам є не лише юридичним обов’язком, але й важливою умовою формування стійкої, надійної та відповідальної системи інформаційної безпеки, здатної ефективно реагувати на сучасні виклики кіберпростору.

2 АНАЛІЗ ІСНУЮЧИХ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

2.1 Симетричні та асиметричні алгоритми шифрування

Шифрування є фундаментальним інструментом криптографічного захисту цифрової інформації як у локальних мережах, так і в глобальному інтернет-просторі. Його основна функція — перетворення даних у форму, незрозумілу для сторонніх осіб, що гарантує конфіденційність при передаванні або зберіганні інформації. Однак на сьогодні функціональність шифрування вийшла далеко за межі простого приховування даних — воно забезпечує контроль цілісності, підтвердження достовірності, неможливість заперечення авторства та реалізацію різноманітних криптографічних сервісів (VPN, SSL/TLS, цифрові підписи, PKI тощо) [3].

Симетричне шифрування

Системи шифрування класифікують на симетричні, асиметричні та комбіновані (гібридні) — залежно від принципу роботи з ключами. Кожна з цих категорій має свої переваги, недоліки, області використання та технологічні особливості, що обумовлюють доцільність їх застосування в певних умовах.

Симетричні алгоритми передбачають використання одного і того самого секретного ключа як для зашифровування, так і для розшифрування даних. Основним плюсом таких методів є висока продуктивність і низьке навантаження на обчислювальні ресурси, що робить їх придатними для систем, які працюють у реальному часі або мають обмежені ресурси (наприклад, мобільні пристрої).

Один з найпоширеніших - це алгоритм AES (Advanced Encryption Standard), який прийнятий як стандарт FIPS 197. Він використовує багатораундову обробку даних і підтримує довжину ключів у 128, 192 або 256 біт [6].

Інші помітні симетричні шифри — це ChaCha20, оптимізований для пристроїв без апаратної підтримки AES; Blowfish, Twofish і RC4 (останній, однак,

вважається застарілим через виявлені вразливості) [13]. Незважаючи на переваги, слабким місцем симетричних систем є управління ключами. Забезпечення їх безпечного обміну, зберігання та відкликання є складним завданням, особливо в розподілених середовищах і хмарних платформах [14].

Асиметричне шифрування

Асиметричне шифрування вирішує проблему захищеного розповсюдження ключів, оскільки оперує двома ключами: відкритим, який доступний будь-кому, і закритим, що зберігається в таємниці у власника. Його криптографічна стійкість ґрунтується на складності певних математичних задач, як-от:

розкладання великих чисел на прості множники (RSA);

обчислення дискретного логарифму (ElGamal, DSA);

операції над еліптичними кривими (ECC — ECDSA, ECDH) [10].

Порівняння симетричного та асиметричного шифрування

Симетричне шифрування	
Переваги	**Недоліки**
• швидкість (на 3 порядки) • простота реалізації • менша довжина ключа для визначення стійкості	• складність управління ключами • складність обміну ключами

Асиметричне шифрування	
Переваги	**Недоліки**
• відсутність необхідності захищеного каналу • наявність тільки одного секретного ключа • число ключів в мережі менше і не росте в квадратичній залежності	• складність проведення зміни алгоритму • неможливість шифрування ID відправника та адресата • велика довжина ключа, порівняно із симетричним шифруванням

Рис. 2.1. Порівняння методів шифрування

Особливу увагу в останні роки привертає еліптична криптографія, що дозволяє отримати високий рівень захисту при менших обсягах ключової інформації. Наприклад, ECC-ключ довжиною 256 біт еквівалентний за стійкістю RSA-ключу в 3072 біти. Це робить ECC особливо привабливим для малопотужних пристроїв, таких як сенсори IoT, мобільні телефони чи смарт-карти. Проте через

відносну складність обчислень, асиметричні методи неефективні для прямого шифрування великих обсягів інформації.

Гібридні криптосистеми

Саме тому гібридні криптографічні системи, які комбінують переваги обох підходів, є найбільш практичними. Зазвичай асиметричний механізм використовується для передачі сеансового симетричного ключа, після чого подальше шифрування даних відбувається за допомогою швидких симетричних алгоритмів [6]. Наприклад, у протоколі TLS, який використовується для забезпечення HTTPS-з'єднань, відкритий ключ сервера застосовується для захищеної передачі симетричного ключа, який потім використовується для шифрування даних сесії. Такий принцип реалізований у багатьох сучасних засобах захисту: VPN (OpenVPN, WireGuard), електронна пошта (PGP), месенджери (Signal, Threema) і системи документообігу [7].

Вибір алгоритмів та нормативна база

Вибір алгоритму шифрування нерозривно пов'язаний із вимогами нормативних актів та міжнародних стандартів[1]. Наприклад, стандарти ISO/IEC 18033 та ISO/IEC 11770, а також настанови NIST, такі як FIPS 197, SP 800-56 та SP 800-57, визначають параметри криптографічних алгоритмів [2]. Вони також визначають протоколи обміну ключами та управління цими ключами, а також окреслюють політики безпеки, яких необхідно дотримуватися [10]. В умовах впровадження законодавств типу GDPR шифрування розглядається як обов'язковий елемент при обробці персональних або конфіденційних даних [2].

Квантові загрози та постквантова криптографія

З розвитком квантових обчислень існує ризик втрати криптостійкості класичних методів шифрування, таких як RSA або ECC. У зв'язку з цим активізувався розвиток постквантової криптографії (PQC), що розглядається як перспектива для довгострокового збереження безпеки даних. У найближчому майбутньому очікується поширення гібридних схем, що поєднують традиційні та квантостійкі алгоритми.

Практичні аспекти застосування

Глибоке розуміння роботи симетричних та асиметричних методів є важливою передумовою для побудови надійних інформаційних систем. Раціональне поєднання різних криптографічних технологій дозволяє створити ефективну архітектуру захисту з урахуванням поточних і майбутніх загроз.

Вибір типу шифрування залежить від характеру середовища, рівня ризиків, технічних можливостей, продуктивності та потреб у масштабованості. У корпоративних структурах, де обробка великих обсягів інформації має виконуватись швидко, як правило, використовуються симетричні алгоритми (переважно AES у режимах GCM, CBC або CTR). За їхньою допомогою можна максимально швидко обробляти дані завдяки командам AES-NI [6].

Асиметричні методи у таких системах часто застосовуються для автентифікації користувачів, цифрового підпису або обміну ключами. Симетричні шифри потокового типу (наприклад, ChaCha20) краще підходять для таких задач, як передача аудіо- й відеоінформації, тоді як блочні алгоритми ефективні для шифрування файлів або баз даних [13].

Рівень криптостійкості в асиметричних системах залежить від довжини ключів і математичних властивостей використовуваних структур. Наприклад, RSA-ключі з довжиною 1024 біти вважаються недостатньо безпечними. На сучасному етапі рекомендується застосування ключів розміром не менше 2048 біт, а в багатьох випадках — перехід на ECC [10]. У системах банківського рівня або державного значення ключі часто зберігаються в апаратних криптомодулях (HSM, TPM), що забезпечує додатковий рівень безпеки [14].

У контексті мобільних і вбудованих систем особливої уваги набуває легка криптографія, що орієнтована на забезпечення достатнього рівня захисту при мінімальних обчислювальних витратах. Серед таких алгоритмів варто згадати SIMON, SPECK, Ascon, рекомендовані NIST для використання в малопотужних пристроях [1].

Найбільш критичним компонентом будь-якої криптосистеми залишається система управління ключами (KMS), яка повинна охоплювати генерацію, розповсюдження, зберігання, відкликання та ротацію ключів. У масштабних інформаційних інфраструктурах використовують централізовані рішення, наприклад HashiCorp Vault, AWS KMS або Azure Key Vault, які тісно інтегруються з PKI та апаратними криптомодулями [14].

Державне та правове регулювання

У сфері електронного врядування, документообігу та eHealth застосування криптографічного захисту є обов'язковим. Електронні підписи, які базуються на асиметричних алгоритмах, набули юридичної сили й активно використовуються в різних секторах. Сертифікаційні центри, що надають відповідні послуги, повинні відповідати стандартам ETSI EN 319 411 і WebTrust [15].

Актуальні тенденції

З огляду на постійну еволюцію засобів криптоаналізу, оновлення використовуваних криптографічних алгоритмів має відбуватись регулярно. Актуальним підходом є криптографічна агрегація — одночасне використання кількох незалежних алгоритмів задля підвищення загальної стійкості системи [3].

Отже, сучасна криптографія є не просто інструментом захисту, а ключовим елементом цифрової безпеки. Для забезпечення її ефективності необхідно поєднувати технічні знання з баченням майбутніх викликів і стратегічним плануванням, що дозволить створити адаптивну, надійну й довготривало захищену інфраструктуру.

2.2 Використання хешування та цифрових підписів для захисту даних

У сучасному цифровому середовищі, де інформація стала одним з найцінніших активів, питання її захисту набуває дедалі більшої актуальності. Зростання обсягів електронного документообігу, впровадження хмарних сервісів, розвиток електронного урядування та банківських онлайн-платформ формують нові виклики для забезпечення інформаційної безпеки.

Організації, державні установи, бізнес-структури та окремі користувачі зіштовхуються з необхідністю не лише захищати дані від стороннього втручання, а й гарантувати їх достовірність, цілісність, а також підтвердити справжність джерела походження. Відтак, ефективні криптографічні інструменти стають основою безпечної цифрової взаємодії. Серед таких засобів особливе місце займають механізми хешування та цифрового підпису, що стали невід'ємною частиною сучасних інформаційних технологій [3].

Принципи хешування

Хешування являє собою процес перетворення даних довільного обсягу у фіксований за довжиною хеш-код, який виступає свого роду цифровим відбитком початкового повідомлення. На відміну від методів шифрування, хешування не передбачає зворотного перетворення, тобто з хешу неможливо відновити оригінальні дані. Основними перевагами хешування є:

Односторонність — незворотність функції, що унеможливлює реконструкцію вхідного повідомлення;

Детермінованість — однакові вхідні дані завжди дають однаковий результат;

Чутливість до змін — навіть незначне редагування інформації призводить до кардинально іншого хеш-значення;

Стійкість до колізій — складність підбору двох різних повідомлень із однаковим хешем [9].

Практичне застосування хешування

Завдяки цим характеристикам, хешування широко використовується для перевірки цілісності даних, а також для зберігання конфіденційної інформації у вигляді дайджестів. Наприклад, під час передавання файлів через мережу або зберігання даних у базах важливо мати можливість впевнено констатувати, що інформація не зазнала жодних змін. Обчислення та подальше порівняння хеш-значень допомагає виявити навіть найменші відхилення, які можуть свідчити про випадкові помилки чи зловмисні дії.

На практиці застосування хешування виявляється особливо корисним у таких випадках:

Перевірка цілісності завантажуваного програмного забезпечення — для підтвердження того, що файл не був змінений сторонніми особами;

Зберігання паролів у системах автентифікації — замість збереження у відкритому вигляді, використовується лише хеш, до якого додається «сіль» (salt), щоб підвищити стійкість до атак;

Цифрове журналювання подій — для захисту системних логів від редагування після запису.

Сучасні хеш-функції

Слід зазначити, що надійність хеш-функцій залежить від криптографічної стійкості використовуваного алгоритму. Застарілі MD5 і SHA-1, що колись були стандартом, на сьогоднішній день вважаються вразливими через можливість генерації колізій [9]. Саме тому сучасні системи безпеки орієнтуються на алгоритми родини SHA-2 (SHA-256, SHA-512) і перспективний SHA-3, який базується на абсолютно новій криптографічній конструкції Keccak. Такі функції застосовуються в багатьох сучасних протоколах захисту: TLS, HTTPS, IPsec, PGP тощо [7].

Цифровий підпис: суть і функції

Окремої уваги заслуговує поняття цифрового підпису, що слугує засобом підтвердження авторства та цілісності повідомлення. На відміну від хешу, цифровий підпис також дозволяє встановити, хто саме створив або надіслав той чи

інший документ. Його функціонування базується на принципах асиметричної криптографії, де використовується пара ключів — відкритого та приватного [3]. Приватний ключ, що зберігається виключно у власника, використовується для підпису, а відкритий — для перевірки достовірності.

Механізм створення і перевірки цифрового підпису

Алгоритм роботи цифрового підпису включає кілька етапів: хешування повідомлення, шифрування хешу приватним ключем, передавання разом із повідомленням, а згодом — перевірка підпису шляхом розшифрування хешу відкритим ключем і порівняння з новим обчисленням хеш-функції від отриманого тексту. Якщо обидва значення збігаються — це свідчить про автентичність повідомлення та підтверджує, що воно не було змінено після підписання.

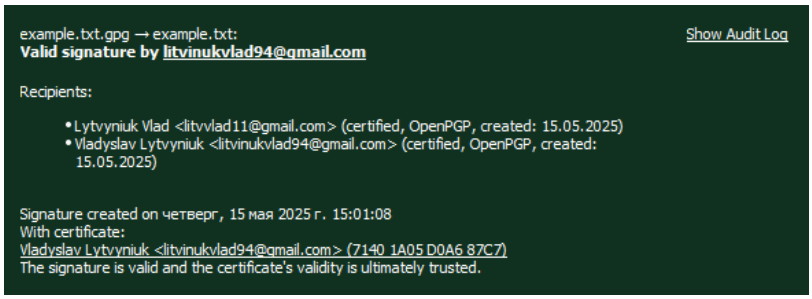

Рис. 2.2. Перевірка цифрового підпису

Окрім перевірки цілісності, цифровий підпис також забезпечує принцип незаперечності — тобто неможливості заперечити факт створення документа. Це має особливо важливе значення у фінансовій сфері, юридичній практиці, державному управлінні, де документи повинні мати доказову силу [12]. Саме тому правові аспекти використання цифрових підписів регламентуються на рівні держави.

Юридичний статус цифрового підпису в Україні

В Україні питання використання електронних підписів врегульоване Законом «Про електронні довірчі послуги», який передбачає поділ на прості, удосконалені та кваліфіковані підписи [2]. Найвищий ступінь довіри має кваліфікований

електронний підпис (КЕП), який прирівнюється до власноручного і вимагає використання сертифікованого програмного або апаратного засобу, а також наявності чинного сертифіката, виданого акредитованим центром сертифікації ключів.

Захист приватного ключа та інфраструктура довіри

Безпека цифрового підпису багато в чому залежить від надійності зберігання приватного ключа. Якщо зловмисник отримає до нього доступ, він зможе створювати фальшиві підписи, що дискредитує систему. Тому з метою захисту ключів застосовуються апаратні засоби — смарт-карти, токени, HSM-модулі, які ізолюють ключовий матеріал від зовнішнього доступу. Крім того, функціонують інструменти перевірки чинності сертифікатів, як-от списки відкликаних сертифікатів (CRL) та протоколи OCSP [14].

Сфери застосування

З огляду на зазначене, обидва інструменти — як хешування, так і цифровий підпис — дедалі активніше інтегруються у найрізноманітніші цифрові сервіси та галузі. Їх застосування охоплює системи електронного урядування, сферу охорони здоров’я, освітнє середовище, банківські установи, транспортну логістику, міжнародний бізнес та інші напрямки, де потрібна висока надійність і підтвердження достовірності даних. Це не лише технічні механізми, а й важливі інструменти формування довіри до цифрових процесів в умовах постійного зростання кіберзагроз.

Таким чином, використання механізмів хешування та цифрових підписів, попри їхню технічну природу, є важливим чинником побудови стабільної, безпечної та юридично значущої інформаційної інфраструктури, що забезпечує прозорість і достовірність цифрового обміну на всіх рівнях — від приватного до державного.

2.3 Методи управління ключами в криптографічних системах

Життєвий цикл ключів

Розбудова надійної системи криптографічного захисту неможлива без належної уваги до одного з найважливіших її аспектів — ефективного управління криптографічними ключами. У структурі комплексної системи інформаційної безпеки ключовий матеріал виконує роль своєрідного «секретного інгредієнта», від якого залежить не лише захист переданих і збережених даних, але й цілісність, автентичність, а також можливість реалізації правового значення електронних транзакцій [3].

На практиці це означає, що навіть при використанні найсучасніших алгоритмів, за відсутності продуманої та впорядкованої системи управління ключами організація може стати вразливою до внутрішніх і зовнішніх загроз. Саме тому управління ключами має розглядатися як основоположна складова системи безпеки, яка охоплює не лише технології, але й управлінські, правові та організаційні підходи [14].

Ключі — це не просто змінні дані в криптографічному протоколі. Це ресурси, які мають життєвий цикл, потребують захисту, контролю, обліку й, за потреби, оперативного відкликання або знищення. У широкому розумінні, управління ключами — це сукупність адміністративних та технічних процедур, які забезпечують безпеку ключового матеріалу протягом усього його існування, починаючи з моменту створення до моменту повного видалення. Без ефективної організації цих процедур система може виявитися неспроможною захистити інформацію навіть у середовищі з високим рівнем шифрування.

Етапи управління ключами

Найтиповішими компонентами системи управління ключами є такі етапи:

Генерація ключів — процес створення ключів з використанням криптографічно стійких алгоритмів, часто у поєднанні з апаратними генераторами випадкових чисел (наприклад, у HSM);

Розповсюдження — механізм передачі ключа уповноваженим користувачам або системам з гарантією його цілісності й конфіденційності;

Зберігання — забезпечення фізичного та логічного захисту ключів у пам’яті пристроїв або спеціалізованих сховищах;

Використання — контрольований доступ до ключів у межах дозволених операцій (шифрування, підпис, автентифікація тощо);

Ротація — регулярна зміна ключів з метою зниження ймовірності їх компрометації;

Відкликання — деактивація ключів, що більше не є безпечними або втратили актуальність;

Знищення — повне та незворотне видалення ключового матеріалу [1].

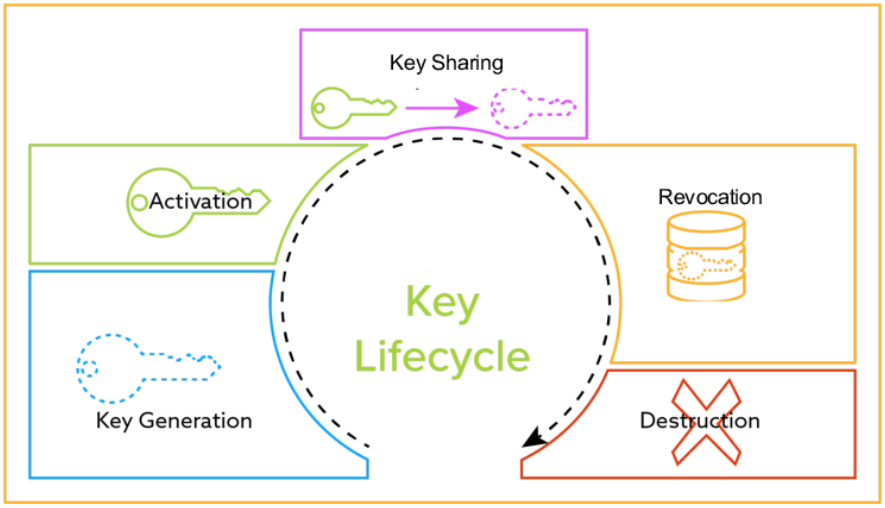

Рис. 2.3. Життєвий цикл ключів

Технічні та організаційні заходи

Кожен із цих етапів вимагає застосування як технічних засобів, так і адміністративного супроводу. Наприклад, генерація ключів у великих організаціях зазвичай здійснюється централізовано, в захищених середовищах, із фіксацією подій у системах журналювання.

Публічні ключі у випадку асиметричних алгоритмів можуть бути відкрито розповсюдженими, але для цього необхідно забезпечити їх перевірку через інфраструктуру відкритих ключів (PKI) [14].

Зберігання ключів — один з найвразливіших етапів. Незалежно від того, чи зберігається ключ у токені, файловій системі або в хмарному середовищі, необхідно забезпечити належний рівень контролю доступу, шифрування та фізичного захисту. Важливим є впровадження систем моніторингу, що дозволяють виявляти підозрілі дії, пов'язані з доступом до ключів. У державному секторі України використання сертифікованих засобів, таких як HSM або смарт-карти, є обов'язковим для захисту ключів, зокрема КЕП [15].

Ротація ключів

Ротація ключів дозволяє мінімізувати ризик довготривалого використання одного й того самого ключа. Це особливо важливо у випадках, коли йдеться про ключі, що використовуються для захисту критично важливої інформації. Політика ротації встановлюється залежно від типу ключа, його призначення та рівня ризику. Наприклад, сесійні ключі можуть оновлюватися при кожному новому сеансі зв'язку, тоді як довгострокові — щомісяця або щокварталу.

Варто зазначити, що автоматизовані інструменти для ротації дозволяють зменшити людський вплив та прискорити оновлення в масштабних системах [14].

Окремо варто розглянути сучасні системи управління ключами — KMS. Вони дозволяють централізувати всі аспекти управління ключами в масштабах організації чи навіть міжорганізаційного середовища.

Такі системи можуть бути реалізовані як у вигляді локальних інсталяцій, так і у формі хмарних сервісів. Найбільш популярними рішеннями в цій галузі є Amazon Web Services (AWS KMS), Microsoft Azure Key Vault, Google Cloud KMS, HashiCorp Vault. Вони забезпечують інтерфейси для генерації, зберігання, розподілу та моніторингу використання ключів, інтегруються з системами ідентифікації користувачів і підтримують аудит доступу [14].

Системи управління ключами

Крім того, сучасні KMS-платформи підтримують політики, які дозволяють застосовувати контроль доступу на основі ролей, географічного розташування чи часових рамок, що істотно підвищує гнучкість управління.

Управління інцидентами

Окрема увага приділяється управлінню інцидентами. Компрометація ключа — це надзвичайна ситуація, що вимагає швидкого реагування. Важливо мати чітко прописані процедури: як виявити факт витоку, кого повідомити, які сервіси заблокувати, як швидко замінити ключі тощо. У системах PKI у таких випадках застосовується відкликання сертифіката — публікація його в CRL або перевірка через OCSP. Крім того, доцільним є впровадження симуляційних сценаріїв інцидентів для перевірки готовності персоналу та технічної інфраструктури до надзвичайних ситуацій.

Людський фактор

Не менш значущим є людський фактор. Багато порушень виникає через недостатню обізнаність співробітників щодо належного поводження з ключами. Саме тому в межах системи управління безпекою необхідно впроваджувати політику навчання персоналу. Це може включати тренінги, тестування, поширення інструкцій і регулярний контроль знань.

Також важливо створити культуру відповідального ставлення до інформаційної безпеки на всіх рівнях організації. Системи мотивації, а також механізми внутрішнього контролю, можуть сприяти підвищенню рівня дисципліни у поводженні з ключами.

Нормативне забезпечення

З точки зору нормативного забезпечення, управління ключами повинно відповідати як міжнародним, так і національним стандартам. Основними орієнтирами тут є ISO/IEC 27001, ISO/IEC 11770, рекомендації NIST (зокрема SP 800-57), а також українські нормативні документи — НД ТЗІ, закони «Про захист інформації» та «Про електронні довірчі послуги» [2].

Наявність внутрішньої документації — політик управління ключами, процедур взаємодії, протоколів резервування — є обов'язковою умовою для проходження аудитів та отримання сертифікатів відповідності. Організації, що прагнуть до міжнародної діяльності, повинні також враховувати вимоги регламентів GDPR щодо захисту персональних даних, у тому числі при роботі з криптографічними інструментами.

Перспективи розвитку

Нарешті, у майбутньому проблема управління ключами ускладнюватиметься через розвиток постквантових обчислень. Уже сьогодні рекомендується впроваджувати гібридні криптографічні системи, здатні працювати як з класичними, так і з постквантовими алгоритмами. Це потребує гнучкої системи управління ключами, здатної адаптуватися до нових форматів ключового матеріалу, процедур генерації та схем довіри [10].

Деякі організації вже починають дослідження в напрямі впровадження алгоритмів, рекомендованих NIST як потенційно стійких до квантових атак.

Таким чином, управління ключами — це складний, багатокомпонентний і стратегічно важливий процес. Його успішна реалізація вимагає поєднання технічної експертизи, чітких політик, ефективного навчання персоналу і постійного моніторингу відповідності встановленим вимогам. Тільки комплексний підхід до побудови системи управління ключами дозволить гарантувати стійкість криптографічного захисту в умовах постійно зростаючих інформаційних загроз.

Розвиток технологій, зростання обсягів переданої інформації та вимоги до конфіденційності тільки підкреслюють важливість інвестування в сучасні засоби управління ключами як у фундаментальну складову цифрової безпеки.

Практичні інструменти

У цьому контексті особливого значення набуває використання практичних інструментів, які поєднують алгоритмічну надійність із зручністю реалізації. Одними з таких засобів є BitLocker, що реалізує механізми повнодискового шифрування на базі симетричних алгоритмів, та Gpg4win, який забезпечує

шифрування, цифрове підписування та обмін відкритими ключами відповідно до стандарту OpenPGP.

BitLocker забезпечує автоматизований захист інформації на фізичному рівні з мінімальним втручанням користувача, що особливо актуально для запобігання компрометації даних у разі втрати або крадіжки пристрою. Gpg4win, у свою чергу, дозволяє будувати систему довіри між користувачами, реалізовувати обмін зашифрованими повідомленнями та автентифікувати їхнє походження за допомогою цифрових підписів [15].

Таким чином, інтеграція подібних рішень у корпоративне середовище є ефективним способом реалізації політик шифрування та управління ключами відповідно до сучасних стандартів безпеки. У наступному розділі розглядаються особливості впровадження BitLocker і Gpg4win у практичну інфраструктуру організації, з урахуванням специфіки їх налаштування, функціональних можливостей і типових сценаріїв використання [16].

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ В ОРГАНІЗАЦІЯХ

3.1 Побудова криптографічної системи захисту для організації

Для впровадження криптографічного захисту таємної інформації в організації було обрано поєднання двох програмних рішень — BitLocker та Gpg4win, котрі взаємно доповнюють одне одного. Такий підхід дозволяє реалізувати як захист на рівні файлової системи, так і захист при передаванні або зовнішньому зберіганні інформації [15].

BitLocker — це вбудований компонент операційної системи Windows, призначений для криптографічного шифрування даних із мінімальною необхідністю взаємодії з користувачем [15].

В стандартній конфігурації BitLocker використовує алгоритм AES для забезпечення високого рівня безпеки на рівні файлової системи [6].

Налаштування автентифікації

Активація BitLocker розпочинається з налаштування автентифікації, основним елементом якої є пароль, що вводиться користувачем до старту операційної системи. (рисунок 3.1). Цей етап критично важливий для запобігання несанкціонованому доступу до даних на диску.

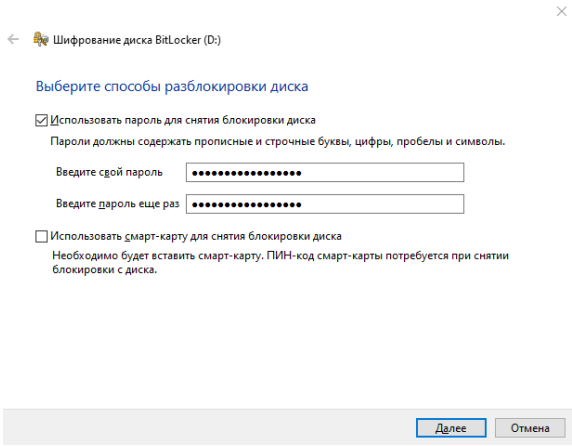

Рис. 3.1. Вікно введення пароля для розблокування BitLocker

Наступним кроком ініціалізації BitLocker є створення та збереження ключа відновлення. У разі втрати пароля чи збою завантаження системи саме цей ключ дозволить розблокувати диск та дістати доступ до важливих даних.

Створення та збереження ключа відновлення

Система пропонує кілька варіантів збереження ключа: у акаунті Microsoft, на зовнішньому носії, у вигляді файла або у роздрукованому вигляді (рисунок 3.2). Рекомендується зберігати ключ у кількох незалежних місцях для підвищення надійності.

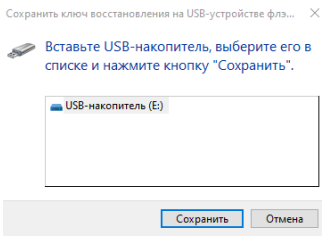

Рис. 3.2. Збереження ключа відновлення

Шифрування диска

Після того як ключ відновлення успішно збережено, BitLocker самостійно розпочинає процес повного шифрування накопичувача без додаткових дій з боку користувача.

Цей процес охоплює всі томи, включаючи системний розділ, розділ даних користувача, тимчасові каталоги та кеш-пам'ять. Шифрування відбувається прозоро для користувача, не вимагаючи жодної взаємодії, і має мінімальний вплив на продуктивність системи (рисунок 3.3).

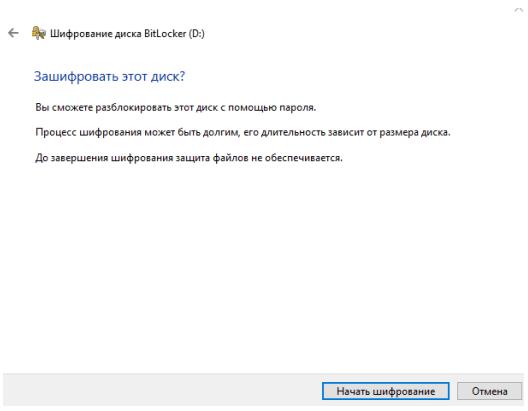

Рис. 3.3. Шифрування диска

По завершенні процесу користувач бачить вказівку про те, що диск тепер зашифрований, а на іконці диска з’являється відповідне зображення замка (рисунок 3.4). Це є візуальним підтвердженням того, що диск перебуває під криптографічним захистом.

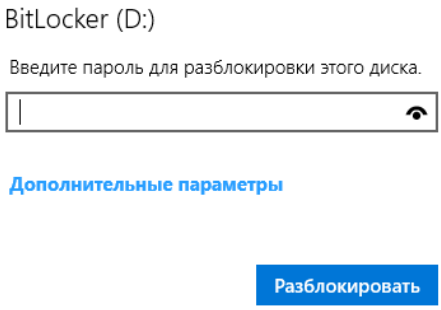

Рис. 3.4. Вікно розблокування

Таким чином, BitLocker дозволяє забезпечити стійкий захист даних у разі втрати або крадіжки пристрою. Проте ця технологія не призначена для захисту даних під час обміну між користувачами або організаціями. Тому з метою забезпечення комплексного захисту додатково впроваджується система Gpg4win, що базується на стандартах OpenPGP [15].

Призначення

Gpg4win являє собою пакет програмного забезпечення з відкритим вихідним кодом, що розповсюджується за вільною ліцензією. Його основна мета - забезпечення криптографічних функцій, таких як шифрування, цифровий підпис та адміністрування криптографічних ключів [15]. Ключовим компонентом Gpg4win є програма Kleopatra, яка надає інструменти для управління сертифікатами, включаючи генерацію, зберігання та імпорт ключових пар [16].

Генерація ключової пари

Процес починається з генерації ключової пари для користувача. Для цього потрібно вказати ім’я та адресу електронної пошти, а за потреби — додати додаткові відомості у вигляді опису (див. рисунок 3.5).

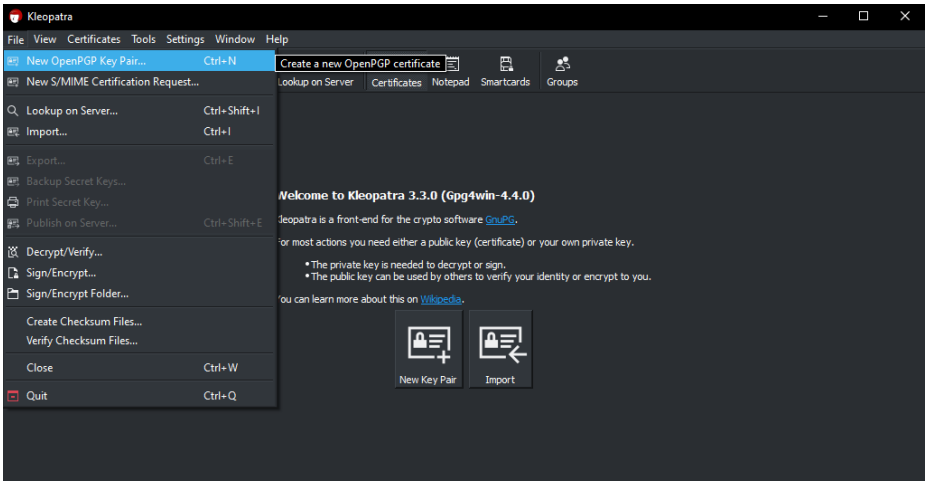

Рис. 3.5. Створення ключової пари

Налаштування параметрів ключа

Далі користувач обирає параметри криптографічного захисту: довжину ключа (наприклад, 3072 або 4096 біт), термін його дії, тип алгоритму (RSA є типовим вибором) та додаткові властивості (рис. 3.6). Усі ці параметри впливають на рівень стійкості шифрування та продуктивність системи.

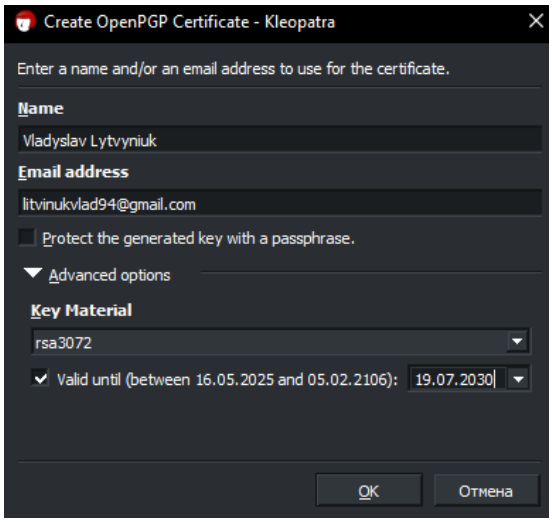

Рис. 3.6. Налаштування параметрів ключа

Створення сертифіката користувача

Після затвердження налаштувань утворюється сертифікат юзера з відкритим та закритим ключами (рисунок 3.7).

Відкритий ключ слугує для шифрування повідомлень іншими користувачами, а закритий — для їх дешифрування.

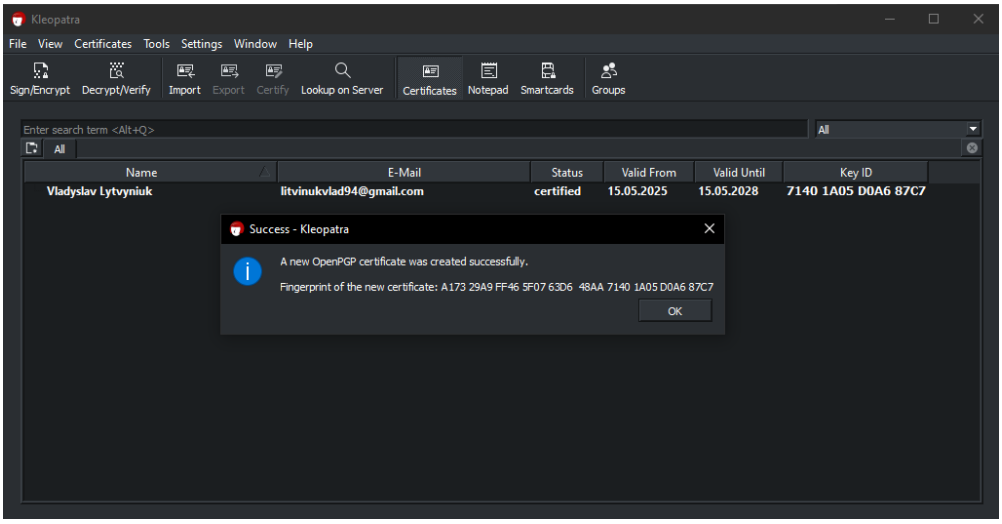

Рис. 3.7. Створений сертифікат користувача

Обмін ключами

Для того щоб інші учасники мали змогу надсилати зашифровану інформацію, відкритий ключ слід експортувати у файл та передати довіреним сторонам (рисунок 3.8). Аналогічно, для розшифрування вхідних повідомлень потрібно імпортувати відкриті ключі сторонніх користувачів.

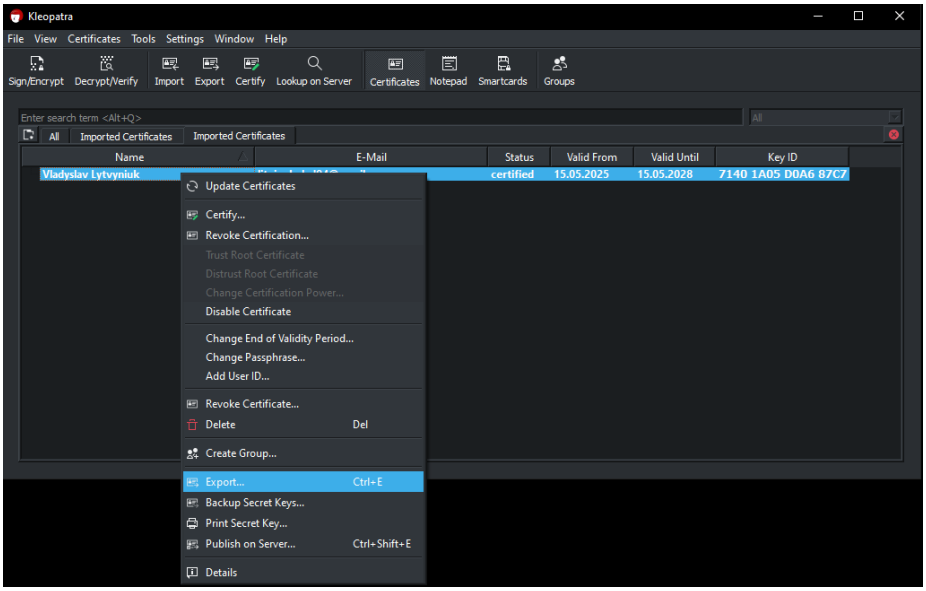

Рис. 3.8. Експорт відкритого ключа для подальшого обміну

Завдяки взаємному обміну сертифікатами формується локальне сховище довіри, що дозволяє безпечно взаємодіяти з кількома сторонами, зберігаючи конфіденційність та автентичність кожного повідомлення.

3.2 Практичне впровадження механізмів криптографічного захисту

Після налаштування ключової інфраструктури користувач може розпочати практичну роботу із зашифрованими документами. Найбільш поширеною процедурою є шифрування текстових або офісних файлів перед передачею через електронну пошту або інші канали зв'язку.

Процес шифрування

На рисунку 3.9 зображено приклад шифрування текстового документа. Користувач обирає файл, визначає одержувача, зазначаючи відповідний відкритий ключ, і формує зашифрований файл з розширенням .gpg.

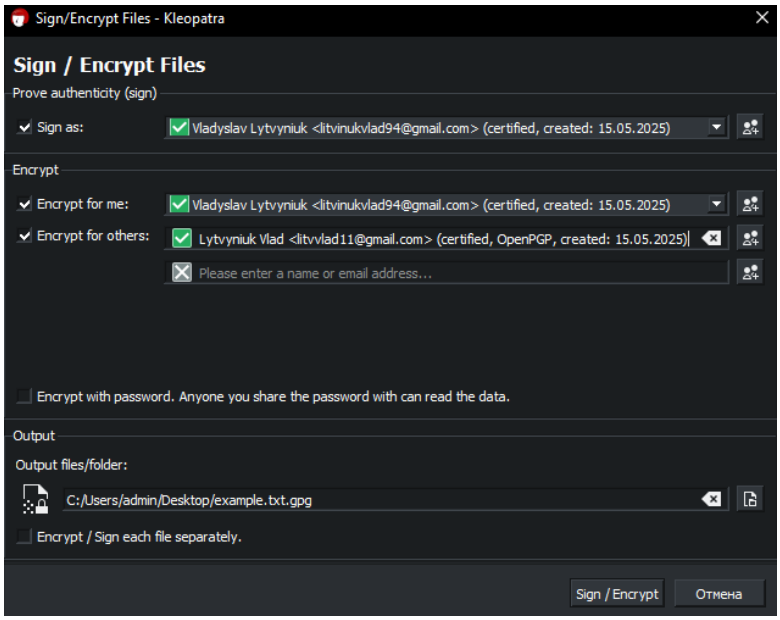

Рис. 3.9. Шифрування файлу з використанням відкритого ключа одержувача

Процес розшифрування

Далі, при отриманні зашифрованого файлу, інший користувач здійснює його розшифрування за допомогою свого закритого ключа. Одночасно система

перевіряє цифровий підпис, накладений відправником (рисунок 3.10). Це підтверджує, що документ не було змінено з моменту його створення і що він дійсно був відправлений вказаною особою.

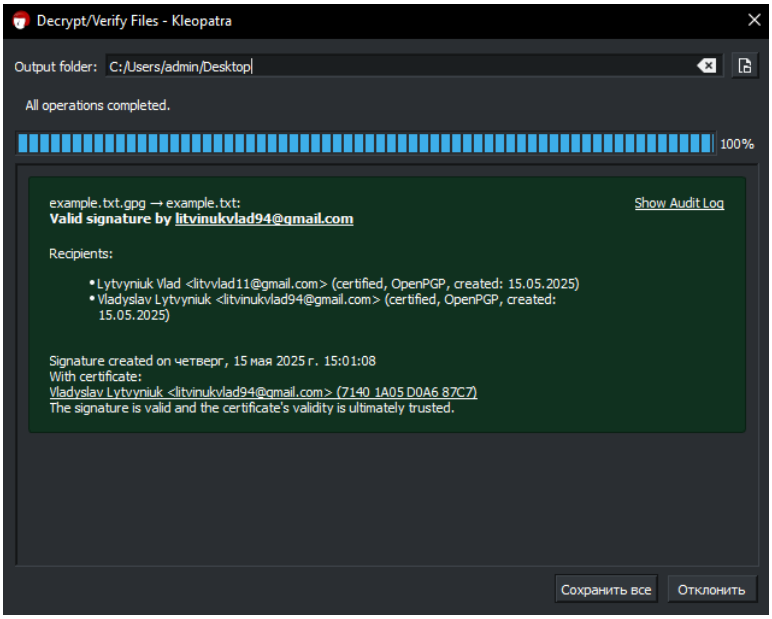

Рис. 3.10. Підтвердження цифрового підпису при розшифруванні

Система Kleopatra детально відображає інформацію про підписувача, дату створення підпису, статус сертифіката та його довіреність. Така перевірка дозволяє уникнути ризиків підміни або фальсифікації документів.

Після завершення процесу розшифрування створюється оригінальний файл, який можна переглянути у будь-якому текстовому або офісному редакторі (рисунок 3.11). Це підтверджує коректність функціонування всієї криптографічної інфраструктури.

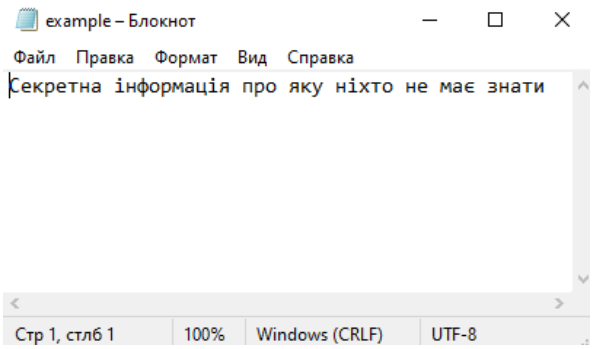

Рис. 3.11. Вміст розшифрованого повідомлення в текстовому редакторі

Таким чином, впровадження Gpg4win забезпечує не лише конфіденційність при передачі даних, але й реалізацію принципів автентичності, цілісності та невідмовності. У поєднанні з BitLocker, який захищає інформацію на рівні пристрою, створюється багаторівнева система криптографічного захисту, що відповідає сучасним стандартам інформаційної безпеки.

3.3 Рекомендації та оцінка ефективності використання криптографічних методів

У процесі впровадження криптографічного захисту в межах організації мені довелося безпосередньо працювати з обраними засобами — BitLocker для шифрування локальних носіїв і Gpg4win для захисту інформації під час обміну [15]. Це дозволило на практиці оцінити не лише технічні характеристики рішень, а й зручність користування ними, стабільність роботи та рівень захисту, який вони забезпечують у реальних умовах [16].

Практична оцінка застосування BitLocker

Одним із перших кроків було налаштування BitLocker на основному робочому комп’ютері. Процес активації виявився зрозумілим і поетапним: від створення пароля доступу до генерації ключа відновлення. Після шифрування продуктивність системи не зазнала помітних змін, що підтверджує ефективність оптимізації цього інструменту. У повсякденному використанні BitLocker забезпечував автоматичний захист даних без створення труднощів для користувача.

Оцінка ефективності під час обміну даними

Для захисту передавання інформації було обрано Gpg4win, який тестувався у зв’язці з поштовим клієнтом Thunderbird. Створення пари ключів, імпорт відкритих ключів колег і підписування документів не викликали труднощів. Після

впровадження Gpg4win у внутрішню комунікацію було зафіксовано зростання довіри серед команди, адже цифрові підписи гарантували автентичність і цілісність листів. Це особливо важливо в умовах збільшення кількості фішингових атак.

Поведінка в умовах ризику

Я свідомо змоделював ситуацію втрати пароля до BitLocker. Завдяки наявності заздалегідь збереженого ключа відновлення вдалося відновити доступ без втрати даних. У той же час я переконався, що у разі відсутності такого ключа доступ до шифрованого розділу відновити неможливо. Це, з одного боку, демонструє високий рівень захисту, а з іншого — підкреслює потребу в політиках резервування і навчанні користувачів.

Зручність використання та ставлення персоналу

На початку були побоювання, що користувачі уникають шифрування через складність. Проте короткий інструктаж зняв усі бар'єри: у Gpg4win усе зводиться до натискання кнопок «Підписати» або «Зашифрувати». Колеги швидко адаптувалися до нових вимог і оцінили переваги — зокрема, можливість перевіряти достовірність листів. Це свідчить про доцільність включення криптографії в щоденні бізнес-процеси без істотного навантаження на користувачів.

Виявлені обмеження

У ході використання були виявлені потенційні вразливості. Наприклад, зберігання приватного ключа Gpg4win на локальному диску без апаратного захисту (HSM або токена) створює ризик у разі фізичного доступу до пристрою [16]. Також варто враховувати обмеження BitLocker: у разі втрати пароля без збереженого ключа відновлення дані повністю недоступні [15].

Рекомендації щодо підвищення ефективності захисту

На основі отриманого досвіду можу запропонувати такі практичні рекомендації:

Запровадити апаратний захист ключів, наприклад, за допомогою смарт-карток або токенів, що знижують ризик компрометації приватних ключів;

Використовувати гібридні криптосистеми, поєднуючи симетричне й асиметричне шифрування для оптимізації швидкодії та надійності;

Реалізувати централізовану систему управління ключами (KMS), яка дозволить забезпечити контроль над життєвим циклом ключів — генерацією, зберіганням, ротацією та відкликанням;

Навчати персонал: обов’язкові інструктажі щодо збереження ключів, користування шифруванням і розпізнавання фішингових повідомлень мають бути частиною інформаційної політики;

Забезпечити інтеграцію криптографічних засобів у систему корпоративної безпеки відповідно до міжнародних нормативів, таких як ISO/IEC 27001, NIST SP 800-57 і GDPR;

Регулярно перевіряти журнали подій і проводити аудити, щоб своєчасно виявляти аномальну активність або порушення політик доступу [14].

ВИСНОВКИ

В рамках бакалаврської роботи було проведено дослідження криптографічних методів захисту конфіденційної інформації в організаціях. Зі зростанням кіберзагроз та вимог до захисту даних це дослідження набуло додаткової актуальності, а його результати є корисними для експертів з кібербезпеки, розробників систем захисту та керівників організацій.

На основі аналізу наукової літератури, нормативно-правової бази та міжнародних стандартів було встановлено, що криптографічні методи є одними з найефективніших засобів для забезпечення конфіденційності, цілісності та автентифікації інформації.

Особливу увагу було приділено симетричним та асиметричним алгоритмам шифрування, хешуванню, цифровому підпису та управлінню ключами. Було визначено, що в сучасних умовах організації стикаються з низкою проблем, пов'язаних із впровадженням криптографії, включаючи вибір відповідних алгоритмів, дотримання законодавчих вимог, безпеку зберігання ключів та інтеграцію з існуючою інфраструктурою.

У роботі детально розглядаються архітектурні аспекти та принципи роботи сучасних криптографічних систем на прикладі AES, RSA, ECC, SHA, а також їхнє застосування в різних сценаріях захисту даних.

За допомогою порівняльного аналізу цих методів визначаються їх переваги, недоліки, а також оптимальні умови застосування. Наприклад, симетричні алгоритми (AES) добре підходять для шифрування великих обсягів даних, тоді як асиметричні (RSA, ECC) використовуються для безпечного обміну ключами та цифрових підписів.

На основі вивчення практичних аспектів впровадження криптографічних засобів було запропоновано рекомендації щодо їх використання в організаціях. Встановлено, що ключовими елементами успішного захисту є:

вибір алгоритмів, що відповідають міжнародним стандартам (NIST, ISO/IEC);

реалізація систем управління ключами (KMS, HSM);

інтеграція з іншими механізмами безпеки (DLP, SIEM);

регулярний аудит та оновлення криптографічних рішень.

Особлива увага була приділена відповідності вимогам GDPR, Закону України "Про захист персональних даних" й інших нормативних документів. Супроводжуючись практичним дослідженням, була сформульована низка рекомендацій щодо впровадження криптографічних засобів в типовій організації.

За основу роботи був узятий детальний алгоритм дій, який передбачає послідовність виконання таких етапів та заходів: оціника ризиків й ідентифікування критичних даних;

вибір методів криптографії;

здійснення налашатувань систем управління ключами;

систематичне проведення тестування й моніторинг ефективності застосованих рішень.

Кожен із зазначених етапів ретельно аналізувався, беручи до уваги специфіку найактуальніших викликів в галузі інформаційної безпеки.

В результаті проведеної роботи досягнуто низку важливих результатів.

По-перше, здійснено комплексний аналіз сучасних криптографічних методів та чітко визначено їх ключову роль у забезпеченні захисту конфіденційної інформації.

По-друге, систематизовано основні загрози та виклики, які виникають при практичному застосуванні криптографічних рішень у організаціях.

По-третє, на основі отриманих даних розроблено практично орієнтовні рекомендації до ефективної інтеграції криптографії, які розглядають технічний аспект та організаційне питання. Крім того, запропонований чіткий алгоритм дій, що гарантує надійний захист даних у всіх стадіях їх обробки та зберігання.

Отримані результати можуть бути використані для підвищення рівня інформаційної безпеки в організаціях, а також у навчальному процесі для підготовки фахівців з кібербезпеки. Запропоновані підходи сприятимуть зменшенню ризиків витоку даних, забезпеченню відповідності законодавчим вимогам та підвищенню довіри клієнтів і партнерів.

Матеріали дослідження можуть бути корисними для подальших наукових робіт, зокрема в галузі розвитку постквантової криптографії та інтеграції нових технологій захисту даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST Cybersecurity Framework. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата звернення: 2.05.2025).
2. ISO/IEC 27001:2022 – Information Security Management. International Organization for Standardization. URL: https://www.iso.org/standard/82875.html (дата звернення: 2.05.2025).
3. What is cryptography? TechTarget. URL: https://www.techtarget.com/searchsecurity/definition/cryptography (дата звернення: 5.05.2025).
4. Types of cyber attacks and how to prevent them. TechTarget. URL: https://www.techtarget.com (дата звернення: 5.05.2025).
5. Cost of a Data Breach Report 2023. IBM Security. URL: https://www.ibm.com/security/data-breach (дата звернення: 9.05.2025).
6. Types of Encryption. IBM. URL: https://www.ibm.com/topics/encryption/ (дата звернення: 9.05.2025).
7. Understanding TLS/SSL. Mozilla. URL: https://developer.mozilla.org/en-US/docs/Web/Security/Transport_Layer_Security (дата звернення: 9.05.2025).
8. What is IBM Security Identity and Access Manager and use cases of IBM Security Identity and Access Manager? DevOpsSchool. URL: https://www.devopsschool.com/blog/what-is-ibm-security-identity-and-access-manager-and-use-cases-of-ibm-security-identity-and-access-manager/ (дата звернення: 12.05.2025).
9. OWASP Cryptographic Storage Cheat Sheet. OWASP Foundation. URL: https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html (дата звернення: 12.05.2025).
10. Post-Quantum Cryptography Standardization. NIST. URL: https://csrc.nist.gov/projects/post-quantum-cryptography (дата звернення: 12.05.2025).

11. CIS Benchmarks. Center for Internet Security. URL: https://www.cisecurity.org/cis-benchmarks/ (дата звернення: 12.05.2025).

12. FIPS 186-5: Digital Signature Standard (DSS). NIST. URL: https://csrc.nist.gov/publications/detail/fips/186/5/final (дата звернення: 15.05.2025).

13. What is data encryption? IBM. URL: https://www.ibm.com/topics/data-encryption (дата звернення: 15.05.2025).

14. What is Key Management and Why is it Important? Venafi. URL: https://www.venafi.com/education-center/key-management (дата звернення: 16.05.2025).

15. BitLocker Drive Encryption Overview. Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows/security/information protection/bitlocker/bitlocker-overview (дата звернення: 16.05.2025).

16. Gpg4win. Official Documentation. URL: https://www.gpg4win.org/ (дата звернення: 16.05.2025).