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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія криптографічного захисту інформації інформаційної системи організації»

зі спеціальності *125 Кібербезпека та захист інформації*
(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

_____ В’ячеслав ХОМЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ХОМЕНКО В’ячеслав
(прізвище, ім’я)

Керівник д.т.н.,проф. КОЖУХІВСЬКИЙ Андрій
(науковий ступінь, вчене звання, прізвище, ім’я)

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

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CIA	—	Confidentiality, Integrity, Availability
IoT	—	Internet of Things
CVE	—	Common Vulnerabilities and Exposures
CaaS	—	Crime-as-a-service
DDoS	—	Distributed Denial of Service
RSA	—	Rivest, Shamir, Adleman
DES	—	Data Encryption Standard
ECC	—	Elliptic-curve cryptography
AES	—	Advanced Encryption Standard
SHA	—	Secure Hash Algorithm

ВСТУП

Актуальність дослідження.

Зростання значення даних у сучасному світі спричинило введення суворих регуляторних вимог до їх захисту. Наприклад, Європейський регламент GDPR (General Data Protection Regulation) вимагає від організацій застосовувати сучасні методи шифрування для забезпечення конфіденційності персональних даних. У разі недотримання цих вимог організація може бути оштрафована на значну суму, що негативно вплине на її репутацію та фінансову стабільність.

В Україні законодавча база також активно адаптується до міжнародних стандартів. Закон України "Про захист персональних даних" та Закон "Про електронні довірчі послуги" передбачають обов'язкове використання криптографічних засобів захисту інформації. Таким чином, впровадження криптографії в інформаційні системи є не лише рекомендацією, а й обов'язковою умовою для дотримання нормативних актів. Тому тема кваліфікаційної роботи «Технологія криптографічного захисту інформації інформаційної системи організації» є актуальною

Об'єкт дослідження – інформаційна система організації.

Предмет дослідження – криптографічні методи та засоби захисту інформації.

Мета роботи – розробити варіант технології криптографічного захисту інформації інформаційної системи організації на основі Boxcryptor, яка відповідає сучасним вимогам до безпеки та ефективності в організаційних інформаційних системах.

Наукові завдання:

- провести аналіз проблеми криптографічного захисту інформації;
- проаналізувати сучасні загрози безпеці інформаційних систем;
- дослідити проблеми впровадження криптографічного захисту;
- проаналізувати нормативно-правову базу, щодо кприптографічного захисту;

- дослідити методи та засоби криптографічного захисту інформації;
- проаналізувати симетричне, асиметричне шифрування, принципи роботи шифрування, хешування та цифрового підпису;
- розробити варіант розгортання технології криптографічного захисту інформації на основі Boxcryptor;
- розробити рекомендації щодо застосування технології криптографічного захисту інформації інформаційної системи організації на основі Boxcryptor.

Методи дослідження – у роботі застосовано аналіз існуючих підходів до криптографічного захисту, опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та державних стандартів.

Практичне значення одержаних результатів полягає в розробці технології криптографічного захисту інформації інформаційної системи організації на основі Boxcryptor та рекомендації щодо застосування даної технології.

1 АНАЛІЗ ПРОБЛЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Сучасні загрози безпеці інформаційних систем

На сьогоднішній день інформація стала найціннішим ресурсом, від якого залежить функціонування організацій, державних установ, підприємств і навіть окремих осіб. Інформаційні системи в свою чергу забезпечують ефективність бізнес-процесів, автоматизацію операцій, управління даними та інтеграцію різних елементів цифрової екосистеми. Проте з розвитком технологій зростає і кількість загроз, що ставлять під загрозу безпеку цих систем. Сучасні кібератаки не тільки стають більш складними, але й набувають нових форм, які враховують слабкі місця організацій, їхні процеси та інфраструктуру.

Загрози інформаційним системам охоплюють широкий спектр ризиків, серед яких: несанкціонований доступ до конфіденційної інформації, її модифікація або знищення, порушення цілісності даних, втручання у функціонування мережевих сервісів тощо і цим самим порушує основні принципи безпеки (CIA Triad) [1]. Більше того, сучасні загрози є високодинамічними — вони постійно еволюціонують у відповідь на нові методи захисту. Це створює постійні перегони між зловмисниками та фахівцями з кібербезпеки.

Рис. 1.1. Тріада інформаційної безпеки (CIA) [1]

Основним рушієм зростання кількості та складності загроз є цифровізація. Збільшення кількості пристроїв, підключених до мережі, інтенсивне впровадження хмарних сервісів, використання мобільних додатків та Інтернету речей (IoT) відкривають нові можливості для злочинців. У той час як організації намагаються оптимізувати свої бізнес-процеси через цифрові технології, вони нерідко нехтують базовими принципами захисту інформації, що робить їх вразливими до атак.

Сучасні загрози мають також соціальний аспект. Зловмисники використовують не тільки технічні інструменти, але й психологічні методи, такі як соціальна інженерія. Вони маніпулюють людьми, змушуючи їх розголошувати конфіденційну інформацію, завантажувати шкідливе програмне забезпечення або виконувати інші дії, що ставлять під загрозу безпеку системи [2].

Окрім того, варто враховувати, що геополітична ситуація також впливає на розвиток загроз у сфері кібербезпеки. Держави все частіше використовують кіберпростір як поле для досягнення своїх стратегічних цілей. Кібератаки можуть бути спрямовані на критично важливі інфраструктури, фінансові системи чи навіть політичні процеси, що має глобальні наслідки.

Рис. 1.2. 10 основних загроз кібербезпеці, на які слід звернути увагу [2]

До них відносяться:

1. Вразливі місця

У 2023 році 26 447 вразливостей було присвоєно загальний номер вразливостей (CVE) у Національній базі даних вразливостей, що перевищує показник 2022 року на понад 1500 CVE. Кожна з них являє собою вразливість, що активно експлуатується, про яку MSP повинні знати.

2. Компрометація ділової електронної пошти

Корпоративна електронна пошта може бути скомпрометована кількома способами, зокрема:

Фішинг.

Зловмисне програмне забезпечення.

Соціальна інженерія.

Слабкі паролі.

3. Злочин як послуга (Crime-as-a-service)

Одним із зростаючих типів загроз кібербезпеці є злочин як послуга (CaaS). CaaS описує надання інструментів, послуг та експертизи кіберзлочинців через підпільний, незаконний ринок. По суті, CaaS дозволяє злочинцям передавати технічні аспекти своєї діяльності іншим кіберзлочинцям з більшим досвідом.

CaaS дозволяє злочинцям отримати доступ до широкого спектру нечесних послуг та інструментів, таких як [2]:

- розробка шкідливого програмного забезпечення;
- програми-вимагачі;
- набори експлойтів;
- брокери початкового доступу;
- набори для фішингу;
- оренда ботнету;
- навчальні посібники з хакерства.

4. Атаки на ланцюжок поставок

Атаки на ланцюжок поставок – це відносно нова інновація в галузі кіберзлочинності, яка продовжує зростати за масштабами та частотою. Хакери проникають у технологію ланцюжка поставок, щоб отримати доступ до вихідних

кодів, кодів збірки та інших компонентів інфраструктури небезпечних програм, їхня кінцева мета полягає в тому, щоб використовувати ці законні платформи як канали для розповсюдження шкідливого програмного забезпечення в системах ланцюга поставок.

5. Хмарні атаки

Хмарні атаки охоплюють широкий спектр хакерських TTPs. З огляду на те, що так багато компаній використовують хмару, а хмарні мережі стають все більш складними [2].

Фахівці з кібербезпеки зосереджуються на так званих «Egregious Eleven». Це 11 найпопулярніших точок проникнення для хмарних загроз. У порядку ступеня вираженості вони бувають:

1. Витік даних.
2. Неправильна конфігурація налаштувань і установок.
3. Погане налаштування та планування хмарної безпеки.
4. Неправильне керування ідентифікаторами, обліковими даними для входу та доступом до облікового запису.
5. Викрадені або викрадені облікові записи.
6. Внутрішні загрози.
7. API та небезпечні програмні інтерфейси.
8. Слабка площина управління.
9. Збої в аппліструктурі та метаструктурі.
10. Видимість обмеженого використання хмари.
11. Зловживання хмарними сервісами.

6. Атаки на дата-центри

Атаки на дата-центри кіберзлочинності можуть набувати різних форм, зокрема:

- DDoS-атаки.
- Атаки шкідливого програмного забезпечення.
- Внутрішні загрози.
- Фішингові атаки.

- Атаки програм-вимагачів.

Центри обробки даних часто є цінними цілями для кіберзлочинців, оскільки вони зберігають і обробляють великі обсяги конфіденційної інформації.

7. Програми-вимагачі

Зловмисне програмне забезпечення, зокрема програми-вимагачі, продовжують становити значну загрозу кібербезпеці. Ця форма кібератаки існує десятиліттями, і хакери продовжують вдосконалювати свої методи доставки [2].

8. Злом пристрою IoT

Оскільки багато співробітників працюють з дому та отримують доступ до конфіденційних платформ компанії та даних із кількох розрізнених кінцевих точок, у поєднанні з прогресом хмарних технологій, хакери мають більше можливостей для проникнення, ніж будь-коли раніше.

Кіберзлочинці часто націлені на наступне:

Паролі за замовчуванням: багато розумних пристроїв мають стандартні облікові дані для входу, які легко вгадати, наприклад «admin/admin» або «admin/password». Кіберзлочинці можуть використовувати ці паролі за замовчуванням, щоб отримати доступ до пристрою та його даних.

Незахищені мережі Wi-Fi: розумні пристрої часто підключаються до мереж Wi-Fi, які можуть бути незахищеними або використовувати слабке шифрування. Кіберзлочинці можуть використовувати вразливості в цих мережах для перехоплення даних, що передаються через Інтернет [1-2].

Отримавши доступ до розумного пристрою, кіберзлочинці можуть здійснити низку атак, таких як:

- Крадіжка даних.
- Встановлення шкідливого програмного забезпечення.
- Запуск DDoS-атак.
- Шпигунство за власником пристрою через його камеру або мікрофон.

9. Внутрішні загрози

Як тільки внутрішні користувачі системи будуть скомпрометовані, вони можуть стати навіть більшою загрозою для системи, ніж зовнішні зловмисники. У звіті Ponemon Institute за 2023 рік про глобальний стан внутрішніх загроз зазначено, що час локалізації інсайдерського інциденту збільшився в середньому до 86 днів.

10. Вимушені компроміси (Drive-by compromises)

У 2024 році спостерігаємо значне зростання кількості компромісів як тактики кіберзагроз. Це коли зловмисники заманюють жертв на шкідливі веб-сайти за допомогою таких методів, як пошукова оптимізація (SEO), poisoning та шкідлива реклама [2].

1.2. Проблеми впровадження криптографічного захисту

Криптографічні питання викликають першорядне занепокоєння в сучасному цифровому ландшафті, де цілісність і безпека даних постійно знаходяться під загрозою. Серед відомих криптографічних проблем кілька виділяються через їх значні наслідки:

1. Слабкі алгоритми шифрування: деякі криптографічні алгоритми, які колись вважалися безпечними, стали вразливими через прогрес у обчислювальній потужності та методах криптоаналізу. Прикладами можуть служити старі версії RSA з маленькими розмірами ключів, DES і MD5. Використання криптографічних примітивів, заснованих на практичній секретності (RSA, ECC, Kyber, Dilithium і т.д.), в загальному випадку має недолік безпеки, поки не буде доведено небезпечність, тобто припустити, що не існує відомого швидкого рішення. Це суперечить системам безпеки, які забезпечують інформаційну теоретичну безпеку, які не страждають від цієї проблеми [3].

2. Недоліки реалізації: Навіть надійні криптографічні алгоритми можуть бути скомпрометовані, якщо їх неправильно виконати. До цієї категорії належать такі проблеми, як атаки на сторонньому каналі, коли зловмисник використовує інформацію, отриману в результаті фізичної реалізації алгоритму.

3. Загрози квантових обчислень: поява квантових обчислень становить значний ризик для класичних криптографічних алгоритмів. Квантові комп'ютери можуть зламати широко використовувані алгоритми, такі як RSA і ECC, що вимагає розробки постквантової криптографії [3].

4. Обчислювальні загрози штучного інтелекту: штучний інтелект використовується військовими криптоаналітиками вже понад 30 років і зараз стає все більш поширеним у повсякденному житті, і оскільки штучний інтелект продовжує розвиватися, він приносить із собою безліч нових викликів безпеці. Системи штучного інтелекту можуть аналізувати величезні обсяги даних з безпрецедентною швидкістю, що може бути як перевагою, так і потенційним ризиком. Зловмисники можуть використовувати штучний інтелект для посилення своїх кібератак, створюючи складніші та складніші для виявлення вторгнення. Крім того, самі алгоритми штучного інтелекту можуть бути вразливими до змагальних атак, коли вхідними даними навмисно маніпулюють, щоб обдурити систему, що призводить до неправильних виходів або рішень. Ці загрози вимагають розробки надійних заходів безпеки штучного інтелекту для захисту від потенційного неправильного використання та вразливостей.

5. Генерація випадкових чисел: криптографічні системи значною мірою покладаються на випадкові числа для генерації ключів та інших процесів. Погано реалізовані генератори випадкових чисел можуть призвести до передбачуваних результатів, роблячи системи вразливими до атак [3].

6. Бекдори: навмисно чи ненавмисно вставлені бекдори в криптографічні системи можуть надати зловмисникам прихований доступ. Ці бекдори може бути надзвичайно важко виявити, і вони можуть підірвати безпеку всієї системи.

7. Вразливості протоколу: криптографічні протоколи, які визначають, як алгоритми використовуються для захисту зв'язку, можуть мати вразливості. Приклади включають атаку POODLE на SSL 3.0 і атаку BEAST на TLS 1.0.

Головними викликами є складність інтеграції криптографічних рішень у існуючі інформаційні системи, необхідність зберігання та управління ключами, а також забезпечення продуктивності системи [4].

1.3. Аналіз нормативно-правових документів, щодо криптографічного захисту інформації

У сфері криптографічного захисту інформації існує низка міжнародних, європейських та національних нормативно-правових актів, які встановлюють вимоги до забезпечення конфіденційності, цілісності та доступності інформації. Ці документи визначають стандарти криптографічного захисту, порядок використання засобів криптографії та вимоги до організацій, що обробляють конфіденційні дані.

Криптографічний захист інформації має відповідати міжнародним стандартам та національним вимогам, зокрема законодавству щодо захисту персональних даних.

До міжнародних стандартів криптографічного захисту інформації відносяться:

1. ISO/IEC 27001:2022 — "Системи управління інформаційною безпекою. Вимоги".

Цей стандарт є основним міжнародним документом у сфері інформаційної безпеки. Він визначає вимоги до створення, впровадження та управління системою захисту інформації. Використання криптографічних методів є однією з ключових вимог цього стандарту для забезпечення безпеки конфіденційних даних [5].

Відповідність до українських вимог:

В Україні цей стандарт адаптовано як ДСТУ ISO/IEC 27001:2023.

2. ISO/IEC 19790:2012 — "Вимоги до безпеки криптографічних модулів".

Цей стандарт встановлює вимоги до проектування та використання криптографічних модулів, які використовуються для шифрування, управління ключами тощо [6].

3. FIPS 140-3 (США) — "Вимоги до криптографічних модулів безпеки".

Документ регламентує стандарти національної безпеки США в криптографії. Він широко застосовується в усьому світі як критерій для оцінки криптографічних засобів [7].

Відповідність до українських вимог:

Хоча цей стандарт є американським, багато українських компаній використовують FIPS 140-3 для міжнародної сертифікації продуктів.

Європейські нормативи та законодавство:

1. GDPR (General Data Protection Regulation) — "Загальний регламент про захист даних"

GDPR (Регламент (ЄС) 2016/679) є основним документом у сфері захисту персональних даних в Європейському Союзі. Регламент зобов’язує організації застосовувати відповідні технічні та організаційні заходи для захисту даних, включаючи криптографічне шифрування, а також псевдонімізацію та анонімізацію персональних даних [8].

Основні вимоги GDPR щодо криптографії:

- захист персональних даних шляхом шифрування (ст. 32);
- забезпечення конфіденційності та цілісності даних при їх передачі чи зберіганні;
- використання криптографічних методів для зменшення ризиків витоку даних (ст. 34).

Національне законодавство України:

1. Закон України "Про захист персональних даних" (№ 2297-VI). Цей закон визначає основні принципи захисту персональних даних, оброблюваних на території України. Він вимагає від організацій забезпечення технічного та організаційного захисту персональних даних. Використання криптографічних методів є рекомендованим для забезпечення конфіденційності інформації [9].

2. ДСТУ 4145-2002 — "Інформаційні технології. Криптографічний захист інформації. Процеси формування та перевірки електронного цифрового підпису". Цей стандарт регламентує використання електронного цифрового підпису (ЕЦП) в

Україні, який базується на криптографічних алгоритмах. ЕЦП є важливим інструментом для автентифікації та захисту електронного документообігу [10].

3. Закон України "Про електронні довірчі послуги" (№ 2155-VIII). Цей документ визначає правові основи використання електронних довірчих послуг, таких як електронний підпис, печатка та часова мітка, що базуються на криптографічних методах. Закон узгоджений із європейським регламентом eIDAS [11].

4. Закон України "Про основні засади забезпечення кібербезпеки" (№ 2163-VIII). Цей закон регламентує захист критичної інформаційної інфраструктури та передбачає використання криптографічних методів для забезпечення безпеки державних і комерційних інформаційних систем [12].

5. НД ТЗІ 2.5-004-99 — " Критерії Оцінки Захищеності Інформації в КС Від НСД". Цей нормативний документ визначає вимоги до організації захисту інформації в державних інформаційних системах, що включає обов’язкове використання сертифікованих криптографічних засобів.

Українське законодавство в цілому відповідає міжнародним стандартам захисту інформації, але потребує постійного оновлення через швидкий розвиток технологій та появу нових загроз. Законодавство України адаптоване до вимог GDPR, що дозволяє забезпечити сумісність із європейськими практиками у сфері захисту персональних даних [13].

Основні відмінності: Законодавство України є менш конкретизованим щодо технічних аспектів впровадження криптографічного захисту. Українські вимоги здебільшого орієнтовані на захист державних даних, тоді як GDPR фокусується на персональних даних приватних осіб.

Висновки до розділу 1

1. Проведено аналіз проблеми криптографічного захисту інформації.

2. Проаналізовано сучасні загрози безпеці інформаційних систем.

3. Досліджено проблеми впровадження криптографічного захисту.

4. Проаналізовано нормативно-правова база, щодо криптографічного захисту.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ

2.1. Симетричне шифрування

Шифрування є однією з найпростіших концепцій у світі кібербезпеки, оскільки воно гарантує, що деяка інформація не потрапить у чужі руки. Існує два основних типи методів шифрування: симетричне та асиметричне [14].

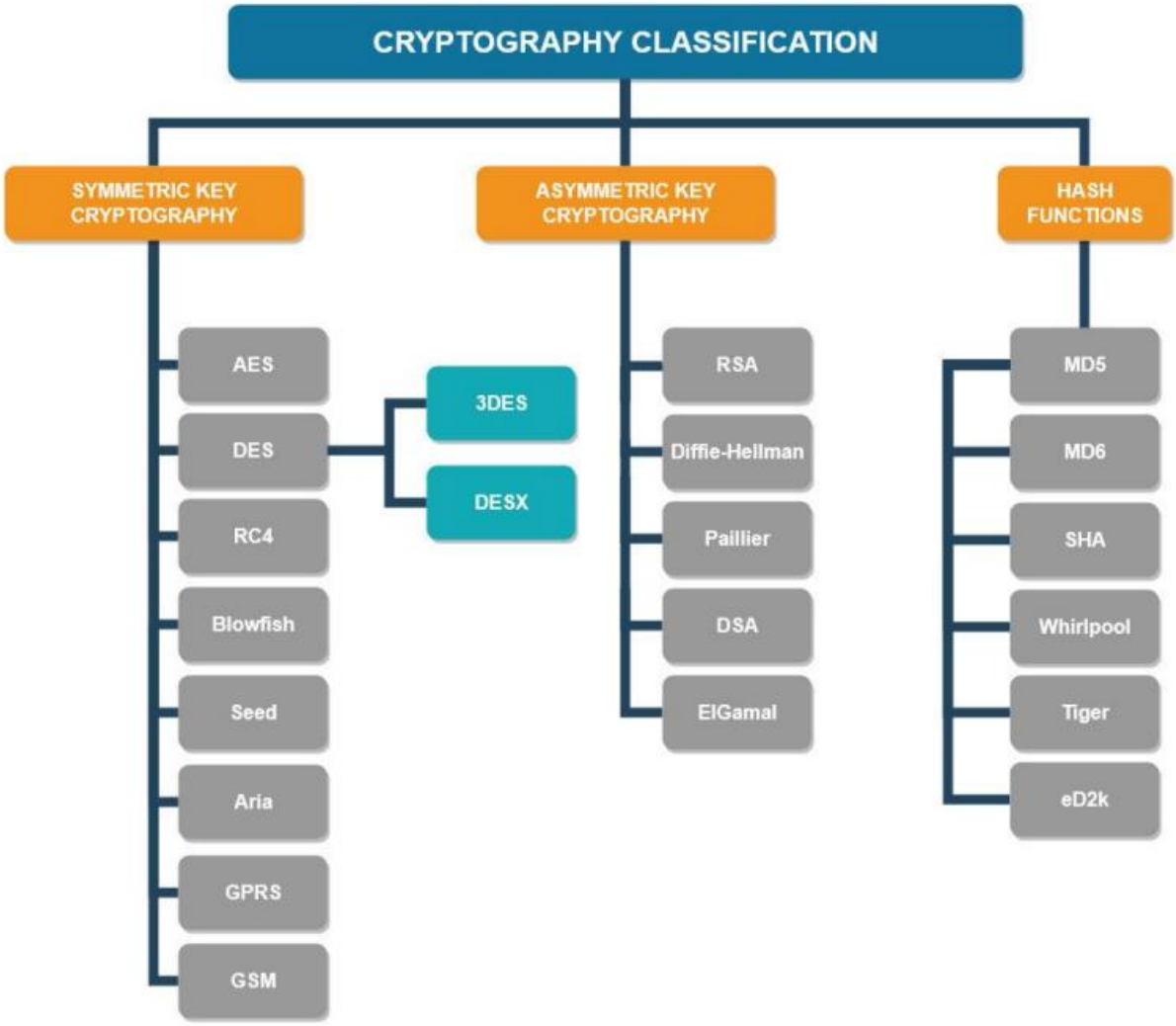

Рис. 2.1. Криптографічна класифікація [15]

Симетричне шифрування (або шифрування «симетричним ключем») — це процес використання одного ключа як для шифрування, так і для розшифрування даних.

Симетричне шифрування – це широко використовувана форма криптографії, яка надає організаціям і користувачам швидшу та доступнішу для розгортання форму безпеки для великих наборів даних.

Симетричне шифрування часто використовується для обробки великих обсягів даних, де важлива швидкість, ефективність і складність. Однак, через свою природу як одноключового рішення, воно створює кілька проблем із безпекою, коли справа доходить до фактичного обміну зашифрованими даними. З цієї причини симетричне шифрування часто поєднується з асиметричним шифруванням (яке використовує різні ключі для шифрування та дешифрування) у багатьох сучасних протоколах безпечного зв'язку (див. 2.2) [16].

Загальний процес шифрування працює наступним чином:

Генерація ключів: секретний ключ генерується за допомогою складних математичних рівнянь, який використовується для кодування даних. Цей ключ передається відправнику та одержувачу для запобігання заплутуванню даних.

Шифрування: Процес використовує складні алгоритми та випадкові дані навколишнього середовища (так звану «ентропію») для перетворення вихідних даних і включає кілька раундів перетворення, щоб гарантувати, що шифротекст не легко розшифровується без ключа [16].

Розшифровка: отримавши дані, одержувач використовує той самий ключ для декодування даних – по суті, виконуючи процес у зворотному порядку, при цьому ключ служить інформацією, необхідною для «розблокування» цих даних.

Крім того, алгоритми симетричного шифрування зазвичай бувають однієї з двох форм:

Потокові шифри: потокові шифри шифрують відкриті текстові повідомлення по одному біту за раз. Вони створюють довільно довгий потік бітів, який потім об'єднується з бітами відкритого тексту один за одним для створення шифротексту.

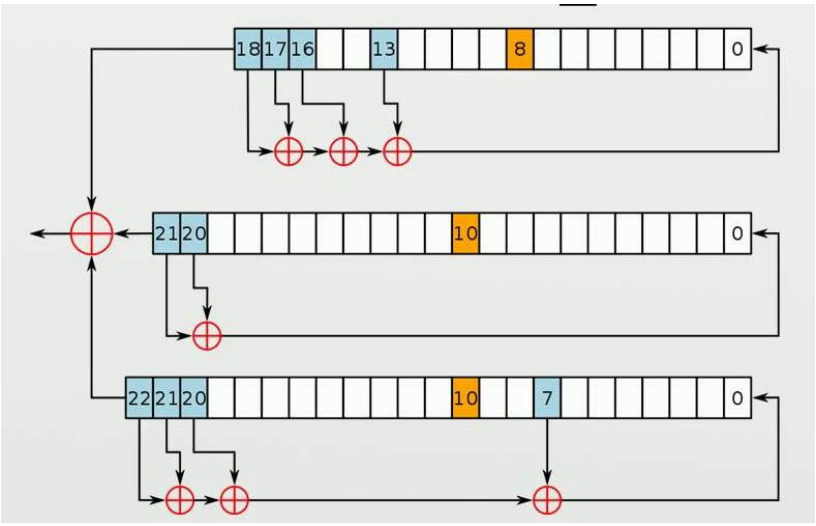

Рис. 2.2. Потоковий шифр [16]

Блокові шифри: блокові шифри беруть шматок або блок даних і перетворюють їх. Потім він працює через набір даних блок за блоком. Деякі блокові шифри будуть багаторазово шифрувати блоки для додаткової безпеки.

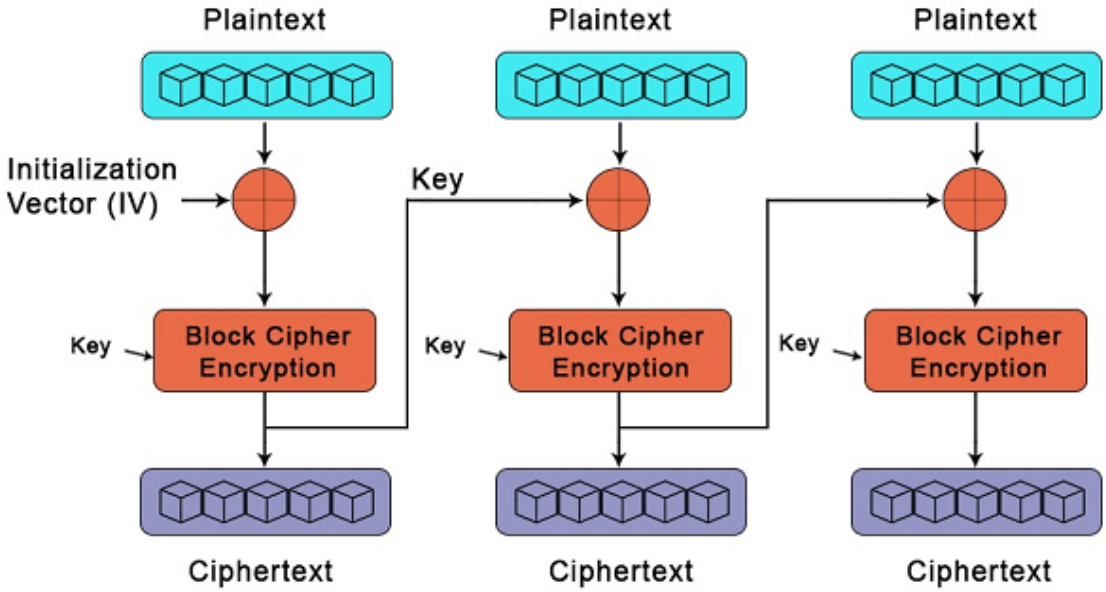

Рис. 2.3. Блоковий шифр [17]

Існує не обмежена кількість алгоритмів шифрування. Деякі з найбільш популярних або, принаймні, добре відомих, симетричних алгоритмів включають:

Advanced Encryption Standard (AES): В даний час це один з найбільш широко використовуваних алгоритмів симетричного шифрування, який підтримується для

національної безпеки (NIST) і промислових додатків. Існує кілька різних складнощів AES (найпоширенішими є 128-бітні та 256-бітні), які означають зростаючий рівень безпеки [18].

Стандарт шифрування даних (DES): цей симетричний алгоритм, який в основному використовувався кілька десятиліть тому, був фактично зламаний і більше не вважається безпечним. Його було відхилено на користь Triple DES або, у випадках федеральних або промислових стандартів шифрування, AES.

Triple DES (3DES): Це розширення нині неіснуючого алгоритму DES, який тричі обробляє відкриті текстові блоки для додаткової безпеки, зі значним компромісом із продуктивністю.

Blowfish і Twofish: Це блокові шифри, розроблені як альтернатива DES. Blowfish має розмір блоку 64 біти, тоді як Twofish має розмір блоку 128 біт. Twofish був одним із фіналістів конкурсу, який обирав AES.

2.2. Асиметричне шифрування

Асиметричне шифрування — це метод шифрування, який використовує два різні ключі — відкритий і закритий — для шифрування та розшифрування даних. Зазвичай воно вважається більш безпечним, хоча і менш ефективним, ніж симетричне шифрування.

Асиметричне шифрування забезпечує безпеку даних за допомогою криптографічних алгоритмів для генерації пари ключів: відкритого ключа та приватного ключа. Будь-хто може використовувати відкритий ключ для шифрування даних, але лише ті, хто має відповідний приватний ключ, можуть розшифрувати ці дані для їх зчитування [19].

Ключі функціонують як складні коди, необхідні для розблокування сейфа. Без правильного криптографічного ключа користувачі не можуть розшифрувати зашифровані дані. Як правило, чим більший розмір ключа, тим вищий рівень безпеки. Асиметричне шифрування відоме тим, що має набагато більшу довжину ключа, ніж симетричне шифрування, що сприяє його вищій безпеці.

В асиметричному шифруванні ці два ключі служать різним цілям:

- відкритий ключ шифрує дані або перевіряє цифрові підписи і може вільно розповсюджуватися та поширюватися;

- приватний ключ розшифровує дані та створює цифрові підписи, але має залишатися секретним для забезпечення безпеки.

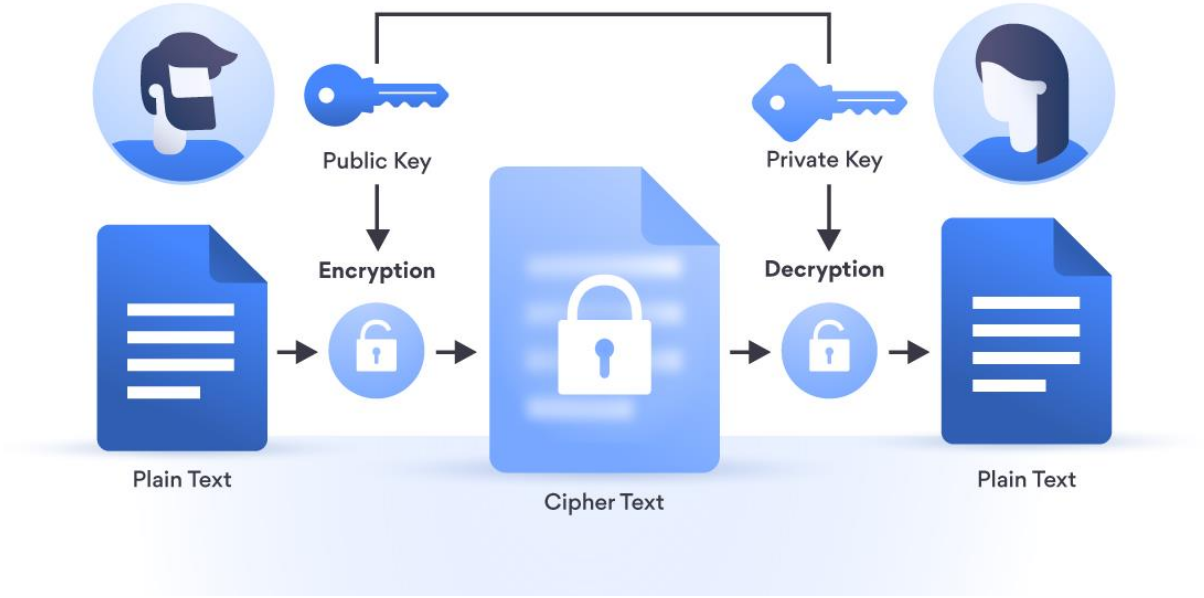

Рис. 2.4. Асиметричне шифрування [19]

Деякі з найбільш значущих алгоритмів асиметричного шифрування включають:

- Рівест-Шамір-Адлеман (RSA)

RSA – це асиметричний алгоритм шифрування, названий на честь його винахідників. Він спирається на математичну складність простих чисел для створення пар ключів. Він використовує пару публічний-закритий ключ для шифрування та дешифрування, що робить його придатним для безпечної передачі даних і цифрових підписів.

Алгоритм RSA часто допомагає захистити протоколи зв'язку, такі як HTTPS, SSH і TLS. Незважаючи на розробку в 1970-х роках, RSA залишається широко використовуваним завдяки своїй надійності та безпеці. Різні програми покладаються на RSA, включаючи безпечну електронну пошту, VPN та оновлення програмного забезпечення [20].

- криптографія з еліптичною кривою (ECC).

ECC — це метод асиметричного шифрування, заснований на математичних властивостях еліптичних кривих над скінченними полями. Він забезпечує надійну безпеку з меншою довжиною ключа, ніж інші алгоритми, що призводить до швидших обчислень і меншого енергоспоживання.

Ефективність ECC робить його ідеальним для додатків з обмеженою обчислювальною потужністю та часом автономної роботи, таких як мобільні додатки, програми для безпечного обміну повідомленнями та пристрої IoT.

- алгоритм цифрового підпису (DSA).

Алгоритм цифрового підпису (DSA) дає змогу організаціям і окремим особам створювати цифрові підписи, які забезпечують автентичність і цілісність повідомлень або документів [20].

Стандартизований NIST, DSA спирається на математичну задачу дискретного логарифма і з'являється в різних протоколах безпеки. DSA часто використовується в додатках, які вимагають безпечного підписання та перевірки документів, включаючи розповсюдження програмного забезпечення, фінансові транзакції та системи електронного голосування.

Таблиця 2.1.

Різниця між симетричним та асиметричним шифруванням [21]

	Симетричне шифрування	Асиметричне шифрування
Конфіденційність	Для цього потрібен лише один ключ як для шифрування, так і для дешифрування.	Для цього потрібні два ключі, відкритий ключ і приватний ключ, один для шифрування, а інший для розшифровки.
Швидкість	Процес шифрування дуже швидкий.	Процес шифрування відбувається повільно.
Довжина клавіш	Виходячи з вимог безпеки, довжина використовуваних ключів зазвичай становить 128 або 256 біт.	Довжина ключів набагато більша, ніж при симетричному шифруванні, наприклад, рекомендований розмір ключа RSA становить 2048 біт або вище.

Продовження таблиці 2.1

Різниця між симетричним та асиметричним шифруванням [21]

	Симетричне шифрування	Асиметричне шифрування
Безпека	Менш безпечний через використання одного ключа для шифрування.	Набагато безпечніше, оскільки в шифруванні та розшифровці беруть участь два ключі.
Розмір даних	Використовується для передачі великих даних.	Використовується для передачі невеликих даних.
Використання ресурсів	Шифрування з симетричним ключем працює при мінімальному використанні ресурсів.	Асиметричне шифрування вимагає великої витрати ресурсів.
Розташування клавіш	Розташування клавіш – велика проблема	Розташування клавіш – це зовсім не проблема.
Ризик	Секретний ключ є спільним. Отже, ризик компромісу вищий.	Приватний ключ не є спільним, і загальний процес є більш безпечним у порівнянні з симетричним шифруванням.
Математичне представлення	P = Д (K, E(K, P)) де K – > ключ шифрування та дешифрування П –> звичайний текст Д –> Розшифровка E(K, P) –> Шифрування відкритого тексту за допомогою K	P = D(Kd, E (Ke,P)) де Ke – > ключ шифрування Kd – ключ розшифровки > Д –> Розшифровка E(Ke, P) –> Шифрування відкритого тексту за допомогою ключа шифрування Ke. П –> звичайний текст
Приклади	Приклади: 3DES, AES, DES і RC4	Приклади: Діффі-Хеллман, ECC, El Gamal, DSA та RSA.

2.3. Хешування та цифрові підписи

Хеш-функція — це алгоритм, який відображає дані будь-якого розміру з фіксованим, зазвичай меншим, значенням, відомим як «хеш» або «дайджест». Ця функція розроблена таким чином, щоб бути ефективною з точки зору часу виконання та генерувати різні хеші для різних типів даних. Хеш-функції зазвичай

використовуються в криптографії, базах даних, інформаційній безпеці та інших областях обчислювальної техніки [22].

SHA-256 (алгоритм безпечного хешування, 256 біт)

SHA-256 є більш безпечною версією алгоритму SHA, який видає дайджест з 256 біт (32 байти). Він широко використовується в програмах інформаційної безпеки та криптографії.

```python
# python script to show an example for sha256
import hashlib

# Dados de entrada
data = "Hello, world!"

# Calculando o hash SHA-256
sha256_hash = hashlib.sha256(data.encode()).hexdigest()
print("SHA-256:", sha256_hash)
```

```
SHA-256: 315f5bdb76d078c43b8ac0064e4a0164612b1fce77c869345bfc94c75894edd3
```

Рис. 2.5. Приклад хеш-функції

Цифрові підписи гарантують, що цифрова інформація є правдивою та безпечною. Вони створюються шляхом обчислення хешу вмісту повідомлення, який потім шифрується за допомогою закритого ключа відправника. Відкритий ключ відправника може бути використаний для виконання математичної перевірки цього підпису. Цілісність і достовірність інформації підтверджується, якщо розшифрований хеш підпису збігається з обчисленим хешем вихідного повідомлення [22]. В іншому випадку підпис або повідомлення вказують на те, що були внесені зміни.

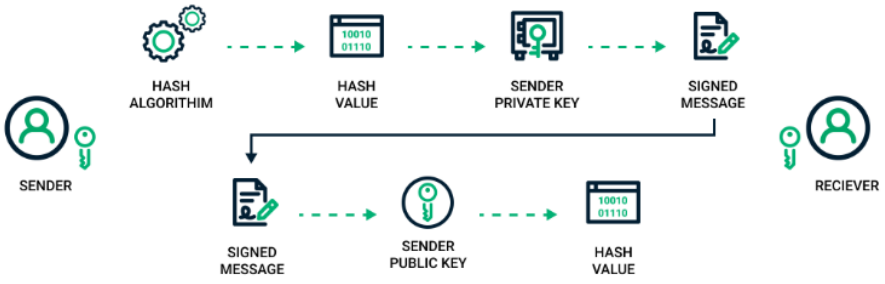

Рис. 2.6. Принцип роботи цифрового підпису [23]

Цифрові підписи ґрунтуються на цифрових сертифікатах, виданих центрами сертифікації (ЦС).

Сертифікати використовуються для зв'язування цифрових посвідчень із парою ключів користувача та містять такі дані, як ім'я, дата закінчення терміну дії сертифіката, копія відкритого ключа та інформація про ЦС, який видав сертифікат.

Відповідний ЦС перевіряє особистість кожного користувача; Після цього користувач може створити цифровий сертифікат і підписати будь-який документ, який він бажає.

У свою чергу, цифрові підписи засновані на асиметричній криптографії і, як уже згадувалося раніше, мають відкритий і закритий ключ [23].

Коли ви бажаєте підписати документ, за допомогою хеш-функції часто створюється хеш (унікальна ідентифікація цифрового документа, яка не підлягає передачі). Цей хеш шифрується за допомогою закритого ключа підписувача та об'єднується з відкритим ключем для формування цифрового підпису.

Таким же чином одержувач використовує відкритий ключ для перевірки ідентичності підпису. Це гарантує, що інформація, надіслана між двома людьми, не буде помічена ніким іншим.

Хеш-функції дозволяють гарантувати цілісність даних, тоді як цифрові підписи забезпечують автентифікацію та достовірність в електронному документообігу.

Висновки до розділу 2

1. Досліджено методи та засоби криптографічного захисту інформації.

2. Проаналізовано симетричне, асиметричне шифрування.

3. Наведено принципи роботи шифрування, хешування та цифрового підпису.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1. Розроблення варіанта розгортання технології криптографічного захисту інформації на основі Boxcryptor

Boxcryptor надає зручний додатковий рівень безпеки для хмарних сховищ, шифруючи файли локально на пристрої. Оскільки Boxcryptor було оптимізовано для хмарних сховищ від самого початку, шифрування відбувається для кожного файлу, а доступ до нього може бути спільним. Це означає, що кожен файл шифрується незалежно від інших. Крім того, підтримуються типові функції хмарного сховища, такі як історія файлів або вибіркова синхронізація [24].

Boxcryptor не є хмарним сховищем даних. Це програмне забезпечення, яке додає рівень безпеки до обраного хмарного сховища. Тому Boxcryptor не зберігає ваші дані. Відповідальність за зберігання та управління вашими файлами лежить на вашому хмарному провайдері.

- Boxcryptor не є клієнтом синхронізації, а це означає, що Boxcryptor на Windows або macOS не синхронізує ваші файли з хмарою. Ця відповідальність також лежить на вашому хмарному провайдері. Тому вам доведеться встановити на свій пристрій програмне забезпечення вашого хмарного провайдера.

- Boxcryptor не призначений для захисту довільних хмарних сервісів. Такі сервіси, як Google Docs або Evernote, не працюють з локально збереженими файлами, а зберігають дані безпосередньо в базах даних на своїх серверах. Boxcryptor може шифрувати лише файли - ваші файли, які ви зберігаєте у хмарі, а не сервіси.

- Boxcryptor не є VPN-рішенням. Хоча співпрацює з різними VPN-провайдерами, ми жодним чином технічно не пов'язані з їхніми продуктами.

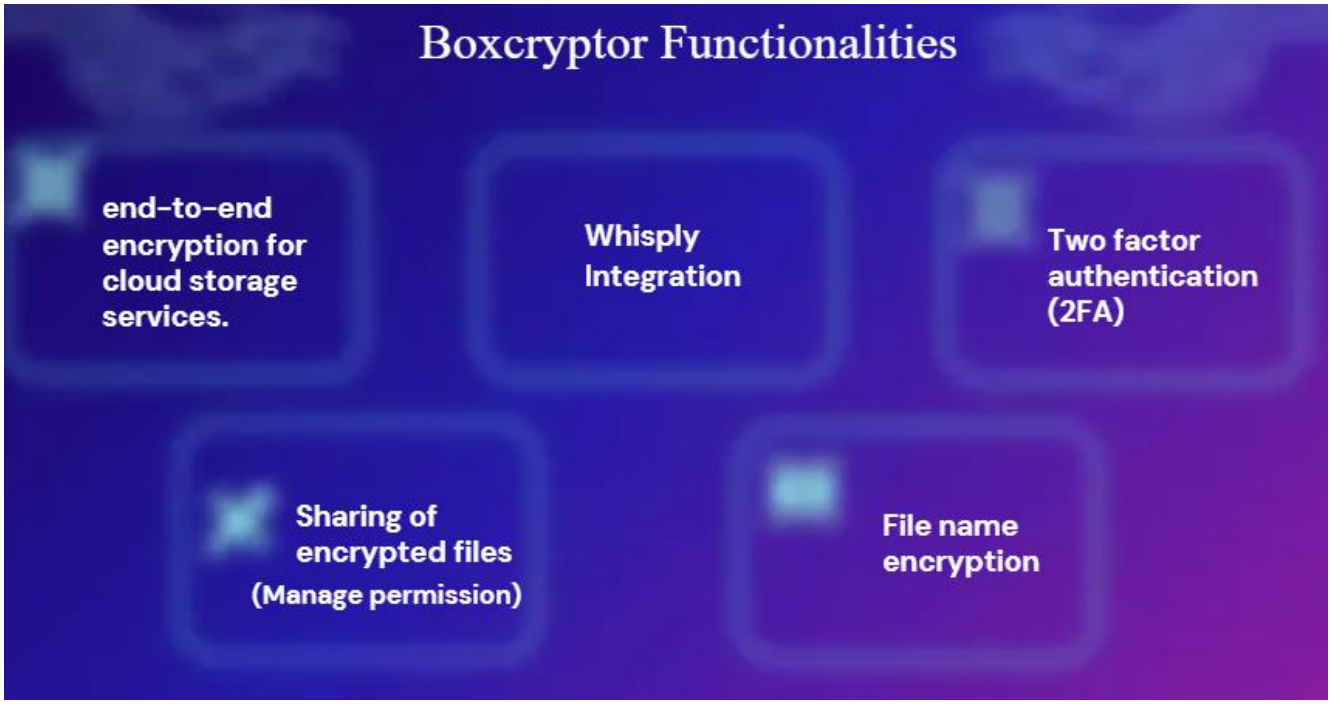

Рис. 3.1. Функції Boxcryptor [24]

Функції Boxcryptor:

1. end-to-end encryption для хмарних сервісів зберігання даних.

Наскрізне шифрування для хмарних сервісів зберігання даних. Тобто Boxcryptor забезпечує безпечне шифрування файлів від моменту створення чи збереження на комп'ютері до передачі та зберігання у хмарі, не дозволяючи стороннім отримати доступ до незашифрованого вмісту.

2. Whisply Integration

Інтеграція з сервісом Whisply. Whisply є інструментом для безпечного обміну зашифрованими файлами та посиланнями через хмарні сервіси, а отже інтеграція з Boxcryptor дає змогу легко та безпечно ділитися файлами із зовнішніми отримувачами.

3. Two factor authentication (2FA)

Наявність двофакторної аутентифікації. Для входу в обліковий запис чи отримання доступу до зашифрованих файлів користувачеві потрібно пройти додатковий етап перевірки (наприклад, код на телефон чи інший спосіб), підвищуючи безпеку облікового запису [24].

4. Sharing of encrypted files (Manage permission).

За допомогою Boxcryptor можна ділитися зашифрованими файлами з іншими користувачами, одночасно керуючи правами доступу. Це означає, що можна налаштовувати, хто саме та який рівень доступу матиме доступ до конкретних файлів чи папок.

5. File name encryption.

Функція шифрування імен файлів. Зазвичай при використанні хмарних сховищ імена файлів можуть бути видимими для операторів сервісу чи потенційних зловмисників. Шифрування імен дозволяє приховати навіть назву файлу, а не лише його вміст [24].

Встановлення та налаштування Boxcryptor

Підготовчим етапом є інсталяція програми в штатному режимі та створення аккаунта на офіційному порталі.

Після встановлення Boxcryptor і входу до свого облікового запису ви зможете отримати доступ до сховища Boxcryptor.

Boxcryptor автоматично додає всі встановлені хмарні сервіси на диск. Диск діє як шар над вашими існуючими файлами. Він дозволяє переглядати, редагувати та зберігати зашифровані файли «в реальному часі».

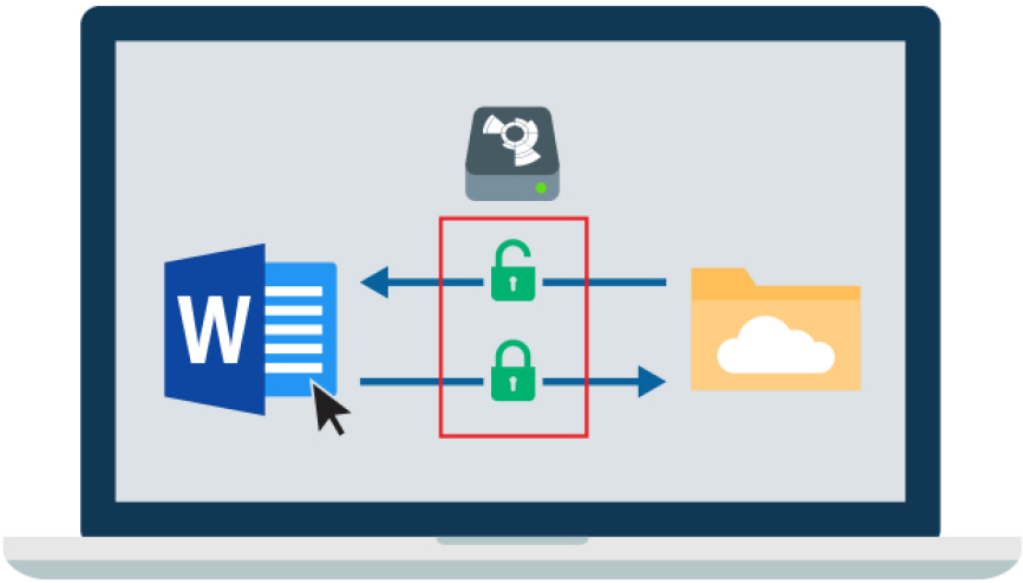

Рис. 3.2. Маленькі іконки позначають файли і показують, чи зашифрований файл або папка чи ні [25]

Усі файли та папки, які додаються до зашифрованої папки в Boxcryptor, будуть зашифровані автоматично.

Рис. 3.3. Зашифрована папка в Boxcryptor

Якщо вже існують файли і папки в хмарі, Boxcryptor дозволяє зашифрувати і їх [25].

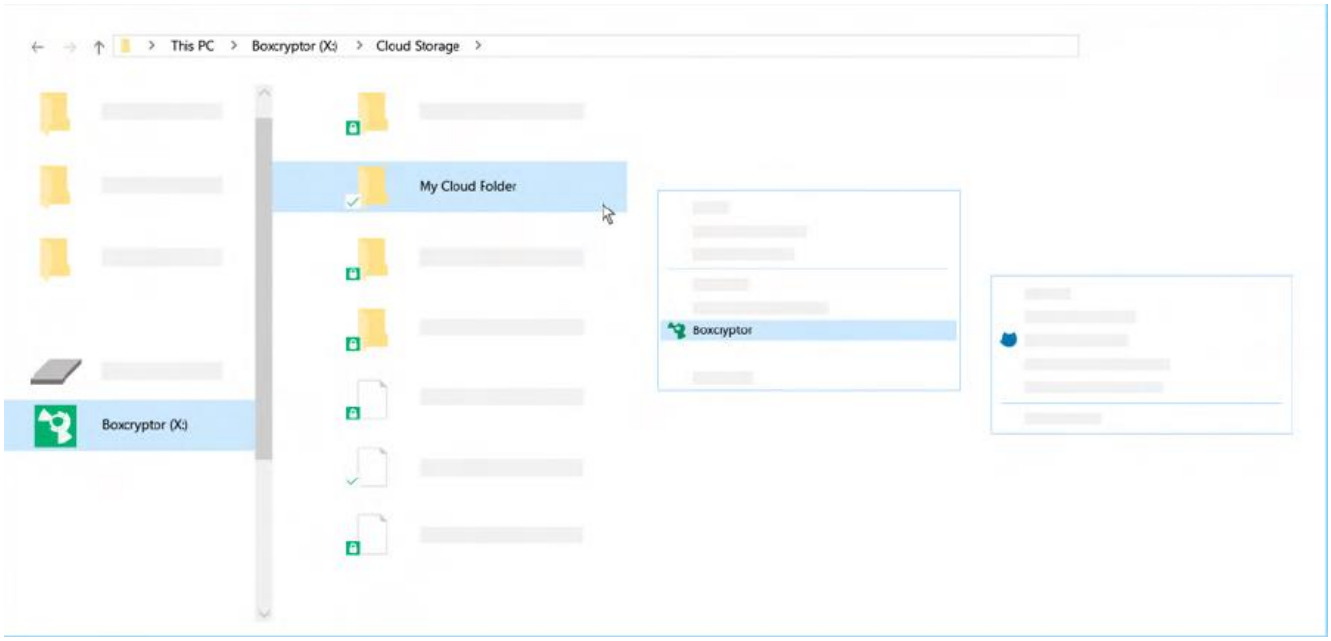

Рис. 3.4. Шифрування файлів хмари

Перейдіть до свого диска Boxcryptor [25].

2. Клацніть правою кнопкою миші на файлі або папці - Boxcryptor --> Зашифрувати [25].

3. Зачекайте, поки клієнт синхронізації вашого хмарного провайдера все синхронізує.

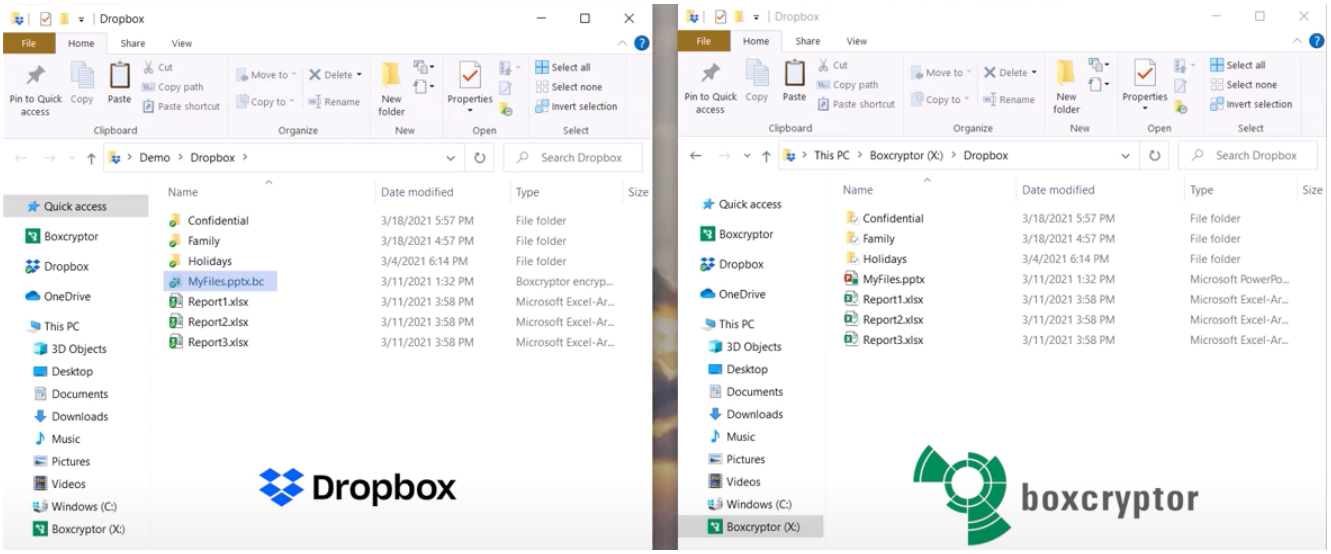

Рис. 3.5. Зашифровані файли Dropbox з розширенням *.bc в Boxcryptor звичайний файл [25]

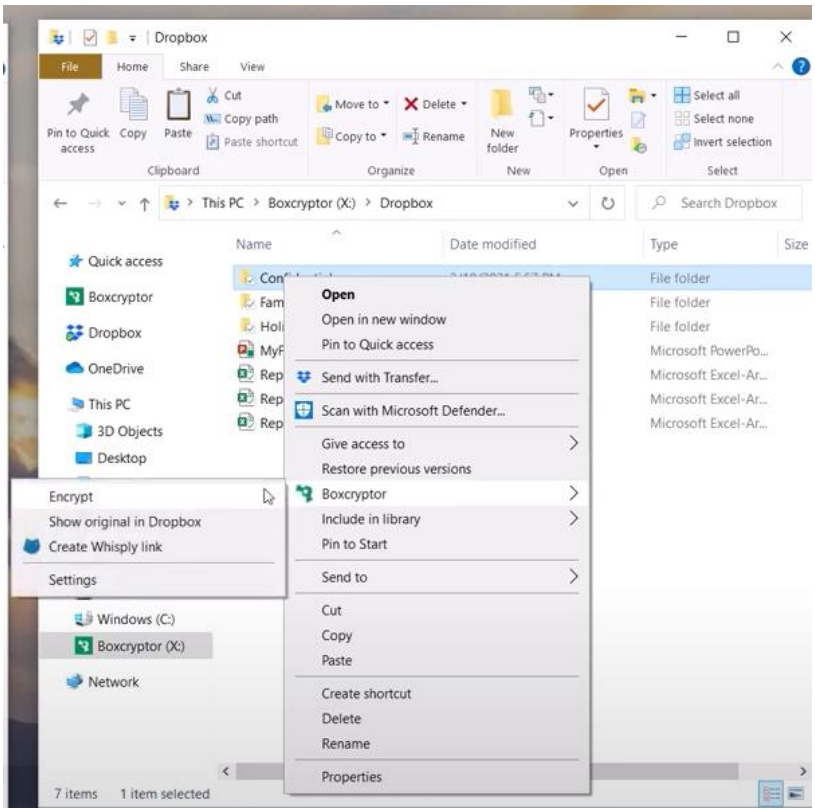

Рис. 3.6. Шифрування папки

Зашиврована папка містить зелену піктограму в правому куті рис. 3.7 і всі файли які будуть додаватися в папку автоматично шифруватимусться [25].

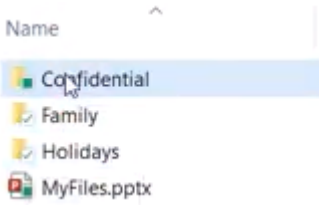

Рис. 3.7. Захищена папка

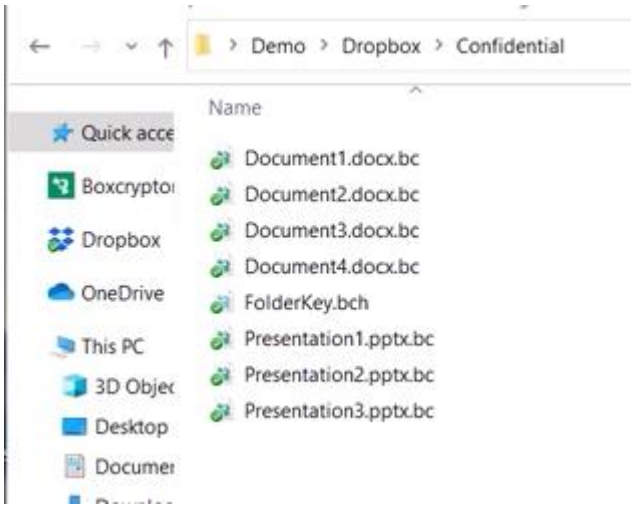

Рис. 3.8. Розширення зашифрованих файлів в Dropbox [25]

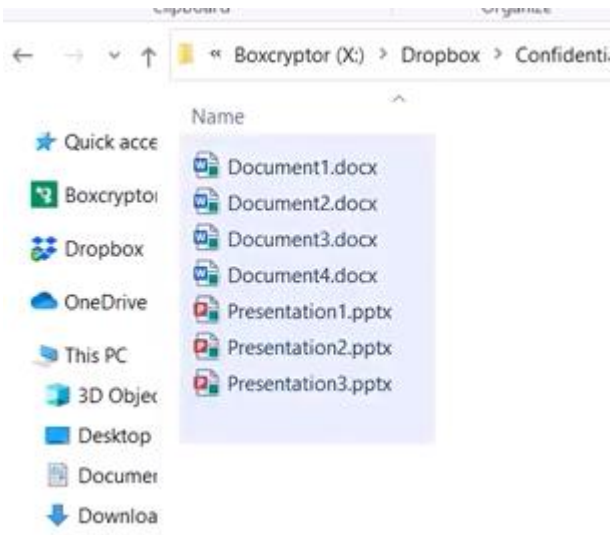

Рис. 3.9. Вміст файлів у Boxcryptor

Керування хмарами та локаціями

Boxcryptor підтримує широкий спектр провайдерів хмарних сховищ з коробки. Крім того, Boxcryptor працює з усіма хмарними провайдерами, які підтримують протокол WebDAV.

Boxcryptor працює як додатковий рівень безпеки для хмарного сховища. Виконує шифрування, а програмне забезпечення хмарного сховища синхронізує файли з хмарою. Тому Boxcryptor вимагає, щоб у системі був встановлений клієнт синхронізації хмарного провайдера [26].

Більшість хмарних сховищ автоматично додаються до Boxcryptor і записуються, як місцезнаходження на диск Boxcryptor. Якщо хмару не виявлено автоматично, її можна додати вручну, як власне розташування.

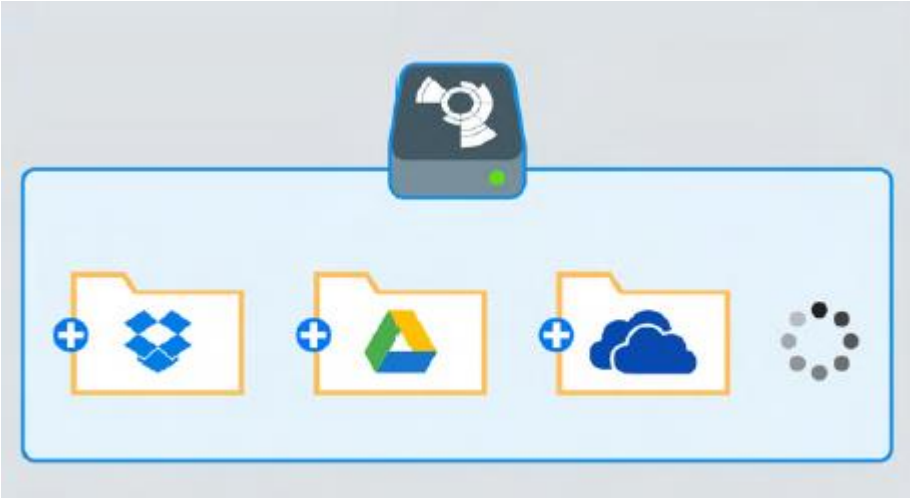

Рис. 3.10. Процес синхронізації хмари з Boxcryptor

Через технічні обмеження Apple, Boxcryptor для macOS розрізняє ICloud і ICloud Drive (тільки для Mac і PC). Якщо використовувати Boxcryptor на iPhone або iPad, необхідно переконатися, що використовуєте ICloud, тому що ICloud Drive (тільки для Mac і PC) доступний тільки на пристроях Mac або PC [26].

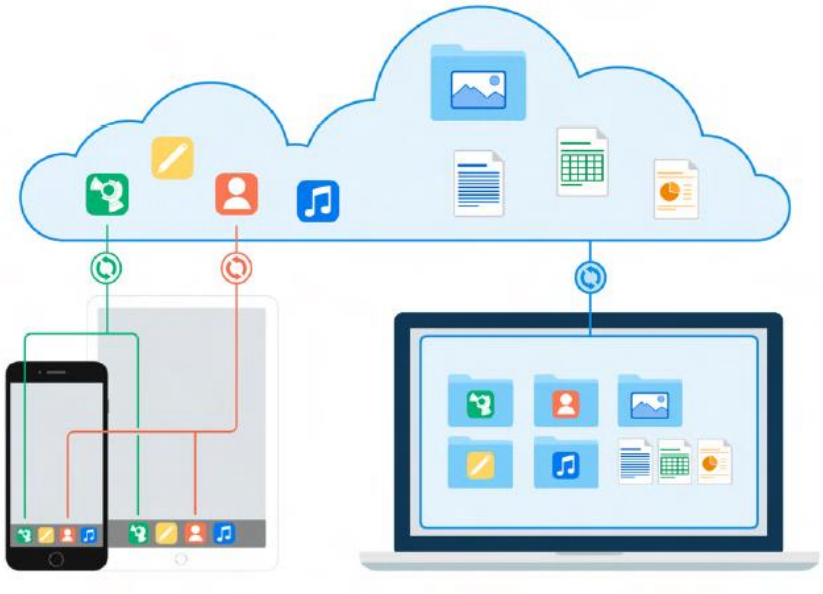

Рис. 3.11. Схема роботи з ICloud та ICloud Drive [26]

Той факт, що існує ICloud Drive (типовий хмарний провайдер) та ICloud (де всіма вашими додатками та їхнім хмарним простором керує Apple), робить налаштування шифрування на різних платформах дещо складнішим, порівняно з іншими хмарними сервісами. На початку необхідно виконати деякі додаткові кроки.

Але як тільки ваш ICloud у поєднанні з Boxcryptor налаштований, працювати з даними так само просто, як і на інших платформах.

3.2. Технологія криптографічного захисту інформації на основі Boxcryptor

Робота з файлами

Після налаштування Boxcryptor не помітно, що файли зашифровані.

Шифрування On-the-fly

Boxcryptor шифрує ваші дані «на льоту», шифруючи кожен файл окремо. Коли працюєте з файлами, немає необхідності в масовому розшифруванні. Просто відкриваєте будь-який зашифрований файл, і його вміст буде розшифровано автоматично у фоновому режимі. Коли зберігаєте зміни, вміст знову автоматично

шифрується. При роботі із захищеними даними за допомогою Boxcryptor, не помічаєте криптографічного процесу, що стоїть за ними [24-26].

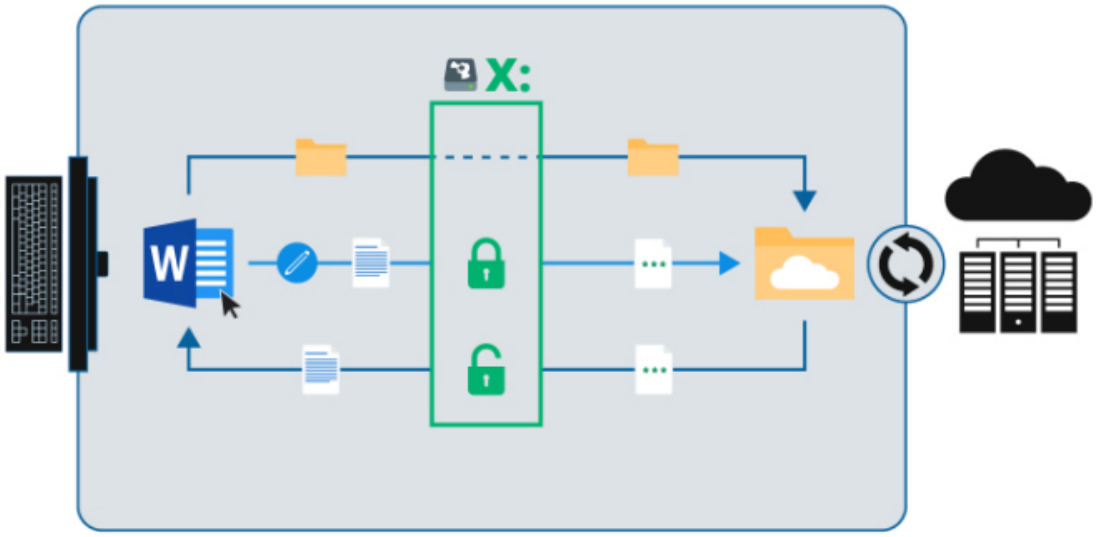

Рис. 3. 12. Схема шифрування On-the-fly

Шифрування та ієрархія дозволів

Для кожного файлу або папки встановлюється окремий рівень безпеки. Boxcryptor дає повний контроль над цим. Існує можливість дозволяти іншим користувачам доступ до файлу, надавши їм відповідні дозволи, додатково існує можливість вибору зашифрування ім'я файлу, або залишити окремі файли і теки незашифрованими.

Для спрощення всі властивості папок успадковуються ієрархічно від теки, яка його містить. Наприклад, якщо у вас є зашифрована тека з назвою «Мої таємні файли» і додаєте до неї файл, цей файл буде зашифровано автоматично, а вибрані дозволи буде успадковано. Те саме стосується цілих тек [24-26].

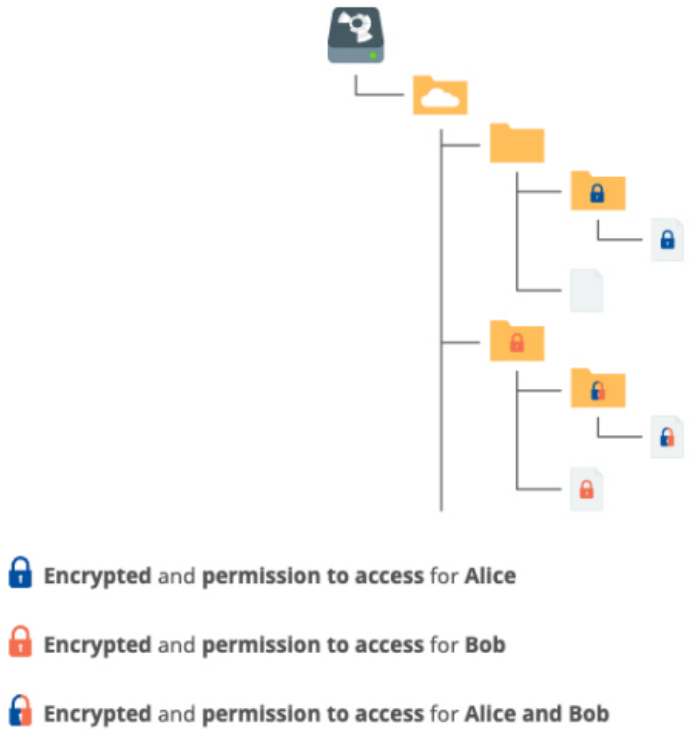

Рис. 3.13. Ієрархія дозволів

Надання спільного доступу до файлів

Однією з головних причин використання хмарних сховищ є простота обміну файлами та можливість спрощення віддаленої групової роботи. Boxcryptor дозволяє залишатися в безпеці під час спільної роботи та обміну файлами з іншими.

Якщо ви зберігаєте незашифрований файл на своєму пристрої або в хмарі, програма, за допомогою якої ви його зберігаєте, зберігає файл та інформацію, що міститься в ньому. Такий файл може прочитати або змінити будь-хто, хто має до нього фізичний доступ. Якщо ж ви зашифруєте файл, інформація всередині нього буде змінена. Для програм і людей зашифрована інформація стає марною. Щоб знову розшифрувати інформацію, вам знадобиться криптографічний ключ, який повертає інформацію до початкового стану [24-26].

Тому ділитися з кимось зашифрованим файлом - це все одно, що писати електронного листа, плутаючись у клавіатурі. Інша людина може прочитати інформацію, але вона марна, оскільки не має жодного смислового значення.

Як наслідок, є два кроки, необхідні для того, щоб поділитися зашифрованим файлом:

1. Надайте фізичний доступ до файлу своєму хмарному провайдеру. Перш за все необхідно ознайомитися з документацією вашого провайдера про те, як надавати спільний доступ до файлів або папок іншим користувачам.

2. Надайте доступ до криптографічного ключа в Boxcryptor. Boxcryptor використовує ключ для кожного файлу. Ключ шифрується вашим обліковим записом Boxcryptor і зберігається в самому файлі. Якщо ви надаєте комусь доступ до файлу, ключ буде зашифрований за допомогою акаунта Boxcryptor одержувача і також зберігатиметься у файлі.

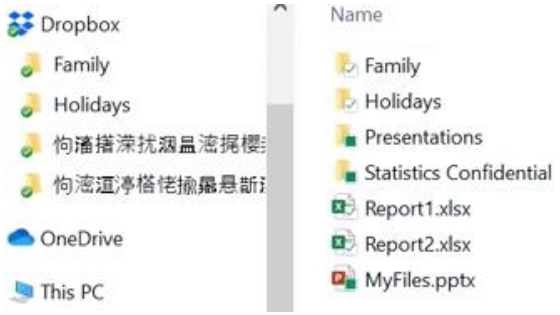

Рис. 3.13. Шифровані імена файлів [24-26]

Шифровані імена файлів відображаються у хмарному середовищі, а не шифровані тільки під вашим Boxcryptor диском.

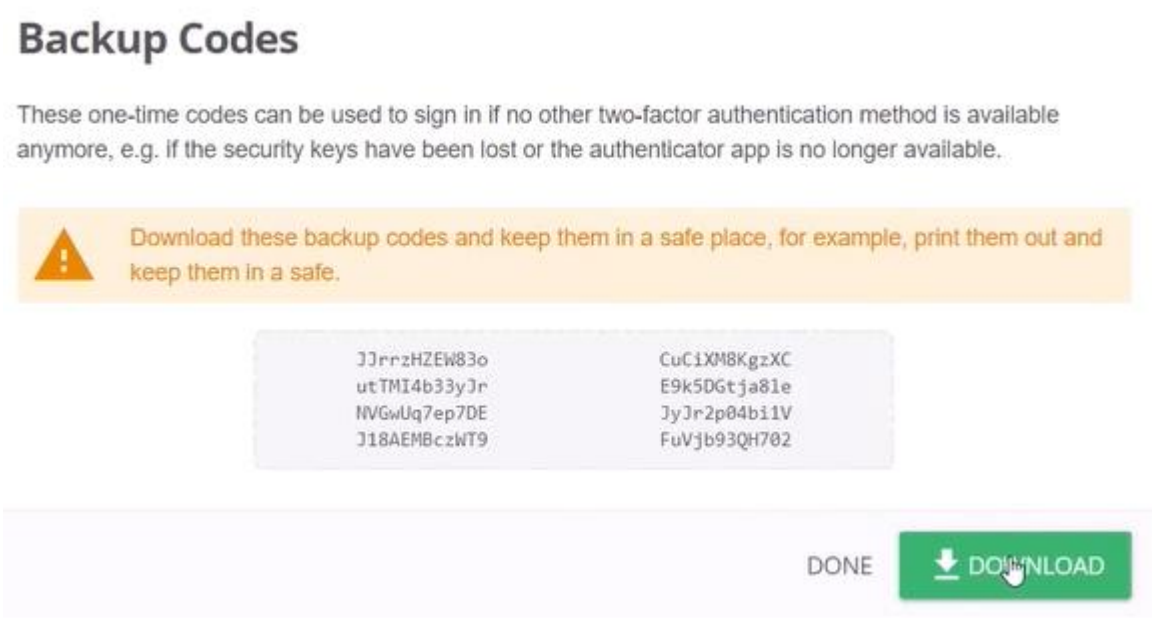

Рис. 3.14. Генерація кодів 2FA

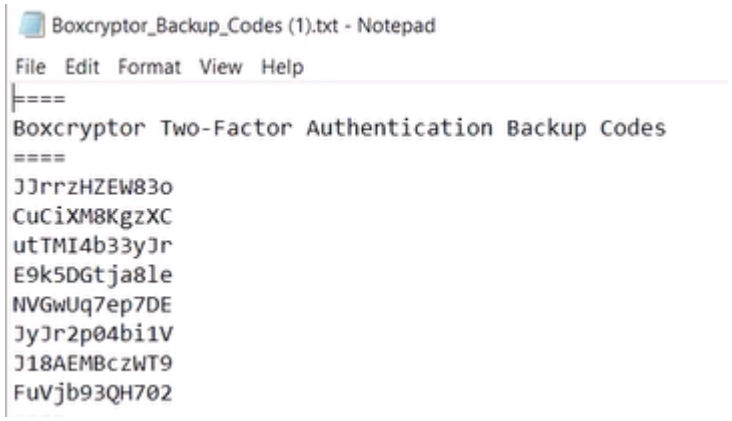

Рис. 3.15. Завантажений файл кодів [24-26]

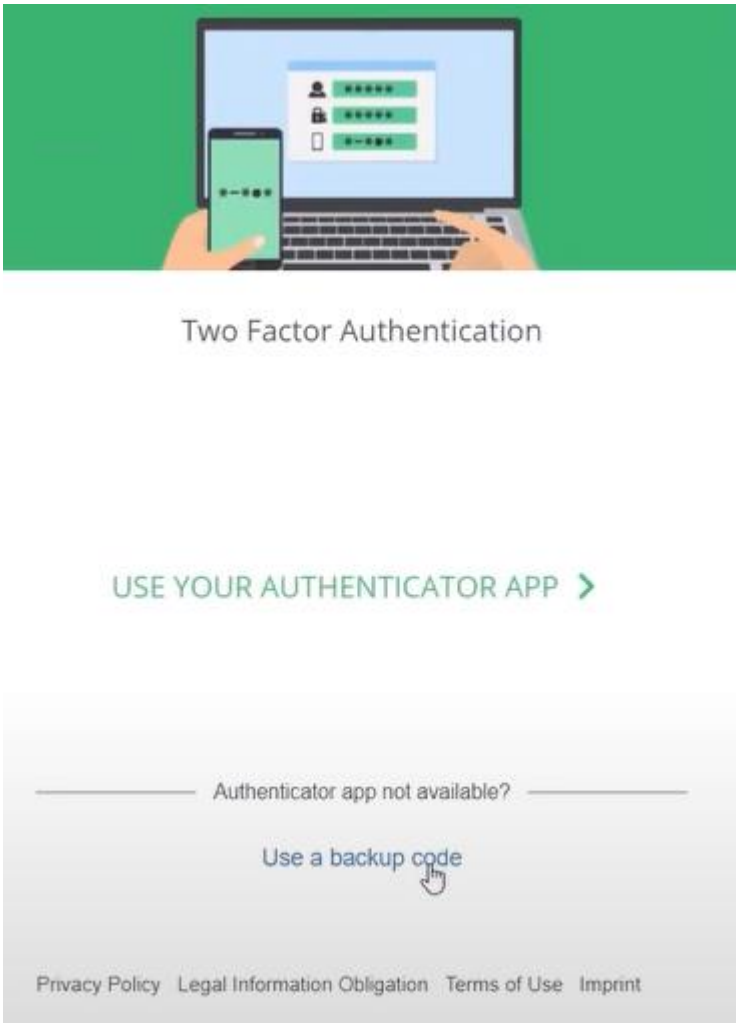

Рис.3.16. Використання 2FA

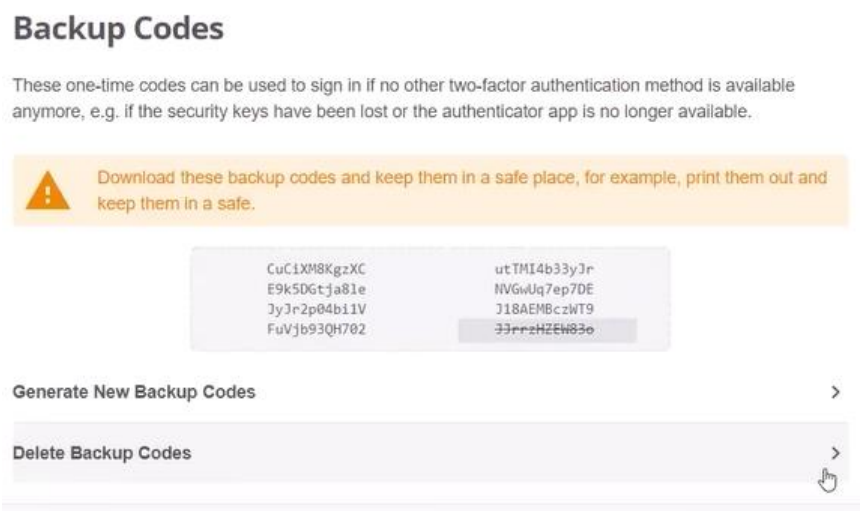

Рис. 3.17. Відображення використаних кодів [27]

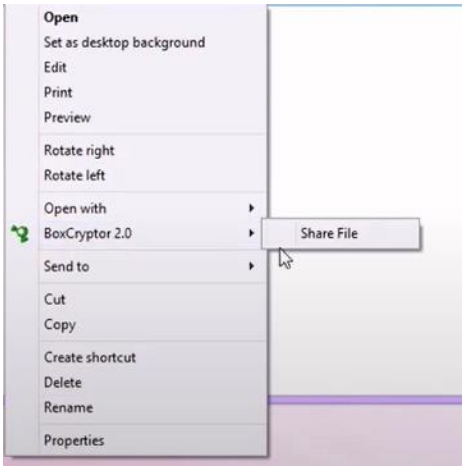

Рис. 3.18. Поділитися файлами

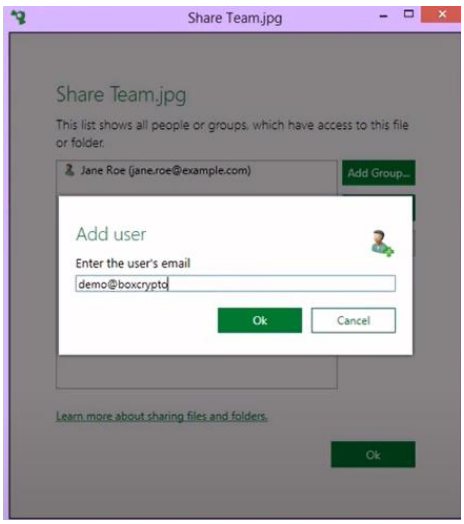

Рис. 3.19. Надання доступу до файлу певним користувачам [28]

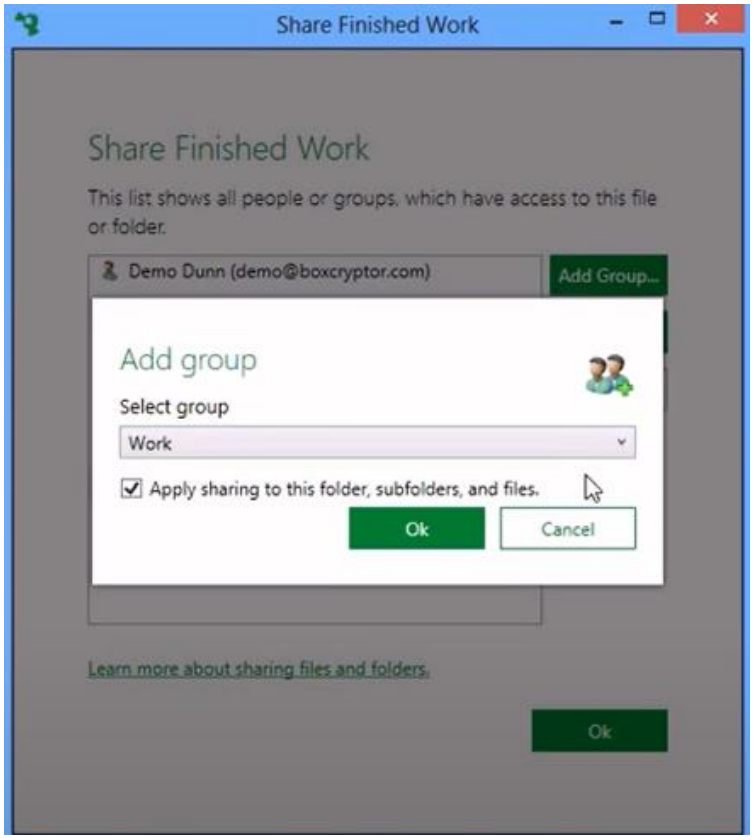

Рис. 3.20. Поділитися файлами з групою людей [28]

3.3. Розроблення рекомендацій щодо застосування технології криптографічного захисту інформації інформаційної системи організації на основі Boxcryptor

В ході виконання кваліфікаційної роботи нижче представлено основні переваги Boxcryptor та розроблено рекомендації щодо застосування технології криптографічного захисту інформації інформаційної системи організації на основі Boxcryptor.

Основні переваги [29]**:**

1. Цільова аудиторія: Boxcryptor обслуговує як індивідуальних користувачів, так і бізнес.

2. Інтеграція з хмарними провайдерами: Boxcryptor підтримує широкий спектр хмарних провайдерів, включаючи Dropbox, Google Drive і OneDrive.

3. Моделі ціноутворення: Boxcryptor пропонує як безкоштовні, так і платні плани, причому платні плани включають функції, специфічні для бізнесу.

4. Відкритий вихідний код: Boxcryptor — це власне програмне забезпечення, яке може більше сподобатися компаніям, які займаються підтримкою та підзвітністю.

5. Підтримка платформ: Boxcryptor підтримує багато платформ, включаючи Windows, macOS, IOS та Android.

6. Набір функцій: Boxcryptor може похвалитися розширеними функціями, такими як наскрізне шифрування, управління командою та інтеграція з Active Directory.

7. Аутентифікація користувача: Boxcryptor включає опції багатофакторної автентифікації (MFA).

8. Підтримка клієнтів: Boxcryptor надає професійну підтримку клієнтів, особливо для бізнес-користувачів [29].

9. Обмін файлами: Boxcryptor дозволяє обмінюватися зашифрованими файлами в командах або за їх межами.

Рекомендації щодо застосування технології криптографічного захисту інформації:

1. Оцінка потреб організації в захисті даних.

Визначте обсяг конфіденційних даних, які потребують шифрування, та розробіть стратегію використання Boxcryptor для захисту цих даних.

2. Інтеграція з хмарними сервісами.

Використовуйте Boxcryptor для шифрування даних у популярних хмарних сховищах, таких як Google Drive, Dropbox, OneDrive, для забезпечення конфіденційності навіть у разі компрометації хмарного акаунта.

3. Навчання персоналу.

Проведіть тренінги для співробітників, щоб навчити їх правильно використовувати Boxcryptor, зокрема створення ключів шифрування та роботи з зашифрованими файлами.

4. Застосування двофакторної аутентифікації.

5. Використовуйте централізовану систему управління ключами Boxcryptor для бізнесу, щоб адміністратори могли відновлювати доступ до даних у разі втрати паролів.

6. Обмеження доступу за ролями для надання доступу до зашифрованих файлів лише уповноваженим особам залежно від їхніх посадових обов'язків.

7. Розробка внутрішніх політик, які зобов’язують шифрувати конфіденційну інформацію та регулярно змінювати паролі.

8. Резервне копіювання зашифрованих даних.

9. Періодичне оновлення Boxcryptor.

10. Використовуйте Boxcryptor для шифрування даних під час їх передачі через мережі в реальному часі.

11. Автоматизація шифрування.

Висновки до розділу 3

1. Розроблено варіант розгортання технології криптографічного захисту інформації на основі Boxcryptor.

2. Продемонстровано технологію криптографічного захисту інформації на основі Boxcryptor.

3. Розроблено рекомендацій щодо застосування технології криптографічного захисту інформації інформаційної системи організації на основі Boxcryptor

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи отримано наступні результати:

1. Проведено аналіз проблеми криптографічного захисту інформації.

2. Проаналізовано сучасні загрози безпеці інформаційних систем.

3. Досліджено проблеми впровадження криптографічного захисту.

4. Проаналізовано нормативно-правова база, щодо кприптографічного захисту.

5. Досліджено методи та засоби криптографічного захисту інформації.

6. Проаналізовано симетричне, асиметричне шифрування.

7. Наведено принципи роботи шифрування, хешування та цифрового підпису.

8. Розроблено варіант розгортання технології криптографічного захисту інформації на основі Boxcryptor.

9. Продемонстровано технологію криптографічного захисту інформації на основі Boxcryptor.

10. Розроблено рекомендацій щодо застосування технології криптографічного захисту інформації інформаційної системи організації на основі Boxcryptor

ПЕРЕЛІК ПОСИЛАНЬ

1. Allers M. The CIA Triad - Defining Integrity. Cimcor | File Integrity Monitoring. URL: https://www.cimcor.com/blog/the-cia-triad-defining-integrity (дата звернення: 23.12.2024).

2. Medlock B. 10 Common Cybersecurity Threats & Attacks [2024 Update] | ConnectWise. MSP Technology and IT Management Software | ConnectWise. URL: https://www.connectwise.com/blog/cybersecurity/common-threats-and-attacks (дата звернення: 23.12.2024).

3. Cryptography Risks & Issues, Mitigating Actions and Consequences of getting it wrong – Incrypteon. Incrypteon – Encryption built for Developers. URL: https://incrypteon.com/cryptographic-risks-issues-mitigation-consequence/ (дата звернення: 23.12.2024).

4. Mehta J. What is Cryptographic Failure? Real-life Examples, Prevention, Mitigation. Certera. URL: https://certera.com/blog/what-is-cryptographic-failure-real-life-examples-prevention-mitigation/ (дата звернення: 23.12.2024).

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. На заміну ISO/IEC 27001:2013. Official edition. 2022. 19 p. URL: https://www.iso.org/standard/27001

6. ISO/IEC 19790:2012. Information technology – Security techniques – Security requirements for cryptographic modules. Replaces ISO/IEC 19790:2006. Official edition. 2012. 72 p. URL: https://www.iso.org/standard/52906.html.

7. FIPS 140-3 Security Requirements for Cryptographic Modules. https://csrc.nist.gov/. URL: https://doi.org/10.6028/NIST.FIPS.140-3 (дата звернення: 23.12.2024).

8. General Data Protection Regulation (GDPR) – Legal Text. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/ (дата звернення: 23.12.2024).

9. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 27 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 23.12.2024).

10. ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Вид. офіц. Київ. 44 с. URL: https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798.

11. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII : станом на 18 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 23.12.2024).

12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 23.12.2024).

13. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : Норм. док. системи техн. зах. інформації від 01.07.1999 № НД ТЗІ 2.5-004-99. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf.

14. GeeksforGeeks. Difference Between Symmetric and Asymmetric Key Encryption - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/ (дата звернення: 23.12.2024).

15. Mircea-Constantin ȘCHEAU, Călin Mihail RANGU, Cătălin UDROIU, "Secure IT Evolution Short Analysis", Romanian Journal of Information Technology and Automatic Control, ISSN 1220-1758, vol. 30(2), pp. 95-108, 2020. https://doi.org/10.33436/v30i2y202008

16. WikiAudio. Stream cipher, 2016. YouTube. URL: https://www.youtube.com/watch?v=mKHnK_w2FMY (дата звернення: 23.12.2024).

17. Sangfor Technologies. What is Ciphertext in Network Cybersecurity. Sangfor Technologies. URL: https://www.sangfor.com/glossary/cybersecurity/what-is-ciphertext (дата звернення: 23.12.2024).

18. MacDonald R. What Is Symmetric Encryption, How Does It Work & Why Use It?. 1Kosmos. URL: https://www.1kosmos.com/blockchain/symmetric-encryption/ (дата звернення: 23.12.2024).

19. Nakutavičiūtė J. What is asymmetric cryptography?. NordVPN. URL: https://nordvpn.com/es-mx/blog/what-is-asymmetric-cryptography/ (дата звернення: 23.12.2024).

20. Badman A., Kosinski M. What is Asymmetric Encryption? | IBM. IBM - United States. URL: https://www.ibm.com/think/topics/asymmetric-encryption (дата звернення: 23.12.2024).

21. Osman J., Difference between Symmetric and Asymmetric Encryption - Differs From. Differs From. URL: https://differsfrom.com/difference-between-symmetric-and-asymmetric/ (дата звернення: 23.12.2024).

22. Andvsilva. Digital Signature with Hash Function–How it works?. Medium. URL: https://andsilvadrcc.medium.com/digital-signature-with-hash-function-how-it-works-f4eed52267f5 (дата звернення: 23.12.2024).

23. Are Digital Signatures Secure? How Do They Works?. Ricoh Malaysia | Empowering Digital Workplaces. URL: https://www.ricoh.com.my/blogs/are-digital-signatures-secure (дата звернення: 23.12.2024).

24. Security Project Boxcryptor. coursehero. URL: https://www.coursehero.com/file/204495114/Security-Project/ (дата звернення: 23.12.2024).

25. Boxcryptor. Boxcryptor Video: How it works 2022, 2021. YouTube. URL: https://www.youtube.com/watch?v=LaHER0pK5n0 (дата звернення: 23.12.2024).

26. Boxcryptor. Filename Encryption | Boxcryptor Tutorial, 2021. YouTube. URL: https://www.youtube.com/watch?v=A24k46cL8Ms (дата звернення: 23.12.2024).

27. Boxcryptor. Boxcryptor | How To Enable Two-Factor Authentication | Backup Codes, 2021. YouTube. URL: https://www.youtube.com/watch?v=bG2py1hv2_E (дата звернення: 23.12.2024).

28. Boxcryptor windows manual. Boxcryptor. URL: https://static.boxcryptor.com/help/Boxcryptor%20for%20Windows%20Manual.pdf.

29. Boxcryptor vs Cryptomator: Key Differences & Benefits Explained. rosettadigital. URL: https://rosettadigital.com/boxcryptor-vs-cryptomator/ (дата звернення: 23.12.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)