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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захищеного обміну документами на основі інфраструктури відкритих ключів»

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

_____ Валентин УСТІНОВ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
Устінов Валентин
(прізвище, ім'я)

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

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

Київ 2024

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
Кібербезпеки
_____ Галина ГАЙДУР
"___" грудня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

УСТІНОВУ Валентину Олександровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія захищеного обміну документами на основі інфраструктури відкритих ключів»

керівник кваліфікаційної роботи Кожухівський Андрій Дмитрович, д.т.н., професор
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» грудня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 13.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інфраструктура відкритих ключей;
програмний комплекс для захисту документів;
наукова та технічна література, експлуатаційна документація, нормативні документи.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблем захисту документів в інфраструктурі відкритих

2. Зміст процесу реагування на загрози цілісності на конфеденціальності документів в інфраструктурі відкритих ключей.

3. Аналіз методів та засобів забезпечення захисту документів в інфраструктурі відкритих ключей.

4. Рекомендації щодо вибору рішення для захисту документів в інфраструктурі відкритих ключей.

5. Перелік графічного матеріалу

1. Тема бакалаврської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Результати аналізу змісту процесу вибору рішення для захисту документів в інфраструктурі відкритих ключей.
4. Результати аналізу методів та засобів захисту документів в інфраструктурі відкритих ключей.
5. Призначення та можливості захисту документів в інфраструктурі відкритих ключей.
6. Рекомендації щодо застосування методів та засобів забезпечення безпеки документів в інфраструктурі відкритих ключей.
7. Висновки за результатами роботи.

6. Дата видачі завдання 15.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми забезпечення захисту документів в інфраструктурі відкритих ключей.	15.10.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	27.10.2024 р.	
3.	Аналіз методів та засобів забезпечення захисту документів в інфраструктурі відкритих ключей на базі OpenSSL.	30.10.2024 р.	
4.	Аналіз методів та засобів захисту документів в інфраструктурі відкритих ключей.	17.11.2024 р.	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту документів в інфраструктурі відкритих ключей.	02.12.2024 р.	
6.	Оформлення результатів дослідження.	03.12.2024 р.	
7.	Підготовка доповіді до захисту.	07.12.2024 р.	

Здобувач вищої освіти _____ Валентин УСТІНОВ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Андрій КОЖУХІВСЬКИЙ
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 71 сторінки, 24 рисунків, 5 таблиць, 15 джерел.

Об'єкт дослідження – процеси забезпечення захисту електронного документообігу.

Предмет дослідження – технології та методи захищеного обміну документами з використання інфраструктури відкритих ключів.

Мета роботи – розробка та дослідження технологічних рішень для захищеного обміну електронними документами на основі інфраструктури відкритих ключів.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

В роботі приведено основні відомості про інфраструктуру відкритих ключей, загрози захисту документів в інфраструктурі відкритих ключей.

Проаналізовано різні види захисту документів та наведено їх класифікацію. Досліджено методи та засоби щодо захисту документів в інфраструктурі відкритих ключей. Досліджено можливості захисту документів безпосередньо в інфраструктурі. На основі досліджень проведених в роботі розроблено рекомендації щодо вибору методу захисту документів в інфраструктурі відкритих ключей.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧЕЙ, ЗАХИСТ ДОКУМЕНТІВ, ВИБІР РІШЕННЯ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧЕЙ.

ABSTRACT

Text part of the qualification work: 71 pages, 24 figures, 5 table, 15 sources.

Object of research – the processes of ensuring the protection of electronic document circulation.

Subject of research – technologies and methods for secure document exchange using Public Key Infrastructure (PKI).

The aim of research – development and research of technological solutions for secure electronic document exchange based on Public Key Infrastructure.

Research methods – literature review on the topic, analysis of operational documentation, international standards, and their comparison.

The work presents the main information about Public Key Infrastructure, the threats to document protection in PKI, and analyzes various types of document protection and their classification.

It investigates methods and tools for protecting documents within the infrastructure. The research conducted in the work leads to the development of recommendations for selecting document protection methods within Public Key Infrastructure.

Field of application – cybersecurity of the information resources of an organization.

PUBLIC KEY INFRASTRUCTURE, DOCUMENT PROTECTION, SOLUTION SELECTION, METHODS AND TOOLS FOR PROTECTING PUBLIC KEY INFRASTRUCTURE.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 10

ВСТУП ……..…… 11

1 **АНАЛІЗ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧЕЙ ТА ЇЇ ХАРАКТЕРИСТИКА**..... 13

1.1 Поняття інфраструктури відкритих ключей та її характеристика……..... 13
1.2 Основні архітектури інфраструктури відкритих ключей …….. 15
1.3 Порівняльний аналіз архітектур PKI …… 24

2 **РИЗИКИ ТА УПРАВЛІННЯ НИМИ В ІНФРАСТРУКТУРІ ВІДКРИТИХ КЛЮЧЕЙ** 34

2.1 Ризик-менеджмент у розвитку інформаційних систем 34
2.2 Процес управління ризиками …… 36
2.3 Ризики в інфраструктурі відкритих ключей 46

3 **РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ТА ОГЛЯД ВИДІВ ТА НАЛАШТУВАНЬ ЗАХИСТУ ДОКУМЕНТІВ В ІНФРАСТКТУРІ ВІДКРИТИХ КЛЮЧЕЙ** 56

3.1 Аналіз налаштування та функцій OpenSSL для захисту документів в інфраструктурі відкритих ключей 56
3.2 Переваги використання кожного з методів захисту документів в PKI 72
3.3 Розробка рекомендацій щодо застосування методів захисту документів в інрфраструктурі відкритих ключей 73

ВИСНОВКИ …….. 77

ПЕРЕЛІК ПОСИЛАНЬ 76

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 79

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PKI - Public Key Infrastructure

CA - Certification Authority

CRL - Certificate Revocation List

RSA - Rivest Shamir Adleman

SHA - Secure Hash Algorithm

TCP - Trusted Computing Platform

CTL - Certificate Trust List

RA - Registration Authority

TLS - Transport Layer Security

X.509 - Standard for digital certificates

ECC - Elliptic Curve Cryptography

SSL - Secure Sockets Layer

OCSP - Online Certificate Status Protocol

AES - Advanced Encryption Standard

PFX - Personal Exchange Format

ВСТУП

Актуальність дослідження. Актуальність полягає у сучасній тенденції до цифровізації, яка охоплює всі сфери діяльності суспільства та вимагає нових підходів до захисту інформації. Зростаюча кількість організацій переходить на електронний документообіг, що забезпечує зручність, швидкість та ефективність роботи. Проте така трансформація супроводжується ризиками, пов'язаними з кіберзагрозами, зокрема крадіжкою даних, підробкою документів та втручанням у процеси передачі інформації.

Інфраструктура відкритих ключів (PKI) є однією з найбільш надійних технологій для забезпечення безпеки електронних документів. Вона дозволяє реалізувати механізми автентифікації, забезпечити цілісність даних та їх конфіденційність завдяки використанню асиметричного шифрування та цифрових підписів. Впровадження таких технологій є важливим як для бізнесу, так і для державного сектору, особливо у сферах, що вимагають високого рівня захисту інформації, таких як фінанси, охорона здоров'я та державне управління.

Додатковим чинником актуальності є нормативно-правові вимоги, що посилюють увагу до безпеки інформації, зокрема законодавство про електронні підписи та захист персональних даних. Такі ініціативи створюють передумови для впровадження PKI як стандарту безпеки.

З технічної точки зору, інфраструктура відкритих ключів має значний потенціал для адаптації до нових викликів, включаючи пост-квантову криптографію, що робить її надійним інструментом для довгострокового забезпечення безпеки. Крім того, цифрові підписи та шифрування сприяють зменшенню витрат, пов'язаних із паперовим документообігом, і відповідають тренду екологічної сталості.

Таким чином, дослідження цієї теми є надзвичайно важливим для створення безпечних та ефективних систем електронного документообігу, що сприятиме вирішенню актуальних проблем цифрового суспільства.

Об’єкт дослідження – процеси забезпечення захисту електронного документообігу.

Предмет дослідження – технології та методи захищеного обміну документами з використання інфраструктури відкритих ключів.

Мета роботи – розробка та дослідження технологічних рішень для захищеного обміну електронними документами на основі інфраструктури відкритих ключів.

Наукові завдання:

дослідити сутність проблеми забезпечення безпечного обміну документами за допомогою інфраструктури відкритих ключей;

проаналізувати підходи до забезпечення безпечного обміну документами за допомогою інфраструктури відкритих ключей;

проаналізувати існуючі рішення із забезпечення безпечного обміну документами за допомогою інфраструктури відкритих ключей;

проаналізувати методи та засоби забезпечення безпечного обміну документами за допомогою інфраструктури відкритих ключей;

розкрити порядок реалізації технології забезпечення безпечного обміну документами за допомогою інфраструктури відкритих ключей.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології забезпечення безпечного обміну документами за допомогою інфраструктури відкритих ключей, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

1. АНАЛІЗ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧЕЙ ТА ЇЇ ХАРАКТЕРИСТИКА

1.1. Поняття інфраструктури відкритих ключей та її характеристика

PKI (Public Key Infrastructure) — складна криптографічна система, яка є фундаментальною технологією забезпечення інформаційної безпеки в цифровому світі. PKI розвинулась як відповідь на зростаючі виклики кібербезпеки та необхідність створення надійних механізмів автентифікації та захисту інформації в мережевих середовищах [1].

Історично концепція PKI бере свій початок у 1970-х роках, коли вчені-криптографи Уїтфілд Діффі та Мартін Гелман розробили принципи асиметричної криптографії. Ця революційна технологія дозволила створити систему, де два різні, але математично пов'язані ключі можуть забезпечувати секретність та автентичність комунікацій.

Використання PKI дозволяє вирішувати фундаментальні завдання інформаційної безпеки з високим рівнем надійності:

- Автентифікація — багатошаровий процес підтвердження особи або системи через криптографічні механізми, які унеможливлюють підроблення ідентичності. Це включає перевірку цифрових підписів, сертифікатів та ланцюжків довіри.
- Конфіденційність — технологія шифрування, що базується на складних математичних алгоритмах (RSA, ECC), які гарантують, що перехоплені дані залишаться повністю незрозумілими для стороннього спостерігача.
- Цілісність — механізми верифікації, які дозволяють миттєво виявляти будь-які несанкціоновані зміни в інформаційних потоках через геш-функції та цифрові підписи.

- Непідробність — юридично значущі механізми, які не лише технічно унеможливлюють заперечення авторства, але й забезпечують forensic-сумісність для подальшого розслідування.

Архітектура PKI складається з взаємопов'язаних компонентів, кожен з яких має критично важливе значення:

1) Центри сертифікації (CA) — складні організаційно-технічні структури, які не просто видають сертифікати, а й підтримують складну ієрархію довіри. Вони функціонують як довірені треті сторони, що гарантують автентичність цифрових посвідчень.

2) Реєстраційні центри (RA) — виконують функцію попередньої перевірки, застосовуючи багаторівневі механізми верифікації особи, включаючи біометричні, документальні та інші методи ідентифікації.

3) Цифрові сертифікати — складні електронні документи, що містять не лише відкритий ключ, але й додаткову metadata: інформацію про власника, терміни дії, алгоритми шифрування тощо.

4) Репозиторії — розподілені системи зберігання, які забезпечують миттєвий доступ до актуальної інформації про статус сертифікатів, включаючи списки відкликаних сертифікатів (CRL) та механізми Online Certificate Status Protocol (OCSP).

Практичне значення PKI набуває особливої ваги в різних галузях:

- У банківській справі PKI захищає онлайн-транзакції
- В державному секторі забезпечує електронний документообіг
- У медицині гарантує конфіденційність персональних даних пацієнтів
- В корпоративному середовищі захищає комунікації та корпоративні мережі

Сучасні тренди розвитку PKI включають інтеграцію blockchain-технологій, впровадження квантостійких алгоритмів шифрування та розширення можливостей IoT-безпеки.

Таким чином, PKI — це не просто технологія, а складна соціотехнічна система, яка забезпечує довіру, безпеку та цілісність комунікацій у цифровому просторі, слугуючи фундаментальною інфраструктурою для сучасної цифрової економіки.

1.2. Основні архітектури інфраструктури відкритих ключей

Існує багато архітектур PKI, але всі вони можуть бути класифіковані як одна з наступних фундаментальних архітектур:

- Проста архітектура PKI (Simple PKI architecture),
- Корпоративна архітектура PKI (Enterprise PKI architecture),
- Гібридна архітектура PKI (Hybrid PKI architecture).

1. Проста архітектура PKI (Simple PKI Architecture)

1) Архітектура з єдиним центром сертифікації (Single CA Architecture).

Ця архітектура є найбільш поширеною на практиці. Один центр сертифікації (CA) надає всі необхідні послуги в середовищі PKI, зокрема:

- видачу сертифікатів,
- публікацію їх у загальнодоступному каталозі,
- створення списків відкликаних сертифікатів (CRL).

У цій архітектурі всі суб'єкти довіряють виключно одному CA. Така модель підходить для невеликих організацій із обмеженою кількістю користувачів. Однак вона не є оптимальною для організацій, які швидко розвиваються, оскільки не дозволяє додавати нові центри сертифікації.

2) Базова архітектура списку довіри (Basic Trust List Architecture)

У цій моделі центри сертифікації (CA) не встановлюють відносин між собою, тому сертифікаційні шляхи відсутні. Замість цього суб'єкти встановлюють відносини довіри з центрами сертифікації на основі списку довіри, який знаходиться у їхньому розпорядженні.

Існують різні інтерпретації списків довіри, оскільки немає єдиного способу їх визначення чи формалізації. Наприклад:

- Список довіри може трактуватися як перелік сертифікатів (наприклад, сховище сертифікатів, яке використовується веббраузером).
- У випадку Microsoft Certificate (Certificate Trust List, CTL) [2], це може бути підписаний список, що містить будь-яку конфіденційну інформацію, таку як хеші сертифікатів або імена файлів.

Архітектура списку довіри є однією з найбільш використовуваних у PKI, оскільки вона поширена через операційні системи та вебзастосунки. Однак її використання може створювати додаткові проблеми, оскільки кожен користувач повинен підтримувати власний список довіри.

З технічної точки зору, така архітектура складається з кількох незалежних CA, тобто з кількох архітектур із єдиним CA. Це означає, що компрометація одного не впливає на інші.

2. Корпоративна архітектура PKI (Enterprise PKI Architecture)

Декілька незалежних центрів сертифікації (CA) встановлюють довірчі відносини між собою, створюючи розширювані архітектури PKI. Центри сертифікації можуть встановлювати відносини, у яких одні CA є вищими (superior) або підлеглими (subordinate) іншим, або ж рівними (peer-to-peer). Усі організаційні структури теоретично можуть бути реалізовані через ієрархічну або сіткову (mesh) PKI.

1) Ієрархічна архітектура PKI (Hierarchical PKI architecture)

Ця модель зазвичай впроваджується в організаціях з ієрархічною структурою, оскільки відповідає їхньому організаційному розвитку. Архітектура будується на основі односторонніх довірчих відносин між вищим (root CA) і підлеглими центрами сертифікації, як показано на малюнку.

На вершині ієрархії розташований один центр сертифікації (кореневий CA), якому довіряють усі користувачі. Root CA розподіляє відкриті ключі всім суб'єктам та ініціює довіру до PKI. Водночас саме Root CA є слабким місцем архітектури: у разі його компрометації вся система стає ненадійною та непридатною до використання [3].

Кореневий CA видає сертифікати лише підлеглим CA, а ті, у свою чергу, видають сертифікати своїм підлеглим або кінцевим суб'єктам. Таким чином, CA може делегувати додаткові функції або обмежувати певні функції підлеглим CA. Довжина сертифікаційного шляху є короткою і дорівнює сумі сертифікатів підлеглих CA плюс сертифікат кінцевого суб'єкта.

Архітектура є досить масштабованою, оскільки може легко адаптуватися до змін у зростаючій організації. Під час розширення створюються довірчі відносини між root CA та новими центрами сертифікації або між підлеглими CA та новими CA. На рисунку 1.1 показано як влаштована Ієрархічна архітектура PKI.

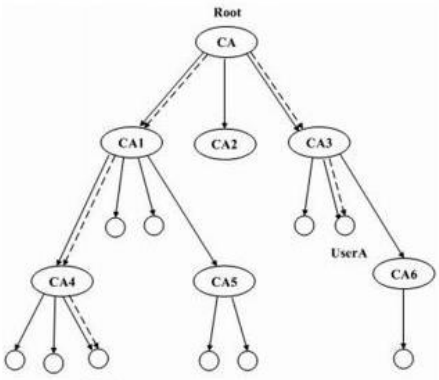

Рис.1.1. Ієрархічна архітектура PKI

2) Сіткова архітектура PKI (Mesh PKI)

У сітковій архітектурі центри сертифікації (CA) надають PKI-послуги та встановлюють рівноправні (peer-to-peer) відносини. Ця модель є альтернативою ієрархічній завдяки своїм перевагам.

Мережна PKI будує двосторонні довірчі відносини між рівними CA, видаючи один одному сертифікати. CA може обмежувати довіру шляхом встановлення обмежень у сертифікатах, таких як обмеження імен, політики чи довжини шляху.

Сіткова архітектура має багато точок довіри, тому компрометація однієї з них не впливає на роботу всієї системи. У разі компрометації довіра до CA відновлюється шляхом відкликання виданих сертифікатів та випуску нових [4].

Побудова сертифікаційного шляху в цій архітектурі є складнішою, ніж в ієрархічній. Це зумовлено численними варіантами шляхів, серед яких деякі можуть виявитися непрацездатними. Максимальна довжина сертифікаційного шляху в сітковій архітектурі дорівнює кількості CA в системі.

Сіткова PKI легко розширюється шляхом додавання нових CA і встановлення з ними довірчих відносин. Однак масштабованість цієї архітектури загалом є недостатньо ефективною через складність сертифікатів, пошуку та перевірки сертифікаційного шляху. На рисунку 1.2 показано як влаштована Сіткова архітектура PKI.

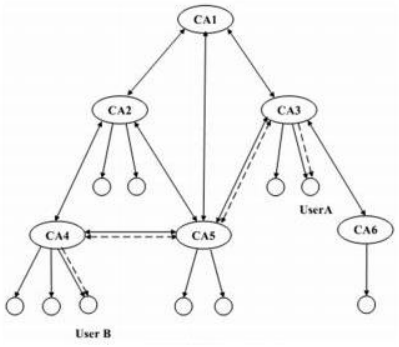

Рис.1.2. Сіткова архітектура PKI (Mesh PKI)

3. Гібридна архітектура PKI (Hybrid PKI Architecture)

Багато організацій використовують електронну комунікацію з іншими організаціями для розширення свого бізнесу. Організація, яка має ієрархічну архітектуру PKI, може зіткнутися з проблемами у спілкуванні з іншою організацією, яка використовує сіткову архітектуру PKI. У такій ситуації PKI потребує впровадження рішення, яке дозволить забезпечити безпечну комунікацію між користувачами різних архітектур PKI. Рішенням є гібридна архітектура PKI, яка дає можливість організаціям із різними архітектурами PKI створювати безпечне середовище для захищеного обміну інформацією.

Існує три типи гібридної архітектури:

- Розширена архітектура довірчих списків,
- Перехресно-сертифікована архітектура PKI,
- Архітектура мостового центру сертифікації.

1) Розширена архітектура довірчих списків (Extended Trust List Architecture)

У цій архітектурі кінцеві суб'єкти, а не центри сертифікації, встановлюють довірчі відносини шляхом підтримки списку довіри. Він містить багато точок довіри, яким довіряють кінцеві суб'єкти.

Ця архітектура може встановлювати довіру як до ієрархічної, так і до сіткової архітектури PKI. Елементи цього списку довіри містять кореневі центри сертифікації з ієрархічної архітектури та деякі центри сертифікації зі сіткової архітектури. Складність побудови сертифікаційного шляху залежить від архітектур, які поєднуються одна з одною [5].

Розширений список довіри створює кеш сертифікатів для усунення подібних проблем. Цей кеш містить усі можливі сертифікаційні шляхи. Механізм шляху може звертатися до кешу та шукати відповідний шлях замість побудови сертифікаційного шляху. Кожен сертифікаційний шлях має своє значення, яке залежить від складності

цього шляху. Ця архітектура може легко розширюватися шляхом додавання нових центрів сертифікації з різних архітектур PKI до списків довіри користувачів. Обслуговування списку довіри та пов'язані з цим проблеми залишаються такими ж, як і в базовій архітектурі довірчих списків. На рисунку 1.3 продемонстрована структура розширеної архітектури довірчих списків.

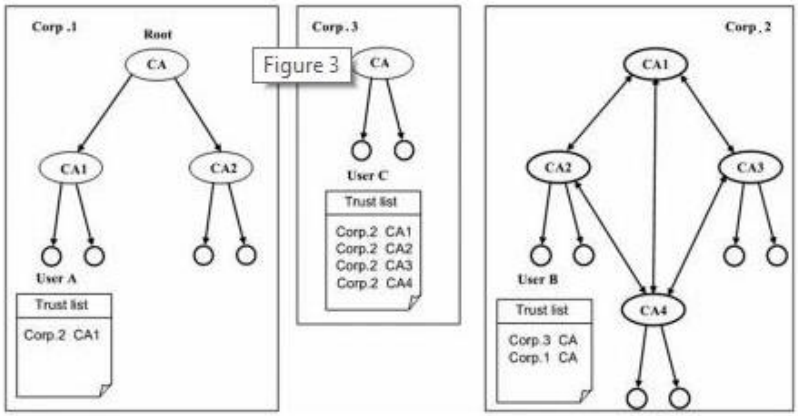

Рис.1.3. Розширена архітектура довірчих списків

Розширена архітектура довірчих списків не має однієї точки довіри, збій якої може зруйнувати всю архітектуру. Точки відмови у цій архітектурі можна розглядати з точки зору функціональності суб'єктів, які встановлюють довіру з іншими архітектурами PKI. Першою точкою відмови є список довіри. Суб'єкт не довірятиме жодному центру сертифікації або архітектурі, якщо список довіри буде пошкоджено. Другою точкою відмови є збої у механізмі кешу сертифікатів та пошуку сертифікаційних шляхів.

Якщо центри сертифікації є точкою відмови, вони можуть відновлюватися шляхом призупинення виданих сертифікатів, створення нового відкритого ключа та видачі нових сертифікатів. У разі збою списку довіри рішенням є створення нового списку довіри та відновлення механізмів кешування та пошуку.

2) Перехресно-сертифікована корпоративна PKI (Cross-Certified Enterprise PKI)

У цій архітектурі відносини довіри "рівний до рівного" встановлюються між однаковими або різними архітектурами організацій. Відносини довіри, створені за допомогою перехресної сертифікації, можуть бути обмежені визначенням обмежень в одному або декількох розширеннях пари перехресних сертифікатів.

Ця архітектура дозволяє додавати одну або більше нових архітектур PKI шляхом простого встановлення пари перехресної сертифікації. Кореневий центр сертифікації (CA) або будь-який підпорядкований CA в ієрархічній архітектурі може встановити відносини довіри "рівний до рівного" з будь-яким CA зі сіткової архітектури, CA з архітектури одного CA або з іншої ієрархічної архітектури. Аналогічно, сіткова архітектура і архітектура одного CA можуть встановлювати відносини довіри з однією або більше такими ж чи різними архітектурами. На Рисунку 1.4. показано відносини довіри "рівний до рівного" і сертифікаційний шлях подвійними лініями між корпоративними PKI архітектурами.

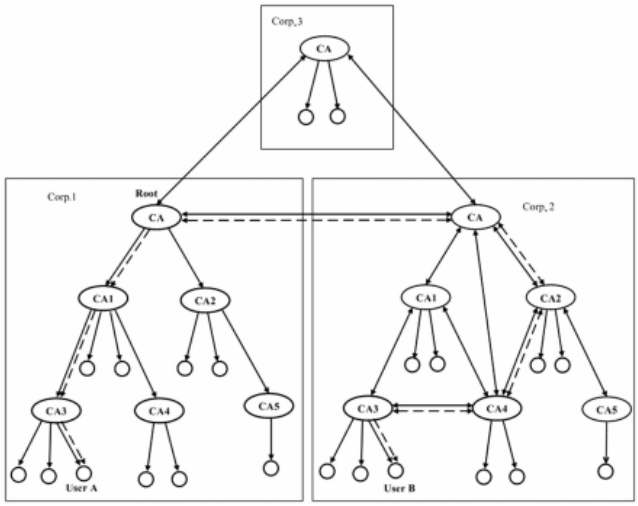

Рис.1.4. Перехресно-сертифікована корпоративна PKI

Коли центри сертифікації (CA) із різних архітектур встановлюють відносини довіри за допомогою перехресних сертифікатів, їхні суб’єкти можуть підтверджувати існування інших суб’єктів. Це забезпечує безпечне спілкування між усіма користувачами в архітектурі PKI. Різні користувачі створюють різні сертифікаційні

шляхи для одного й того ж сертифіката кінцевого суб’єкта в перехресно-сертифікованій PKI-архітектурі. Сертифікаційний шлях починається з точки довіри. Метод створення залежить від початкових архітектур, між якими встановлено відносини довіри.

Збій кореневого CA, підпорядкованого CA або CA в сітковій PKI-архітектурі призведе до повного або часткового збою архітектури, якщо розглядати перехресно-сертифіковану архітектуру. Скомпрометований CA відновлюється способом, описаним раніше в цьому документі, у розділі про корпоративну PKI-архітектуру. Новий CA може встановлювати відносини довіри з CA з інших PKI-архітектур.

Цей тип архітектури не підходить для підключення більшої кількості корпоративних архітектур, тому можна сказати, що її масштабованість є обмеженою.

4. Архітектура Мостового Центру Сертифікації (Bridge Certification Authority Architecture)

Архітектура Bridge Certification Authority (архітектура Bridge CA) була впроваджена федеральним урядом США для спрощення підключення PKI-архітектур за допомогою перехресно-сертифікованих пар. Ця архітектура з'єднує різні PKI-архітектури через впровадження нового центру сертифікації (Bridge CA), який встановлює відносини між PKI.

Bridge CA не є точкою довіри та не видає цифрові сертифікати користувачам. Користувачі Bridge CA сприймають його як посередника між різними PKI-архітектурами. Корпоративна архітектура встановлює відносини довіри з Bridge CA (Principal CA) через кореневий CA або якийсь CA із сіткової архітектури. Новий CA або Enterprise PKI-архітектури можуть бути легко додані шляхом встановлення однорангових відносин довіри.

Кожне розширення є прозорим для користувачів, оскільки точка довіри не змінюється. На рисунку 1.5 показано Bridge CA, який встановлює відносини довіри з трьома PKI (Comp.1., Comp.2. і Comp.3.).

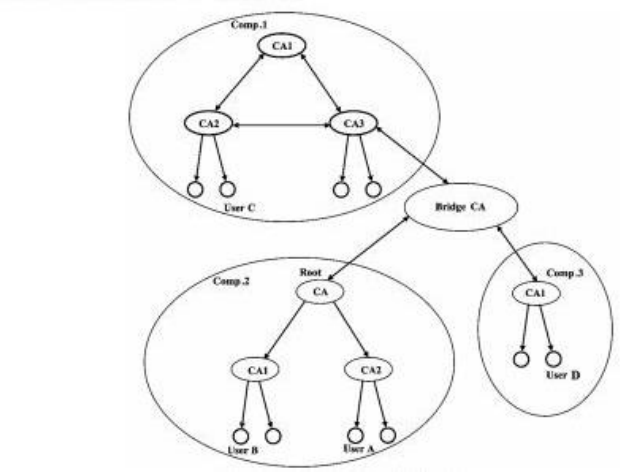

Рис.1.5. Архітектура Мостового Центру Сертифікації

Bridge CA може бути скомпрометована повністю або частково. Повна компрометація стосується порушення безпеки всіх приватних ключів, які використовувалися для підписання сертифікатів Principal CAs. Якщо в цій архітектурі скомпрометовано Principal CA, це унеможливлює для Enterprise PKI архітектури встановлення безпечного зв’язку з іншими PKI архітектурами. Якщо Principal CA використовує лише один приватний ключ для підписання сертифікатів, компрометація цього ключа призводить до повного провалу архітектури Bridge CA. Також апаратні або програмні збої можуть спричинити повний провал PKI архітектури [6].

Відновлення довірчих відносин із кожним Principal CA дозволяє Enterprise PKI архітектурі встановлювати довіру між різними або аналогічними архітектурами.

Користувачі знають шлях до Bridge CA і їм потрібно лише визначити шлях від центру сертифікації до сертифіката об'єкта. Однак, залежно від довжини

сертифікаційного ланцюга, обробка може бути ускладнена вимогами в сертифікатах, наприклад, політиками імені, статусом сертифікатів, або відображенням політик.

Ця архітектура розширюється шляхом додавання нових Enterprise PKI архітектур. Архітектури Bridge CA повинні встановлювати взаємні зв'язки, але це супроводжується багатьма технічними й операційними проблемами, описаними раніше.

1.3. Порівняльний аналіз архітектур PKI

У побудові PKI на практиці існують технічні та політичні проблеми. Організація повинна обрати архітектуру, яка найкраще відповідає її вимогам. Поєднання різних архітектур може створити оптимальну архітектуру PKI.

У цьому розділі наведено порівняльний аналіз через аспекти переваг і недоліків архітектур PKI та аспекти обраних параметрів. Маємо такі параметри:

- Довіра (Trust). Точка довіри — це точка або CA, з якої користувач сертифіката починає перевірку шляху сертифікації. Довірчі відносини — це зв'язок між сертифікатом користувача та CA, якому користувач довіряє, припускаючи, що CA видав відповідний дійсний сертифікат [7].
- Шлях сертифікації (Certification path). Шлях сертифікації — це ланцюг сертифікатів, створений через довірчі відносини між центрами сертифікації, щоб визначити, чи підписаний перевірюваний сертифікат його видавцем.
- Масштабованість (Scalability). Масштабованість — це здатність архітектури PKI розширюватися шляхом додавання нових CA або нових PKI, або зменшуватися шляхом виключення одного чи кількох CA з архітектури PKI, або виключення однієї чи кількох архітектур PKI.
- Гнучкість (Flexibility). Цей параметр показує здатність архітектури PKI адаптуватися до збоїв і розширення архітектури.

- Збій (Failure). Точка збою — це найслабше місце в архітектурі PKI, дисфункція якого ставить під сумнів роботу частини або всієї архітектури PKI. Точкою збою в архітектурі PKI є CA із скомпрометованим закритим ключем. Відновлення після збою — це процес відновлення довіри в архітектурі PKI [8].

Архітектура одного CA є найпростішою для впровадження серед усіх описаних архітектур PKI у цій статті. Ця архітектура не має можливості розширення шляхом встановлення довірчих відносин з іншими CA. В результаті обробка шляху сертифікації є набагато швидшою. Однак ця архітектура має одну точку довіри, що ставить під загрозу всю архітектуру. Це закрита архітектура, оскільки довірчі відносини існують лише між її елементами. Тому вона підходить для невеликих організацій. В таблиці 1.1. наведено детальний порівняльний аналіз всіх архітектур.

Таблиця 1.1.

Порівняльний аналіз переваг та недоліків архітектур PKI

Архітектура	Переваги	Недоліки
Проста архітектура PKI		
Архітектура з єдиним центром сертифікації	Проста архітектура, Легка реалізація, Проста обробка сертифікаційних шляхів, Підходить для малих організацій з обмеженою кількістю користувачів.	Не масштабований, Злам усієї архітектури при компрометації CA, Не встановлює довірчі відносини з іншими CA.
Базова архітектура списку довіри	Дозволяє безпечну комунікацію між різними архітектурами з однією ЦС, Дозволяє розширення архітектури.	Не обмінюється сертифікатами між CA. Існують проблеми з управлінням списком довіри.

Продовження таблиці 1.1.

Порівняльний аналіз переваг та недоліків архітектур PKI

Архітектура	Переваги	Недоліки
Корпоративна архітектура PKI		
Ієрархічна архітектура PKI	Регульований в межах ієрархічної організаційної структури, Проста виявлення та обробка сертифікаційного шляху, Сертифікаційні шляхи короткі.	Не може бути однієї CA у світі, Організації не обов'язково повинні мати ієрархічну структуру, Компрометація кореневої CA призводить до компрометації всієї архітектури.
Сіткова архітектура PKI	Гнучка архітектура, Користувачі довіряють CA, яка видала сертифікат, незалежно від того, де ця CA знаходиться в архітектурі PKI, Пряме створення пари перехресних сертифікатів. Це прискорює побудову сертифікаційного шляху, Процедура відновлення проста через малу кількість користувачів.	Будівництво сертифікаційного шляху є складним, Є непотрібні тупикові шляхи або нескінченні цикли сертифікатів, Погана масштабованість, оскільки збільшення кількості CA призводить до зниження продуктивності.

Продовження таблиці 1.1.

Порівняльний аналіз переваг та недоліків архітектур PKI

Архітектура	Переваги	Недоліки
Гібридна архітектура PKI		
Розширена архітектура довірчих списків	Просте встановлення довіри між організаціями з різними архітектурами PKI, Проста розширюваність архітектури, Користувачі мають повний контроль над списком довіри.	Суб'єкт сертифіката не визначає, до яких архітектур належить цей сертифікат, Існують проблеми з визначенням початкової точки сертифікаційного шляху, Архітектура може ставати складнішою з часом, Існують проблеми з управлінням списком довіри.
Перехресно-сертифікована корпоративна PKI	Воно може складатися з однакових або різних архітектур Enterprise PKI, Просте додавання нових архітектур PKI, Безпечна комунікація між сутностями з різних архітектур, Може бути необхідним встановлення довірчих відносин між архітектурами PKI.	Обмежена масштабованість, Складний сертифікаційний шлях, залежність від наївної архітектури PKI.

Продовження таблиці 1.1.

Порівняльний аналіз переваг та недоліків архітектур PKI

Архітектура	Переваги	Недоліки
Архітектура Мостового Центру Сертифікації	Видалення недоліків ієрархічної та мерж-архітектури, Проста розширюваність архітектури. Вона є прозорою для користувачів, Надійна після компрометації ключів, Проста обробка сертифікаційного шляху.	Компрометація Bridge CA призводить до зламу всієї архітектури, Виявлення сертифікаційного шляху є складнішим, ніж в ієрархічній архітектурі, Довжина сертифікаційного шляху приблизно вдвічі більша, ніж в ієрархічній архітектурі, Більше проблем з підключенням архітектур Bridge CA.

Таблиця 1.2.

Порівняльний аналіз архітектур PKI на основі вибраних параметрів

Параметри	Single CA	Basic Trust List	Hierarchical PKI	Mesh CA
Довіренний якір	Одна CA	Одна CA	Корнева CA	Будь яка CA в архітектурі
Довіренні відносини	-	Довіренний список	Ненаправлений	Двосторонній

Продовження таблиці 1.2.

Порівняльний аналіз архітектур PKI на основі вибраних параметрів

Параметри	Single CA	Basic Trust List	Hierarchical PKI	Mesh CA
Шлях сертифікату	Один сертифікат	Один сертифікат	Сума підлеглих CA сертифікатів на обраному шляху	Сума всіх CA сертифікатів на обраному шляху
Шлях сертифікату Будова	-	Простий	Простий	Комплексний
Масштабованість	Погана	Погана	Хороша	Погана
Гнучкість	Погана	Погана	Погана	Хороша
Точка відмови	Одна CA	Немає	Корнева CA	Немає
Відновлення після компрометації	Простий	Простий	Наполовину комплексний	Простий

Таблиця 1.3.

Порівняльний аналіз архітектур PKI на основі вибраних параметрів

Параметри	General Extended Trust	Cross-Certified Enterprise	Bridge CA
Довіренний якір	Будь яка CA	Довіренна точка в PKI архітектурі	Довіренна точка в PKI архітектурі

Продовження таблиці 1.3.

Порівняльний аналіз архітектур PKI на основі вибраних параметрів

Параметри	General Extended Trust	Cross-Certified Enterprise	Bridge CA
Довіренні відносини	Довіренний список	Ненаправлений або двосторонній	Ненаправлений або двосторонній
Шлях сертифікату	Один сертифікат	Сума найдовших шляхів сертифікату архітектури PKI	Сума найдовших шляхів сертифікату архітектури PKI
Шлях сертифікату Будова	-	Комплексний	Наполовину комплексний
Масштабованість	Погана	Погана	Хороша
Гнучкість	Хороша	Найкраща	Найкраща
Точка відмови	Будь яка CA в архітектурі і в довіреному списку	Характеристична точка встановлення довірених відносин	Міст CA та характеристична інфраструктура, що встановлює довірчі відносини
Відновлення після компрометації	Залежить наскільки комплексна	Простий або комплексний	Простий

Архітектура Basic Trust List вирішує проблему закритої архітектури. Вона вводить список довіри на стороні кінцевих сутностей різних архітектур PKI. Кінцева сутність управляє списком довіри. З одного боку, це добре, оскільки кінцева сутність визначає інші сутності, з якими буде встановлено захищену комунікацію. З іншого

боку, існує проблема підтримки та управління списком довіри. Ця архітектура підходить для встановлення невеликої кількості довірчих відносин між різними PKI.

Ієрархічна архітектура підходить для організацій з ієрархічною структурою, оскільки вона може слідувати їхньому розвитку. Вона має автоматизований механізм перевірки довіри, який вбудований у процес обробки сертифікаційного шляху, тому кінцева сутність не повинна оновлювати список довіри. Довіра залежить від приватного ключа кореневої CA, який є точкою відмови. Компрометація цієї точки призводить до зламу всієї архітектури. Це велика проблема цієї архітектури. Ієрархічна архітектура має більшу масштабованість порівняно з архітектурами Single CA і Trust List, оскільки вона може легко слідувати розширенню організації. Однак вона не є гнучкою, оскільки має одну точку відмови.

Сіткова архітектура PKI є більш гнучкою, ніж ієрархічна архітектура, оскільки має більше точок відмови. Компрометація будь-якої з точок довіри не призводить до зламу архітектури PKI. Масштабованість цієї архітектури знижена, оскільки численні довірчі відносини між CA ускладнюють обробку сертифікаційного шляху. Виявлення сертифікаційних шляхів складніше, ніж в ієрархічній архітектурі, оскільки існує більше сертифікаційних шляхів до кінцевої сутності. Наслідки більшої кількості сертифікаційних шляхів — двосторонні довірчі відносини. Обмеження цієї архітектури двосторонні, тоді як в ієрархічній архітектурі вони односторонні.

Гібридні архітектури PKI є результатом необхідності комунікації між організаціями з різними архітектурами PKI. Гібридні архітектури PKI створюють середовище для безпечного обміну інформацією між організаціями.

Архітектура Extended Trust List схожа на архітектуру Basic Trust List. Однак ця архітектура є більш складною, оскільки встановлює довірчі відносини між різними архітектурами PKI. Сертифікати кінцевих сутностей не можуть вказувати, до яких архітектур належить сертифікат. Це створює додаткові проблеми при визначенні початкової точки сертифікаційного шляху. Ця архітектура може бути легко

розширена, але призводить до проблем з підтримкою списку довіри, що є причиною поганої масштабованості. Архітектура Extended Trust List не має єдиної точки відмови, яка спричинила б злам всієї архітектури. Компрометація CA в списку довіри користувачів перешкоджає встановленню відносин з користувачами цієї конкретної CA, але залишає комунікацію з користувачами інших CA незмінною. Найбільша проблема виникає, коли список довіри та механізм генерації кешу сертифікатів виходять з ладу. Користувачі не зможуть комунікувати з користувачами інших PKI в такій ситуації.

Перехресно-сертифікована корпоративна PKI архітектура вирішує проблеми архітектур Extended Trust List. Ця архітектура встановлює довірчі відносини між кількома різними архітектурами PKI. Встановлення довірчих відносин за допомогою перехресно сертифікованої пари з кількома CA створює більше сертифікаційних шляхів від користувача до кінцевої сутності та робить цю архітектуру більш гнучкою. Компрометація CA з встановленими довірчими відносинами з іншими архітектурами PKI не впливає на безпечну комунікацію між користувачами інших архітектур. Збільшення кількості відносин між CA ускладнює виявлення та обробку сертифікаційних шляхів, що впливає на обмежену масштабованість.

Архітектура Мостового Центру Сертифікації (Bridge CA) була розроблена для підвищення масштабованості та гнучкості гібридних архітектур PKI, зменшення кількості перехресно сертифікованих і сертифікаційних шляхів та забезпечення простої розширюваності архітектури. Архітектура Bridge CA має коротший шлях довіри, ніж mesh PKI з такою ж кількістю CA. Механізм для виявлення сертифікаційного шляху є більш складним, ніж в ієрархічній архітектурі, а сертифікаційний шлях приблизно в два рази довший. Кожна основна CA (коренева CA ієрархії або CA mesh архітектури) в архітектурі Bridge CA встановлює одну довірчу відносину з Bridge CA. Мережна перехресно сертифікована архітектура встановлює довірчі відносини між CA, тоді як ця архітектура встановлює n довірчих

відносин. Bridge CA не має функції вищої CA щодо архітектур PKI, для яких вона створює перехресні сертифікати.

Висновки до першого розділу

У першому розділі було розглянуто ключові поняття PKI, включаючи її компоненти, функції та характеристики. Проведено аналіз основних архітектур, таких як ієрархічна, сіткова та мостова, їх переваги, недоліки та сфери застосування. Порівняльний аналіз продемонстрував вплив архітектур на масштабованість, стійкість до збоїв та ефективність управління сертифікатами, що є основою для вибору оптимальної моделі для конкретних умов використання.

2. РИЗИКИ ТА УПРАВЛІННЯ НИМИ В ІНФРАСТРУКТУРІ ВІДКРИТИХ КЛЮЧЕЙ

2.1 Ризик-менеджмент у розвитку інформаційних систем

Успіх і невдача бізнесу значною мірою залежать від інформаційних систем, тому будь-яка політика організації щодо виявлення вразливостей, загроз і ризиків має бути проактивною.

Ризики відрізняються від однієї організації до іншої, і ми можемо запитати, чому? Відповідь на це запитання проста: оскільки кожна організація унікальна і в тій чи іншій мірі схильна до загроз, які можуть перетворитися на ризики, їх необхідно ідентифікувати, аналізувати, контролювати та пом'якшувати.

Ризик можна визначити як:

- Імовірність зазнати збитків у результаті певної деструктивної дії шляхом дослідження вразливостей системи.
- Можлива подія в майбутньому, настання якої вплине на цілі проекту з точки зору вартості, календарної програми або технічних аспектів.
- Можливість того, що щось станеться і вплине на ваші цілі - шанс отримати прибуток або зазнати збитків. Ризик вимірюється з точки зору ймовірності та наслідків [9].

Ризик, так би мовити, - це не будь-який факт, що вже відбувся і заважає просуванню проекту; це вказує на речі, які, на вашу думку, можуть статися в майбутньому. В останні роки життєво важлива для будь-якого бізнесу розробка системної інформації повинна бути дешевою, а також потрібно скоротити час її виконання. Через такі обставини розробники можуть почати свої роботи, не передбачивши можливих проблем на етапі запуску проекту, і нехтувати ознаками нових проблем, а невжиття відповідних контрзаходів може призвести до справжніх

проблем, які можуть наражати проект на кризу перевищення бюджету, затримки доставки та низької якості.

Перехід до відкритої системи в 1990-х роках став бумом, зосередженим у Сполучених Штатах. У Румунії після розпаду економічної бульбашки та стагнації скорочення витрат стало головним пріоритетом. Після 1999 року відкрита система набула швидкого поширення, оскільки її спеціалізація полягала в тому, щоб зменшити витрати шляхом прийняття скорочення та відкритої технології. У такому потоці кардинально змінилося середовище розвитку системи. До цього головна рамкова система була основним потоком для базової системи Організації. Однак з розповсюдженням відкритої системи різні постачальники почали постачати сервери, комп'ютери, операційні системи або програми, унаслідок чого кожен компонент системи став чорним ящиком.

Розширення відкритої системи скорегувало розвиток системи та метод впровадження Організації, відповідно до головного пріоритету зниження витрат, про який йдеться на попередній сторінці, розвиток інформаційної системи мав немає вибору, окрім як розробити систему в рамках обмеженого бюджету. З появою нової відкритої технології розвиток системи став складним в рамках Організації з огляду на вартість і технологію. Тому аутсорсинг розробки став популярним. У результаті стало складно накопичувати ноу-хау розробки системи та управління проектами в рамках Організації. З іншого боку, інша організація, яка спробувала розробити систему, була змушена реагувати на зниження витрат і нову технологію, а в результаті вони також передали розробку системи зовнішнім сторонам [10].

Через таку зміну середовища розробки системи стало важко утримувати та керувати розвитком системи в цілому. Завдяки цьому стало також досить жорстко запобігти системному збою або виникненню збою раніше та визначити причину системного збою або аварії. За таких обставин керівники проектів змушені досягати цілей з обмеженими ресурсами; їм необхідно досягти цілей за допомогою

управління проектами шляхом передбачення появи ризиків, планування та впровадження відповідних контрзаходів для зменшення впливу.

2.2 Процес управління ризиками

Управління ризиками — це термін, який позначає зрозумілий і систематизований процес виявлення, аналізу, лікування та моніторингу ризиків, причетних до будь-якої діяльності чи процесу.

Управління ризиками - це методологія, яка допомагає менеджерам найкращим чином використовувати наявні ресурси. Практика управління ризиками широко використовується в державному та приватному секторах, охоплюючи широкий спектр видів діяльності та операцій. Управління ризиками зараз невід'ємна частина бізнес-планування. Етапи процесу управління ризиками є загальним посібником для будь-якої організації, незалежно від типу бізнесу, діяльності чи функції [11].

1) Основні етапи процесу:
2) Встановіть контекст;
3) Визначити ризики;
4) Проаналізуйте ризики;
5) Оцінити ризики;
6) Лікуйте ризики;
7) Моніторинг та огляд;
8) Спілкування та консультації.

«Ризик» динамічний і підлягає постійним змінам, тому процес включає поточні:

- Моніторинг та огляд;

- Спілкування та консультації.

1. Встановіть контекст

Встановлення контексту в управлінні ризиками є фундаментальним і надзвичайно важливим етапом, який передбачає глибокий та всебічний аналіз середовища організації. Його мета - створити комплексне уявлення про внутрішні та зовнішні фактори, що впливають на діяльність підприємства та можуть генерувати потенційні ризики.

Внутрішній контекст включає детальне вивчення організаційної структури, корпоративної культури, наявних ресурсів, фінансових можливостей, бізнес-процесів та кадрового потенціалу. Водночас зовнішній контекст охоплює макроекономічне середовище, галузеві особливості, законодавче регулювання, політичну ситуацію, технологічні тренди, конкурентне середовище та соціально-культурні фактори.

Методологія встановлення контексту базується на використанні різноманітних аналітичних інструментів: стратегічному аналізі, PEST-аналізі, SWOT-аналізі, бенчмаркінгу, експертних оцінках та статистичному аналізі. Ключовими завданнями цього етапу є ідентифікація потенційних зон ризику, визначення критеріїв оцінки ризиків, встановлення допустимих меж ризикованості та формування методології подальшого аналізу.

Практична реалізація передбачає залучення експертів різного профілю, використання актуальної та достовірної інформації, регулярне оновлення контекстного аналізу та забезпечення міждисциплінарного підходу. Результатом цього етапу має стати чітке розуміння середовища організації, визначені параметри ризик-менеджменту та підготовка до наступних етапів оцінки ризиків.

Важливо розуміти, що встановлення контексту - це не одноразовий акт, а безперервний процес, який вимагає постійної уваги, аналітичного мислення та

здатності адаптуватися до мінливих умов зовнішнього та внутрішнього середовища організації.

2. Визначте ризики

Раніше контекст було визначено, тепер необхідно ідентифікувати ризики. Це дуже важливий етап процесу оцінки ризиків, адже будь-які ризики, які не були ідентифіковані, не будуть враховані. Ризик, який не ідентифікований, все одно існує і може створити проблеми в майбутньому.

Зазвичай використовуються чотири методи для ідентифікації ризиків :

1) Консультація зі зацікавленими сторонами – є ефективним методом для визначення можливих ризиків під час проведення оцінки ризиків. Цей процес зазвичай включає визначення, хто саме є зацікавленими сторонами, яких необхідно опитати. Консультації можуть відбуватися формально або неформально, і зазвичай найкраще проводити їх особисто; використання електронної пошти може прискорити процедуру.

2) Фізична інспекція – огляд місця, де проводиться ідентифікація ризиків, є важливим, особливо якщо оцінка ризиків раніше не проводилася. Фізична інспекція передбачає відвідування місць, де проводиться оцінка ризиків, і пошук усіх можливих загроз.

3) Оцінка досвіду – цей процес включає консультування зі спеціалістами та отримання експертної інформації або перспективи. Перспективи базуються на специфічному досвіді та знаннях у їхній галузі.

4) Аналіз звітів, інформації та наявних даних – існує багато джерел інформації, які можуть бути використані для ідентифікації ризиків. Сюди входять дані про обладнання, що вказують його розміри та обмеження використання до моменту відмови, або статистичні звіти про інциденти на публічних заходах та їхній характер. Якщо ведеться належна документація попередніх проєктів, проблем або

незавершених операцій, цей метод може бути використаний для перегляду такої документації, як:

- Уроки, отримані з досвіду;
- Попередні плани управління ризиками;
- Огляди моніторингу ризиків;
- Списки проблем або неполадок.

3. Проаналізуйте ризики

Аналіз ризиків є критичним етапом у процесі управління ризиками, який вимагає глибокого та всебічного підходу до збирання та оцінювання інформації. Його мета - максимально точно визначити потенційний вплив та ймовірність виникнення кожного ідентифікованого ризику.

Основна методологія аналізу базується на математичній формулі: Рівень ризику дорівнює добутку наслідку та ймовірності виникнення події. Це дозволяє кількісно оцінити потенційну загрозу для організації, враховуючи як масштаб можливих негативних наслідків, так і вірогідність їх настання.

Принципово важливим є збирання максимально повної та достовірної інформації про кожен потенційний ризик. Чим серйознішим є ризик, тим більше уваги та ресурсів має бути спрямовано на його ретельне вивчення та аналіз. На початкових етапах оцінки визначення достатності зібраної інформації часто залежить від суб'єктивного експертного судження [12].

Процес аналізу ризиків не є лінійним і вимагає постійного уточнення та перегляду зібраної інформації. Важливо використовувати різноманітні джерела даних, залучати експертів з різних галузей та застосовувати як кількісні, так і якісні методи оцінки.

Кінцева мета аналізу ризиків - не лише виявити потенційні загрози, але й створити надійне підґрунтя для розроблення ефективних стратегій реагування та

мінімізації негативних наслідків. В таблиці 2.1. проведено детальний аналіз ризиків PKI.

Таблиця 2.1.

Аналіз ризику – ймовірність виникнення події

Наслідок / Ймовірність	Єкстримально виской	Дуже високий	Помірний	Низький	Мізерний
Майже впевнено (A)	Серйозний	Серйозний	Високий	Основний	Значний
Ймовірно (B)	Серйозний	Високий	Основний	Значний	Помірний
Помірний (C)	Високий	Основний	Значний	Помірний	Низький
Малоймовірний (D)	Основний	Значний	Помірний	Низький	Дуже низький
Рідкісний (E)	Значний	Помірний	Низький	Дуже низький	Дуже низький

4. Оцініть ризики

Оцінка ризиків є критичним етапом у процесі управління ризиками, що передбачає системний підхід до визначення пріоритетності та значущості виявлених ризиків для організації. Після попереднього аналізу та встановлення рівня кожного ризику, інформація вноситься до спеціального реєстру або програми управління ризиками.

Основна мета оцінки - встановити чітку послідовність реагування на різні типи ризиків, визначивши, які з них потребують негайної уваги та яким слід приділити

пріоритетну увагу для мінімізації потенційних серйозних збитків. Цей процес дозволяє раціонально розподілити обмежені ресурси організації, зосередивши зусилля на найбільш критичних напрямках.

Методологія оцінки передбачає диференційований підхід: високі та середні ризики потребують детального опрацювання стратегій реагування, водночас як незначні ризики можуть бути оперативно розглянуті, якщо витрати на їх обробку будуть мінімальними та не потребуватимуть значних ресурсів.

Важливою складовою є створення ієрархії ризиків, де кожен ризик отримує чітку оцінку за шкалою пріоритетності. Це дозволяє менеджменту приймати обґрунтовані рішення щодо послідовності та інтенсивності заходів з мінімізації ризиків.

Процес оцінки ризиків є динамічним і потребує постійного моніторингу та корегування, враховуючи зміни як внутрішнього, так і зовнішнього середовища організації.

5. Вжийте заходів щодо ризиків

Вжиття заходів щодо ризиків - це критичний етап процесу управління ризиками, який передбачає активні дії з мінімізації або контролю виявлених ризиків. Для кожного ідентифікованого ризику існує чотири основні стратегії реагування: прийняття ризику, уникнення ризику, передача ризику та зменшення ризику. Прийняття ризику означає свідоме рішення не вживати жодних дій, якщо ризик є несуттєвим або витрати на його мінімізацію перевищують потенційні збитки. Уникнення ризику передбачає повне виключення діяльності або процесу, що створює ризик. Передача ризику здійснюється шляхом перекладання відповідальності на третю сторону, наприклад, через страхування або аутсорсинг. Зменшення ризику полягає в розробці та впровадженні заходів, спрямованих на зниження ймовірності настання ризику або мінімізацію його негативних наслідків.

При виборі стратегії реагування на ризик необхідно враховувати пріоритети організації, включаючи стратегічні цілі, операційні обмеження та можливості, а також довгострокову стратегію розвитку. Важливу роль відіграють ресурсні обмеження: наявність людських ресурсів, фінансові можливості та технічні спроможності. Рівень ризику також впливає на вибір стратегії: низькі ризики можуть бути прийняті з постійним моніторингом, тоді як середні та високі ризики вимагають активних заходів.

Документування плану управління ризиками є ключовим елементом процесу. Необхідно детально зафіксувати причини вибору конкретної стратегії для кожного ризику, обґрунтування методу його обробки, розподіл відповідальностей між учасниками, процеси моніторингу та оцінки ефективності заходів, а також припущення щодо залишкового ризику після впровадження заходів.

Процес реалізації заходів включає розробку детального плану дій, визначення конкретних виконавців, встановлення термінів реалізації, створення системи проміжного контролю та налаштування механізмів звітування. Важливим аспектом є постійний моніторинг та оцінка ефективності впроваджених заходів, періодичний перегляд та коригування стратегії, оцінка залишкового ризику та внесення коректив у разі неефективності обраних заходів.

Наприклад, якщо в IT-компанії виявлено ризик витоку даних, можливі заходи можуть включати посилення систем кібербезпеки, навчання персоналу, впровадження багатофакторної аутентифікації, шифрування конфіденційної інформації та страхування від кіберризиків. Важливо пам'ятати, що управління ризиками - це безперервний циклічний процес, який вимагає постійної уваги та адаптації до змінних умов.

6. Моніторинг і огляд

Моніторинг та огляд є невід'ємною частиною ефективного управління ризиками, що забезпечує динамічність та адаптивність ризик-менеджменту. Цей

процес визнає мінливість зовнішнього та внутрішнього середовища організації, де обставини, припущення та контексти можуть змінюватися з часом. Основна мета моніторингу полягає в постійній оцінці актуальності та ефективності раніше розроблених стратегій управління ризиками.

Організації мають усвідомлювати, що припущення та висновки, зроблені під час ідентифікації та оцінки ризиків, не є статичними. Зовнішні фактори, такі як зміни на ринку, технологічний прогрес, законодавчі трансформації, можуть суттєво впливати на раніше визначені ризики. Внутрішні зміни в структурі компанії, її стратегії, операційних процесах також можуть призводити до трансформації ризикового ландшафту.

Систематичний моніторинг передбачає регулярний перегляд політик та рішень щодо управління ризиками. Керівники та відповідальні особи мають критично оцінювати раніше прийняті заходи, перевіряючи їхню релевантність, результативність та відповідність поточним умовам. Це включає детальний аналіз дій та процедур, спрямований на підтвердження достовірності початкових припущень та оцінку спроможності впроваджених контрзаходів ефективно нівелювати або мінімізувати ідентифіковані ризики.

Процес моніторингу та огляду не обмежується лише формальними перевірками, але й вимагає гнучкості та готовності до адаптації. Якщо виявляється, що поточні стратегії управління ризиками втрачають свою ефективність або з'являються нові несподівані фактори ризику, організація має бути готова швидко переглянути та скоригувати свій підхід. Це може включати перерозподіл ресурсів, зміну пріоритетів, розробку нових контрольних механізмів або навіть фундаментальну переоцінку ризик-стратегії [13].

Ефективний моніторинг та огляд також передбачають створення культури безперервного навчання та вдосконалення в організації. Важливо не лише виявляти недоліки в поточних підходах, але й систематизувати набутий досвід, вилучати уроки

з минулих ситуацій та використовувати їх для постійного вдосконалення систем управління ризиками. Це допомагає організації не лише реагувати на ризики, але й передбачати їх, перетворюючи ризик-менеджмент з реактивного на проактивний інструмент стратегічного управління.

Таким чином, моніторинг та огляд - це не одноразовий захід, а безперервний, динамічний процес, який вимагає уваги, аналітичного мислення та готовності до змін. Він є критичним для забезпечення стійкості, адаптивності та конкурентоспроможності організації в мінливому бізнес-середовищі.

7. Комунікація та консультація

Комунікація і консультація є фундаментальними складовими ефективного управління ризиками, які забезпечують прозорість, залучення та підтримку всіх зацікавлених сторін у процесі ризик-менеджменту. Цей процес виходить далеко за межі простого інформування та передбачає активне, змістовне спілкування, яке дозволяє організації отримувати різнобічну експертизу, розуміти контекст ризиків та забезпечувати підтримку прийнятих рішень.

Ключова мета комунікації та консультацій полягає в створенні середовища відкритого діалогу, де різні стейкхолдери можуть вільно обмінюватися інформацією, висловлювати занепокоєння, пропонувати ідеї та insights щодо потенційних ризиків. Це багатосторонній процес, який включає внутрішніх учасників (співробітники, менеджмент) та зовнішніх стейкхолдерів (постачальники, клієнти, інвестори, регулятори, партнери).

Комунікація має бути неперервною та здійснюватися на кожному етапі процесу управління ризиками. На етапі ідентифікації ризиків консультації дозволяють залучити різні перспективи та експертні знання, виявити потенційні загрози, які можуть бути непомітними з одного погляду. Під час оцінки ризиків спілкування допомагає краще зрозуміти їхню природу, потенційний вплив та взаємозв'язки.

Важливим аспектом комунікації є не лише передача інформації, але й забезпечення її зрозумілості та доступності для різних груп стейкхолдерів. Це вимагає адаптації повідомлень, використання різних каналів комунікації, врахування особливостей сприйняття різних учасників. Технічні деталі для технічних спеціалістів, стратегічні узагальнення для керівництва, конкретні практичні наслідки для операційних команд.

Консультації передбачають активне залучення стейкхолдерів до процесу прийняття рішень. Це означає не просто інформування, але й створення механізмів зворотного зв'язку, врахування думок та пропозицій різних учасників. Такий підхід не лише покращує якість ризик-менеджменту, але й сприяє формуванню культури спільної відповідальності, підвищує мотивацію та прихильність до впроваджуваних заходів.

Комунікація та консультації також відіграють критичну роль у managing очікуваннями та сприйняттям ризиків. Вони допомагають долати страх, невизначеність, знижувати опір змінам. Прозоре та послідовне спілкування формує довіру, демонструє компетентність організації у складних ситуацій.

Організаційна культура має бути налаштована на відкритість, де кожен співробітник розуміє свою роль у ризик-менеджменті та відчуває себе уповноваженим комунікувати про потенційні загрози. Це означає створення безпечного середовища, де повідомлення про ризики не сприймаються як критика, а як цінний внесок у забезпечення стійкості організації.

Технологічні рішення, такі як спеціалізовані платформи, регулярні наради, звіти, можуть підтримувати ефективну комунікацію. Важливо обирати канали, які відповідають корпоративній культурі та перевагам конкретної організації.

Таким чином, комунікація і консультація - це не адміністративна формальність, а стратегічний інструмент, який допомагає організаціям бути адаптивними та

успішними в управлінні невизначеністю. На рисунку 2.1. показано як працює процес управління ризиками.

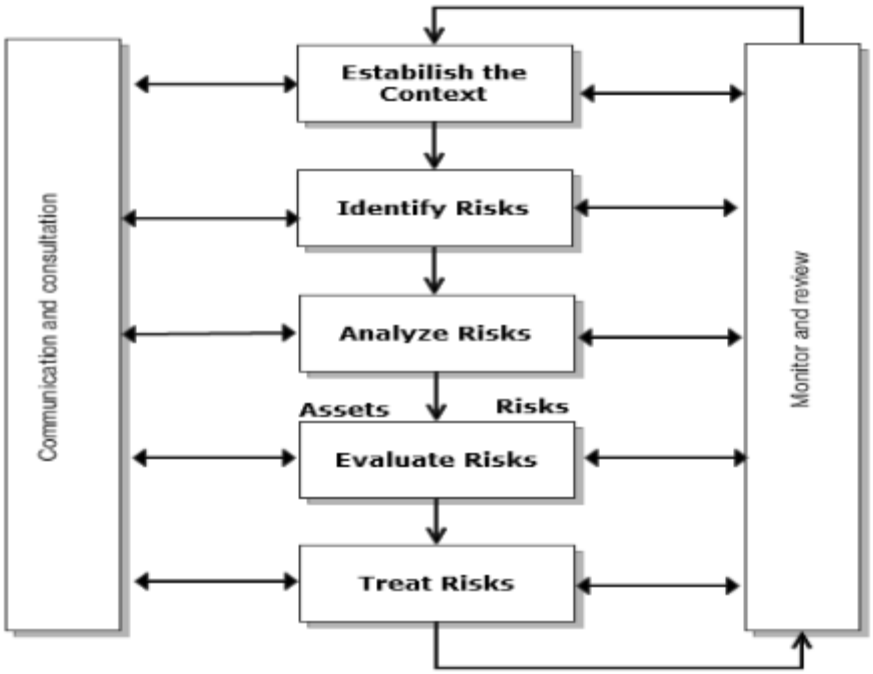

Рис.2.1. Процеси управління ризиками

2.3 Ризики в інфраструктурі відкритих ключей

PKI — це відмінна технологія, яка допомагає користувачам підтверджувати, що люди чи компанії, з якими вони ведуть кореспонденцію, є тими, за кого вони себе видають. Вона довела свою корисність у сфері електронної комерції та в інших галузях. Однак, як і будь-яка технологія, вона не позбавлена своїх власних ризиків безпеки. Хоча PKI вважається необхідною технологією, як і будь-яке інше рішення з безпеки, вона не є на 100% безпечною, і має свої власні ризики, але якщо ми їх ідентифікуємо та знизимо, результатом буде сильне безпекове рішення [14].

Можливі ризики та загрози, пов'язані з PKI:

1) Відповідність законодавству;
2) Встановлення довіри;

3) Генерація ключів;

4) Захист приватного ключа;

5) Доступність CRL.

1. Відповідність законодавству

Ризики інфраструктури відкритих ключей (PKI) є складним і багатогранним питанням, яке включає численні технічні, організаційні та юридичні аспекти. З точки зору безпеки, PKI має низку потенційних вразливостей, які можуть становити значну загрозу для цілісності та конфіденційності електронних комунікацій.

Технічні ризики PKI включають декілька критичних напрямків. По-перше, це ризики компрометації приватних ключів, коли криптографічні ключі потрапляють до неправомочних осіб внаслідок хакерських атак, витоку інформації або соціальної інженерії. Така ситуація може призвести до несанкціонованого доступу, підробки цифрових підписів та повної дискредитації системи автентифікації.

Друга група ризиків пов'язана з управлінням сертифікатами. Центри сертифікації (CA) є критичними вузлами інфраструктури, і будь-яка вразливість у їхній роботі може мати масштабні наслідки. Зловмисники можуть намагатися отримати неправомірні сертифікати, здійснювати атаки типу "людина посередині" або компрометувати процеси верифікації. Особливо небезпечними є так звані "skeleton keys" - механізми, які дозволяють зловмиснику генерувати легітимні сертифікати для будь-якого домену.

Організаційні ризики PKI часто пов'язані з людським фактором. Недостатня підготовка персоналу, відсутність чітких протоколів безпеки, неналежне зберігання криптографічних ключів можуть створювати суттєві вразливості. Корпоративна культура та рівень технологічної грамотності співробітників відіграють критичну роль у забезпеченні безпеки PKI.

Юридичні ризики мають особливе значення в контексті транскордонних комунікацій. Різні юрисдикції мають відмінні підходи до регулювання PKI, що створює потенційні колізії та невизначеності. Наприклад, невідповідність між

європейськими директивами та national implementations може призводити до правових лакун.

Специфічні ризики для Європейського Союзу включають:

1) Варіативність імплементації Директиви про електронні підписи в різних країнах-членах

2) Складності транскордонного визнання електронних підписів

3) Потенційні розбіжності в тлумаченні та застосуванні регуляторних норм

У romanian контексті додаткові ризики випливають з особливостей локальної нормативної бази. Множинність нормативних актів (Закон № 455/2001, Постанови уряду) створює потенційні зони неоднозначності в регулюванні PKI.

Технологічні тренди додатково ускладнюють ризик-ландшафт PKI. Квантові обчислення, розвиток штучного інтелекту, поява нових криптографічних атак постійно змінюють парадигму безпеки інфраструктури відкритих ключів.

Ефективне управління ризиками PKI вимагає комплексного підходу, який включає:

- Регулярний аудит систем
- Постійне оновлення криптографічних протоколів
- Впровадження багаторівневих механізмів автентифікації
- Навчання персоналу
- Моніторинг та швидке реагування на інциденти

Кожен з цих аспектів є критичним для забезпечення цілісності, конфіденційності та доступності інфраструктури відкритих ключів.

2. Встановлення довіри

Встановлення довіри в цифрових системах є складним і багатошаровим процесом, який виходить далеко за межі простої технічної автентифікації. Це фундаментальне питання, що торкається соціальних, психологічних та технологічних аспектів взаємодії між суб'єктами в інформаційному просторі.

Традиційні моделі довіри, засновані на фізичній присутності та безпосередній комунікації, втрачають свою ефективність у цифровому середовищі. Онлайн-комунікації вимагають принципово нових механізмів верифікації особистості та оцінки надійності. Цифровий сертифікат сам по собі не є гарантією того, що його власник є дійсно тим, за кого себе видає.

Психологічний аспект довіри передбачає подолання природного скептицизму користувачів щодо анонімних онлайн-взаємодій. Люди інстинктивно оцінюють надійність співрозмовника через невербальні сигнали, міміку, інтонації, які повністю відсутні в цифровому форматі. Тому системи встановлення довіри мають компенсувати цей брак контексту через складні технологічні та соціальні механізми.

Технологічні механізми встановлення довіри включають багаторівневі системи автентифікації. Це не лише перевірка цифрового сертифіката, але й аналіз поведінкових патернів, використання біометричних даних, крос-референцій з різними базами даних. Штучний інтелект та машинне навчання дедалі більше залучаються до процесів оцінки достовірності цифрових суб'єктів.

Важливу роль відіграють репутаційні системи, які накопичують та аналізують історію взаємодій конкретного цифрового профілю. Кожна транзакція, кожен факт комунікації може додавати або віднімати "бали довіри". Такі системи дозволяють формувати більш контекстуальне уявлення про надійність суб'єкта.

Соціальні мережі та професійні платформи стають додатковими джерелами верифікації. Чим більше перевірених зв'язків, чим складніша та прозоріша цифрова екосистема навколо суб'єкта, тим вища ймовірність встановлення довіри. Механізми колективної експертизи та crowd-verification стають дедалі важливішими.

Юридичний вимір встановлення довіри передбачає створення чітких нормативних рамок, які регулюють цифрову автентифікацію. Європейські директиви, national legislations поступово формують уніфіковані підходи до верифікації цифрової особистості, встановлюючи стандарти та відповідальність.

- Виклики встановлення довіри включають:

- Постійне технологічне ускладнення механізмів шахрайства
- Баланс між приватністю та прозорістю
- Культурні відмінності в сприйнятті довіри
- Швидкість технологічних змін

Майбутнє встановлення довіри пов'язане з розвитком децентралізованих систем, блокчейн-технологій, які дозволяють створювати прозорі, незалежні від центрального контролю механізми верифікації. Самоврядні системи, де довіра вбудована в технологічний протокол, поступово замінюють традиційні ієрархічні моделі.

Важливо розуміти, що встановлення довіри - це не технічне, а соціотехнічне завдання. Воно вимагає постійного діалогу між технологіями, правилами, соціальними очікуваннями та індивідуальними практиками взаємодії.

3. Генерація ключів

Генерація ключів є критичним процесом у криптографічних системах, який безпосередньо впливає на безпеку всієї інформаційної інфраструктури. Це складний технологічний процес, що вимагає глибокого розуміння математичних принципів, алгоритмічних особливостей та потенційних вразливостей криптографічних систем.

Криптографічні алгоритми генерації ключів базуються на складних математичних принципах, які мають забезпечувати максимальну непередбачуваність та складність відтворення приватного ключа. Основна мета - створити такий механізм генерації, який би робив практично неможливим зворотню інженерію та відновлення приватного ключа за відкритим.

Ризики генерації ключів мають декілька принципових вимірів. Технічний вимір пов'язаний з потенційними вразливостями конкретних криптографічних алгоритмів. Навіть визнані свого часу потужними алгоритми з розвитком обчислювальних технологій можуть втрачати свою стійкість. Квантові обчислення, штучний інтелект та суперкомп'ютери постійно розширюють можливості криптоаналізу.

Довжина ключа є критичним параметром безпеки. Чим довший ключ, тим

складніше його зламати методом повного перебору. Сучасні стандарти безпеки рекомендують використовувати ключі довжиною принаймні 2048 біт для RSA та еліптичних кривих, а в окремих високочутливих системах - до 4096 біт. Короткі ключі практично миттєво можуть бути зламані сучасними обчислювальними потужностями.

Джерело ентропії під час генерації ключів має принципове значення. Псевдовипадкові генератори чисел можуть мати приховані систематичні вразливості, які дозволяють частково передбачати їхню поведінку. Саме тому криптографічно стійкі генератори використовують складні алгоритми, зовнішні джерела випадковості та постійно оновлюють свої механізми.

Людський фактор також створює significant ризики в процесах генерації ключів. Недосвідчені адміністратори можуть використовувати застарілі алгоритми, нехтувати оновленнями безпеки, мати погані практики зберігання ключів. Корпоративна культура кібербезпеки має бути налаштована на постійну настороженість та превентивні дії.

Еволюція криптографічних стандартів відбувається надзвичайно динамічно. Алгоритми, які вважалися абсолютно надійними десять років тому, сьогодні можуть мати відомі вразливості. RSA, SHA, еліптичні криві - всі ці технології постійно переглядаються та вдосконалюються міжнародними експертними спільнотами.

Сучасні підходи до генерації ключів включають:

- Використання тільки перевірених, стандартизованих алгоритмів
- Постійне оновлення довжини ключів
- Впровадження багаторівневих механізмів генерації
- Використання апаратних криптографічних модулів
- Регулярна ротація ключів
- Мультифакторні механізми генерації

Важливо розуміти, що генерація ключів - це не статичний процес, а динамічна система, яка вимагає постійної уваги, оновлення та вдосконалення. Жоден алгоритм не може бути названий абсолютно безпечним назавжди - безпека є перманентним

процесом адаптації до нових технологічних викликів.

4. Захист приватного ключа

Захист приватного ключа є критичним елементом інформаційної безпеки, який виходить далеко за межі простих технічних заходів і торкається складної взаємодії технологічних, психологічних та організаційних факторів. Приватний ключ по суті є унікальним цифровим еквівалентом особистої підписи, паспорта та банківської картки водночас, тому його компрометація може мати катастрофічні наслідки.

Технологічні механізми захисту приватного ключа включають багаторівневі системи безпеки. Це не лише шифрування, але й використання апаратних криптографічних модулів,ізольованих середовищ виконання, trusted platform modules. Сучасні рішення дозволяють зберігати приватні ключі в повністю ізольованих середовищах, які унеможливлюють несанкціонований доступ навіть при фізичному володінні пристроєм.

Психологічний аспект захисту ключів пов'язаний з human factor - навичками, обізнаністю та дисципліною користувачів. Найскладніші технологічні рішення можуть бути миттєво знецінені елементарною недбалістю: написанням паролів на папірцях, використанням очевидних послідовностей, довірою до сторонніх осіб. Освіта та формування культури кібербезпеки стають критичними компонентами захисту.

Соціальна інженерія є одним з найнебезпечніших векторів атак на приватні ключі. Зловмисники дедалі частіше використовують маніпулятивні психологічні техніки замість складних технічних атак. Підробка електронних листів, телефонні шахрайства, фішингові кампанії - все це безпосередньо спрямовано на отримання доступу до приватних ключів через довірливість користувачів.

Організаційні ризики включають внутрішні загрози - співробітники, які мають технічний доступ до систем. Навіть за умови бездоганної технічної безпеки, корумпований або недобросовісний співробітник може становити величезний ризик. Саме тому сучасні системи захисту передбачають принципи розподіленої відповідальності, мінімізації привілеїв та постійного моніторингу.

Криптографічні механізми захисту включають:

- Багатофакторну автентифікацію
- Біометричні параметри
- Динамічну генерацію додаткових ключів
- Розподілене зберігання компонентів ключа
- Періодично змінні ключі
- Блокування після серії невдалих спроб входу

Технологічні тренди демонструють дедалі більшу інтеграцію апаратних та software-рішень. Платформа довірених обчислень, захищає анклави в мобільних пристроях, апаратні криптогаманці - всі ці технології формують новий ландшафт захисту приватних ключів.

Юридичний вимір передбачає встановлення чітких регуляторних рамок відповідальності. У разі компрометації ключа користувач може нести повну матеріальну та кримінальну відповідальність за всі дії, здійснені з використанням його ідентифікаторів.

Майбутнє захисту приватних ключів пов'язане з розвитком біометричних технологій, блокчейн-рішень та штучного інтелекту. Системи, де автентифікація відбувається на основі унікальних фізіологічних характеристик, постійно ускладнених алгоритмів машинного навчання, становитимуть принципово новий рівень захисту.

Ключовий висновок полягає в тому, що захист приватного ключа - це не технічне, а комплексне соціотехнічне завдання, яке вимагає постійної уваги, освіти та адаптації до нових викликів кібербезпеки.

5. Доступність CRL

Доступність Списку Відкликаних Сертифікатів (CRL) є критичним аспектом функціонування інфраструктури відкритих ключів (PKI), який безпосередньо впливає на безперервність та надійність електронних комунікацій. Це складний технологічний процес, що вимагає комплексного підходу до забезпечення неперервного оновлення та миттєвого доступу до актуальної інформації про статус сертифікатів.

Технологічні виклики доступності CRL мають декілька принципових вимірів. По-перше, це infrastructure resilience - здатність системи підтримувати роботу навіть за умов часткових збоїв або навантажень. Централізовані репозиторії CRL можуть становити потенційну точку відмови, особливо в умовах масштабних кібератак або технічних несправностей.

Механізми оновлення та поширення CRL є надзвичайно чутливими. Кожен сертифікат у ланцюжці автентифікації вимагає перевірки через CRL, що створює складну мережу залежностей. Застарілий або недоступний CRL миттєво блокує всі подальші процеси автентифікації, фактично паралізуючи роботу інформаційних систем.

Архітектурні рішення щодо забезпечення доступності CRL включають:

- Розподілені мережеві структури
- Кешування актуальних версій
- Резервування серверів
- Використання CDN-мереж
- Впровадження механізмів швидкого оновлення

Організаційні ризики пов'язані з управлінням життєвим циклом сертифікатів. Постійна ротація, моніторинг статусів, швидке реагування на компрометацію - все це критичні процеси, які вимагають високої технологічної культури та дисципліни.

Альтернативні протоколи, такі як OCSP (Online Certificate Status Protocol), намагаються вирішити обмеження Traditional CRL, забезпечуючи майже миттєву перевірку статусу сертифікатів. Проте вони також мають власні архітектурні обмеження та вразливості [15].

Технологічні тренди демонструють еволюцію від статичних до динамічних, майже real-time механізмів перевірки сертифікатів. Блокчейн-технології, розподілені реєстри пропонують принципово нові підходи до верифікації електронних посвідчень.

Психологічний аспект доступності CRL пов'язаний з user experience. Користувачі очікують миттєвої автентифікації, тому будь-які затримки або збої

сприймаються як критичні системні помилки. Це вимагає не лише технічної досконалості, але й уваги до суб'єктивного сприйняття процесів безпеки.

Юридичний контекст додатково ускладнює managment CRL. Різні юрисдикції мають відмінні вимоги до термінів оновлення, зберігання та поширення інформації про статус сертифікатів. Транскордонні комунікації вимагають надзвичайно гнучких та адаптивних систем.

Майбутнє доступності CRL пов'язане з розвитком штучного інтелекту, машинного навчання та передбачувальної аналітики. Системи, здатні прогнозувати потенційні навантаження, автоматично балансувати потоки даних, миттєво реагувати на аномалії, становитимуть новий рівень еволюції PKI.

Ключовий висновок полягає в тому, що доступність CRL - це не просто технічне завдання, а складна соціотехнічна система, яка вимагає постійної уваги, адаптації та випередження технологічних викликів.

Висновки до другого розділу

У цьому розділі проведено аналіз ризиків, характерних для інфраструктури відкритих ключів (PKI), та процесів управління ними. Визначено, що ефективний ризик-менеджмент є ключовим елементом розвитку інформаційних систем, дозволяючи ідентифікувати, оцінювати та мінімізувати потенційні загрози. Розглянуто основні етапи управління ризиками, такі як аналіз загроз, оцінка їх впливу та впровадження захисних заходів.

Особливу увагу приділено ризикам, притаманним PKI, зокрема компрометації ключів, відмові у доступі до CRL, вразливостям у процесах аутентифікації та несанкціонованому доступу до приватної інформації. Запропоновано підходи до зниження цих ризиків, що базуються на посиленні архітектури PKI, впровадженні резервних механізмів і дотриманні стандартів безпеки.

3.РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ТА ОГЛЯД ВИДІВ ТА НАЛАШТУВАНЬ ЗАХИСТУ ДОКУМЕНТІВ В ІНФРАСТКТУРІ ВІДКРИТИХ КЛЮЧЕЙ

3.1 Аналіз налаштування та функцій OpenSSL для захисту документів в інфраструктурі відкритих ключей

OpenSSL - це потужний криптографічний інструмент з відкритим вихідним кодом, який відіграє ключову роль у забезпеченні безпеки інформаційних систем та побудові інфраструктури відкритих ключів (PKI).

Основна мета OpenSSL - надати розробникам та системним адміністраторам надійний механізм для захисту комунікацій, шифрування даних та управління цифровими сертифікатами. Він підтримує широкий спектр криптографічних алгоритмів, включаючи симетричне та асиметричне шифрування, забезпечуючи високий рівень захисту інформації.

Архітектура OpenSSL дозволяє створювати повноцінні інфраструктури відкритих ключів, включаючи генерацію кореневих та проміжних центрів сертифікації, управління життєвим циклом сертифікатів та реалізацію складних механізмів автентифікації. Інструмент підтримує різні криптографічні протоколи, зокрема SSL/TLS, що робить його незамінним для захищених комунікацій у мережі.

Унікальність OpenSSL полягає в його крос-платформенності, відкритості вихідного коду та постійному вдосконаленні спільнотою розробників. Він широко використовується в різних галузях - від веб-серверів та поштових служб до банківських систем та корпоративних мереж.

Важливою перевагою є підтримка сучасних стандартів безпеки, таких як Perfect Forward Secrecy, механізми захисту від криптографічних атак та динамічне оновлення

параметрів шифрування. OpenSSL забезпечує не лише шифрування, але й надійну автентифікацію, перевірку цілісності даних та створення електронних цифрових підписів.

Інструмент підтримує різноманітні алгоритми шифрування - від класичних RSA до сучасних еліптичних кривих, що дозволяє розробникам обирати найбільш оптимальні для конкретних завдань криптографічні рішення. Гнучкість налаштувань та широкий функціонал робить OpenSSL стандартним рішенням для забезпечення криптографічного захисту в інформаційних системах.

Розберемо як можна захистити документ на прикладі:

Для цієї роботи я буду використовувати версію OpenSSL 3.4.0 22 Oct 2024 (Library: OpenSSL 3.4.0 22 Oct 2024)

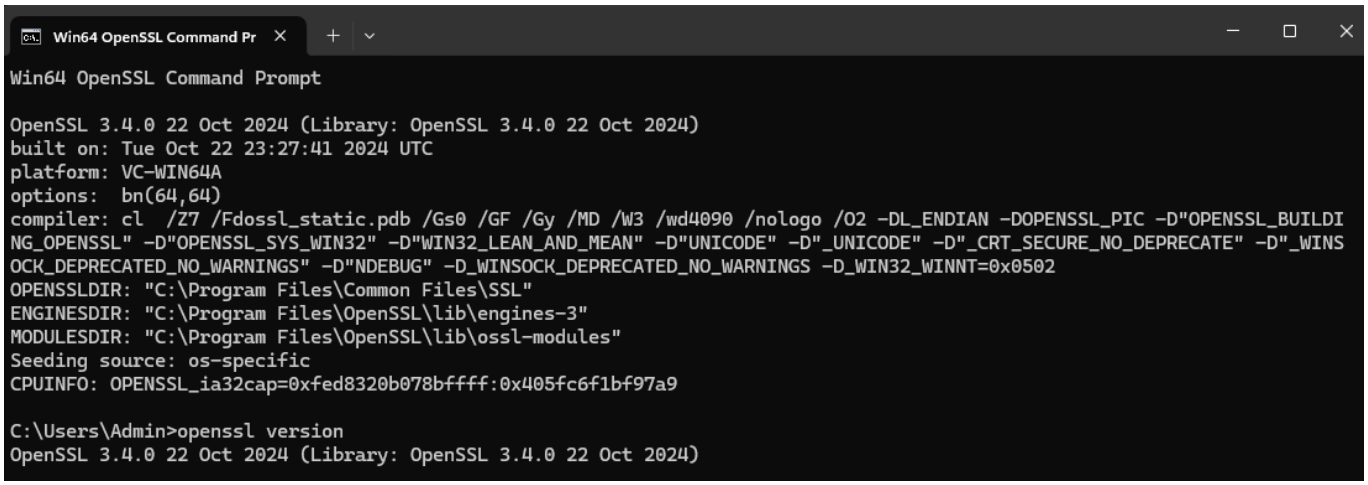

Рис.3.1. Версія OpenSSL для досліду

Створюємо структуру директорій для зручної організації всіх файлів, які ми будемо використовувати. Вони допомагають розділити різні типи даних за категоріями, що полегшує управління, пошук і аналіз.

```
C:\Users\Admin>mkdir PKI_Test && cd PKI_Test

C:\Users\Admin\PKI_Test>mkdir keys certs signed_docs encrypted_docs
```

Рис.3.2. Створюємо директорію для організації робочих файлів

1. mkdir PKI_Test && cd PKI_Test

1) mkdir PKI_Test:

- Створює головну директорію з назвою PKI_Test, яка стане робочим середовищем.
- У цій директорії будуть зберігатися всі файли, пов'язані з тестуванням.

2) cd PKI_Test:

- Переходить у створену директорію PKI_Test, щоб всі наступні команди виконувалися саме в цьому робочому середовищі.

2. mkdir keys certs signed_docs encrypted_docs

1) keys

У цій директорії зберігаються всі приватні, публічні та симетричні ключі. Ці приватні ключі особливо важливі, їх потрібно захищати і тримати окремо для зменшення ризику компрометації.

2) certs

У цій директорії зберігаються сертифікати:

- Сертифікат кореневого центру сертифікації (Root CA).
- Сертифікати користувачів.
- Файли запитів на сертифікати (CSR).

Сертифікати потрібні для перевірки автентичності публічних ключів, і їх зручно зберігати централізовано.

3) signed_docs

Ця директорія призначена для файлів підписів (*.sig) та документів, що були підписані. Зберігання підписів окремо спрощує перевірку автентичності документів.

4) encrypted_docs

У цьому каталозі зберігаються зашифровані документи (*.enc) та інші файли, пов’язані з шифруванням.Зберігання зашифрованих файлів окремо допомагає легко знаходити ті, які потребують дешифрування.

Тепер створимо базову інфраструктуру відкритих ключей (PKI) згенерувавши ключі та сертифікати:

Створюємо приватний ключ для кореневого центру сертифікації (Root CA). Це головний ключ, який використовується для підпису сертифікатів інших учасників. Використання алгоритму RSA забезпечує асиметричне шифрування.

Рис.3.3. Створення приватного ключа для Root CA

Ключові параметри:

- -algorithm RSA: вказує, що використовується алгоритм RSA.
- -out keys/rootCA.key: визначає місце збереження ключа.
- -aes256: додає шифрування приватного ключа симетричним алгоритмом AES-256. Це забезпечує додатковий рівень захисту (потрібен пароль для доступу).

Приватний ключ Root CA використовується для підпису сертифікатів інших учасників, забезпечуючи їх автентичність і зв’язок з довіреним центром сертифікації.

Створюємо сертифікат Root CA, який є самопідписаним. Сертифікат підтверджує автентичність Root CA і дозволяє іншим довіряти його підписам.

```
C:\Users\Admin\PKI_Test>openssl req -x509 -new -key keys/rootCA.key -sha256 -days 3650 -out certs/rootCA.crt
Enter pass phrase for keys/rootCA.key:

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:UA
State or Province Name (full name) [Some-State]:Kyiv
Locality Name (eg, city) []:Kyiv
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Test
Organizational Unit Name (eg, section) []:Test
Common Name (e.g. server FQDN or YOUR name) []:Test
Email Address []:Test
```

Рис.3.4. Створення самопідписаного сертифіката для Root CA

Ключові параметри:

- -x509: вказує, що створюється сертифікат, а не запит на сертифікат.
- -key keys/rootCA.key: використовує приватний ключ Root CA для підпису.
- -sha256: обирає хеш-функцію SHA-256 для підпису.
- -days 3650: встановлює термін дії сертифіката (10 років).
- -out certs/rootCA.crt: визначає місце збереження сертифіката.

Сертифікат Root CA є основою довіри в PKI. Інші учасники використовуватимуть його для перевірки підписів.

Створюємо приватний ключ для користувача, який використовуватиметься для підпису або дешифрування документів.

Рис.3.5. Генерація приватного ключа для користувача (власника документів)

Ключові параметри є аналогічними параметрам команд для Root CA.

Користувач використовує приватний ключ для підпису своїх документів або для дешифрування повідомлень, зашифрованих його публічним ключем.

Генеруємо запит на сертифікат (CSR) для користувача. CSR містить публічний ключ користувача і інформацію про нього (ім’я, email, організація тощо).

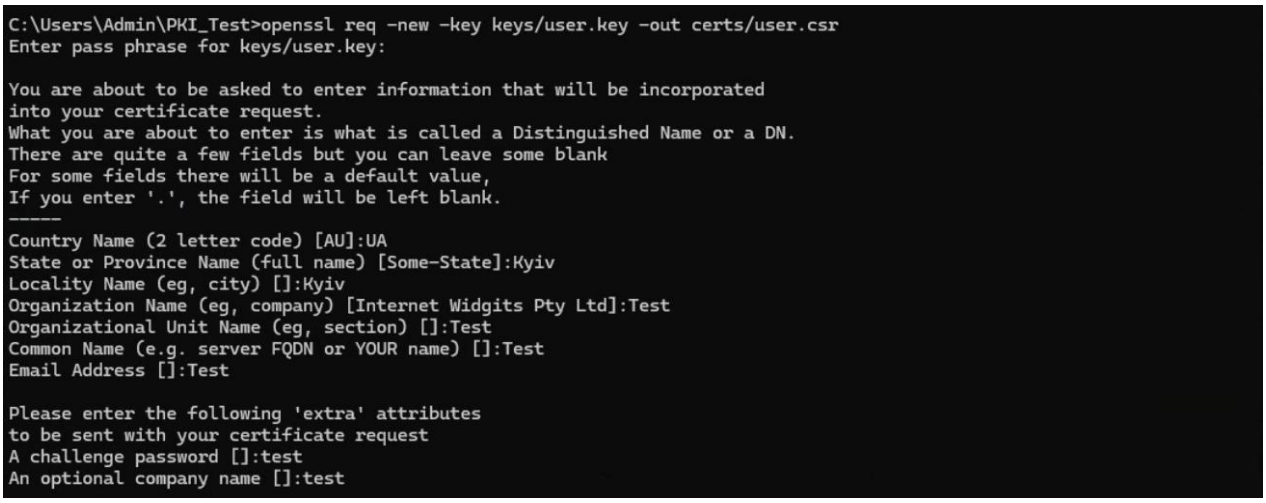

Рис.3.6. Генерація запиту на сертифікат (CSR) для користувача (власника документів)

Ключові параметри:

- -new: створює новий запит на сертифікат.

- -key keys/user.key: вказує приватний ключ користувача для зв’язку з публічним ключем.
- -out certs/user.csr: визначає місце збереження запиту.

CSR відправляється в Root CA для підпису, щоб отримати сертифікат, який підтверджує, що цей публічний ключ належить користувачу. Root CA підписує запит користувача (CSR), створюючи сертифікат для публічного ключа користувача.

```
C:\Users\Admin\PKI_Test>openssl x509 -req -in certs/user.csr -CA certs/rootCA.crt -CAkey keys/rootCA.key -CAcreateseri
al -out certs/user.crt -days 365 -sha256
Certificate request self-signature ok
subject=C=UA, ST=Kyiv, L=Kyiv, O=Test, OU=Test, CN=Test, emailAddress=Test
Enter pass phrase for keys/rootCA.key:
```

Рис.3.7. Генерація підпису сертифікату користувача Root CA для користувача (власника документів)

Ключові параметри:

- -req: вказує, що вхідний файл — це CSR.
- -in certs/user.csr: визначає місце збереження запиту на сертифікат.
- -CA certs/rootCA.crt: використовує сертифікат Root CA.
- -CAkey keys/rootCA.key: використовує приватний ключ Root CA для підпису.
- -CAcreateserial: створює унікальний серійний номер для сертифіката.
- -out certs/user.crt: визначає місце збереження сертифіката користувача.
- -days 365: встановлює термін дії сертифіката (1 рік).
- -sha256: використовує хеш-функцію SHA-256.

Сертифікат користувача підтверджує автентичність його публічного ключа. Інші учасники можуть перевіряти цей сертифікат, щоб упевнитися, що публічний ключ належить користувачу.

Цими діями ми створорили базову PKI-інфраструктуру і забезпечили механізм для автентифікації публічних ключів. Тепер ми можемо безпечно обмінювати зашифрованими повідомленнями та підписаними документами.

Тепер спробуємо ахистити дані використавши цифровий підпис. Розганемо як простий так і більш надійніший, складний, метод.

1. Простий метод

Для початку, створимо документ для підпису.

```
C:\Users\Admin\PKI_Test>echo "test_doc" > document.txt
```

Рис.3.8. Створення документу для підпису

Уявімо що в цьому документі є якась важлива для нас інформація.

Тепер підпишимо документ приватним ключем.

```
C:\Users\Admin\PKI_Test>openssl dgst -sha256 -sign keys/user.key -out signed_docs/document.sig document.txt
Enter pass phrase for keys/user.key:
```

Рис.3.9. Підписання документу приватним ключем

Ця команда генерує цифровий підпис для документа document.txt:

- Використовує хеш-функцію SHA-256 (-sha256), щоб створити унікальний хеш документа.
- Шифрує цей хеш за допомогою приватного ключа користувача (keys/user.key).
- Зберігає підпис у файлі signed_docs/document.sig.

Цифровий підпис гарантує, що документ не був змінений (перевіривши його цілісность) та що ідпис належить власнику приватного ключа (автентичність).

Тепер спробуємо перевірити цей підпис.

```
C:\Users\Admin\PKI_Test>openssl dgst -sha256 -verify certs/user.crt -signature signed_docs/document.sig document.txt
Verified OK
```

Рис.3.10. Перевірка цифровго підпису

Ми перевірили підпис від лиця отримувача використавши публічний ключ, що міститься в сертифікаті користувача (certs/user.crt).

Ця команда:

- Відкриває підписаний хеш, використовуючи публічний ключ.
- Генерує новий хеш з отриманого документа.
- Порівнює ці два хеші.

Хеші збіглись і це підтверджує автентичність та цілісність документа.

Тепер ми впевнились, що документ підписав саме той, хто володіє приватним ключем, а його вміст не змінювався.

2. Ускладнений метод

Документ залишаемо той самий.

```
C:\Users\Admin\PKI_Test>cat document.txt certs/user.crt > combined_document.txt

C:\Users\Admin\PKI_Test>openssl dgst -sha256 -sign keys/user.key -out signed_docs/combined_document.sig combined_docum
ent.txt
Enter pass phrase for keys/user.key:
```

Рис.3.11. Підписання документа із включенням сертифіката

Команда cat document.txt certs/user.crt > combined_document.txt створює файл combined_document.txt, тобто об’єднує їх в один, який містить, окумент (document.txt) та сертифікат користувача (certs/user.crt).

Це гарантує, що сертифікат завжди зберігається разом із документом.

Це дозволяє не лише перевіряти підпис, а й включає сертифікат, щоб отримувач міг переконатися, хто саме підписав документ.

Тепер знову перевімо наш підпис.

```
C:\Users\Admin\PKI_Test>openssl dgst -sha256 -verify certs/rootCA.crt -signature signed_docs/combined_document.sig com
bined_document.txt
Verified OK
```

Рис.3.12. Перевірка підпису документа із включенням сертифіката

Отримувач може переконатися не лише в автентичності підпису, але й у тому, що підписант має дійсний сертифікат, виданий довіреним Root CA.

Якщо би перевірка не проходила, ми би отримували результат у вигляді Verification Failure

Порівняємо простий та ускладненний метод:

Таблиця 3.1.

Порівняння просто та ускладненого методу

Функція	Простий варіант	Ускладнений варіант
Перевірка цілісності	Є	Є
Перевірка автентичності	Є	Є
Включення сертифікату	Відсутній	Є
Перевірка сертифіката	Відсутній	Є

Далі розглянемо як можна захистити документ шляхом шифрування

1. Простий метод

Спробуємо зашифрувати документ.

```
C:\Users\Admin\PKI_Test>openssl pkeyutl -encrypt -inkey certs/user.crt -pubin -in document.txt -out encrypted_docs/document.enc
Enter pass phrase for keys/user.key:
```

Рис.3.13. Шифрування документа публічним ключем отримувача

Ця команда шифрує файл document.txt за допомогою публічного ключа отримувача (certs/user.crt). Тільки володар відповідного приватного ключа може розшифрувати документ.

Ключові параметри:

- rsautl: Використовує RSA для утиліт шифрування та дешифрування.
- -encrypt: Вказує, що необхідно виконати шифрування.
- -inkey certs/user.crt: Вказує файл з публічним ключем отримувача.
- -pubin: Повідомляє OpenSSL, що вхідний ключ є публічним.
- -in document.txt: Вхідний файл для шифрування.
- -out encrypted_docs/document.enc: Вихідний зашифрований файл.

А тепер дешифруємо його:

```
C:\Users\Admin\PKI_Test>openssl rsautl -decrypt -inkey keys/user.key -in encrypted_docs/document.enc -out decrypted_document.txt
Enter pass phrase for keys/user.key:
```

Рис.3.13. Дешифрування документа публічним ключем отримувача

```
C:\Users\Admin\PKI Test>cat decrypted_document.txt
test_doc
```

Рис.3.14. Перевірка вмісту дешифрованого документа

Ця команда розшифровує файл encrypted_docs/document.enc за допомогою приватного ключа отримувача (keys/user.key). Оригінальний документ відновлюється в decrypted_document.txt.

Параметри:

- rsautl: Використовує RSA для утиліт шифрування та дешифрування.
- -decrypt: Вказує, що необхідно виконати дешифрування.
- -inkey keys/user.key: Вказує файл з приватним ключем отримувача.
- -in encrypted_docs/document.enc: Вхідний зашифрований файл.
- -out decrypted_document.txt: Вихідний розшифрований файл.

Це дозволяє отримувачу відновити оригінальний документ, забезпечуючи, що лише він має доступ до змісту.

2. Ускладнений метод

Цей варіант поєднує асиметричне та симетричне шифрування для ефективного захисту великих файлів. Асиметричне шифрування використовується для захисту симетричного ключа, а симетричне — для шифрування самого документа.

Зараз ми згенеруємо симетричний ключа для AES-256 і відразу перевірим наш результат:

```
C:\Users\Admin\PKI_Test>openssl rand -hex 32 > keys/symmetric.key

C:\Users\Admin\PKI_Test>cat keys/symmetric.key
c8fb1f75c8d32e456ty84gy5f787c62de2f9e45b6a7b3c9d8024561f89a3b1c75
```

Рис.3.15. Генерація симетричного ключа для AES-256

Генерація симетричного ключа створює нам випадковий ключ довжиною 256 біт (32 байти) для алгоритму AES-256. Використання випадкового ключа забезпечує високий рівень захисту.

Ключові параметри:

- rand: Генерує випадкові байти.

- -hex: Виводить результат у шістнадцятковому форматі.
- 32: Вказує кількість байтів (32 байти * 8 = 256 біт).
- > keys/symmetric.key: Зберігає згенерований ключ у файл keys/symmetric.key.

Симетричне шифрування (AES-256) є більш ефективним для великих файлів, порівняно з асиметричним (RSA).

```
C:\Users\Admin\PKI_Test>openssl enc -aes-256-cbc -salt -in document.txt -out encrypted_docs/document_aes.enc -pass file:keys/symmetric.key
C:\Users\Admin\PKI_Test>openssl rsautl -encrypt -inkey certs/user.crt -pubin -in keys/symmetric.key -out keys/symmetric.key.enc
```

Рис.3.16. Шифрування документа симетричним ключем

та додаткова шифровка ключа публічним ключем

Симетричне шифрування шифрує файл document.txt за допомогою симетричного ключа (keys/symmetric.key) з використанням алгоритму AES-256 CBC.

Ключові параметри:

- enc: Використовується для симетричного шифрування.
- -aes-256-cbc: Вказує алгоритм шифрування (AES-256 у режимі CBC).
- -salt: Додає випадкову сіль для підвищення безпеки.
- -in document.txt: Вхідний файл для шифрування.
- -out encrypted_docs/document_aes.enc: Вихідний зашифрований файл.
- -pass file:keys/symmetric.key: Вказує файл з симетричним ключем.

Асиметричне шифрування симетричного ключа шифрує симетричний ключ (keys/symmetric.key) за допомогою публічного ключа отримувача (certs/user.crt). Лише отримувач з відповідним приватним ключем може розшифрувати симетричний ключ.

Ключові параметри::

- rsautl: Використовує RSA для утиліт шифрування та дешифрування.

- -encrypt: Вказує, що необхідно виконати шифрування.
- -inkey certs/user.crt: Вказує файл з публічним ключем отримувача.
- -pubin: Повідомляє OpenSSL, що вхідний ключ є публічним.
- -in keys/symmetric.key: Вхідний симетричний ключ для шифрування.
- -out keys/symmetric.key.enc: Вихідний зашифрований симетричний ключ.

Це дозволяє безпечно передати симетричний ключ отримувачу, який зможе його розшифрувати та використовувати для дешифрування документа.

Тепер дешифруємо цей документ:

```
C:\Users\Admin\PKI_Test>openssl rsautl -decrypt -inkey keys/user.key -in keys/symmetric.key.enc -out keys/symmetric.key.dec

C:\Users\Admin\PKI_Test>openssl enc -aes-256-cbc -d -in encrypted_docs/document_aes.enc -out decrypted_document.txt -pass file:keys/symmetric.key
.dec
```

Рис.3.16. Дешифрування документа симетричним ключем

та дешифровка ключа публічним ключем

Так як консоль не видає у відповідь нічого, значить дешифровка успішна. Якщо ключ був невірним то нам би видавало помилку RSA operation error або bad decrypt.

Дешифрування симетричного ключа, розшифровує зашифрований симетричний ключ (keys/symmetric.key.enc) за допомогою приватного ключа отримувача (keys/user.key). Отримувач отримує оригінальний симетричний ключ для дешифрування документа.

Ключові параметри:

- rsautl: Використовує RSA для утиліт шифрування та дешифрування.
- -decrypt: Вказує, що необхідно виконати дешифрування.
- -inkey keys/user.key: Вказує файл з приватним ключем отримувача.
- -in keys/symmetric.key.enc: Вхідний зашифрований симетричний ключ.

- -out keys/symmetric.key.dec: Вихідний розшифрований симетричний ключ.

Отримувач розшифровує симетричний ключ, щоб використовувати його для дешифрування зашифрованого документа.

Симетричне дешифрування, розшифровує файл який продемонстрованно encrypted_docs/document_aes.enc за допомогою симетричного ключа (keys/symmetric.key.dec), відновлюючи оригінальний документ decrypted_document.txt.Відновлює доступ до вмісту документа для отримувача.

Ключові параметри:

- enc: Використовується для симетричного шифрування/дешифрування.
- -aes-256-cbc: Вказує алгоритм шифрування (AES-256 у режимі CBC).
- -d: Вказує, що необхідно виконати дешифрування.
- -in encrypted_docs/document_aes.enc: Вхідний зашифрований файл.
- -out decrypted_document.txt: Вихідний розшифрований файл.
- -pass file:keys/symmetric.key.dec: Вказує файл з розшифрованим симетричним ключем.

Отримувач відновлює оригінальний документ, використовуючи симетричний ключ, який було безпечно передано та розшифровано.

Тепер спробуємо захистити сертифікати від атак:

Перевіримо валідності сертифікатів.

```
C:\Users\Admin\PKI_Test>openssl verify -CAfile certs/rootCA.crt certs/user.crt
certs/user.crt: OK
```

Рис.3.17. Перевірка валідності сертифікатів

У відповідь на команду ми отримали certs/user.crt: OK, це значить:

- Сертифікат користувача user.crt був підписаний CA з сертифікатом rootCA.crt.
- Сертифікат ще не протермінований.
- Ланцюжок довіри успішно перевірено.

Якби сертифікат був невалідний, ми би отримали таке повідомлення error 20 at 0 depth lookup: unable to get local issuer certificate. Це означає:

- Сертифікат user.crt не був підписаний CA, сертифікат якого вказаний у rootCA.crt.
- Сертифікат або недійсний, або rootCA.crt не відповідає сертифікату CA, який підписав user.crt.

Якщо сертифыкат протермынованний, то буде така помилка error 10 at 0 depth lookup: certificate has expired. Це означає, що термін дії сертифікату закінчився. Його просто треба буде перегенерувати.

Якщо сертифыкат протермынованний скомпрометований або відкликаний (з CRL), то error 23 at 0 depth lookup: certificate revoked. Це означає, що Сертифікат user.crt знаходиться у списку відкликаних сертифікатів (CRL).

```
C:\Users\Admin\PKI_Test>openssl ca -gencrl -keyfile keys/rootCA.key -cert certs/rootCA.crt -out certs/rootCA.crl
Using configuration from C:\Program Files\Common Files\SSL\/openssl.cnf
Enter pass phrase for keys/rootCA.key:

Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 01:57:45:67:89:gh:cd:ef:12:214:59:58:90:ar:fk:ch
        Validity
            Not Before: Dec  6 12:00:00 2024 GMT
            Not After : Dec  6 12:00:00 2025 GMT
...
Data Base Updated
```

Рис.3.18. Додавання CRL

Ця команда створює список відкликаних сертифікатів (CRL), використовуючи приватний ключ та сертифікат кореневого CA. CRL містить серійні номери всіх сертифікатів, які були відкликані CA.

Ключові параметри:

- ca: Використовується для управління сертифікатами CA.
- -gencrl: Вказує, що потрібно створити CRL.
- -keyfile keys/rootCA.key: Приватний ключ кореневого CA.
- -cert certs/rootCA.crt: Сертифікат кореневого CA.
- -out certs/rootCA.crl: Вихідний файл CRL.

Він дозволяє повідомляти клієнтів про відкликані сертифікати, які більше не є дійсними, а також захищає від атак, коли зловмисник використовує скомпрометований або відкликаний сертифікат.

При перевірці видається така сама відповідь як і при перевірці сертифікату.

3.2 Переваги використання кожного з методів захисту документів в PKI

Використання методів захисту документів у системах PKI забезпечує низку переваг. Цифровий підпис гарантує автентичність документа, підтверджуючи, що його підписав власник приватного ключа. Завдяки цьому забезпечується цілісність інформації, адже будь-яка зміна в документі робить підпис недійсним. Крім того, підпис забезпечує незаперечність, оскільки підписувач не може заперечити факт свого підпису. Ускладнений підпис із включенням метаданих додає додатковий рівень захисту, оскільки він містить сертифікат користувача, що підвищує довіру до підпису та дозволяє виявляти фальсифікації.

Що стосується шифрування, простий метод із використанням RSA захищає конфіденційність документа, оскільки лише власник приватного ключа може його розшифрувати. Це ідеальне рішення для невеликих файлів, адже воно не потребує передачі симетричних ключів. Ускладнений варіант із використанням гібридного шифрування (AES та RSA) підвищує ефективність, дозволяючи швидко шифрувати великі обсяги даних за допомогою AES. Одночасно симетричний ключ,

зашифрований RSA, гарантує безпечну передачу. Таким чином, гібридний метод поєднує швидкість симетричного та безпеку асиметричного шифрування.

Захист від атак на сертифікати є ще одним важливим аспектом. Перевірка валідності сертифікатів дозволяє переконатися, що вони були видані довіреним центром сертифікації, та запобігає атакам, які можуть використовувати підроблені або протерміновані сертифікати. Додавання списків відкликаних сертифікатів (CRL) допомагає уникнути використання скомпрометованих сертифікатів, забезпечуючи надійність навіть у разі компрометації ключа. Це також дозволяє централізовано управляти довірою до сертифікатів у масштабній інфраструктурі.

У сукупності ці методи створюють надійний, багаторівневий захист документів у системах PKI. Вони забезпечують довіру, автентичність, цілісність та конфіденційність даних, що робить їх незамінними для безпечного цифрового обміну інформацією.

3.3 Розробка рекомендацій щодо застосування методів захисту документів в інрфраструктурі відкритих ключей

Рекомендації щодо використання методів захисту документів у PKI залежать від характеру інформації, яка обробляється, та рівня безпеки, необхідного в конкретному сценарії.

Для забезпечення цілісності та автентичності документа варто використовувати цифровий підпис. Простий підпис підходить для звичайних документів, де важливо підтвердити особу підписувача та гарантувати, що документ не змінювався. Ускладнений підпис із включенням метаданих рекомендується застосовувати в ситуаціях, коли необхідний підвищений рівень довіри, наприклад, у юридичних або фінансових транзакціях, оскільки він забезпечує додаткову перевірку сертифікатів.

Для забезпечення конфіденційності під час передачі даних доцільно застосовувати шифрування. Простий метод із використанням RSA підходить для невеликих файлів або передачі чутливих повідомлень, де не потрібне шифрування великих обсягів інформації. У випадках, коли необхідно захищати великі документи чи масиви даних, рекомендовано використовувати гібридний метод шифрування. Генерація симетричного ключа AES для шифрування даних та його подальше шифрування RSA забезпечують як ефективність, так і високий рівень безпеки.

Для захисту від атак на сертифікати необхідно регулярно перевіряти валідність сертифікатів, особливо під час обробки критично важливих транзакцій. Це гарантує, що використовуються лише сертифікати, видані довіреними центрами сертифікації. Додавання списків відкликаних сертифікатів (CRL) рекомендовано для захисту від скомпрометованих або протермінованих сертифікатів. У сценаріях із високими вимогами до безпеки, таких як захист персональних даних або фінансових операцій, CRL має регулярно оновлюватися.

Усі ці методи найкраще працюють у поєднанні, створюючи багаторівневий захист, який відповідає сучасним викликам інформаційної безпеки. Рекомендується інтегрувати їх у єдину інфраструктуру PKI для забезпечення максимальної надійності.

Висновки до третього розділу

У цьому розділі досліджено налаштування та функції OpenSSL, як одного з основних інструментів для захисту документів в інфраструктурі відкритих ключів (PKI). Визначено, що OpenSSL забезпечує широкий спектр можливостей, включаючи генерацію ключів, сертифікацію та шифрування, що є основою для безпечного документообігу.

Проаналізовано переваги різних методів захисту документів у PKI, таких як цифровий підпис, шифрування та використання сертифікаційних ланцюгів. Ці методи забезпечують конфіденційність, цілісність та автентичність документів, що робить їх важливими для підтримання безпеки.

На основі проведеного аналізу розроблено рекомендації щодо вибору та застосування методів захисту залежно від потреб організації, рівня загроз та вимог до інформаційної безпеки. Зроблено акцент на важливості дотримання стандартів безпеки, регулярного оновлення сертифікатів та моніторингу системи для мінімізації ризиків.

ВИСНОВКИ

Технологія захищеного обміну документами на основі інфраструктури відкритих ключів (PKI) є ефективним і надійним рішенням для забезпечення безпеки в цифровому середовищі. Інтеграція PKI дозволяє досягти ключових цілей інформаційної безпеки: забезпечення автентичності, цілісності, конфіденційності даних та незаперечності дій користувачів.

У процесі дослідження було показано, що цифровий підпис є ключовим механізмом для підтвердження авторства документа та захисту його від несанкціонованих змін. Використання шифрування, як симетричного, так і асиметричного, забезпечує надійний захист конфіденційності даних при їхньому передаванні. Додатково, впровадження механізмів перевірки валідності сертифікатів і управління списками відкликаних сертифікатів (CRL) мінімізує ризики компрометації ключів і забезпечує довіру до учасників системи.

PKI демонструє високу гнучкість і масштабованість, що робить її придатною для широкого спектра застосувань, від особистого обміну даними до корпоративних систем і державних сервісів. Завдяки використанню стандартизованих протоколів та алгоритмів, технологія PKI відповідає сучасним вимогам до інформаційної безпеки, водночас залишаючись відкритою до інтеграції з новітніми технологіями.

Застосування PKI дозволяє організаціям і користувачам впевнено працювати з електронними документами, знижуючи ризики кібератак і захищаючи критично важливу інформацію. Таким чином, впровадження інфраструктури відкритих ключів є невід'ємною частиною побудови безпечного цифрового середовища, що особливо актуально в умовах постійного зростання обсягів і складності електронного документообігу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Pfleeger, C.P., Pfleeger, S.L., Margulies, M. (2015) Security in Computing, 5th Edition Prentice Hall.

2. Microsoft, (2016) Certificate Trust List Overview. [Online]. Available: https:/msdn.microsoft.com/en-us/library/windows/desktop/aa376545%28vevs.85%29.aspx

3. Hierarchical PKI Architecture for Secure Trust Management (2023). Available: https://michaelwaterman.nl/2023/08/30/pki-part-1-introduction-to-public-key-infrastructure/

4. Santesson, S., Farrell, S., Boeyen R., Housley, S., Polk, W. (2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Network Working Group Request for Comments, IETF RFC 5280.

5. DPKI: A Blockchain-Based Decentralized Public Key Infrastructure System.(2023). Available: https://ieeexplore.ieee.org/document/9119673

6. An overview of PKI trust models (2023). Available: https://ieeexplore.ieee.org/document/806987

7. Shirey, B. (2007) Internet Security Glossary, Version 2, RFC 4949, IETF.

8. Prodanović, R. L, Vulić, LB. (2017) Failure Points in the PKI Architecture, Vojnotehnicki glasnik/Military Technical Courier, Vol 65, Issue 3, pp. 771-784.

9. IT Risk Management Strategies and Processes (2021). Available: https://www.upguard.com/blog/it-risk-management

10. The Risk Management Process: An Interagency Security Committee Standard (2024 Edition) Available: https://www.cisa.gov/sites/default/files/2024-07/The_Risk_Management_Process_2024_Edition.pdf

11. NIST Risk Management Framework (RMF) (2020) Available: https://www.nist.gov/risk-management

12. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST SP 800-37 Rev. 2, 2018) Available: https://csrc.nist.rip/pubs/sp/800/37/r2/iprd

13. Communication and Consultation in Risk Management (2020). Available: https://www.researchgate.net/publication/329324923_Dakwah_dalam_Mewujudkan_Interaksi_dan_Kerukunan_Antar_Umat_Beragama_Di_Palopo_Sulawesi_Selatan
14. PKI Security: Challenges and Mitigation Strategies (2022). Available: https://securityboulevard.com/2024/08/top-trends-in-2024-reshaping-the-pki-landscape/
15. PKI – Understanding Certificate Revocation List (CRL) – Part 1 (2023). Available: https://www.netprojnetworks.com/pki-understanding-certificate-revocation-list-crl-part-1/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)