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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Інфраструктури відкритих ключів для забезпечення інформаційної безпеки організації»

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

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

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

_____ Поплавець Ярослав
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
Поплавець Ярослав
(прізвище, ім'я)

Керівник к.т.н., доцент, Борсуковський Ю.В
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Поплавцю Ярославу Васильовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
Система захисту кінцевих точок організації на базі FortiEDR»

керівник кваліфікаційної роботи Борсуковський Юрій, к.т.н.,доцент
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Fortinet FortiEDR;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту кінцевих точок організації.
2. Аналіз методів та засобів захисту кінцевих точок організації на базі FortiEDR.
3. Розроблення рекомендацій щодо захисту кінцевих точок організації на базі FortiEDR.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок організації.	03.03.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	04.04.2025	
3.	Аналіз методів та засобів захисту кінцевих точок організації на базі FortiEDR.	13.04.2025	
4.	Практична реалізація варіанту захисту кінцевих точок організації на базі FortiEDR.	27.04.2025	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту кінцевих точок організації.	15.05.2025	
6.	Оформлення результатів дослідження.	31.05.2025	
7.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Ярослав Поплавець
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій Борсуковський
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача Поплавця Ярослава
на тему: «Дослідження шляхів та розроблення рекомендацій щодо захисту кінцевих точок організації на базі FortiEDR»

Актуальність: Забезпечення безпеки кінцевих точок організацій, такі як сервери, комп'ютери, ноутбуки та мобільні пристрої має важливе значення для запобігання несанкціонованому доступу, витоку даних і втраті даних. Системи EDR забезпечують безперервний моніторинг кінцевих точок, дозволяючи організаціям підтримувати видимість стану безпеки та завчасно реагувати на нові загрози.

Кібератаки, які порушують або компрометують кінцеві точки організації, може призвести до простою, що впливає на продуктивність і безперервність бізнесу. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту кінцевих точок організації та визначено мету та завдання даного виду забезпечення, а також його складові частини.
2. Досліджено методи та засоби захисту кінцевих точок організації на базі FortiEDR.
3. Запропоновано варіант системи захисту кінцевих точок організації на базі FortiEDR та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз змісту захисту кінцевих точок на прикладі конкретної організації.
2. Запропонований порядок застосування методів та засобів захисту кінцевих точок бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"добре"**, а здобувач(ка) Поплавець Ярослав – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

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

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Поплавець Ярослав до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Система захисту кінцевих точок організації на базі FortiEDR».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***Поплавець Ярослав*** обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***Поплавець Ярослав*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***Поплавця Ярослава*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій Борсуковський
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **Поплавець Ярослав** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

Реферат

Текстова частина кваліфікаційної роботи: 59 сторінки, 3 таблиці, 14 джерела.

Об’єкт дослідження: процеси забезпечення інформаційної безпеки організації.

Предмет дослідження: інфраструктура відкритих ключів (PKI) як інструмент для гарантування конфіденційності, цілісності та автентичності даних.

Мета роботи: проаналізувати та розробити ефективну модель використання PKI в контексті захисту інформації організації.

Методи дослідження: аналіз наукових джерел, порівняльний аналіз, моделювання, проєктування архітектури PKI.

Галузь використання: інформаційна безпека підприємств, державні та корпоративні IT-системи, електронний документообіг, цифровий підпис, кібербезпека в медичній, банківській, освітній сферах.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PKI (Public Key Infrastructure) Інфраструктура відкритих ключів - інтегрований комплекс методів та засобів, призначених забезпечити впровадження та експлуатацію криптографічних систем із відкритими ключами.

CA (Certification Authority) Центр сертифікації - довірена третя сторона, яка видає, поновлює, відкликає та керує цифровими сертифікатами.

RA (Registration Authority) Реєстраційний центр - проміжна ланка між користувачем і CA, яка перевіряє особу користувача перед видачею сертифікату.

CRL (Certificate Revocation List) Перелік відкликаних сертифікатів – реєстр, де фіксуються сертифікати, чинність яких було припинено достроково.

OCSP (Online Certificate Status Protocol) Протокол перевірки стану сертифікатів в реальному часі. Його завданням є миттєве отримання інформації про дійсність сертифіката.

X.509 Стандарт, що окреслює формат цифрових сертифікатів, визначаючи їхню будову та правила використання.

CSR (Certificate Signing Request) Запит на підписання сертифіката-це повідомлення, сформоване користувачем і відправлене до центру сертифікації для отримання цифрового сертифіката.

SSL/TLS (Secure Sockets Layer / Transport Layer Security) Комплекс протоколів шифрування, що забезпечують захищене передавання даних через мережу, гарантуючи конфіденційність та цілісність даних.

HSM (Hardware Security Module) Апаратний модуль безпеки, фізичний пристрій, що використовується для безпечного зберігання та обробки криптографічних ключів.

DNSSEC Розширення системи доменних імен (DNS), що забезпечує автентифікацію джерела DNS-записів за допомогою цифрових підписів.

LDAP (Lightweight Directory Access Protocol) Протокол доступу до інформаційних каталогів, часто використовується для зберігання та отримання сертифікатів PKI.

ВСТУП

У нинішньому світі інформація стала одним з найцінніших ресурсів для кожної організації. Розвиток цифрових технологій та збільшення обсягі вобміну даними в електронному вигляді зумовлюють зростання вимог до безпеки інформаційних систем. Інформаційна безпека перетворюється на ключовий стратегічний виклик для бізнесу,організацій та державних структур,а не просто технічну складову. Побудова безпечного цифрового простору з начною мірою залежить від інфраструктури відкритих ключів (PKI - Public Key Infrastructure), що виступає одним з основних компонентів. Цей інструмент надає змогу гарантувати автентичність, цілісність, конфіденційність і неможливість відмови від авторства електронних повідомлень і документів. Це досягається завдяки застосуванню криптографічних алгоритмів, які використовують відкритий та закритий ключі. PKI використовується для захисту електронної пошти, мережевого трафіку, електронного документообігу, ідентифікації користувачів, цифрових підписів тощо. Водночас впровадження PKI у реальних умовах пов’язане з низкою технічних, організаційних та правових викликів:необхідністю коректного проєктування архітектури, захистом приватних ключів, управлінням життєвим циклом сертифікатів, дотриманням стандартів та нормативів.

Актуальність дослідження. У зв’язку з активною цифровізацією, переходом до безпаперового документообігу, а також зростаючими кіберзагрозами, забезпечення інформаційної безпеки за допомогою PKI є актуальною темою для дослідження. Особливо це стосується організацій, які працюють із конфіденційними даними - банків, медичних установ, освітніх закладів, державних органів тощо.

Метою дипломної роботи є дослідження теоретичних та практичних аспектів побудови інфраструктури відкритих ключівзадлязабезпечення інформаційної безпеки організації, а також розробка власного варіанта архітектури PKI з урахуванням особливостей конкретної організації.

Завдання дослідження:

• Проаналізувати принципи функціонування PKI та її роль у забезпеченні кібербезпеки.

•Дослідитинаявні технічніта програмні рішення для реалізації PKI.

• Вивчити приклади використання PKI у різних сферах діяльності.

• Розробити модель архітектури PKI, адаптовану під потреби організації.

• Надати рекомендації щодо впровадження та експлуатації PKI.

Предмет дослідження - Інфраструктура відкритих ключів як інструмент захисту інформації та управління цифровими сертифікатами.

Методи дослідження - Аналіз наукових джерел, порівняльний аналіз рішень, моделювання, системний підхід, експертне оцінювання.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ (PKI)

1.1 Поняття та значення інформаційної безпеки

1. **Поняття інформаційної безпеки**

Інформаційна безпека - це стан захищеності інформації, за якого забезпечуються її конфіденційність, цілісність та доступність (CIA - Confidentiality, Integrity, Availability).

- **Конфіденційність** - забезпечення такого режиму обігу інформації, при якому доступ до неї мають лише уповноважені особи.
- **Цілісність** - гарантування того, що інформація не буде змінена або знищена сторонніми особами без дозволу.
- **Доступність** - забезпечення своєчасного та гарантованого доступу до інформації для уповноважених користувачів.

У деяких підходах до основних властивостей безпеки додають також:

- **Незаперечність** (Non-repudiation) - впевненість у тому, що відправник інформації не зможе заперечити факт її відправлення.
- **Автентичність** (Authenticity) - підтвердження достовірності джерела інформації.

2. **Мета та завдання інформаційної безпеки**

Головною метою інформаційної безпеки є захист інформаційних ресурсів від загроз, що можуть спричинити їхню втрату, модифікацію, розголошення або порушення доступності.

Завданнями ІБ є:

- Виявлення активів, що підлягають захисту;
- Ідентифікація можливих загроз і вразливостей;

- Розробка та впровадження заходів захисту;
- Реагування на інциденти безпеки;
- Проведення аудиту та контролю політик ІБ;
- Формування культури безпечної поведінки користувачів

3. Основні компоненти інформаційної безпеки

Інформаційна безпека охоплює кілька ключових сфер:

- **Технічна** використання засобів шифрування, антивірусного захисту, міжмережевих екранів, систем виявлення вторгнень тощо.
- **Програмна** - захист програмного забезпечення від уразливостей, зокрема через регулярне оновлення, аудит коду, дотримання принципів безпечної розробки.
- **Фізична** - охорона фізичного доступу до інформаційних систем (серверних, дата-центрів тощо).
- **Організаційна** - розробка політик, інструкцій, процедур безпечного поводження з інформацією.
- **Правова** - відповідність нормативно-правовим актам щодо захисту інформації (GDPR, ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», ISO/IEC 27001 тощо).
- **Соціальна** - підвищення обізнаності працівників щодо загроз соціальної інженерії, фішингу тощо.

4. Класифікація загроз інформаційній безпеці

Загрози ІБ можна класифікувати за кількома ознаками:

За джерелом походження:

- Внутрішні загрози (помилки або зловмисні дії співробітників);

- Зовнішні загрози (хакери, конкуренти, державні структури інших країн).

За характером впливу:

- Техногенні - збої обладнання, аварії;
- Програмні -шкідливе ПЗ, вразливості;
- Соціальні - маніпуляції, фішинг;
- Природні - пожежі, повені, стихійні лиха.

За способом реалізації:

- Несанкціонований доступ;
- Порушення цілісності;
- Витік або крадіжка даних;
- Атаки типу «відмова в обслуговуванні» (DoS, DDoS);
- Атаки типу "людина посередині" (Man-in-the-Middle);
- Шкідливе програмне забезпечення (віруси, трояни, шпигунські програми тощо).

5. Правові та нормативні аспекти інформаційної безпеки

Правове забезпечення ІБ є важливим чинником, що визначає загальні вимоги до захисту даних у різних країнах та організаціях.

В Україні ключовими нормативними документами є:

- Закон України «Про інформацію»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Постанови КМУ та накази Держспецзв'язку; Стандарти серії ДСТУ ISO/IEC 27000.

Міжнародні стандарти:

- ISO/IEC 27001 - міжнародний стандарт системи управління інформаційною безпекою (ISMS);
- NIST SP 800 - серія рекомендацій американського інституту стандартів;
- GDPR (ЄС) -Загальний регламент захисту персональних даних.

6. Роль людського фактора

Незважаючи на наявність потужних технічних засобів, людський фактор залишається однією з основних загроз. Помилки користувачів, нехтування політиками безпеки, довіра до фішингових листів - усе це призводить до інцидентів. Тому важливими аспектами є:

- Підвищення обізнаності персоналу;
- Проведення тренінгів; Впровадження політик «найменших привілеїв»;
- Контроль дій користувачів; Соціальні симуляції (фішинг-тести).

1.2 Основи криптографії: симетричне та асиметричне шифрування

Криптографія є однією з ключових галузей інформаційної безпеки, що забезпечує конфіденційність, цілісність, автентичність та невідмовність інформації. Історично криптографія розвивалась як мистецтво приховування повідомлень, проте в сучасному цифровому світі вона стала математичною дисципліною, яка є основою для побудови безпечних інформаційних систем. Основними методами криптографії є симетричне та асиметричне шифрування. Кожен із цих методів має свої переваги, недоліки, сфери застосування та математичні основи. У цьому розділі розглянемо детально обидва типи шифрування, їхню роль у забезпеченні інформаційної безпеки, а також порівняльну характеристику.

Симетричне шифрування (англ. symmetric encryption) - це криптографічний метод, при якому для шифрування та розшифрування інформації використовується один і той самий секретний ключ. Передача цього ключа між

сторонами комунікації має бути захищеною, оскільки компрометація ключа призводить до втрати безпеки. Принцип роботи симетричне шифрування працює за наступною схемою: Відправник і отримувач мають спільний ключ. Відправник шифрує повідомлення за допомогою цього ключа. Отримувач розшифровує зашифроване повідомлення тим самим ключем. Формально: Нехай M - відкритий текст (message), C - шифротекст (ciphertext), K - секретний ключ, тоді: C = E(K, M) - шифрування M = D(K, C) - розшифрування основні алгоритми симетричного шифрування найпоширенішими симетричними алгоритмами є: **AES (Advanced Encryption Standard)** - сучасний стандарт шифрування, прийнятий NIST у 2001 році. Має розмір ключа 128, 192 або 256 біт. Використовується у більшості безпечних систем. **DES (Data Encryption Standard)** - раніше популярний стандарт із 56-бітним ключем. Сьогодні вважається недостатньо безпечним. **3DES (Triple DES)** - удосконалення DES, яке застосовує DES тричі з різними ключами. **Blowfish, Twofish** - альтернативні алгоритми з відкритим кодом, використовуються в деяких програмних продуктах. **RC4, RC5, RC6** - поточні або блочні шифри, розроблені компанією RSA.

Переваги симетричного шифрування:

- **Висока швидкість**: алгоритми симетричного шифрування працюють значно швидше за асиметричні.
- **Мала обчислювальна складність**: особливо важливо для вбудованих систем і пристроїв з обмеженими ресурсами.
- **Простота реалізації**: менше математичних операцій порівняно з асиметричними методами.

Недоліки:

- **Проблема розповсюдження ключів**: секретний ключ потрібно передати захищеним каналом.

- **Масштабованість**: у мережі з n користувачами потрібно зберігати n(n-1)/2 унікальних ключів.
- **Компрометація ключа**: при втраті ключа вся інформація стає вразливою.

Асиметричне шифрування (англ. asymmetric encryption) - це метод, при якому використовуються два ключі: відкритий (public key) та закритий (private key). Відкритий ключ призначений для шифрування, а закритий - для розшифрування. На відміну від симетричного шифрування, відкритий ключ може бути розповсюджений без обмежень, тоді як приватний має зберігатися у таємниці. Принцип роботи кожен користувач генерує пару ключів — відкритий та закритий. Відкритий ключ публікується або передається іншій стороні. Відправник шифрує повідомлення відкритим ключем отримувача. Лише отримувач може розшифрувати повідомлення своїм приватним ключем. Формально: C = E(PubKey, M) - шифрування M = D(PrivKey, C) -розшифрування Основні алгоритми асиметричного шифрування **RSA (Rivest–Shamir–Adleman)** - найпоширеніший алгоритм, заснований на складності факторизації великих чисел. **ElGamal** - алгоритм, який базується на дискретному логарифмі. **ECC (Elliptic Curve Cryptography)** - криптографія на еліптичних кривих, яка забезпечує високий рівень безпеки при коротших ключах. **DSA (Digital Signature Algorithm)** - використовується переважно для створення електронних підписів.

Переваги асиметричного шифрування:

- **Безпечний обмін ключами**: відсутня потреба в захищеному каналі для передачі ключів.
- **Масштабованість**: кожен користувач має одну пару ключів незалежно від кількості співрозмовників.
- **Цифровий підпис**: надає можливість перевірки автентичності та цілісності повідомлень.

Недоліки:

- **Повільна швидкість**: асиметричне шифрування у 100–1000 разів повільніше за симетричне.
- **Високі обчислювальні витрати**: вимагає значних ресурсів для операцій із великими числами.
- **Складність реалізації**: потребує ретельного математичного аналізу та точного програмного втілення.

Порівняння симетричного та асиметричного шифрування Симетричне та асиметричне шифрування — це два основні підходи до захисту відомостей. Вони мають різні принципи діяльності, особливості використання та переваги.

Наприклад, у протоколі TLS/SSL (що забезпечує захищений доступ до вебсайтів) для встановлення з’єднання використовується асиметричне шифрування для обміну ключами, після чого передача даних відбувається вже за допомогою симетричного шифрування. Таким чином: Асиметричне шифрування використовується на початковому етапі для безпечного обміну ключами. Симетричне - для основної передачі даних, де важлива швидкість. Цей підхід дозволяє забезпечити і безпечність, і ефективність роботи системи.

1.3 Інфраструктура відкритих ключів: визначення, призначення, основні компоненти

Зі зростанням цифрових обмінів та переходом на електронний документообіг, питання автентичності, цілісності, конфіденційності та безперечності даних набувають надзвичайної ваги. Сучасні інформаційні системи мають містити засоби для надійної ідентифікації користувачів, охорони каналів зв'язку та унеможливлення несанкціонованого доступу. Саме цим потребам відповідає інфраструктура відкритих ключів (Public Key Infrastructure, PKI) - технологічна та організаційна система, що забезпечує керування відкритими та закритими ключами, а також цифровими сертифікатами. Визначення та призначення PKI інфраструктура відкритих ключів (PKI) представляє собою сукупність апаратного та програмного забезпечення, людей, політик і процедур, необхідних для

створення, управління, поширення, використання, збереження та анулювання цифрових сертифікатів. Основна мета PKI - гарантувати довіру до електронної взаємодії між суб'єктами інформаційного середовища. PKI базується на принципах асиметричної криптографії, де кожен користувач отримує унікальну пару ключів: відкритий і закритий. Відкритий ключ може вільно розповсюджуватися, тоді як закритий - повинен зберігатися конфіденційно. Цифровий сертифікат, підписаний акредитованим центром сертифікації (CA), засвідчує, що певний відкритий ключ належить конкретному користувачу чи організації.

Призначення PKI охоплює:

- Автентифікацію особи або пристрою;
- Забезпечення конфіденційності даних, що передаються;
- Перевірку цілісності інформації;
- Надання механізмів цифрового підпису;
- Організацію юридично значимого документообігу;

Управління життєвим циклом ключів та сертифікатів.

PKI є основою для таких технологій, як електронний підпис, SSL/TLS-сертифікати, VPN, захищена електронна пошта (S/MIME), автентифікація в Active Directory та інші засоби гарантування інформаційної безпеки. Основні складові PKI складається з кількох ключових елементів, кожен з яких виконує свою функцію в межах захищеної системи. Розглянемо їх докладніше.

1. Центр сертифікації (CA - Certification Authority) - це надійний орган, який видає, підписує, оновлює та анулює цифрові сертифікати. CA виступає гарантом того, що відкритий ключ, який міститься в сертифікаті, дійсно належить певній особі або пристрою. CA також відповідає за збереження політик сертифікації та ведення журналів усіх операцій, пов’язаних із сертифікатами. Існують: Рівень кореневого CA (Root CA) - найвищий рівень довіри. Його сертифікат

самопідписаний. Проміжні CA (Intermediate CA) - делеговані кореневим центром, для розподілу навантаження та посилення безпеки. Внутрішні корпоративні CA - розгортаються в організаціях для внутрішніх потреб.

2. Центр реєстрації (RA - Registration Authority) є посередником між користувачем та центром сертифікації. RA здійснює ідентифікацію та перевірку особи, що подає заявку на сертифікат. Після підтвердження даних RA передає запит до CA для генерації сертифіката. Це дозволяє розподілити обов’язки та збільшити масштабованість PKI.

3. Сховище сертифікатів (Certificate Repository) це база даних або інша система зберігання, що містить видані сертифікати та списки анульованих сертифікатів (CRL - Certificate Revocation List). Сховище має бути доступним для користувачів та систем, для перевірки статусу сертифікатів. Сховище може бути реалізовано у вигляді: LDAP-каталогу (наприклад, Active Directory), веб-сервера з відкритим доступом до сертифікатів, OCSP - сервісу для перевірки статусу сертифіката в реальному часі.

4. Списки скасованих сертифікатів (CRL - Certificate Revocation Lists) це спеціальні документи, що містять ідентифікатори сертифікатів, анульованих до завершення терміну їхньої дії. Причини анулювання можуть включати компрометацію ключа, звільнення працівника або організаційні зміни. CRL публікуються CA з визначеною періодичністю, згідно з встановленою політикою. Альтернативним рішенням CRL є OCSP(Online Certificate Status Protocol)-протокол, що дозволяє перевірити статус сертифіката в режимі реального часу.

1.4 Системи сертифікації: центри сертифікації (CA), реєстраційні органи (RA), списки відкликаних сертифікатів (CRL), OCSP

Центри сертифікації (Certificate Authority, CA) - це організація, що видає цифрові сертифікати, підтверджуючи зв'язок між відкритим ключем та особистістю суб'єкта. Це дає змогу іншим сторонам вірити підписаним даним, знаючи, що вони надходять від надійного джерела. CA відповідає за перевірку інформації,

наданої заявником, перед видачею сертифіката. Це може включати перевірку доменного імені, організації або особи заявника. Після успішної перевірки CA підписує сертифікат своїм закритим ключем, що дає змогу будь-кому перевірити його справжність за допомогою відкритого ключа. CA також відповідає за управління життєвим циклом сертифікатів, включаючи анулювання та поновлення.У випадку компрометації ключа або інших проблем, CA може скасувати сертифікат, щоб запобігти його подальшому використанню. Реєстраційні органи (RA) Реєстраційний орган (Registration Authority, RA) виступає посередником між заявником і CA. RA відповідає за перевірку особи заявника перед передачею запиту на сертифікат до CA. Це може включати перевірку документів, особисту ідентифікацію або інші способи автентифікації. RA не випускає сертифікати самостійно, але відіграє важливу роль у забезпеченні довіри до процесу видачі сертифікатів. У великих організаціях або децентралізованих системах RA дозволяє масштабувати процес видачі сертифікатів, розподіляючи навантаження з перевірки ідентифікації. Списки скасованих сертифікатів (CRL)Списку анульованих сертифікатів (Certificate Revocation List, CRL) - це перелік сертифікатів, які були анульовані CA до закінчення терміну їх дії. CRL дає змогу сторонам перевіряти, чи є сертифікат дійсним на момент перевірки. CRL публікується CA та регулярно оновлюється. Кожен запис у CRL містить серійний номер анульованого сертифіката, дату анулювання та, зазвичай, причину анулювання. Сторони, які покладаються на сертифікати, повинні регулярно перевіряти CRL, щоб переконатися, що сертифікатне було анульовано. Однак використання CRL має певні обмеження, такі як затримки в оновленні та розмір списку, що може впливати на продуктивність системи. Протокол OCSP (Online Certificate Status Protocol) було розроблено як альтернатива CRL для забезпечення більш оперативної перевірки статусу сертифікатів. OCSP дає змогу клієнтам надсилати запит до OCSP-сервера (відповідача) для перевірки статусу конкретного сертифіката в режимі реального часу. Це забезпечує більш ефективну перевірку, зменшуючи затримки та навантаження на мережу, оскільки клієнт отримує

відповідь лише щодо одного сертифіката, а не завантажує весь список CRL. OCSP широко використовується в сучасних браузерах та інших додатках для забезпечення актуальної інформації про статус сертифікатів. Варто зазначити, що де-які браузери можуть мати різні налаштування щодо використання OCSP, що може впливати на поведінку перевірки сертифікатів.

1.5 Роль PKI у забезпеченні автентифікації, конфіденційності, цілісності даних

Автентифікація: засвідчення особистості PKI забезпечується через електронні сертифікати, котрі видаються довіреними центрами сертифікації (CA). Ці сертифікати засвідчують взаємозв'язок між відкритим ключем та особистістю суб'єкта, дозволяючи сторонам впевнено розпізнавати один одного. Процес автентифікації включає перевірку цифрового сертифіката, підписаного CA, що гарантує, що сертифікат належить заявленому власнику. Це особливо важливо в електронній комерції, онлайн-банкінгу та інших сферах, де необхідно надійно ідентифікувати користувачів або сервіси.

Конфіденційність: захист інформації від несанкціонованого доступу, забезпечується через шифрування даних за допомогою пари відкритого та закритого ключів. Відправник шифрує повідомлення відкритим ключем одержувача, і лише власник відповідного закритого ключа може розшифрувати його. Цей механізм гарантує, що навіть якщо дані будуть перехоплені, вони залишаться недоступними для сторонніх осіб без відповідного закритого ключа. Таким чином, PKI забезпечує захист конфіденційної інформації під час передачі через незахищені мережі.

Цілісність: гарантія незмінності даних цілісність даних означає, що інформація не була змінена або пошкоджена під час передачі. PKI забезпечує цілісність через використання цифрових підписів, які створюються за допомогою хеш-функцій та закритого ключа відправника. Одержувач може перевірити цифровий підпис, використовуючи відкритий ключ відправника, і впевнитися, що дані не були

змінені. Це критично важливо в сферах, де навіть незначні зміни в даних можуть мати серйозні наслідки, таких як фінансові транзакції або медична інформація.

1.6 Нормативно-правова база застосування PKI в Україні та світі

Автентифікація: засвідчення особистості PKI забезпечується крізь електронні сертифікати, котрі видаються надійними центрами сертифікації (CA). Ці сертифікати засвідчують зв'язок між відкритим ключем та ідентичністю суб'єкта, дозволяючи сторонам впевнено розпізнавати один одного. Процес автентифікації включає перевірку цифрового сертифіката, підписаного CA, що гарантує, що сертифікат належить заявленому власнику. Це надзвичайно важливо в електронній комерції, онлайн-банкінгу та інших галузях, де необхідно надійно розпізнавати користувачів чи сервіси.

Конфіденційність: захист інформації від несанкціонованого доступу. Таємність забезпечується за допомогою шифрування даних за допомогою пари відкритого та закритого ключів. Відправник шифрує повідомлення відкритим ключем одержувача, і лише власник відповідного закритого ключа може розшифрувати його. Цей механізм гарантує, що навіть якщо дані будуть перехоплені, вони залишаться недоступними для сторонніх осіб без відповідного закритого ключа. Таким чином, PKI забезпечує захист конфіденційної інформації під час передачі через незахищені мережі. **Цілісність:** гарантія незмінності даних Цілісність даних означає, що інформація не була змінена або пошкоджена під час передачі. PKI забезпечує цілісність через використання цифрових підписів, які створюються за допомогою хеш-функцій та закритого ключа відправника. Отримувач може перевірити цифровий підпис, використовуючи відкритий ключ відправника, й переконатися, що дані не були змінені. Це надзвичайно важливо в сферах, де навіть невеличкі зміни в даних можуть мати серйозні наслідки, як-от фінансові операції чи медична інформація.

1.7 Огляд сучасних платформ і рішень для реалізації PKI (OpenSSL, Microsoft CA, EJBCA)

Огляд сучасних платформ та розв'язків для впровадження PKI (OpenSSL, Microsoft CA, EJBCA тощо). Інфраструктура відкритих ключів (PKI) є основою цифрової безпеки, забезпечуючи автентифікацію, конфіденційність та цілісність відомостей в нашому повсякденному цифровому світі. Ці три аспекти є ключовими для захисту інформації та довіри в електронних комунікаціях. OpenSSL - це потужна бібліотека з відкритим кодом, яка реалізує протоколи SSL та TLS, а також надає інструменти для створення та управління сертифікатами X.509. Вона широко використовується для налаштування власних центрів сертифікації (CA) та управління ключами. Основні можливості: Генерація пар ключів та сертифікатів. Створення запитів на підпис сертифікатів (CSR). Підпис сертифікатів та управління їх життєвим циклом. Підтримка списків відкликаних сертифікатів (CRL) та протоколу OCSP. OpenSSL є багатоплатформним рішенням, що підтримує Windows, Linux, macOS та інші операційні системи. Воно ідеально підходить для організацій, які бажають мати повний контроль над своєю PKI-інфраструктурою. Microsoft Active Directory Certificate Services (AD CS) Microsoft AD CS — це роль Windows Server, яка дозволяє створювати та керувати інфраструктурою відкритих ключів в організаціях, інтегруючись з Active Directory.

Основні можливості:

- Випуск та управління цифровими сертифікатами для користувачів, комп'ютерів та служб.
- Підтримка шаблонів сертифікатів для автоматизації процесів.
- Інтеграція з Group Policy для автоматичного розповсюдження сертифікатів.
- Підтримка протоколів SCEP, NDES та інших.
- AD CS забезпечує гнучке та масштабоване рішення для організацій, які використовують екосистему Microsoft.

- EJBCA (Enterprise Java Beans Certificate Authority) — це потужне рішення з відкритим кодом для створення та управління PKI-інфраструктурою. Воно підтримує широкий спектр протоколів та стандартів, що робить його універсальним вибором для різних сценаріїв.

Ключові функції:

- Підтримка протоколів SCEP, CMP, EST, ACME, OCSP, REST API.
- Можливість розгортання в контейнерах Docker, Kubernetes та хмарних середовищах.
- Гнучке управління сертифікатами, включаючи підтримку різних профілів та політик.
- Підтримка апаратних модулів безпеки (HSM) для зберігання ключів. EJBCA підходить як для малих організацій, так і для великих підприємств, які потребують масштабованого та надійного PKI-рішення.

Порівняльна таблиця

Платформа	**Тип**	**Основні переваги**	**Підтримка протоколів**	**Підтримка HSM**	**Інтеграція з AD**
OpenSSL	Відкритий код	Гнучкість, контроль	OCSP,CRL	Так	Обмежена
Microsoft AD CS	Пропрієтарне	Інтеграці з Windows	SCEP,NDES	Так	Повна
EJBCA	Відкритий код	Масштабність, підтримка стандартів	SCEP,CMP,EST,ACME,OCSP	Так	Можлива

РОЗДІЛ 2 АНАЛІЗ І ЗАСТОСУВАННЯ PKI В РЕАЛЬНИХ УМОВАХ

2.1 Аналіз вимог до безпеки IT-систем у організаціях

У нинішньому цифровому середовищі безпека інформаційних технологій (IT) є критично важливою для організацій будь-якої галузі. Зростання кількості кіберзагроз, розвиток хмарних технологій, мобільних пристроїв та Інтернету речей (IoT) створюють нові виклики для захисту конфіденційної інформації та забезпечення цілісності систем. Інфраструктура відкритих ключів (PKI) є одним із ключових інструментів для досягнення високого рівня безпеки в IT-системах.

Основні вимоги до безпеки IT-систем згідно з моделлю CIA (Confidentiality, Integrity, Availability), основними вимогами до безпеки IT-систем є:

- **Конфіденційність (Confidentiality):** забезпечення доступу до інформації лише авторизованим користувачам.
- **Цілісність (Integrity):** гарантія того, що дані не були змінені або пошкоджені без відповідного дозволу.
- **Доступність (Availability):** забезпечення своєчасного та безперебійного доступу до інформації та ресурсів для авторизованих користувачів.

Додатково, сучасні IT-системи повинні враховувати: Автентифікацію: перевірку особистості користувачів або пристроїв перед наданням доступу до системи. Авторизацію: надання користувачам прав доступу відповідно до їхніх ролей та обов'язків. Відстежуваність (Auditability): здатність фіксувати та аналізувати дії користувачів для виявлення порушень безпеки. Роль PKI у забезпеченні вимог безпекиPKI забезпечує механізми для досягнення вищезазначених вимог: Конфіденційність: через використання шифрування даних за допомогою публічних та приватних ключів. Цілісність: забезпечується за допомогою цифрових підписів, які дозволяють виявити будь-які несанкціоновані зміни в даних. Автентифікація: цифрові сертифікати дозволяють перевірити особистість користувачів та пристроїв. Авторизація: на основі сертифікатів можна

визначати рівень доступу користувачів до ресурсів. Відстежуваність: журнали аудиту та сертифікати дозволяють фіксувати дії користувачів для подальшого аналізу. Вимоги до впровадження PKI в організаціях Для ефективного впровадження PKI в організації необхідно враховувати наступні аспекти: Планування та дизайн: визначення структури PKI, включаючи вибір типу сертифікаційного центру (наприклад, ієрархічного або сіткового), політик сертифікації та процедур управління ключами. Управління сертифікатами: створення процесів для видачі, відкликання та оновлення сертифікатів, а також моніторинг їхнього стану. Безпека приватних ключів: забезпечення захисту приватних ключів від несанкціонованого доступу, включаючи використання апаратних засобів безпеки (HSM). Інтеграція з існуючими системами: забезпечення сумісності PKI з існуючими IT-системами та додатками організації. Навчання персоналу: підготовка співробітників до роботи з PKI, включаючи розуміння принципів його роботи та процедур безпеки.

2.2 Приклади використання PKI в корпоративному середовищі (бізнес, освіта, медицина)

Інфраструктура відкритих ключів (PKI) набула широкого поширення в багатьох сферах діяльності, зокрема у бізнесі, освіті та медицині. У кожній із цих галузей PKI виконує критичну функцію захисту даних, забезпечення автентичності користувачів, електронного підпису документів і шифрування комунікацій. Ефективне використання PKI дає змогу організаціям дотримуватись вимог безпеки, знижувати ризики витоку конфіденційної інформації та відповідати нормативно-правовим вимогам.

1. PKI у бізнесі

1.1 Безпечний документообіг у корпоративному середовищі електронний документообіг є невіддільною частиною щоденних бізнес-процесів.

Завдяки PKI компанії можуть:

- Підписувати електронні документи цифровим підписом, що надає їм юридичної сили (згідно з eIDAS у ЄС чи законом «Про електронні довірчі послуги» в Україні).
- Використовувати цифрові сертифікати для гарантування автентичності відправника та цілісності змісту документів.
- Автоматизувати вхід/вихід документів за допомогою внутрішніх порталів з підтримкою PKI.

1.2 Контроль доступу до внутрішніх ресурсів PKI використовується для автентифікації працівників у внутрішній мережі компанії.

Наприклад:

- VPN-доступ з двофакторною автентифікацією на основі сертифікатів.
- Вхід до корпоративної пошти або CRM-систем через смарт-карти або токени з сертифікатом користувача.
- Підпис файлів у внутрішньому архіві компанії або системі контролю версій (наприклад, Git) за допомогою PKI.

1.3 Підписання програмного забезпечення компанії, які розробляють ПЗ, використовують PKI для підписання коду та інсталяційних файлів, щоб користувачі були впевнені в його справжності:

- Microsoft Authenticode чи Java Code Signing.
- Уникнення повідомлень про "невідоме джерело" під час встановлення ПЗ.

1.4 B2B-захист комунікацій у випадках взаємодії між компаніями (B2B), особливо у фінансовому та юридичному секторах, PKI забезпечує захищене надсилання конфіденційної інформації:

- Шифрування email-листування між партнерами.

- PKI-захист веб-інтерфейсів для ділових клієнтів (SSL/TLS з двосторонньою автентифікацією).

2. PKI в освіті

2.1 Ідентифікація викладачів і студентів Університети та школи впроваджують системи автентифікації користувачів на основі цифрових сертифікатів:

- Вхід до навчальних платформ (Moodle, Google Classroom тощо) через сертифікат.
- Облік відвідувань і збереження результатів навчання на захищених платформах.

2.2 Безпечна передача інформаціїНавчальні заклади обробляють значний обсяг персональних даних (успішність, медичні довідки, реєстраційні документи тощо), які потребують надійного захисту:

- Шифрування документів перед передачею або архівуванням.
- Підписання цифровим підписом дипломів, сертифікатів, залікових книжок (електронних).

2.3 PKI у дистанційному навчанні з розвитком онлайн-освіти PKI використовується для:

- Гарантування ідентичності студентів під час здачі іспитів онлайн.
- Підписання результатів тестування викладачем із цифровим підписом.
- Захищене підключення до відеоконференцій через TLS-сертифікати.

3. PKI в медицині

3.1 Захист медичних даних медичні організації працюють із надзвичайно чутливою інформацією.

Використання PKI дає можливість:

- Шифрувати електронні медичні картки (ЕМК) пацієнтів.
- Обмежити доступ до ЕМК лише авторизованим медпрацівникам (через смарт-карти).
- Підписувати результати аналізів, рецепти, епікризи цифровим підписом лікаря.

3.2 Телекомунікації в охороні здоров'я PKI використовується для:

- Захищеного обміну інформацією між лікарнями, лабораторіями, страховими компаніями.
- Підключення до інформаційних медичних систем (MIS) через TLS/SSL.
- Верифікації пацієнтів під час телемедичних консультацій.

3.3 Виконання нормативних вимог у країнах ЄС, США та Україні існують чіткі вимоги до обробки персональних медичних даних (HIPAA, GDPR, Закон України "Про захист персональних даних").

PKI допомагає медичним закладам:

Відповідати цим вимогам завдяки функціям шифрування та автентифікації. Зберігати правовий статус електронних документів.

2.3 Налаштування захищеного електронного документообігу за допомогою PKI

У сучасному цифровому середовищі електронний документообіг (ЕДО) став основним способом обміну офіційними документами в бізнесі, державному секторі, медицині, освіті та багатьох інших сферах. Проте з переходом до без паперового обміну виникає потреба в надійному механізмі автентифікації, захисту цілісності та юридичного підтвердження документів. Інфраструктура відкритих ключів (PKI) є найбільш ефективним засобом забезпечення захищеного ЕДО, оскільки дозволяє застосовувати електронні підписи, шифрування та сертифікацію автентичності.

Основні принципи захищеного електронного документообігу захищений ЕДО передбачає виконання наступних вимог:

- **Автентичність** – підтвердження особи, яка створила або підписала документ.
- **Цілісність** – гарантія, що зміст документа не змінено після підпису.
- **Конфіденційність** – забезпечення, що інформація доступна лише уповноваженим особам.
- **Незаперечність** – підтвердження факту створення чи підписання документа визначеною особою. Всі ці функції досягаються через механізми PKI, зокрема за допомогою **електронного цифрового підпису (ЕЦП)** або **кваліфікованого електронного підпису (КЕП)**, а також шляхом використання сертифікатів X.509.

Ключові компоненти PKI для ЕДО

- **Центр сертифікації (CA):** Видає цифрові сертифікати користувачам та організаціям. У контексті ЕДО саме CA підтверджує, що особа, яка підписує документ, є тим, за кого себе видає.
- **Цифрові сертифікати:** Вони містять публічний ключ, інформацію про власника і підписані CA. У контексті ЕДО вони використовуються для: Підписання документів. Шифрування документів. Автентифікації користувачів у системах документообігу.
- **Програмне забезпечення для ЕЦП:** Найпоширеніші рішення: **Дія.Підпис**, **КЕП від АЦСК України**, **OpenSSL**, **Cryptoserver**, **ІІТ Користувач ЦСК**. Вони забезпечують накладання і перевірку підписів, шифрування документів.
- **Системи електронного документообігу**: До них належать: **M.E.Doc**, **Вчасно**, **СЕДО**, **Paperless**, **Docflow**, **SharePoint**, **1С:Документообіг** тощо.

Вони інтегруються з PKI для автоматизації процесів і дотримання вимог безпеки.

Етапи налаштування захищеного ЕДО за допомогою PKI

- Етап 1. **Аналіз потреб організації** Визначення типів документів, що будуть підписуватись. Ідентифікація користувачів, які матимуть право підпису. Визначення рівня безпеки (чи потрібен лише ЕЦП, чи КЕП, чи додаткове шифрування).
- Етап 2. **Отримання цифрових сертифікатів** Звернення до **акредитованого центру сертифікації ключів (АЦСК)**. Встановлення сертифікатів на робочі станції або сервери. Налаштування зберігання закритих ключів: токени, смарт-карти, HSM (апаратні модулі).
- Етап 3. **Інтеграція PKI в систему документообігу** Підключення модулів цифрового підпису до СЕД/CRM/ERP. Налаштування політик підпису (наприклад, хто має право підписувати певні типи документів). Реалізація журналів підписів і перевірки сертифікатів (через OCSP чи CRL).
- Етап 4. **Навчання користувачів** Ознайомлення з процедурами підпису, перевірки, відкликання сертифікатів. Інструкції для користування ПЗ. Пояснення юридичної сили електронного підпису.
- Етап 5. **Підтримка і аудит** Регулярне оновлення сертифікатів. Перевірка наявності сертифікатів у списках відкликаних (CRL). Збереження архівів підписаних документів відповідно до законодавчих вимог.

Практичні приклади:

- **Бізнес** у банках документи між відділеннями та центральним офісом підписуються ЕЦП. Контракти з партнерами укладаються онлайн з використанням КЕП, що прискорює бізнес-процеси.

- **Державні установи** Портал e-Data, Дія, ЄДЕБО використовують ЕЦП для підписання звітності та міжвідомчого обміну.
- **Медицина**: Лікарі підписують електронні рецепти, направлення, висновки з використанням КЕП. Електронна медична картка пацієнта шифрується і підписується для передачі між клініками. Переваги використання PKI для ЕДО
- **Зниження витрат**: немає потреби друкувати, зберігати і пересилати паперові документи.
- **Прискорення процесів**: документ обробляється за хвилини.
- **Юридична сила**: підписані документи визнаються судами та регуляторами.
- **Контроль доступу**: тільки авторизовані особи можуть створювати/підписувати документи.
- **Інтеграція з іншими системами**: CRM, ERP, бухгалтерські програми.

Недоліки та виклики:

- Складність впровадження: потребує технічної підготовки.
- Необхідність навчання персоналу.
- Витрати на сертифікати та апаратні ключі.
- Регулярна підтримка сертифікаційної інфраструктури.

2.4 Використання цифрових сертифікатів для автентифікації користувачів і пристроїв

У контексті зростання цифрових загроз і масштабної діджиталізації автентифікація стає критично важливою функцією в системах інформаційної безпеки. Просте введення логіну і пароля вже не забезпечує достатній рівень захисту від несанкціонованого доступу, фішингових атак чи перехоплення даних. Цифрові сертифікати, як ключовий компонент інфраструктури відкритих ключів

(PKI), надають потужний механізм для сильної автентифікації користувачів та пристроїв. Основи цифрової автентифікації - це процес перевірки особи або об'єкта, який намагається отримати доступ до системи або ресурсу. У моделі PKI для цього використовується пара ключів: приватний (який зберігається у користувача) та публічний (який міститься у цифровому сертифікаті, підписаному центром сертифікації – CA). Успішна перевірка сертифіката дозволяє системі впевнено ідентифікувати користувача або пристрій, що забезпечує вищий рівень безпеки порівняно з традиційними методами.

Цифрові сертифікати: принцип роботи

Цифровий сертифікат – це файл у форматі X.509, що містить:

Ідентифікаційні дані суб’єкта (ПІБ, організація, email), публічний ключ користувача або пристрою дані про сертифікаційний центр, який видав сертифікат термін дії цифровий підпис CA для перевірки автентичності коли користувач намагається автентифікуватися, його сертифікат перевіряється за такими параметрами: Дійсність (термін дії, не відкликаний CRL/OCSP) довіра до CA цілісність підпису типи автентифікації за допомогою сертифікатів

1. **Клієнтська автентифікація (Client Authentication)**Користувач надає цифровий сертифікат у відповідь на запит сервера. Сторона, яка перевіряє, має доступ до довіреного списку CA та перевіряє підпис сертифіката. **Використовується в:** VPN-доступі Веб-додатках (HTTPS із клієнтською автентифікацією) Доступі до корпоративних систем (SharePoint, Citrix тощо)

2. **Автентифікація пристроїв (Machine Authentication)** Комп'ютери, принтери, сервери та інші пристрої також можуть мати цифрові сертифікати для взаємної аутентифікації в мережі. **Приклади:** 802.1X (мережевий доступ через сертифікати) IPsec VPN для пристроїв SSL/TLS-комунікації між серверами

3. **Автентифікація в Active Directory через Smart Card Logon**Сертифікат користувача розміщено на смарт-карті або токені. Після введення PIN-коду сертифікат використовується для входу в домен Windows.

Переваги: Неможливість фішингу і підбору пароля

Інфраструктура для автентифікації через сертифікати

1. **Центри сертифікації (CA)** Створюють та підписують сертифікати. У великих організаціях можливе використання власних внутрішніх CA (наприклад, Microsoft AD CS).

2. **Реєстраційні органи (RA)**Проводять перевірку особи перед випуском сертифіката.

3. **Сховища сертифікатів** Локальні (у браузері, системному сховищі Windows/Linux/macOS) Апаратні (токени, смарт-карти, HSM) У хмарі (Cloud HSM, Azure Key Vault, AWS Certificate Manager)

Приклади використання в організаціях

1. **Банківський сектор:** Співробітники отримують токени з сертифікатами для автентифікації в банківських платформах Обмін зашифрованими повідомленнями з клієнтами (наприклад, SWIFT)

2. **Освітні заклади:** Сертифікати використовуються для безпечного входу до електронних журналів, систем дистанційного навчання верифікація студентських робіт (електронні підписи)

3. **Медицина:** Лікарі автентифікуються в електронних медичних системах підпис електронних рецептів, історій хвороб переваги використання сертифікатів для автентифікації.

Перевага

- **Висока безпека:** складність підробки чи перехоплення ключа
- **Юридична сила:** у разі використання КЕП
- **Зручність при інтеграції:** працює з більшістю корпоративних платформ
- **Масштабованість:** можливість централізованого керування ключами

- **Можливість двофакторної автентифікації:** комбінування сертифікатів із PIN, біометрією

Виклики та недоліки

- **Необхідність управління сертифікатами** (видача, відкликання, продовження)
- **Початкові витрати на інфраструктуру PKI**
- **Навчання персоналу**
- **Можливість втрати приватного ключа** (наприклад, якщо токен зламався або втрачено): Актуальні платформи для впровадження платформ, опис **Microsoft Active Directory Certificate Services (AD CS),** вбудоване рішення для підприємств **OpenSSL,** безкоштовне та широко підтримуване рішення **EJBCA,** потужна Java-базована система CA**XCA** GUI для управління сертифікатами **AWS Certificate Manager / Azure Key Vault,** хмарні сервіси PKI .

2.5 Порівняльний аналіз ефективності PKI-рішень у різних умовах

Інфраструктура відкритих ключів (PKI) є важливою складовою сучасних систем кібербезпеки, забезпечуючи довіру, автентифікацію, конфіденційність та цілісність у цифровому середовищі. У процесі впровадження PKI в організаціях різного масштабу та галузевої специфіки постає необхідність вибору оптимального рішення, яке буде відповідати технічним, економічним і юридичним вимогам. У цьому підрозділі проведено порівняльний аналіз популярних PKI-рішень (OpenSSL, Microsoft AD CS, EJBCA, Let's Encrypt, AWS Certificate Manager та ін.) з урахуванням різних сценаріїв їх застосування: для малого бізнесу, великих корпоративних структур, державного сектору, хмарних інфраструктур. Ключові критерії оцінки ефективності PKI-рішень

Для об’єктивного порівняння використовуються такі критерії:

- **Функціональність**: підтримка стандартів, алгоритмів, масштабованість, наявність OCSP/CRL.
- **Простота впровадження та адміністрування**: інтерфейс, документація, навчання персоналу.
- **Безпека**: підтримка HSM, захист приватних ключів, аудит.
- **Вартість**: ліцензії, підтримка, інфраструктурні витрати.
- **Інтеграція**: сумісність із іншими системами, ОС, протоколами (LDAP, Active Directory, S/MIME тощо).
- **Гнучкість налаштування та автоматизація**: API, CLI, підтримка скриптів, DevOps.
- **Підтримка та оновлення**: спільнота, офіційна технічна підтримка.

Огляд та порівняння поширених рішень

Платформа	Тип	Переваги	Обмеження	Рекомендоване застосування
OpenSSL	Open-source CLI-інструмент	Безкоштовне, кросплатформне, підтримує всі сучасні алгоритми	Відсутній GUI, складність адміністрування	Скриптові PKI, лабораторії, DevOps-середовища
Microsoft AD CS	Вбудоване у Windows Server	Повна інтеграція з Active Directory, GUI, шаблони сертифікатів	Працює лише в середовищі Windows, складне масштабування	Внутрішні корпоративні мережі, домени
EJBCA	Java-базоване, open-source CA	Потужна функціональність, підтримка HSM, Web GUI, OCSP, REST API	Вимогливе до ресурсів, складна початкова конфігурація	Високонавантажені підприємства, держустанови

Let's Encrypt	Безкоштовна хмарна CA	Автоматизоване видавання TLS-сертифікатів, підтримка ACME	Лише TLS-сертифікати, обмежений контроль	Сайти малого/середнього бізнесу, SaaS
AWS Certificate Manager	Хмарне рішення	Інтеграція з AWS-сервісами, автооновлення сертифікатів	Обмежено використанням в екосистемі AWS	Хмарні додатки, DevOps, e-commerce
Venafi, DigiCert	Комерційні CA	Підтримка корпоративного масштабу, SLA, аналітика, HSM	Висока вартість	Банки, фармацевтика, телекомунікації

Порівняння ефективності в залежності від умов впровадження

1. **Малі та середні підприємства (SMB)**

Потреби: Мінімальні витрати, просте адміністрування, сертифікати для вебсайтів та VPN.

Рекомендовані рішення:

- **Let's Encrypt** – автоматичне отримання TLS-сертифікатів для вебресурсів
- **OpenSSL** – ручне генерування сертифікатів для внутрішнього використання

Аналіз: Let's Encrypt повністю покриває потреби для публічного TLS. Для внутрішніх сервісів краще використати OpenSSL або XCA з обмеженим числом сертифікатів.

2. **Корпоративне середовище (великі організації)**

Потреби: Автентифікація пристроїв і користувачів VPN, Wi-Fi, доступ до серверів, масштабованість і централізоване керування.

Рекомендовані рішення:

- **Microsoft AD CS** – для організацій з Active Directory
- **EJBCA** – для гетерогенних середовищ з Linux/Windows, складних сценаріїв

Аналіз: AD CS оптимізований для Windows-середовища, підтримує групову політику. EJBCA є потужним, але вимагає кваліфікованого персоналу.

3. **Державний сектор**

Потреби: Підтримка КЕП (кваліфікованих електронних підписів), відповідність національним нормативам, високий рівень безпеки.

Рекомендовані рішення:

- **EJBCA** з інтеграцією HSM
- **Національні CA** (український ДП «Дія», АЦСК ІДД, тощо)

Аналіз: У держсекторі критичною є відповідність стандартам (наприклад, DSTU, ETSI), тому доцільно використовувати сертифікацію у національних акредитованих центрах або адаптовані EJBCA-рішення з сертифікованим HSM.

4. **Хмарні середовища**

Потреби: Автоматизація, CI/CD-процеси, динамічне оновлення сертифікатів
Рекомендовані рішення:

- **AWS Certificate Manager**
- **Azure Key Vault**
- **Let's Encrypt з ACME-клієнтами**

Аналіз: Хмарні CA дозволяють автоматично видавати та відкликати сертифікати для сервісів (наприклад, ELB, CloudFront), що ідеально підходить для DevOps.

Рівень безпеки та управління ключами

Рішення	**Захист приватного ключа**	**Підтримка HSM**	**Аудит**
OpenSSL	Низький (локальні ключі)	Можлива інтеграція	Відсутній
AD CS	Середній/високий	Так (nCipher, Thales)	Вбудований у Windows
EJBCA	Високий	Повна підтримка	Повноцінний журнал
Let's Encrypt	Обмежений	Ні	Немає аудиту
AWS Certificate Manager	Високий (CloudHSM)	Так	Вбудований в AWS CloudTrail

2.6 Визначення типових проблем при впровадженні PKI та методів їх усунення

Інфраструктура відкритих ключів (PKI) є потужним інструментом для забезпечення інформаційної безпеки, однак її впровадження часто супроводжується низкою технічних, організаційних і юридичних проблем. Ці складнощі можуть суттєво вплинути на ефективність системи, привести до втрат у функціонуванні або безпеці. У цьому підрозділі розглянемо основні виклики, які виникають під час проектування, розгортання та експлуатації PKI, а також методи їх подолання.

Основні складнощі при впровадженні PKI

Рекомендовані дії:

- Ретельне попереднє проектування з оглядом на перспективи масштабування та потреби користувачів.
- Впровадження багаторівневої моделі з основним та підпорядкованими центрами сертифікації.
- Орієнтація на міжнародні стандарти (наприклад, RFC 5280, ETSI) якосновудляреалізації.

1.Управління життєвим циклом сертифікатів

Процедури видачі, оновлення та відкликання сертифікатів вимагають точного контролю. Затримка у відкликанні або закінчення терміну дії сертифіката може викликати проблеми у функціонуванні сервісів.

Що допоможе:

- Автоматизація з використанням сучасних PKI-платформ.
- Впровадження протоколів негайної перевірки статусу (OCSP).
- Регулярний аудит активних сертифікатів та систем моніторингу.

2.Захист приватних ключів

Компрометація закритого ключа призводить до втрати довіри до PKI. Проблема часто полягає у неналежному зберіганні або низькому рівні контролю доступу.

Підхід до вирішення:

- Використання апаратних пристроїв безпеки (HSM) для створення та зберігання ключів.
- Обмеження доступу до ключів лише уповноваженим особам.
- Шифрування ключів та аудит дій, пов’язаних з їх використанням.

4.Нестача досвідченого персоналу

Робота з PKI вимагає специфічних знань, яких не завжди вистачає внутрішньому IT-персоналу організації.

Оптимальні рішення:

- Навчання команди через професійні курси чи сертифікаційні програми.
- Залучення зовнішніх експертів чи підрядників.
- Вибір зручних для користувача рішень з інтуїтивно зрозумілим інтерфейсом.

5.Складнощі інтеграції з наявними IT-системами

PKI повинна без проблем працювати з Active Directory, VPN, поштовими сервісами та іншими елементами IT-інфраструктури.

Практичні кроки:

- Передбачити потреби в інтеграції ще на етапі проектування.
- Віддати перевагу продуктам, що підтримують відкриті протоколи та стандарти.
- Провести тестування інтеграції у відокремленому середовищі до впровадження в робочу систему.

6.Різноманіття стандартів

- Існує багато різноманітних нормативних актів, як міжнародних, так і локальних, що може ускладнити впровадження єдиної системи.
- Що допоможе уникнути помилок: Вивчення вимог українського законодавства, зокрема Закону України «Про електронні довірчі послуги».
- Дотримання загально прийнятих міжнародних норм (ISO, RFC, ETSI). Створення гнучкої архітектури, здатної адаптуватися до різних вимог.

7.Значні витрати на впровадження та обслуговування

Придбання обладнання, ліцензійне програмне забезпечення та навчання персоналу вимагають значних фінансових ресурсів.

Можливі підходи:

- Проведення оцінки витрат до старту проекту.
- Використання рішень з відкритим вихідним кодом там, де це дозволяється вимогами безпеки.

- Поступове впровадження PKI – від малого до більшого.
- Типові технічні проблеми, неправильні налаштування центру сертифікації(терміни дії сертифікатів, політики, рівень шифрування).
- Несумісність форматів ключів та сертифікатів між різними платформами.
- Відсутність резервних копій або процедур аварійного відновлення. Нестача централізованого контролю за станом безпеки системи.
- Організаційні бар'єри, відсутність чітко прописаних процедур видачі та відкликання сертифікатів.
- Недостатня координація між різними відділами.
- Невизначені правила щодо використання електронних підписів та захисту ключів.
- Недостатня підтримка з боку керівництва.
- Юридичні проблеми, невідповідність функціоналу PKI вимогам законодавства.
- Неправильна сертифікація або її відсутність, що робить електронні підписи юридично незначущими.
- Відсутність контролю відповідності нормативам у сфері кібербезпеки.

Рекомендовані заходи для підвищення ефективності PKI:

- **Стратегічне планування:** Визначення цілей впровадження та оцінка потенційних ризиків. Розробка адаптивної архітектури з урахуванням безпеки та масштабованості.
- **Регламентація:** Розробка політику правління сертифікатами. Призначення відповідальних за ключові процеси.

- **Технічні захисні механізми:** Впровадження HSM, забезпечення оновлень ПЗ та регулярного резервного копіювання. Розвиток компетенцій: Навчання команди, проведення тренінгів, ознайомлення з актуальними стандартами.
- **Автоматизація та інтеграція:** Впровадження PKI-рішень, які легко інтегруються з наявною інфраструктурою. Налаштування систем моніторингу для оперативного реагування на інциденти.

РОЗДІЛ 3 РОЗРОБКА АРХІТЕКТУРИ PKI ДЛЯ ОРГАНІЗАЦІЇ ТА РЕКОМЕНДАЦІЇ

3.1 Проектування архітектури PKI відповідно до потреб організації

Проектування інфраструктури відкритих ключів (PKI) — це комплексний процес, що вимагає детального аналізу бізнес-вимог організації, рівня безпеки, існуючої IT-інфраструктури та майбутніх потреб. Метою проектування є створення надійної системи управління цифровими сертифікатами, яка гарантуватиме автентифікацію, конфіденційність і цілісність даних. Аналіз потреб організації Перший етап проектування PKI — визначення основних вимог організації: Які типи користувачів і пристроїв будуть залучені? Які сервіси і додатки мають бути захищені? Чи потрібно інтегрувати PKI з наявними системами управління ідентифікацією (LDAP, Active Directory)? Який рівень безпеки очікується? Які нормативні вимоги треба виконати? Відповіді на ці питання визначають масштаби і складність архітектури.

Основні компоненти архітектури PKI Ключовими складовими є:

- **Кореневий центр сертифікації (Root CA)** - найвищий рівень довіри, який підписує сертифікати підлеглих центрів. Він повинен бути максимально захищений, часто працює в автономному режимі.
- **Підлеглі центри сертифікації (Subordinate CA)** - видають сертифікати користувачам і сервісам, працюють у безпосередньому контакті з клієнтами.
- **Реєстраційні органи (RA)** - відповідають за верифікацію особи користувача, який подає заявку на сертифікат, перевіряють документи і підтверджують право на отримання сертифіката.
- **Списки відкликаних сертифікатів (CRL)** і **служби перевірки статусу сертифікатів (OCSP)** - забезпечують механізми перевірки дійсності сертифікатів.

- **Репозитарій сертифікатів** - бази даних або каталоги, де зберігаються та публікуються сертифікати та їх статус.

Вибір типу архітектури в залежності від організаційних потреб вибирають структуру PKI:

Однорівнева (Single-tier) - Root CA без підлеглих, підходить для невеликих організацій з обмеженим числом користувачів. Перевага - простота, недолік - менша гнучкість та безпека.

Дворівнева або багаторівнева (Hierarchical multi-tier) - Root CA, який підписує підлеглі CA, а ті вже видають сертифікати кінцевим користувачам. Це підвищує безпеку, оскільки Root CA може бути в офлайн режимі, а робочі CA - в мережі. Визначення політик і процедур проектування включає розробку політик використання PKI (Certificate Policy - CP) і процедур (Certification Practice Statement - CPS). Вони визначають правила: Видачі, оновлення і відкликання сертифікатів. Захисту приватних ключів. Верифікації особистості. Вимоги до апаратного і програмного забезпечення. Ці документи слугують юридичною основою для роботи PKI. Інтеграція з існуючими системами PKI повинна безперешкодно працювати з існуючими службами ідентифікації, наприклад, Active Directory, LDAP, SSO. Це дозволяє автоматизувати процес видачі сертифікатів і спрощує керування користувачами. Врахування масштабованості і гнучкості Система має бути розроблена з урахуванням можливого розширення кількості користувачів, появи нових сервісів, зміни політик безпеки. Гнучкість архітектури важлива для швидкої адаптації до нових викликів.

3.2 Вибір засобів реалізації: програмне та апаратне забезпечення

Реалізація інфраструктури відкритих ключів (PKI) в організації потребує ретельного вибору як програмних, так і апаратних засобів. Від правильного підбору залежить надійність, безпека та ефективність всієї системи. У цьому підрозділі розглянемо основні критерії та приклади популярних рішень, а також рекомендації щодо їх інтеграції. Програмне забезпечення для PKI програмне

забезпечення PKI - це основа для управління цифровими сертифікатами, їх генерації, видачі, відкликання і перевірки. Сучасний ринок пропонує широкий спектр рішень - від відкритих безкоштовних до комерційних продуктів зі складним функціоналом. **OpenSSL** - найпоширеніший відкритий інструмент для роботи з криптографією, що підтримує стандарти X.509, PKCS і багато інших. OpenSSL включає бібліотеки для генерації ключів, створення сертифікатів і їх перевірки, а також серверні та клієнтські інструменти. Він використовується у багатьох системах завдяки своїй гнучкості та відкритості. Однак для побудови повноцінного PKI з централізованим управлінням часто потрібні додаткові інструменти або розробка власних рішень на основі OpenSSL. **Microsoft Certificate Services (Microsoft CA)** - інтегроване рішення, що входить до складу операційних систем Windows Server. Microsoft CA тісно взаємодіє з Active Directory, що дозволяє автоматизувати управління сертифікатами в корпоративному середовищі Windows. Це рішення підходить для організацій, що вже використовують Windows Server та хочуть швидко впровадити PKI з підтримкою стандартних протоколів. **EJBCA (Enterprise Java Beans Certificate Authority)** - це потужна платформа з відкритим кодом для створення корпоративних PKI-систем. EJBCA підтримує всі основні функції CA, включаючи видачу сертифікатів, відкликання, перевірку статусу через OCSP, інтеграцію з LDAP, різні методи автентифікації користувачів. Вона підходить для складних і масштабних проектів, де потрібна висока гнучкість і розширюваність. **Комерційні продукти** від компаній, таких як DigiCert, Entrust, Sectigo, забезпечують готові рішення зі службами підтримки, регулярними оновленнями, сертифікацією за міжнародними стандартами та можливістю інтеграції з різними платформами. Вони зазвичай мають простіший інтерфейс для користувача і додаткові функції, такі як керування життєвим циклом сертифікатів, аналітика та звітність. Апаратне забезпечення: захист приватних ключів безпека приватних ключів є найважливішим аспектом PKI. Компрометація ключа призводить до втрати довіри до всієї інфраструктури. Тому для зберігання і роботи з ключами використовують спеціальні апаратні засоби - **апаратні модулі безпеки (HSM)**.

HSM - це пристрої, які забезпечують генерацію, зберігання та криптографічні операції з приватними ключами у фізично захищеному середовищі. Вони запобігають витоку ключів навіть у разі атаки на сервер, оскільки ключі ніколи не покидають модуль у відкритому вигляді. HSM мають сертифікації відповідно до стандартів FIPS 140-2 або Common Criteria, що підтверджує їх надійність. Використання HSM є обов'язковим у критично важливих системах, наприклад у банках, державних установах, де потрібен високий рівень безпеки. Вони можуть працювати як у вигляді зовнішніх пристроїв, підключених по USB або мережі, так і у вигляді внутрішніх карт розширення. Крім захисту ключів, HSM прискорюють криптографічні операції, що особливо важливо у масштабних системах з високим навантаженням. Інтеграція та сумісність для ефективної роботи PKI необхідно, щоб обране програмне і апаратне забезпечення було сумісним з існуючими системами організації - операційними системами, системами управління ідентифікацією (IAM), мережевими сервісами, браузерами та додатками. Підтримка стандартів X.509, PKCS #11, CMP, SCEP, OCSP і LDAP є обов'язковою умовою для інтеграції. Це забезпечує можливість безперешкодної взаємодії між компонентами PKI і різними сервісами, зокрема для автоматичного оновлення і перевірки сертифікатів.

Критерії вибору при виборі програмного та апаратного забезпечення слід враховувати:

- **Безпеку**: наявність сертифікатів безпеки, використання HSM, надійність механізмів автентифікації.
- **Сумісність**: підтримка стандартів, інтеграція з наявними системами.
- **Масштабованість**: здатність системи підтримувати зростання кількості користувачів і пристроїв.
- **Зручність адміністрування**: наявність графічних інтерфейсів, автоматизація процесів.

- **Вартість володіння**: ліцензійні витрати, вартість обладнання, техпідтримка.
- **Підтримка і спільнота**: наявність документації, технічної підтримки, активність спільноти.

Приклади використання:

- **Малі та середні підприємства** часто обирають Microsoft CA через інтеграцію з Windows і відсутність додаткових ліцензійних витрат.
- **Великі корпоративні середовища** використовують EJBCA або комерційні рішення, щоб забезпечити розгалужену структуру CA, відповідність вимогам аудиту і гнучке управління.
- **Організації з високими вимогами безпеки** (банки, уряд) обов'язково застосовують HSM і сертифіковані продукти з багаторівневою архітектурою PKI.

Висновок:

Вибір засобів реалізації PKI - це баланс між безпекою, вартістю, зручністю та технічними можливостями. Для ефективної реалізації необхідно: Оцінити конкретні потреби організації. Вибрати програмне забезпечення, що відповідає вимогам. Інвестувати в апаратні засоби захисту, особливо HSM. Забезпечити сумісність і масштабованість системи. Планувати подальше обслуговування і підтримку. Правильно обрана і реалізована інфраструктура відкритих ключів є фундаментом інформаційної безпеки організації.

3.3 Опис алгоритму створення та керування сертифікатами

Інфраструктура відкритих ключів (PKI) є основою для забезпечення безпечної цифрової ідентифікації та шифрування даних. Ефективне управління життєвим циклом цифрових сертифікатів - від їх створення до відкликання або знищення - є критично важливим для підтримки цілісності та довіри в інформаційних

системах. Розглянемо ключові етапи створення та керування сертифікатами в рамках PKI.

Етап 1: Генерація пари ключів Процес починається з генерації пари криптографічних ключів: приватного та публічного. Приватний ключ зберігається в захищеному середовищі, наприклад, у апаратному модулі безпеки (HSM), тоді як публічний ключ використовується для створення запиту на сертифікат (CSR).
Етап 2: Створення запиту на сертифікат (CSR) Запит на сертифікат (Certificate Signing Request, CSR) містить публічний ключ та інформацію про суб'єкта (наприклад, ім'я, організацію, доменне ім'я). Цей запит підписується приватним ключем і надсилається до сертифікаційного центру (CA) для перевірки та видачі сертифіката.

Етап 3: Видача сертифіката Сертифікаційний центр перевіряє інформацію в CSR відповідно до встановлених політик. Після успішної перевірки CA підписує сертифікат своїм приватним ключем, створюючи таким чином цифровий сертифікат, який підтверджує автентичність публічного ключа суб'єкта.

Етап 4: Розповсюдження сертифіката після видачі сертифікат розповсюджується до відповідних систем або користувачів. Це може включати встановлення сертифіката на веб-сервери, клієнтські пристрої або інші системи, які потребують автентифікації або шифрування.

Етап 5: Валідація сертифіката під час використання сертифіката важливо регулярно перевіряти його дійсність. Це включає перевірку терміну дії, а також статусу відкликання через списки відкликаних сертифікатів (CRL) або протокол OCSP. Регулярна валідація забезпечує, що сертифікати, які більше не є дійсними, не використовуються в системі.

Етап 6: Відкликання сертифіката сертифікати можуть бути відкликані до закінчення терміну їх дії у випадках компрометації приватного ключа, зміни інформації про суб'єкта або порушення політик безпеки. Відкликані сертифікати

додаються до CRL або позначаються як відкликані через OCSP, щоб інші системи могли виявити їх недійсність.

Етап 7: Оновлення та продовження сертифіката перед закінченням терміну дії сертифіката необхідно ініціювати процес його оновлення або продовження. Це може включати генерацію нової пари ключів та створення нового CSR. Автоматизація цього процесу допомагає уникнути простоїв у роботі систем через прострочені сертифікати.

Етап 8: Знищення сертифіката після відкликання або закінчення терміну дії сертифіката важливо забезпечити безпечне знищення пов'язаних з ним приватних ключів та інших конфіденційних даних. Це запобігає можливому несанкціонованому використанню або компрометації. Автоматизація управління сертифікатами у великих організаціях з великою кількістю сертифікатів ручне управління стає неефективним та ризикованим. Використання систем автоматизованого управління життєвим циклом сертифікатів (CLM) дозволяє: автоматично виявляти та відстежувати всі сертифікати в системі. Налаштовувати автоматичне оновлення та відкликання сертифікатів. Забезпечувати централізоване управління політиками безпеки. Генерувати звіти та сповіщення про стан сертифікатів.

Рекомендації щодо управління сертифікатами:

- **Використовуйте апаратні модулі безпеки (HSM)** для зберігання приватних ключів.
- **Регулярно перевіряйте статус сертифікатів** через CRL або OCSP. **Автоматизуйте процеси оновлення та відкликання** сертифікатів.
- **Проводьте регулярні аудити** для виявлення потенційних ризиків.
- **Забезпечуйте навчання персоналу** щодо найкращих практик управління сертифікатами.

3.4 Визначення політик безпеки для сертифікаційного центру

Сертифікаційний центр (ЦС) є ключовим елементом інфраструктури відкритих ключів (PKI), виконуючи функції видачі, перевірки та анулювання цифрових сертифікатів. З огляду на надзвичайну важливість ЦС у побудові довіри в цифровому просторі, чітке визначення та впровадження політик безпеки є критично важливим для захисту від потенційних загроз та дотримання нормативних вимог.

3.5 Забезпечення захисту закритих ключів

Закриті ключі є наріжним каменем інфраструктури відкритих ключів (PKI), оскільки вони гарантують автентичність, цілісність і конфіденційність цифрової комунікації. Злам закритого ключа може спричинити серйозні наслідки, серед яких несанкціонований доступ до чутливої інформації, підробка цифрових підписів та підрив довіри до всієї PKI. Тому забезпечення надійного захисту закритих ключів є найважливішим завданням для кожної організації, яка використовує PKI.

3.6 Розробка плану впровадження PKI в організації

Впровадження PKI є складним проектом, що потребує чіткої стратегії і планування.

Основні етапи:

- Оцінка поточного стану безпеки і IT-інфраструктури.
- Визначення цілей впровадження і технічних вимог.
- Розробка архітектури і політик PKI.
- Вибір та закупівля необхідного обладнання і ПЗ.
- Підготовка персоналу, навчання адміністраторів.
- Розгортання центрів сертифікації і реєстраційних органів.
- Інтеграція PKI з існуючими системами.

- Тестування і валідація системи. Запуск у продуктивне середовище. Моніторинг і підтримка системи.

Ретельне планування мінімізує ризики і забезпечує ефективне впровадження.

3.7 Рекомендації для керівників і IT-відділів щодо управління PKI

Управління життєвим циклом сертифікатів (Certificate Lifecycle Management, CLM) є критично важливим процесом в інфраструктурі відкритих ключів (PKI), що забезпечує безперервну безпеку цифрових комунікацій та захист даних. Цей процес охоплює всі етапи існування сертифіката - від його створення до відкликання або знищення. Ефективне управління життєвим циклом сертифікатів дозволяє уникнути збоїв у роботі систем, запобігти витокам даних та забезпечити відповідність нормативним вимогам.

Етапи життєвого циклу сертифіката Життєвий цикл сертифіката включає кілька ключових етапів:

- **Реєстрація (Enrollment)**: Процес, під час якого користувач або пристрій подає запит на отримання сертифіката до сертифікаційного центру (CA). Запит містить публічний ключ та іншу необхідну інформацію для ідентифікації.
- **Видача (Issuance)**: Після перевірки запиту CA видає сертифікат, підписуючи його своїм приватним ключем.
- **Розповсюдження (Distribution)**: Сертифікат доставляється до заявника або відповідної системи для подальшого використання.
- **Використання (Usage)**: Сертифікат використовується для аутентифікації, шифрування або підпису даних.
- **Моніторинг (Monitoring)**: Постійне відстеження стану сертифіката, включаючи терміни дії та можливі компрометації.

- **Оновлення (Renewal)**: Перед закінченням терміну дії сертифікат оновлюється для забезпечення безперервної безпеки.
- **Відкликання (Revocation)**: У випадку компрометації або зміни статусу сертифікат може бути відкликаний до закінчення терміну дії.
- **Знищення (Destruction)**: Після завершення використання сертифікат та пов'язані з ним ключі повинні бути безпечно знищені. Ці етапи забезпечують повний контроль над сертифікатами протягом усього їхнього існування, що є основою для підтримки надійної PKI.

Найкращі практики управління життєвим циклом сертифікатів для ефективного управління життєвим циклом сертифікатів рекомендується дотримуватися наступних практик:

- **Розробка політик та процедур**: Створення чітких політик, що регламентують процеси видачі, оновлення, відкликання та знищення сертифікатів, допомагає забезпечити узгодженість та відповідність нормативним вимогам.
- **Автоматизація процесів**: Використання автоматизованих інструментів для управління сертифікатами зменшує ризик людських помилок та забезпечує своєчасне оновлення сертифікатів.
- **Моніторинг та сповіщення**: Постійне відстеження стану сертифікатів та налаштування сповіщень про наближення терміну дії або інші критичні події дозволяє вчасно реагувати на потенційні проблеми.
- **Централізоване управління**: Впровадження централізованої системи управління сертифікатами забезпечує повний огляд та контроль над усіма сертифікатами в організації.
- **Регулярні аудити**: Проведення періодичних аудитів допомагає виявити невідповідності, оцінити ефективність поточних процесів та впровадити необхідні покращення.

- **Навчання персоналу**: Забезпечення належного навчання співробітників, відповідальних за управління сертифікатами, підвищує рівень безпеки та ефективність процесів.

Виклики та ризики незважаючи на наявність найкращих практик, управління життєвим циклом сертифікатів може стикатися з наступними викликами:

- **Зростаюча кількість сертифікатів**: Зі збільшенням кількості пристроїв та сервісів, що потребують сертифікатів, управління ними стає більш складним.
- **Скорочення терміну дії сертифікатів**: Сучасні стандарти вимагають коротших термінів дії сертифікатів, що збільшує частоту їх оновлення.

3.8 Пропозиції щодо підвищення ефективності PKI (використання HSM, багатофакторна автентифікація)

Для покращення безпеки та функціональності PKI радиться: Застосування апаратних модулів безпеки (HSM) для створення й утримування ключів, що значно зменшує ризики компрометації. Запровадження багатофакторної автентифікації для користувачів та адміністраторів PKI, що ускладнює несанкціонований доступ. Інтеграція PKI з сучасними системами управління доступом (IAM), що збільшує результативність контролю та знижує адміністративне навантаження. Автоматизація процесів керування сертифікатами для запобігання зупинкам тап омилкам. Використання сучасних алгоритмів криптографії, що відповідають актуальним стандартам безпеки. Постійний аудит та оновлення системи у відповідності до нових кіберзагроз. Ці кроки забезпечують нетільки безпеку, а й масштабованість та зручність експлуатації PKI.

ВИСНОВКИ

У ході виконання дипломної роботи було досліджено теоретичні та практичні аспекти побудови і використання інфраструктури відкритих ключів (PKI) як важливого засобу забезпечення інформаційної безпеки організацій. Аналіз сучасних методів криптографічного захисту дозволив зробити висновок, що PKI є фундаментальною складовою для реалізації надійної автентифікації, забезпечення конфіденційності, цілісності та юридичної значущості електронної інформації в різних сферах діяльності. У першому розділі було розглянуто основи криптографії, типи шифрування, базові елементи PKI, а також нормативно-правову базу її застосування в Україні та світі. Особливу увагу приділено системам сертифікації, включаючи роботу центрів сертифікації (CA), реєстраційних органів (RA), механізмів відкликання сертифікатів (CRL, OCSP) та сучасних рішень для реалізації PKI (OpenSSL, EJBCA, Microsoft CA тощо). Другий розділ було присвячено аналізу реального використання PKI в різних галузях: бізнесі, медицині, освіті. Було описано налаштування захищеного електронного документообігу, автентифікацію користувачів і пристроїв, а також порівняльний аналіз різних підходів до впровадження PKI. Також окреслено типові проблеми, з якими стикаються організації під час впровадження PKI, та можливі шляхи їх вирішення. У третьому розділі розроблено архітектуру PKI для умовної організації з урахуванням її потреб. Було запропоновано алгоритм створення та керування сертифікатами, визначено політики безпеки та заходи захисту приватних ключів, а також сформульовано практичні рекомендації для IT-відділу й керівництва щодо впровадження та експлуатації PKI. Окрему увагу приділено питанням підвищення ефективності PKI шляхом впровадження апаратних модулів безпеки (HSM), багатофакторної автентифікації та інших сучасних технологій. Загалом, результати дослідження підтверджують, що PKI є надійним і гнучким інструментом для забезпечення кібербезпеки. Правильно спроєктована та впроваджена PKI дозволяє організації ефективно управляти цифровими сертифікатами, знижувати ризики, пов’язані з витоком інформації,

підвищувати рівень довіри до електронної взаємодії та відповідати вимогам національного і міжнародного законодавства. Таким чином, PKI може і повинна стати базовим елементом інформаційної безпеки сучасної організації в умовах цифрової трансформації та зростаючих кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

Що таке сертифікація (CA) - **https://www.techtarget.com/searchsecurity/definition/certificate-authority**

Інтернет-протокол статусу сертифіката - **https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol**

Що таке інфраструктура відкритих ключів (PKI)? Як вона працює? - https://www.fortinet.com/resources/cyberglossary/public-key-infrastructure

Криптографія: Розуміння інфраструктури відкритих ключів (PKI) та її критичної ролі в безпеці даних - https://medium.com/@cybersecrealm/cryptography-understanding-public-key-infrastructure-pki-and-its-critical-role-in-data-security-0f6417c0c942

Інфраструктура відкритих ключів - https://en.wikipedia.org/wiki/Public_key_infrastructure

Що таке інфраструктура відкритих ключів (PKI)? - https://www.ibm.com/think/topics/public-key-infrastructure

Підручник OpenSSl PKI - https://pki-tutorial.readthedocs.io/en/latest/

Підручник OpenSSl CA – Повнофункціональна інфраструктура відкритих ключів OpenSSl - https://grimoire.carcano.ch/blog/openssl-ca-tutorial-a-full-featured-openssl-pki/

Microsoft Learn: Захист PKI https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786431%28v%3Dws.11%29

Проектування інфраструктури відкритих ключів для департаменту охорони здоров'я - https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786431%28v%3Dws.11%29

Розуміння PKI - автентифікації - https://www.keyfactor.com/blog/understanding-pki-authentication/

Оволодіння корпоративною PKI - https://www.keyfactor.com/blog/mastering-enterprise-pki-5-challenges-and-how-to-outsmart-them/

Найкращі практики управління PKI - https://www.appviewx.com/blogs/best-practices-for-pki-management/

OpenSSL - https://www.openssl.org/

Розуміння інфраструктури відкритих ключів (PKI): Огляд та концепції - https://www.globalsign.com/en/blog/understanding-pki-overview-and-key-concepts