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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розроблення рекомендацій щодо захищеного обміну інформації на базі інфраструктури відкритих ключів»

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

_____ Вячеслав БАТУЄВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
БАТУЄВ Вячеслав
(прізвище, ім'я)

Керівник _____
(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 ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Батуєва Вячеслава Ігоровича
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо захищеного обміну інформації на базі інфраструктури відкритих ключів»

керівник кваліфікаційної роботи Бондаренко Зоя,
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 27 » _лютого_ 2024 року № __36__.

2. Строк подання здобувача вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи
програмний комплекс для віртуалізації;
рішення та рекомендації для інфраструктури
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблематики та виявлення загроз
2. Аналіз наявних рішень напрямку інфраструктури відкритих ключів, детальний огляд рішення їх проблем
3. Розроблення рекомендацій щодо захищеного обміну інформації на базі інфраструктури відкритих ключів
4. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 27.02.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми	27.02.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	15.03.2024 р.	
3.	Аналіз проблематики та виявлення загроз	18.04.2024 р.	
4.	Аналіз наявних рішень напрямку інфраструктури відкритих ключів, детальний огляд рішення їх проблем	20.04.2024 р.	
5.	Розроблення рекомендацій щодо захищеного обміну інформації на базі інфраструктури відкритих ключів	03.05.2024 р.	
6.	Оформлення результатів дослідження.	20. 05.2024 р.	
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Вячеслав БАТУЄВ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Зоя БОНДАРЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача БАТУЄВА Вячеслава

на тему: ««Дослідження шляхів та розроблення рекомендацій щодо захищеного обміну інформації на базі інфраструктури відкритих ключів»

Актуальність: Використання PKI є одним із важливих способів забезпечення інформаційної безпеки, і дослідження в цій галузі мають вирішальне значення для розробки сучасних інформаційних систем.

Актуальність цього дослідження обумовлена необхідністю підвищення рівня кібербезпеки в умовах постійно зростаючих кіберзагроз.

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 на базі інфраструктури відкритих ключів.
3. Запропоновано використання інфраструктури відкритих ключів 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 щодо використання інфраструктури відкритих ключів
2. Запропонований порядок застосування методів та засобів захисту інфраструктури відкритих ключів 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) **Батуєв Вячеслав** – 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 ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач БАТУЄВ Вячеслав до захисту кваліфікаційної роботи
(прізвище, ім'я)

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

на тему: «Дослідження шляхів та розроблення рекомендацій щодо захищеного обміну інформації на базі інфраструктури відкритих ключів».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***БАТУЄВ Вячеслав*** обрав тему роботи, метою якої було з'ясування основних принципів та переваг використання інфраструктури відкритих ключів та, аналіз документації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***БАТУЄВ Вячеслав*** 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 БАТУЄВА ***Вячеслава*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Зоя БОНДАРЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **БАТУЄВ Вячеслав** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 30 сторінок, 15 рисунків, 21 джерело.

Об'єкт дослідження – організація захищеного обміну інформації на базі інфраструктури відкритих ключів.

Предмет дослідження – методи та засоби захищеного обміну інформації на базі інфраструктури відкритих ключів.

Методи дослідження – опрацювання технічної літератури та наукових джерел для з'ясування основних принципів та переваг використання PKI та, аналіз документації та випадків використання інфраструктури відкритих ключів для забезпечення безпеки застосунків; проведення експериментального аналізу з використанням інфраструктури відкритих ключів на тестових проєктах для оцінки ефективності виявлення вразливостей; порівняльний аналіз рішень для визначення рекомендацій щодо захищеного обміну

Дослідження охоплює методи і засоби застосування інфраструктури відкритих ключів, , для підвищення безпеки їх використання в повсякденному житті. Аналізовано технічну літературу та наукові джерела, проведено експериментальний аналіз за допомогою gp4win , і виявлено переваги застосування цього рішення порівняно з альтернативними методами.

В результаті дослідження розроблено рекомендації щодо інтеграції gpg4win у процеси роботи, спрямовані на забезпечення вищого рівня безпеки використання інфраструктури відкритих ключів Практичне застосування результатів роботи може знайти використання у сферах, де критично важливим є забезпечення надійності і безпеки програмного забезпечення.

Галузь використання – кібербезпека інформаційних ресурсів організації.

КІБЕРБЕЗПЕКА, ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ, БЕЗПЕКА ЗАСТОСУНКІВ, PKI, ПОШУК ВРАЗЛИВОСТЕЙ, АВТОМАТИЗАЦІЯ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PKI	—	Public Key Infrastructure
VPN	—	Virtual Proxy Network
GPG4win	—	GNU Privacy Guard for Windows
CA	—	Центр Сертифікації
RA	—	Реєстраційний орган
TLS	—	Transport Layer Security

ВСТУП

Актуальність цього дослідження обумовлена необхідністю підвищення рівня кібербезпеки в умовах постійно зростаючих кіберзагроз. Використання PKI є одним із важливих способів забезпечення інформаційної безпеки, і дослідження в цій галузі мають вирішальне значення для розробки сучасних інформаційних систем.

Об'єкт дослідження – інфраструктура відкритих ключів

Предмет даного дослідження є методи і засоби забезпечення безпеки обміну інформацією на основі інфраструктури відкритих ключів. Однак, незважаючи на високу ефективність PKI, існують деякі проблеми та проблеми, пов'язані з його впровадженням та використанням. Це включає складність управління ключами, вразливість до атак та необхідність забезпечення сумісності з різними системами та протоколами. Крім того, важливим аспектом є розробка та впровадження ефективної політики безпеки, яка регулює використання ОКТ. Також завданням цього дослідження є вивчення методів безпечного обміну інформацією на основі інфраструктури відкритих ключів та розробка рекомендацій. Це включає аналіз існуючих рішень PKI, виявлення вразливостей та розробку методів підвищення безпеки обміну інформацією.

Метою цього дослідження є вивчення методів безпечного обміну інформацією на основі інфраструктури відкритих ключів та розробка рекомендацій. Це включає аналіз існуючих рішень PKI, виявлення вразливостей та розробку методів підвищення безпеки обміну інформацією. В ході дослідження були використані методи аналізу науково-технічної літератури Рекомендації, розроблені в рамках дослідження, можуть бути використані для вдосконалення існуючих систем PKI та підвищення їх безпеки та ефективності

PKI надає засоби для створення, управління, зберігання та розповсюдження цифрових сертифікатів, які використовуються для шифрування даних та забезпечення їх надійності. PKI забезпечує безпечний обмін інформацією між

організаціями за допомогою відкритих та приватних ключів та забезпечує захист від несанкціонованого доступу та змін.

Рекомендації, розроблені в рамках дослідження, можуть бути використані для вдосконалення існуючих систем PKI та підвищення їх безпеки та ефективності

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту кінцевих точок організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЩОДО ОБМІНУ ІНФОРМАЦІЇ НА БАЗІ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

1.1 Огляд існуючих систем PKI

Інфраструктура відкритих ключів (PKI) - це рішення, яке використовує сертифікати для автентифікації замість ідентифікаторів електронної пошти та паролів. PKI також шифрує з'єднання за допомогою асиметричного шифрування за допомогою відкритого та приватного ключів. PKI управляє сертифікатами та ключами та створює високозахищене середовище, яке також може використовувати користувачів, програми та інші пристрої. Це PKI X.It 509 використовує сертифікат і відкритий ключ, а ключі використовуються для наскрізних зашифрованих з'єднань, щоб обидві сторони могли довіряти один одному для перевірки їх надійності.

Варто відзначити поширеність та важливість існуючих систем PKI. Багато компаній, урядових установ та інших установ використовують PKI для захисту конфіденційної інформації, перехоплення мережевих комунікацій та забезпечення взаємодії між користувачами та системами

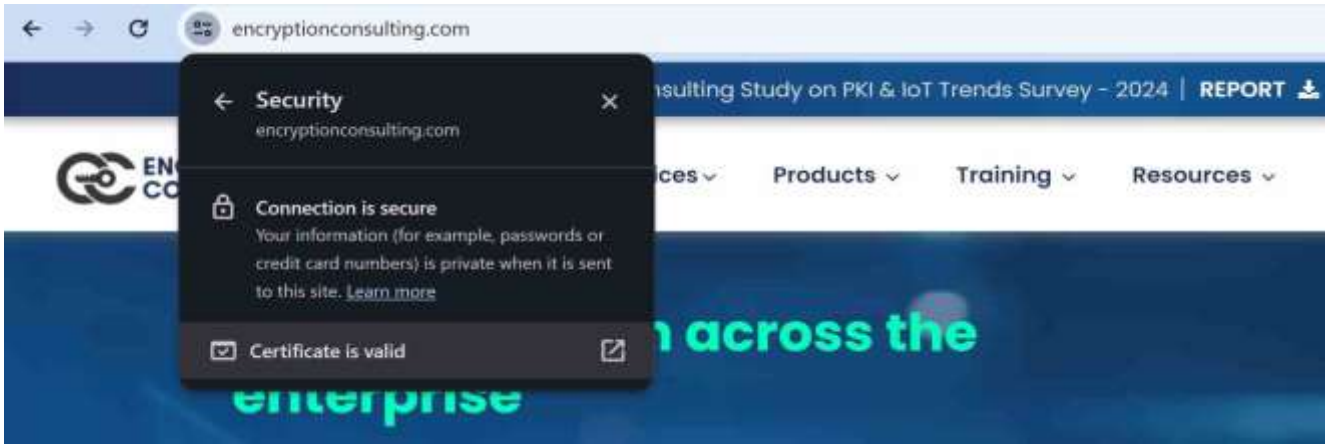

Рис. 1.1. Інформація про використання PKI при завантаженні інформації сайту

Одним з ключових компонентів існуючої системи PKI є центр сертифікації (ЦС). Ці центри відіграють важливу роль у видачі та управлінні цифровими

сертифікатами, які перевіряють особу користувачів та їх відкритий ключ. Відкритий ключ, що міститься в сертифікаті, використовується для шифрування даних або підпису повідомлень, тоді як приватний ключ залишається приватним і використовується для розшифровки або перевірки підпису.

Рис 1.2. Trust Manager логотип та кількість країн в яких вони працюють

Важливо також відзначити роль інфраструктури управління ключами (Kmi) у системах PKI. Ці системи відповідають за створення, зберігання та розповсюдження ключів шифрування та підпису, а також забезпечення безпеки та цілісності.

Системи PKI також використовують різні протоколи та стандарти. Наприклад, X. Стандарт 509 визначає формат цифрових сертифікатів, а протокол TLS / SSL забезпечує безпечний обмін даними через Інтернет. Незважаючи на широке використання існуючих систем PKI, вони також мають свої недоліки та обмеження. Наприклад, якщо система PKI неправильно налаштована або запущена, можуть виникнути проблеми з безпекою, а також проблеми з автентифікацією та управлінням ключами.

У наступній частині нашого дослідження ми детальніше розглянемо ці проблеми та проаналізуємо, як їх вирішити та захистити від атак на системи PKI.

Наприклад, недоліки існуючих безконтактних систем включають серйозні адміністративні проблеми, які можуть призвести до витоку конфіденційної інформації або несанкціонованого доступу до системи. Окрім проблем, пов'язаних із зломом самого центру сертифікації, існують також інші проблеми, які можуть поставити під загрозу всю екосистему PKI

Це включає такі проблеми, як автентифікація та управління цифровими сертифікатами, а також своєчасне оновлення або відкликання сертифікатів, які втратили актуальність або були скомпрометовані. Це знижує безпеку системи і надає доступ зловмисникам.

Проблеми сумісності та переривання зв'язку між різними системами, не пов'язаними з ПК, особливо коли ці системи використовують різні стандарти або протоколи, можуть ускладнити реалізацію взаємодій між різними системами та зберегти анонімність витрат на відключення їх інтеграції.

Існує кілька популярних систем PKI, які активно використовуються в різних галузях, включаючи корпоративне середовище, Державні установи та фінансові установи. До них відносяться:

1. *Microsoft Active Directory Certificate Services* (AD CS): широко використовується у корпоративних середовищах для управління цифровими сертифікатами.

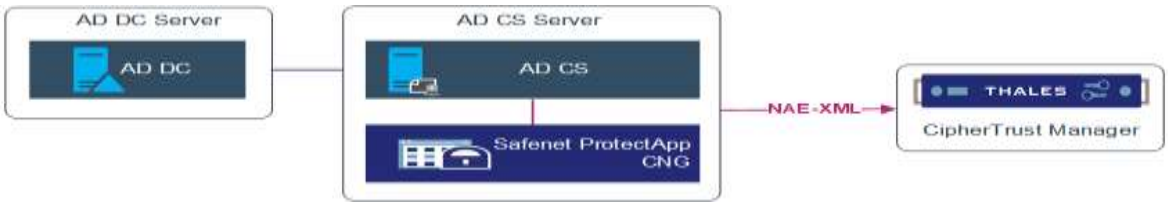

Рис 1.3 огляд фунціоналу MADCS

2. *OpenSSL*: відкрите рішення, що надає інструменти для створення та управління сертифікатами.

Рис 1.4. Open SSL та їх варіативність їх методів захисту клієнтів

3. *Let's Encrypt*: безкоштовний сервіс, що надає автоматизовану видачу SSL/TLS сертифікатів для забезпечення захищеного з'єднання на веб-сайтах.

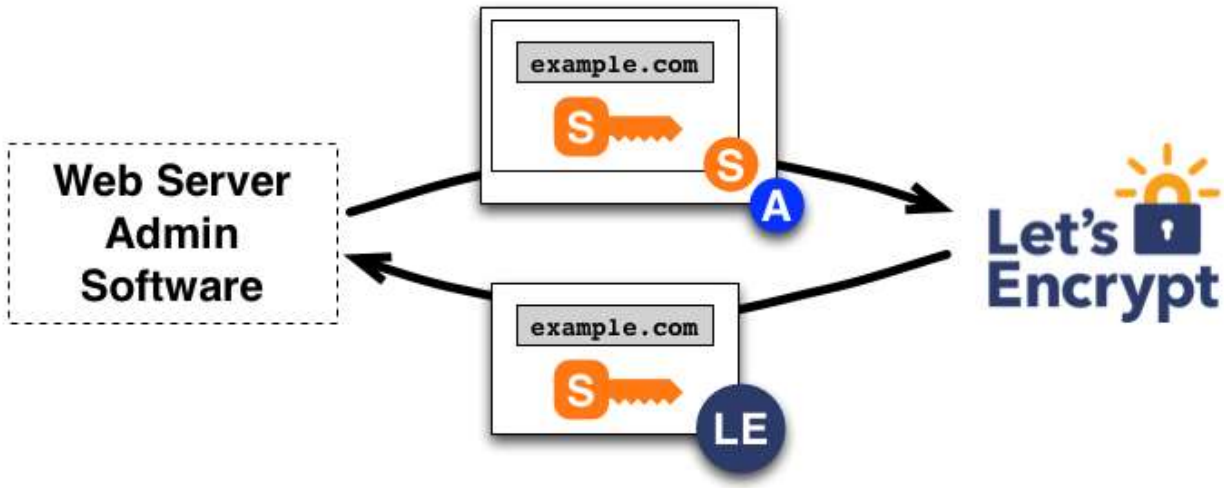

Рис 1.5 основа функцій сервісу Let`s Encrypt

Entrust: комерційне рішення, що пропонує широкий спектр послуг у сфері PKI, включаючи управління сертифікатами, шифрування даних та автентифікацію користувачів.

1.2 Аналіз проблеми захищеного обміну інформації на базі інфраструктури відкритих ключів

1. Складність Системи PKI-це складна система, що складається з багатьох компонентів, включаючи центр сертифікації (CA), центр реєстрації (RA), сховище сертифікатів та різні клієнтські програми. Оскільки кожен із цих компонентів має свої вразливості, їх важко виявити та усунути. Наприклад, вразливість центру сертифікації може поставити під загрозу всю систему. Якщо зловмисник має доступ до приватного ключа центру сертифікації, він може видати підроблений сертифікат, який вважається дійсним.

2. Управління криптографічними ключами є одним з найважливіших і водночас найскладніших аспектів PKI. Проблеми зі створенням, зберіганням, розповсюдженням та відкликанням ключів можуть призвести до серйозних вразливостей безпеки. Генерація ключів якщо процес генерації ключів не забезпечує достатньої ентропії або використовує слабкий алгоритм, це може призвести до генерації крихкого ключа.

Зберігання ключів недостатній захист закритого ключа може призвести до його порушення. Це стосується як апаратного модуля безпеки (HSM), так і сховища програмного забезпечення. Передача ключів передача ключів через незахищений канал може призвести до втручання зловмисників. Скасування ключа непрацююче або неправильне скасування скомпрометованого ключа може призвести до використання недійсних сертифікатів для шифрування або автентифікації.

3. Проблеми з перевіркою сертифікатів Перевірка сертифіката має вирішальне значення для забезпечення безпеки PKI. Деякі проблеми з перевіркою включають:

— Недостатня перевірка: недостатня перевірка сертифіката може призвести до прийняття недійсних або підроблених сертифікатів.

— Помилка алгоритму: помилка в реалізації алгоритму перевірки підпису дозволяє зловмиснику використовувати підроблений сертифікат.

— Відсутній список відкликання сертифіката (Crl): якщо оновлення Crl відсутнє або не працює, відкликаний сертифікат доступний.

— Атаки на центри сертифікації (ЦС) CA є центральним елементом PKI, і цей компроміс може мати серйозні наслідки. Основними типами атак на ЦС є:

— Інфраструктурна атака – зловмисник може атакувати інфраструктуру ЦС для доступу до приватних ключів або створення підроблених сертифікатів.

— Фішинг-атаки – зловмисник може використовувати фішинг-атаку для отримання несанкціонованого доступу до облікового запису адміністратора центру сертифікації.

— Атака на процес перевірки – зловмисник може спробувати обійти процес перевірки за допомогою соціальної інженерії або інших методів.

5. Людський фактор. Людський фактор є важливим аспектом безпеки ІКТ. Помилки і недбалість персоналу можуть привести до серйозних вразливостей в системі безпеки. Основними проблемами є:

— Недостатня підготовка: недостатня підготовка персоналу щодо навичок безпечного управління ключами та сертифікатами може призвести до помилок.

— Помилка конфігурації: неправильне налаштування компонента PKI може призвести до вразливості.

— Недбале ставлення до безпеки: недбале ставлення до безпеки, таке як зберігання ключів у місцях, де безпека не передбачена, або використання слабких паролів, може поставити під загрозу вашу систему.

— Проблеми сумісності та сумісності Оскільки PKI використовує різні стандарти та протоколи, проблеми сумісності та декомунізації можуть виникати в різних системах та додатках. Це може призвести до вразливостей через неправильну інтеграцію компонентів.

— Невідповідність стандартам: використання різних стандартів та протоколів шифрування може спричинити проблеми сумісності.

— Помилка інтеграції: неправильна інтеграція компонентів PKI може

створити вразливість, яку може використати зловмисник.

6. Актуальність протоколу та алгоритму. Криптографічні протоколи та алгоритми мають обмежений термін придатності через постійний розвиток обчислювальної потужності та методів атаки. Основними проблемами є застарілі алгоритми: використання застарілих алгоритмів шифрування та підпису може створити вразливості. Наприклад, алгоритми, які раніше вважалися безпечними, можуть бути зламані з використанням новітніх обчислювальних потужностей. Необхідність оновлення необхідно постійно відстежувати нові вразливості та оновлювати алгоритми та протоколи, що використовуються в PKI

2. АНАЛІЗ МЕТОДІВ ЩОДО ЗАХИЩЕНОГО ОБМІНУ ІНФОРМАЦІЇ НА БАЗІ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

2.1 Інфраструктура відкритих ключів (PKI)

1. *PKI* -це комплексна система управління ключами шифрування та сертифікатами, яка забезпечує безпечний обмін інформацією між користувачами та системами. Основними компонентами PKI є:

— Центр сертифікації (ЦС) є центральним компонентом PKI, який видає, управляє та анулює цифрові сертифікати. Центр сертифікації діє як довірена третя сторона, яка перевіряє справжність активів (користувачів, серверів та пристроїв) шляхом видачі сертифікатів. Основними функціями центру сертифікації є:

— Видача сертифіката: Створіть і підпишіть сертифікат, який пов'язує відкритий ключ з ідентифікатором суб'єкта.

— Управління сертифікатами: включає оновлення, поновлення та скасування сертифікатів за необхідності.

2. Підтримка списку відкликання сертифікатів (CRL): зберігайте та розповсюджуйте список відкликаних сертифікатів, щоб перевірити їх дійсність. Реєстраційний орган (RA) є посередником між кінцевим користувачем і ЦС. РА виконує наступні функції:

— Аутентифікація: перед видачею сертифіката перевірте особу фізичної або юридичної особи.

— Надіслати запит: надсилання запиту на сертифікацію до ЦС після перевірки автентичності.

— Підтримка користувачів: забезпечує підтримку користувачів у процесі реєстрації та управління сертифікатами.

— Сховище сертифікатів-це база даних, яка зберігає цифрові сертифікати та CRL. Вони гарантують, що сертифікати будуть доступні для перевірки надійності та цілісності підписаних або зашифрованих даних.

2.2 Основні методи безпечного обміну інформацією

1. Шифрування – важливий спосіб забезпечення конфіденційності інформації. Він складається з перетворення відкритого тексту в зашифрований за допомогою криптографічних алгоритмів та ключів. PKI використовує 2 основні типи шифрування: симетричне та асиметричне.

Симетричне шифрування - використовує один ключ для шифрування та дешифрування даних. Основні характеристики симетричного шифрування:

Швидкість: симетричні алгоритми, такі як AES, працюють швидше, ніж асиметричні алгоритми, тому вони ефективні для шифрування великих обсягів даних.

Ключова безпека: основною проблемою симетричного шифрування є передача та зберігання ключів. Якщо ключ скомпрометований, зловмисник може отримати доступ до зашифрованих даних.

2. Асиметричне шифрування використовує пару відкритих і приватних ключів. Відкритий ключ використовується для шифрування, а приватний ключ - для дешифрування. Основні характеристики асиметричного шифрування:

Безпека: асиметричне шифрування забезпечує високий рівень безпеки з використанням ПАР ключів. Відкритий ключ може вільно поширюватися, а приватний ключ зберігається в таємниці. Складність: асиметричні алгоритми, такі як RSA, обчислювально складні і не дуже ефективні при шифруванні великих обсягів даних. З цієї причини він зазвичай використовується для шифрування симетричного ключа, але симетричний ключ використовується для шифрування даних.

3. Цифрові підписи забезпечують цілісність і надійність повідомлення. Він створюється за допомогою приватного ключа відправника та перевіряється за допомогою відкритого ключа. Основні етапи створення та перевірки цифрового підпису:

— Хешування: вихідне повідомлення обробляється хеш-функцією (наприклад, SHA-256), яка генерує унікальний хеш-код (контрольну суму) для повідомлення.

— Хеш-шифрування: хеш-код шифрується за допомогою приватного ключа відправника для створення цифрового підпису.

— Додати підпис: цифровий підпис додається до оригінального повідомлення та надсилається разом із ним одержувачу

— Хеш повідомлення: одержувач використовує хеш-функцію для обробки отриманого повідомлення та отримує його хеш-код.

— Розшифровка підпису: цифровий підпис розшифровується за допомогою відкритого ключа відправника для відновлення оригінального хеш-коду.

— Порівняння хешів: отриманий хеш-код порівнюється з розшифрованим хеш-кодом. Якщо вони збігаються, підпис вважається дійсним і підтверджує справжність та цілісність повідомлення.

4. Управління ключами Управління ключами є ключовим компонентом PKI, включаючи створення, зберігання, розповсюдження та відкликання ключів шифрування. Генерація ключів. Процес генерації ключів передбачає створення надійних ключів шифрування для шифрування та підписання. Основні аспекти генерації ключів:

— Алгоритми: використовуйте надійні алгоритми шифрування (RSA, ECC тощо) Для забезпечення безпеки ваших ключів.

— Довжина ключа: виберіть найкращу довжину ключа, щоб збалансувати безпеку та продуктивність. Наприклад, 2048-бітний ключ RSA забезпечує високий рівень безпеки.

— Зберігання ключів: надійне зберігання ключів важливо для забезпечення безпеки. Спосіб зберігання первинного ключа виглядає наступним чином:

— Модуль апаратної безпеки (HSM): це спеціалізований апаратний пристрій, який дозволяє створювати, зберігати та використовувати ключі шифрування в безпечному середовищі.

5. Безпечне програмне середовище: використовуйте програмні рішення для шифрування та захисту ключів, такі як маркери шифрування та смарт-картки. Розподіл ключів: процес розподілу ключів декомпонує передачу ключів шифрування між об'єктами. Метод розподілу ключів:

— Безпечний канал зв'язку використовуйте безпечний канал зв'язку (наприклад, TLS) для безпечної передачі ключів.

— Використовуйте сертифікати поширюйте відкритий ключ за допомогою цифрового сертифіката, підписаного довіреним центром сертифікації.

6. Скасування ключа Процес відкликання ключа включає відкликання скомпрометованих або недійсних ключів. Основні способи скасування ключа:

— Список відкликання сертифікатів (Crl): список сертифікатів, відкликаних центром сертифікації, періодично оновлюється. Список сертифікатів, відкликаних сертифікаційними органами на 2018-12 роки, періодично оновлюється.

— Протокол статусу сертифіката в Інтернеті (OCSP): це протокол, який дозволяє перевіряти статус сертифіката в режимі реального часу.

7. Як реалізувати PKI Інтеграція з системами і додатками PKI може бути інтегрований з різними системами і додатками для забезпечення безпечного обміну інформацією. Основними областями інтеграції є:

— Електронна пошта використання цифрових підписів та шифрування для забезпечення конфіденційності та надійності Електронної Пошти.

— Веб-сайт використовуйте сертифікати SS/TLS, щоб забезпечити безпечне з'єднання між веб-сервером та клієнтом.

— Мобільний додаток: інтеграція PKI для забезпечення безпечної аутентифікації та передачі даних у мобільних додатках.

— Мережеві пристрої використовуйте цифрові сертифікати для забезпечення безпеки мережевих пристроїв та інфраструктури Інтернету речей.

8. Стандарти та протоколи PKI підтримує широкий спектр стандартів і протоколів, які забезпечують сумісність і безпеку. Основними стандартами та протоколами є:

— X. 509: формат цифрового сертифіката та стандарт шляху сертифікації.

— PKCS (стандарти шифрування з відкритим ключем): набір стандартів для алгоритмів і протоколів шифрування, включаючи PKCS # 1 (шифрування RSA), PKCS # 7 (шифрування повідомлень) і PKCS # 12 (формат зберігання ключів).

— Безпека транспортного рівня (TLS): це протокол, який використовується для забезпечення безпечного підключення до мережі.

— S/MIME (захищені / багатоцільові розширення інтернет-пошти): це стандарт захищеної електронної пошти, що підтримує шифрування та цифрові підписи.

9. Безпечні канали зв'язку PKI дозволяє створити безпечний канал зв'язку для відправки конфіденційної інформації. Основними методами є:

SSL / TLS: використовує цифровий сертифікат для автентифікації сервера та перериває безпечне декомпонуюче з'єднання між Клієнтом та сервером.

VPN (віртуальна приватна мережа): використовує PKI для автентифікації користувачів та забезпечує безпечний доступ до корпоративної мережі через захищений тунель.

10. Контроль доступу та ідентифікація PKI Він використовується для перевірки доступу та автентифікації користувачів у різних системах. Основними напрямками є:

— Одноразовий пароль (10 місяців): використовує одноразовий пароль, створений за допомогою PKI, для забезпечення додаткового рівня безпеки. жовтень. 2-факторна аутентифікація (2FA): комбінація паролів і зашифрованих токенів для забезпечення надійної аутентифікації користувача.

— Контроль доступу. На основі ролей (RBAC): використовуйте цифрові сертифікати для адміністрування. доступом користувачів до ресурсів на основі їх ролей у системі.

11. *Інфраструктура відкритих ключів* (PKI) - це базова технологія для забезпечення безпечного обміну інформацією в сучасних системах зв'язку. Основні методи захисту включають шифрування, цифрові підписи та управління ключами для забезпечення конфіденційності, цілісності, надійності та відсутності дека даних.

Gpg4win (GNU Privacy Guard для Windows) - популярний інструмент для реалізації криптографічних заходів безпеки, заснованих на стандартах OpenPGP і S / MIME. Він забезпечує шифрування та підпис електронної пошти та файлів, що дозволяє застосовувати основні принципи PKI в рамках безпечного обміну інформацією.

Шифрування забезпечує конфіденційність повідомлень за допомогою алгоритмів шифрування для перетворення відкритого тексту в зашифрований. Асиметричне шифрування використовує пари ключів (відкритий та приватний ключі) для забезпечення високого рівня безпеки та використовується для шифрування симетричних ключів та шифрування даних.

12. Цифрові підписи забезпечують цілісність і надійність повідомлення. Він створюється за допомогою приватного ключа відправника та автентифікується за допомогою відкритого ключа, що дозволяє одержувачу перевірити справжність та цілісність отриманого повідомлення.

Управління ключами включає створення, зберігання, розповсюдження та відкликання ключів шифрування. Генерація ключів забезпечує створення надійного ключа шифрування, зберігання ключів передбачає використання апаратних модулів безпеки (HSM) або захищених програмних середовищ, розповсюдження ключів здійснюється за допомогою захищених каналів або цифрових сертифікатів, а скасування ключів забезпечує скасування скомпрометованих або недійсних ключів.

Інтеграція PKI з різними системами та програмами забезпечує безпечний обмін інформацією між електронною поштою, веб-сайтами, мобільними додатками

та мережевими пристроями. Декомпонування даних PKI дозволяє безпечно обмінюватися інформацією між електронною поштою, веб-сайтами, мобільними додатками та мережевими пристроями. X. використання стандартів і протоколів, таких як 509, PKCS, TLS і S/MIME, забезпечує сумісність і безпеку системи.

Gpg4win є важливим інструментом для реалізації криптографічних заходів безпеки, заснованих на стандартах OpenPGP і S / MIME. Він забезпечує шифрування та підпис електронної пошти та файлів, що дозволяє застосовувати основні принципи Pki в рамках безпечного обміну інформацією.

В цілому, PKI-це потужна технологія, що забезпечує надійний захист інформації в цифровому світі. Використання методів шифрування, цифрових підписів і управління ключами забезпечує високий рівень безпеки і захисту даних, що є критично важливим у сучасних комунікаційних системах.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ПОШУКУ ВРАЗЛИВОСТЕЙУ ВЕБЗАСТОСУНКАХ

3.1 Вибір методів та засобів для практичного експерименту

1. Для проведення практичних експериментів з безпеки систем обміну інформацією на основі інфраструктури відкритих ключів необхідно вибрати найкращі методи і засоби, що забезпечують максимальну ефективність і надійність отриманих результатів.

По-перше, необхідно ретельно проаналізувати формулювання проблеми експерименту і визначити його мету. Чітке визначення мети дозволяє вибрати правильні методи та інструменти для проведення досліджень. У той же час необхідно враховувати поточні проблеми і тенденції в розвитку шифрування та інформаційної безпеки.

Потім необхідно ретельно проаналізувати наукову літературу і стандарти в області шифрування та інформаційної безпеки. Це дозволяє вибрати кращі методи дослідження, що відповідають останнім вимогам і стандартам безпеки.

Після того, як я обрав метод дослідження, потрібно вибрати відповідні інструменти та програмне забезпечення для їх застосування. Наприклад, спеціальні інструменти та алгоритми криптографічного аналізу можуть бути використані для перевірки стабільності криптографічних алгоритмів.

Також важливо враховувати практичні аспекти експерименту, такі як час, бюджет та наявні ресурси. Ретельне планування гарантує, що я ефективно використаю свій час та ресурси та отримую найкращі результати досліджень.

Таким чином, вибір методів та інструментів для практичних експериментів з безпеки систем обміну інформацією на основі інфраструктури відкритого ключа являє собою складний і багатогранний процес, що вимагає детального аналізу та обґрунтування кожного вибору з урахуванням деталей предмета дослідження і цілей.

2. Практичне застосування безпечного обміну інформацією на основі інфраструктури відкритих ключів (PKI) є важливим етапом досліджень. У цьому розділі детально описується процес забезпечення конфіденційності, цілісності та надійності при обміні даними з використанням gpg4win. Gpg4win (GNU Privacy Guard для Windows) - це потужний криптографічний інструмент інформаційної безпеки, який підтримує широкий спектр функцій, необхідних для реалізації PKI.

3. Огляд Gpg4Win - це набір програм, що використовуються для управління ключами шифрування та забезпечення безпечного обміну інформацією. Основними компонентами Gpg4win є:

GnuPG: це основний інструмент шифрування, який дозволяє шифрувати, розшифровувати, підписувати та перевіряти підписи.

Клеопатра: графічний інтерфейс, який використовується для управління ключами та сертифікатами.

GPA (GNU Privacy Assistant): додатковий графічний інтерфейс для GnuPG. жовтня 2011 р.

GpgOL: надбудова для Microsoft Outlook, яка дозволяє інтегрувати функції шифрування в електронну пошту.

3.2 Прототипування захищеної системи обміну інформацією на основі PKI

1. Встановлення та налаштування Gpg4win Першим кроком у програмі є встановлення Gpg4win на мій комп'ютер. Для цього я завантажив інсталяційний файл з офіційного веб-сайту Gpg4Win і запустіть його. Після завершення установки необхідно задати основні параметри програми. На фото показаний сайт офіційного представника gpg4win

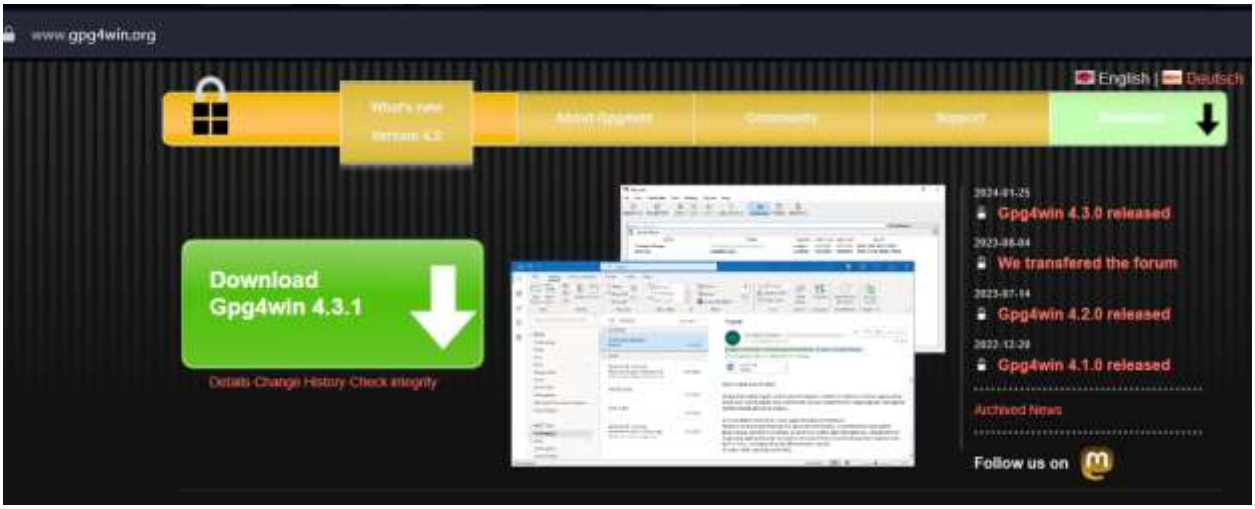

Рис 3.1. Основний сайт Gpg4win для отримання свіжої інформації та завантаження

2. Створення ключової пари: У Kleopatra потрібно створити нову ключову пару, що складається з відкритого та закритого ключів. Цей процес включає введення особистої інформації, такої як ім'я та електронна адреса.

На рисунку (3.2) зображено все інстальована Kleopatra а також початок для створення нової пари ключів

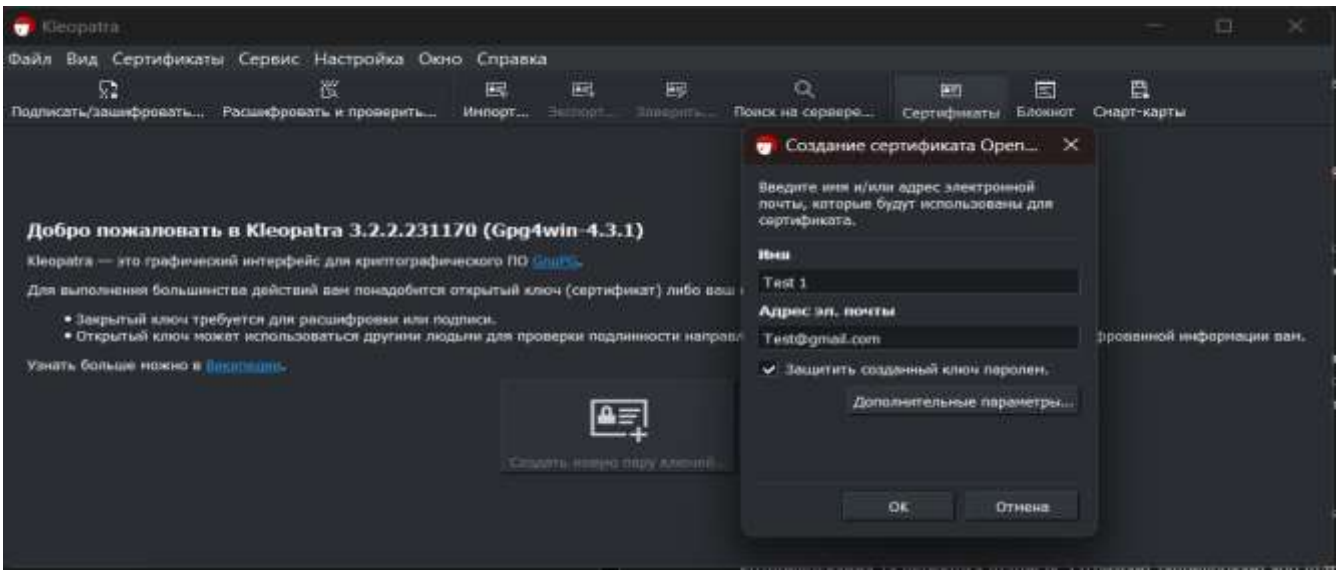

Рис 3.2 Початок для створення нової пари ключів

3. Експорт відкритого ключа: Після створення ключової пари, відкритий ключ необхідно експортувати та передати його іншим учасникам для шифрування повідомлень, адресованих вам.

На цьому рисунку зображено створений сертифікат для нової пари ключів за допомогою Kleopatra

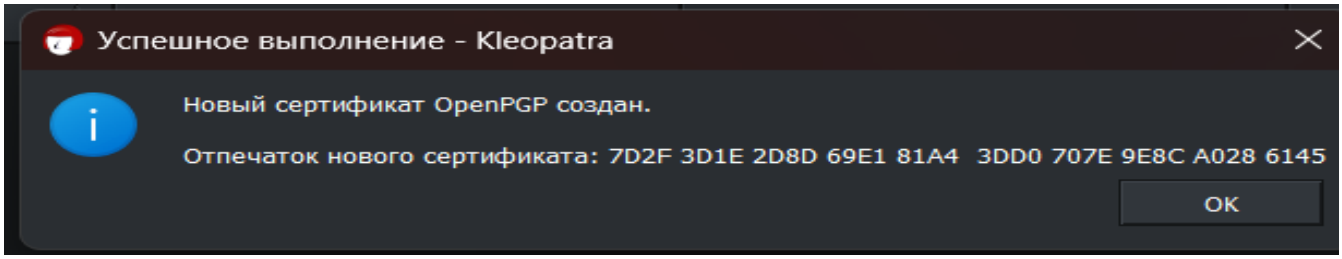

Рис 3.3. Створений сертифікат для нової пари ключів

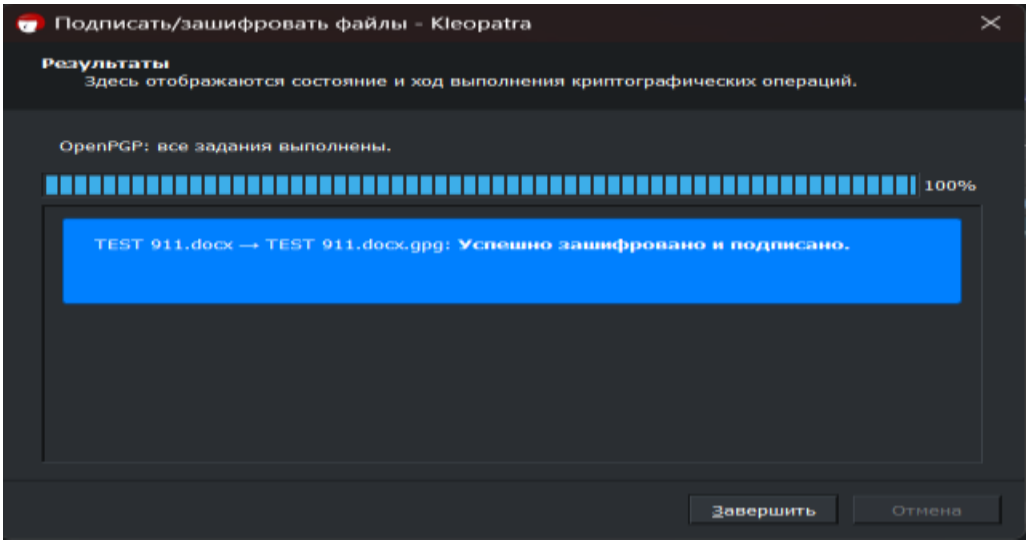

Рис 3.4. Успішне шифрування файлу під назвою «TEST_911» розширення .gpg

3.3 Проведення експериментів

Для забезпечення конфіденційності обміну інформацією, повідомлення потрібно шифрувати перед відправленням і розшифровувати після отримання. Використання Gpg4win дозволяє легко виконати ці операції за допомогою Kleopatra та GnuPG:

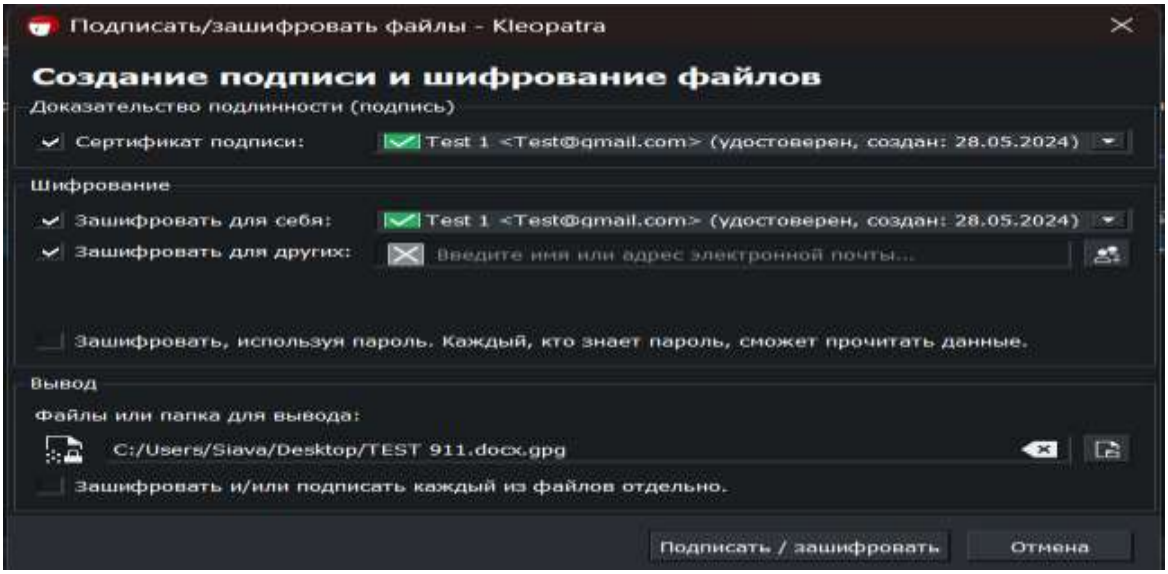

Рис 3.5. Створення підпису шифрування файлів

Розшифровка повідомлення: після отримання зашифрованого файлу я відкрив його в Kleopatra і вибрав "розшифрувати / перевірити", Також я можу розшифрувати повідомлення за допомогою приватного ключа.|

3. Підпис та перевірка підпису Підписання повідомлення гарантує цілісність і надійність повідомлення, і одержувач може підтвердити, що повідомлення не було змінено і дійсно прийшло від вас На рисунку показано, що одержувач підтвердив, що має доступ до надісланого файлу, і в цьому випадку у вас є можливість розшифрувати його без зволікання (рис. 3.6).

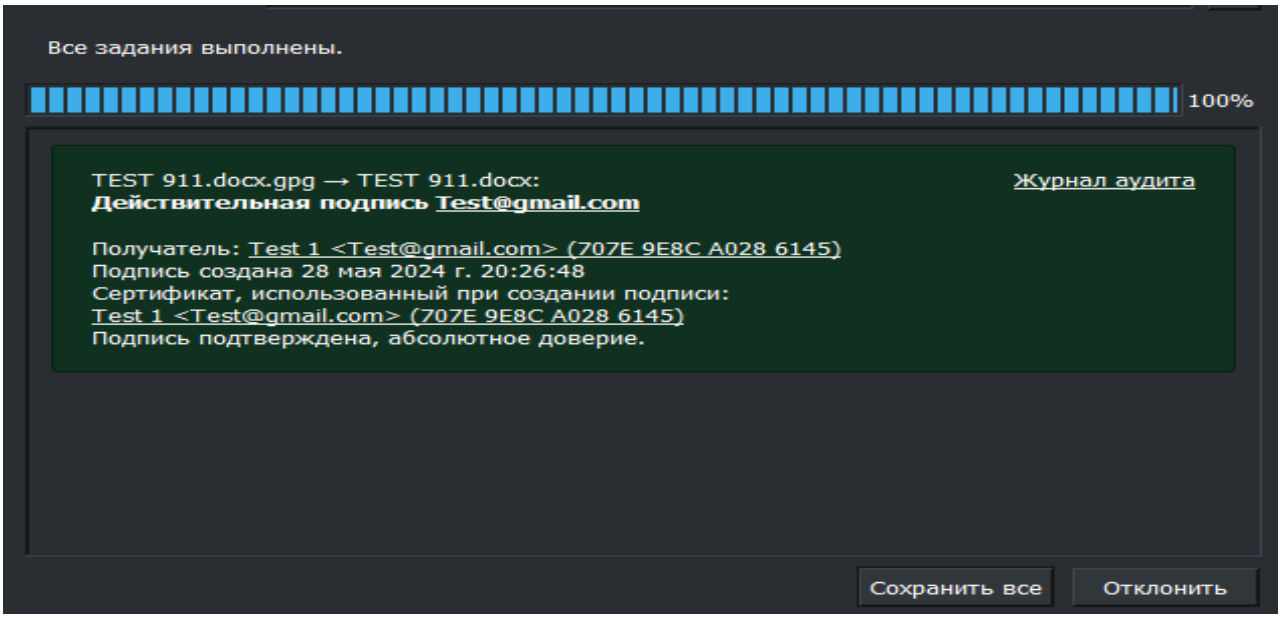

Рис 3.6 Підтвердження, що отримувач має доступ до файлу який йому надіслали

4. Підписання повідомлення: У Kleopatra обирається опція "New Plaintext File", де вводиться текст повідомлення. Після цього вибирається "Sign", і використовується ваш закритий ключ для підписання.

5. Перевірка підпису: Після отримання підписаного файлу, його можна відкрити у Kleopatra та обрати "Decrypt/Verify", що дозволить перевірити підпис за допомогою вашого відкритого ключа.

3.4 Інтеграція з Microsoft Outlook

1. Для зручності використання криптографічних функцій у електронній пошті, Gpg4win включає плагін GpgOL для Microsoft Outlook. Цей плагін дозволяє шифрувати, розшифровувати, підписувати та перевіряти підписи електронних листів безпосередньо у поштовому клієнті

2. Шифрування електронних листів: Після встановлення плагіну, у вікні створення нового листа з'являються опції для шифрування та підписання. Microsoft Outlook після отримання повної версії та повного функціоналу

інструментів Mircosoft Outlook вибираючи ці опції, можна захистити лист перед відправленням.

2. Шифрування повідомлення: У Kleopatra обирається опція "New Plaintext File", де вводиться текст повідомлення. Після цього вибирається И"Encrypt", вказується відкритий ключ одержувача.

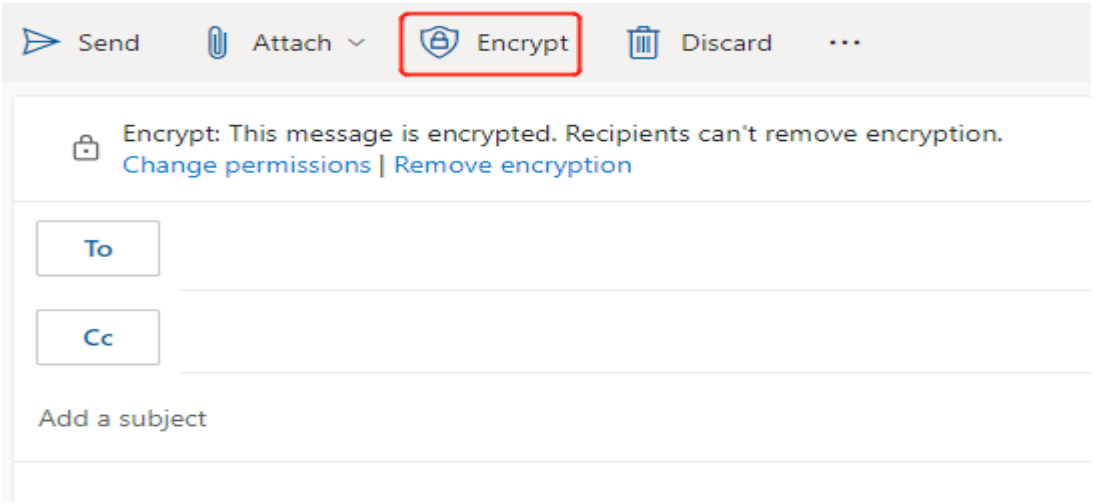

Рис 3.7. Функція шифрування документів у Microsoft Outlook

3. Розшифрування та перевірка підписів: Отримані зашифровані або підписані листи автоматично розшифровуються або перевіряються при відкритті, якщо відповідні ключі зберігаються у вашому сховищі ключів.

На рис (3.8) зображено повідомлення про вже отриманий лист на іншу електронну адресу, це сповіщення освідомлює нас про те що нам насілали зашифрований файл за допомогою сервісу Microsoft Outlook.

На цьому рисунку зображено вже отримане повідомлення та його вигляд на пошті, за рахунок доступу який ми надаємо при відправці файлу а також формату шифрування, отримувач буде мати обмежений функціонал, якщо це вказано одразу при відправці повідомлення

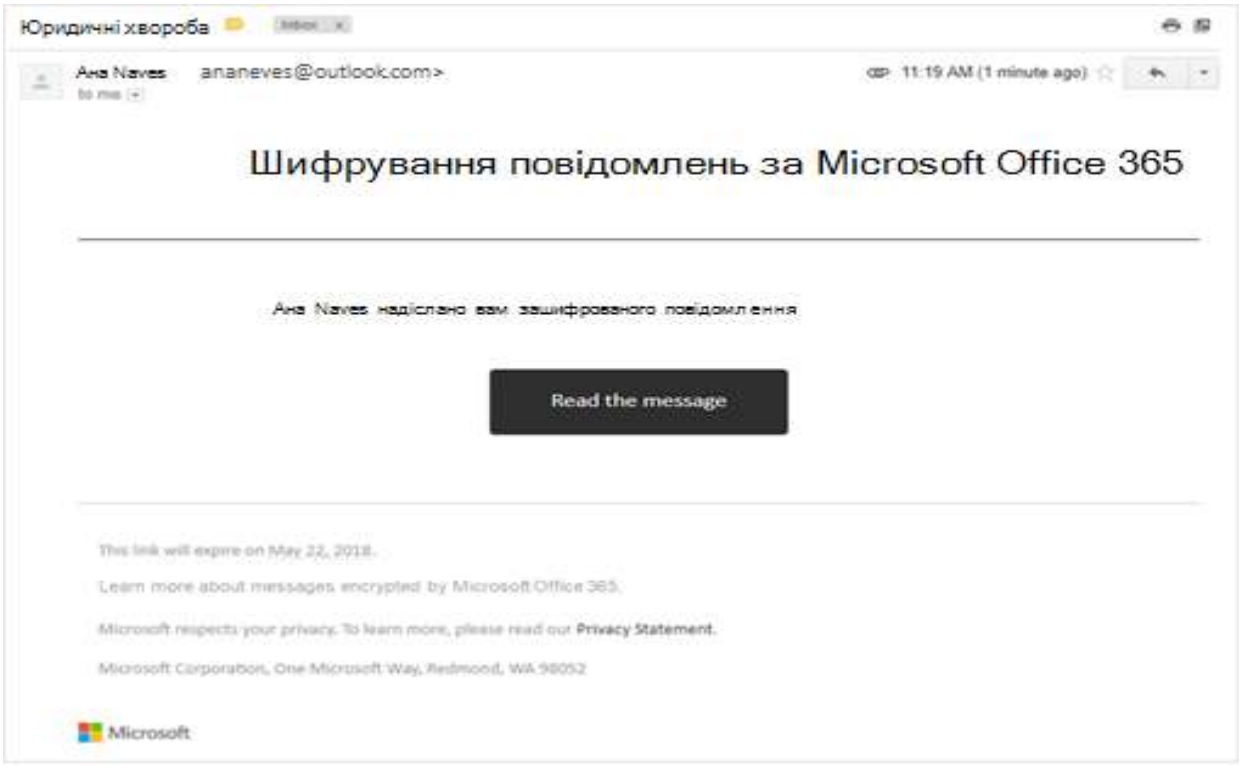

Рис 3.8. Повідомлення про вже отриманий лист на іншу електронну адресу

4. Наразі Outlook.com використовує протокол TLS, щоб зашифрувати з'єднання з отримувачем електронної пошти. Тобто за домогою протокола TLS повідомлення які я надсилаю залишаються не зашифрованими. Шифрується тільки з’єднання з отримувачем електронного листа.

Крім того, шифрування TLS забезпечує неможливість пересиланню повідомлення.

Повідомлення, зашифровані за допомогою Microsoft 365 залишаються в зашифрованому вигляді та залишаються в Microsoft 365 Персональний. Це допомагає захистити електронну пошту, коли її отримано.

5. Управління ключами – ефективне управління ключами є важливим аспектом забезпечення безпеки інформації. Kleopatra надає широкий спектр функцій для цього

6. Скасування ключів – У разі компрометації закритого ключа, його необхідно скасувати, щоб інші користувачі більше не могли його використовувати для шифрування повідомлень. Це можна зробити у Kleopatra, обравши відповідний ключ та вибравши опцію у функціоналі Kleopatra "Revoke".

На рисунку 3.9 зображено можливість скасування вже зареєстрованого ключа

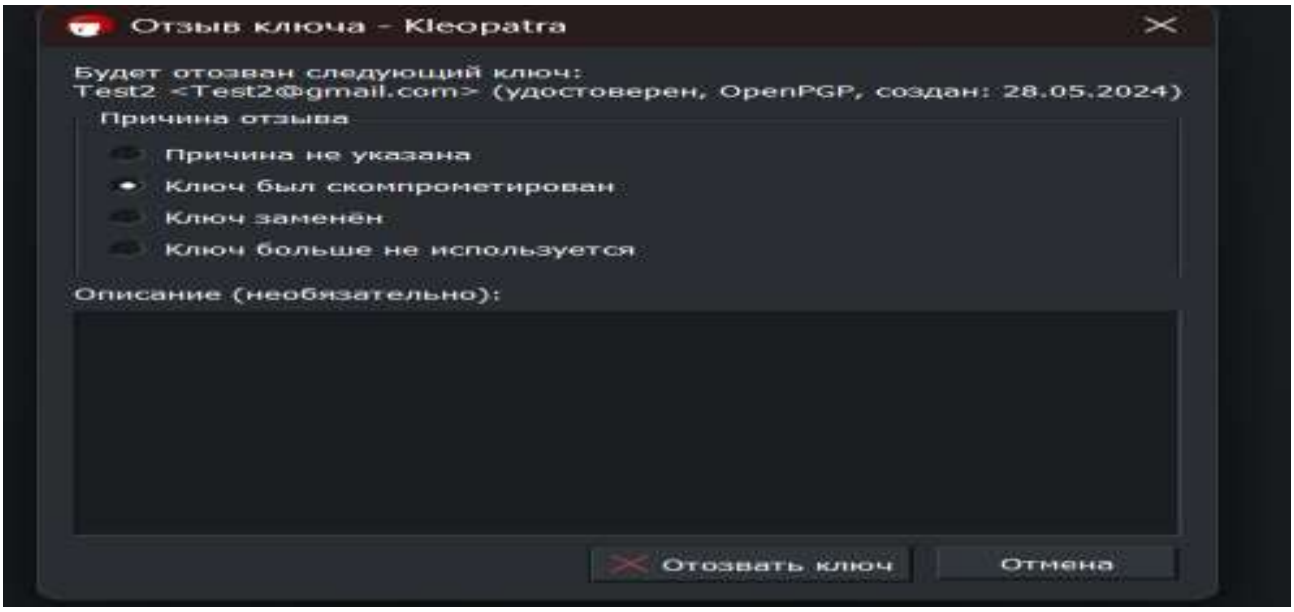

Рис 3.9. Можливість скасування вже зареєстрованого ключа

Поновлення ключів. У разі необхідності зміни ключової пари, можна створити новий ключ та оновити відкритий ключ у всіх користувачів, з якими ви обмінюєтеся інформацією.

3.5 Рекомендації на основі проведених експериментів

1. Чітке визначення мети і завдання збереження. Перед впровадженням РКІ необхідно чітко визначити мету і призначення захисту інформації. Це допоможе вибрати правильні алгоритми та протоколи шифрування та спланувати дії, необхідні для їх реалізації.

2. Виберіть надійний алгоритм шифрування-використовуйте лише найновіші та найнадійніші алгоритми шифрування. Алгоритми, використані в експерименті (RSA, AES тощо) повинні бути правильно налаштовані для забезпечення високого рівня безпеки.

3. Створення політики управління ключами - Створіть детальні політики для створення, зберігання, розповсюдження та відкликання ключів. Це включає вибір методу генерації безпечного ключа, використання безпечного сховища приватних ключів та періодичні оновлення ключів.

4. Автоматизація процесу перевірки сертифікатів - використовуйте автоматизовану систему для забезпечення надійності процесу перевірки сертифіката. Це знижує ризик помилок і забезпечує своєчасне оновлення списків відкликання сертифікатів (CRL).

5. Захист інфраструктури центру сертифікації (ЦС) - Вживайте заходів для захисту інфраструктури ЦС від можливих атак. Це включає використання апаратного модуля безпеки (HSM) для зберігання приватних ключів, періодичних перевірок безпеки та доступу до критичних систем.

6. Навчання персоналу та професійний розвиток - регулярно проводьте навчання персоналу щодо безпечного використання PKI та управління ключами. Це знижує ризик людських помилок і підвищує загальний рівень безпеки.

7. PKI та інтеграція існуючих систем - переконайтеся, що ваш PKI сумісний з вашою існуючою інформаційною системою. Це може вимагати розробки інтерфейсу користувача та конфігурації програмного забезпечення для забезпечення належної роботи всіх компонентів.

8. Регулярний моніторинг та аудит безпеки - впроваджуйте періодичні системи моніторингу та аудиту безпеки для виявлення та усунення потенційних вразливостей. Це дозволяє швидко реагувати на нові загрози і забезпечувати високий рівень захисту.

9. Шифрування та підпис даних за допомогою Gpg4Win - шифрування і підписання даних за допомогою Gpg4Win забезпечує конфіденційність і цілісність інформації. Інструменти, включені в gpg4win (Клеопатра, GnuPG тощо).Це полегшує реалізацію основних функцій PKI.

10. Оцінка та управління ризиками регулярно оцінюйте ризики, пов'язані з використанням ІПП, і розробляйте план їх мінімізації. Це включає виявлення

потенційних загроз, аналіз їх впливу та розробку відповідних контрзаходів.

ВИСНОВКИ

У цьому дослідженні ми провели комплексне дослідження існуючих систем інфраструктури відкритих ключів (PKI) і методів безпечного обміну інформацією. Основною метою дослідження є виявлення вразливостей і розробка рекомендацій щодо підвищення безпеки інформаційної системи.

На першому етапі дослідження було проведено детальний огляд науково-технічної літератури з метою виявлення основних проблем і загроз, пов’язаних із впровадженням і використанням відкритих ключів. Було виявлено, що основні проблеми включають складність керування ключами, вразливість до атак і необхідність забезпечення сумісності з різними системами та протоколами.

На другому етапі розроблено та випробувано прототип системи безпечного обміну інформацією на базі RKI. Проведені експерименти включають тести для виявлення вразливостей та оцінки ефективності запропонованих методів захисту. Зокрема, PKI інтегрується з Microsoft Outlook для безпечної доставки електронної пошти та демонструє практичну застосовність та ефективність розробленого рішення.

Результати дослідження показують, що використання PKI значно покращує рівень безпеки інформаційної системи, але вимагає ретельного управління ключами та розробки ефективних політик безпеки на основі отриманих результатів, а також впровадження сучасних інструментів статичного аналізу безпеки. Розробіть відповідну політику безпеки та заходи для покращення цілісності системи. Підготовлено пропозиції щодо вдосконалення системи.

Таким чином, проведене дослідження має практичне значення для підвищення рівня кібербезпеки організацій, особливо в умовах зростання кіберзагроз. Отримані результати та рекомендації можуть бути використані для вдосконалення існуючих систем PKI та розробки нових рішень для безпечного обміну інформацією

ПЕРЕЛІК ПОСИЛАНЬ

1. Public Key Infrastructure (PKI) URL: https://www.nist.gov/glossary-term/30091

2. Public Key Infrastructure (PKI)

3. Published under Glossary URL: https://www.enisa.europa.eu/topics/incident-response/glossary/public-key-infrastructure-pki?v2=1&tab=details

4. Allgemeine Informationen zur Verwaltungs-PKI URL: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Verwaltungs-PKI/AllgInformationen/allginformationen_node.html

5. MetaPKI, version 9.2.5 URL: https://cyber.gouv.fr/produits-certifies/metapki-version-925

6.URL:https://www.cse-cst.gc.ca/

7. Design and build a privately hosted Public Key Infrastructure URL: https://www.ncsc.gov.uk/collection/in-house-public-key-infrastructure/introduction-to-public-key-infrastructure/components-of-a-pki

8. OpenPGP & S/MIME URL:https://www.gpg4win.org/features.html

9. Encryption in Outlook URL:https://support.microsoft.com/uk-ua/office/%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D0%B2-outlook-17149eb8-a82e-405b-af5a-4fb89ce4a418

10. PKI Consortium Unveils the first PKI Maturity Model for feedback URL:https://pkic.org/2023/08/10/pki-consortium-unveils-the-first-pki-maturity-model-for-feedback/

11. EU Urged to Prepare for Quantum Cyber-Attacks - Infosecurity Magazine URL: infosecurity-magazine.com

12. #CRESTCon: Jon Geaber Discusses Latest Supply Chain Security Best Practices - Infosecurity Magazine URL: infosecurity-magazine.com

13. How Much is In-House PKI Management Truly Costing You? - Infosecurity Magazine URL:infosecurity-magazine.com

14. SEALSQ Enhances Security of Electric Vehicle (EV) Charging Stations with Semiconductors and a Decentralized Physical Infrastructure Networks (DePINs) URL: https://www.finanznachrichten.de/nachrichten-2024-05/62357495-sealsq-enhances-security-of-electric-vehicle-ev-charging-stations-with-semiconductors-and-a-decentralized-physical-infrastructure-networks-depins-399.htm

15. 10 Questions and Answers When Deploying a PKI URL: https://www.isaca.org/resources/news-and-trends/industry-news/2019/10-questions-and-answers-when-deploying-a-pki

16. 7 PKI and Cybersecurity Trends for 2024 URL: https://www.globalsign.com/en/blog/pki-cybersecurity-trends-2024

17. A Guidance Framework for Deploying PKI URL: https://www.gartner.com/en/documents/3641317

18. PKI-Based Passkeys Lead The Way For A Passwordless Future URL: https://securityboulevard.com/2024/05/pki-based-passkeys-lead-the-way-for-a-passwordless-future/

19. DC and PKI Market on Path to Significant Expansion, Aiming for USD 56,902.1 Million by 2033 URL: https://www.fmiblog.com/2024/05/24/dc-and-pki-market-size/

20. Key changes that will affect PKI in 2023 - 2024. URL: https://www.globalsign.com/ru-ru/company/news-events/news/be-prepared-major-pki-changes-beginning-autumn-through-2024

21. PKI Predictions for 2023: A Focus on Software Supply Chain Security, IoT device Standards, and More URL: https://www.keyfactor.com/blog/pki-predictions-for-2023-a-focus-on-software-supply-chain-security-iot-device-standards-and-more/