Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студента *Ляш Данила Вячеславовича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Підвищення рівня захищеності мультимедійного контенту в інформаційно-телекомунікаційній системі підприємства*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту ***Ляш Данилу Вячеславовичу*** **академічної групи** ***125м-21-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Підвищення рівня захищеності мультимедійного контенту в інформаційно-телекомунікаційній системі підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.22р. № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Підвищення рівня захищеності електронного документа, що містить потік відео, для віддалених та мобільних користувачів	20.10.2022
Розділ 2	Визначити проблеми безпеки та розробити алгоритм розгортання інфраструктури доставки відео контенту віддаленим та мобільним співробітникам підприємства; розробити алгоритми створення, зберігання, доставки та використання документа	16.11.2022
Розділ 3	Виконати розрахунок економічної ефективності створення та впровадження рекомендацій та алгоритму захисту інформації	05.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 05.09.2022 р.

Дата подання до екзаменаційної комісії: 12.12.2022 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 102 с., 11 рис., 5 табл., 4 додатка, 20 джерел.

Об'єкт розробки: інформаційно-комунікаційна система підприємства, що виробляє, зберігає і постачає мультимедійний контент віддаленим та мобільним співробітникам.

Мета роботи: підвищення рівня захищеності електронного документа, що містить потік відео, для віддалених та мобільних користувачів.

У спеціальній частині дана характеристика предмету досліджень; визначені проблеми безпеки та розроблено алгоритм розгортання інфраструктури доставки відео контенту віддаленим та мобільним співробітникам підприємства; розроблено алгоритми створення, зберігання, доставки та використання документа; розроблено архітектуру інформаційно-комунікаційної системи, що здатна реалізувати ці алгоритми.

У роботі наведені програмні елементи інфраструктури для реалізації алгоритмів та рекомендації щодо політики видачі, відкликання і відновлення сертифікатів для віддалених та мобільних користувачів; проведена експериментальна перевірка отриманих результатів.

В економічному розділі виконаний розрахунок економічної ефективності створення та впровадження рекомендацій та алгоритму захисту інформації.

Новизна: розроблено алгоритми створення інфраструктури інформаційної системи, яка підвищує рівень захищеності електронного документа, алгоритми створення, зберігання, доставки та використання документа співробітником поза контрольованої зони підприємства.

ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ, СИСТЕМА ЗАХИСТУ ІН-ФОРМАЦІЇ, ADOBE MEDIA SERVER, ВПРОВАДЖЕНЕ ВІДЕО, ПОЛІТИКА БЕЗПЕКИ, МОБІЛЬНИЙ КОРИСТУВАЧ, СЕРТИФІКАТ КОРИСТУВАЧА.

ABSTRACT

Explanatory note: 102 p., 11 pic., 5 tabl., 4 app., 20 sources.

Object of development: information and communication system of the enterprise that produces, stores and delivers multimedia content to remote and mobile employees.

Purpose: to increase the level of security of an electronic document containing a video stream for remote and mobile users.

In the special part, the characteristics of the subject of research are given; security problems are identified and an algorithm for deploying the infrastructure for delivering video content to remote and mobile employees of the enterprise is developed; algorithms for creating, storing, delivering and using the document are developed; the architecture of an information and communication system that can implement these algorithms is developed.

The paper presents the software elements of the infrastructure for the implementation of algorithms and recommendations on the policy of issuing, revoking and restoring certificates for remote and mobile users; experimental verification of the results obtained.

The economic section calculated the cost-effectiveness of the creation and implementation of recommendations and algorithm for information protection.

Novelty: algorithms for creating an information system infrastructure that increases the level of security of an electronic document, algorithms for creating, storing, delivering and using a document by an employee outside the controlled area of the enterprise.

PUBLIC KEY INFRASTRUCTURE, INFORMATION SECURITY SYSTEM, ADOBE MEDIA SERVER, EMBEDDED VIDEO, SECURITY POLICY, MOBILE USER, USER CERTIFICATE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AVAPI – Antivirus Application Programming Interface;

CA – Certificate Authority;

PKI – Public Key Infrastructure;

SUS – Software Update Services;

TLS – Transport Layer Security;

VPN – Віртуальна приватна мережа;

ЗЦ – Засвідчуваний центр;

КС – комп'ютерна система;

ІС – інформаційна система;

МК – мобільні користувачі;

МП – мобільні пристрої;

НД ТЗІ – нормативний документ технічного захисту інформації;

ОС – операційна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПЗС – політика застосування сертифікатів;

ПК – персональний комп'ютер;

ПЕОМ – персональна електронно-обчислювальна машина;

РС – робоча станція;

РЦ – реєстраційний центр;

САС – список анульованих сертифікатів;

СВС – список відкликаних сертифікатів.

ЗМІСТ

с.

ВСТУП

Перед сучасними підприємствами гостро стоять проблеми забезпечення інформаційної безпеки (ІБ). Це пов'язано з розвитком інформатизації підприємств, з постійно зростаючою конкуренцією й, як наслідок, вартістю інформації, що зростає. Інформація, яка складає комерційну таємницю, може використовуватися компаніями-конкурентами, шахраями, у своїх корисних цілях, наносячи при цьому значний матеріальний або моральний збиток репутації підприємства-власникові цієї інформації.

На сучасному підприємстві порушення ІБ спричиняє:

– порушення бізнес-процесів;
– втрату доходів;
– зниження довіри інвесторів і клієнтів;
– погіршення репутації;
– втрату або перекручування даних;
– правові наслідки.

Рішення питань організації захисту інформації на підприємстві шляхом впровадження сучасних захищених інформаційних технологій і надійних засобів захисту інформації є рішенням важливого практичного завдання керівництвом підприємства й відповідних підрозділів безпеки.

Адекватний рівень інформаційної безпеки в організації може бути забезпечений тільки на основі комплексного підходу, що припускає використання як програмно-технічних, так і організаційних мір захисту.

Питання забезпечення безпеки інформаційного простору в організації здобувають все більшу актуальність. З розвитком інформаційних технологій з'являється усе більше погроз функціонування інформаційної системи (ІС). У результаті це стимулює розвиток технічних і програмних засобів протидії порушенням безпеки інформаційного середовища.

На цей час питання забезпечення безпечного інформаційного простору виносяться в організаціях різного типу на перший план, а забезпечення конфіденційності та цілісності даних є невід'ємною частиною успішного функціонування організації в сфері своєї діяльності

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Основні компоненти PKI

Інфраструктура відкритих ключів являє собою комплексну систему, сервіси якої реалізуються та надаються з використанням технології відкритих ключів. Мета PKI полягає в управлінні ключами і сертифікатами, за допомогою якого корпорація може підтримувати надійну мережеву середу. PKI дозволяє використовувати сервіси шифрування і вироблення цифрового підпису узгоджено з широким колом додатків, що функціонують в середовищі відкритих ключів.

Основними компонентами ефективної PKI є:

– засвідчувальний центр;

– реєстраційний центр;

– репозиторій сертифікатів;

– архів сертифікатів;

– кінцеві суб'єкти (користувачі).

Взаємодію компонентів PKI ілюструє рисунок 1.1. У складі PKI повинні функціонувати підсистеми випуску та анулювання сертифікатів, створення резервних копій і відновлення ключів, виконання криптографічних операцій, управління життєвим циклом сертифікатів і ключів. Клієнтське програмне забезпечення користувачів повинно взаємодіяти з усіма цими підсистемами безпечним, узгодженим і надійним способом рішень [1], спрямованих на захист інформації й асоційованих ресурсів.

1.1.1 Засвідчувальний центр

Фундаментальна передумова криптографії з відкритими ключами полягала в тому, що два незнайомих суб'єкта повинні мати можливість безпечно зв'язува тися один з одним.

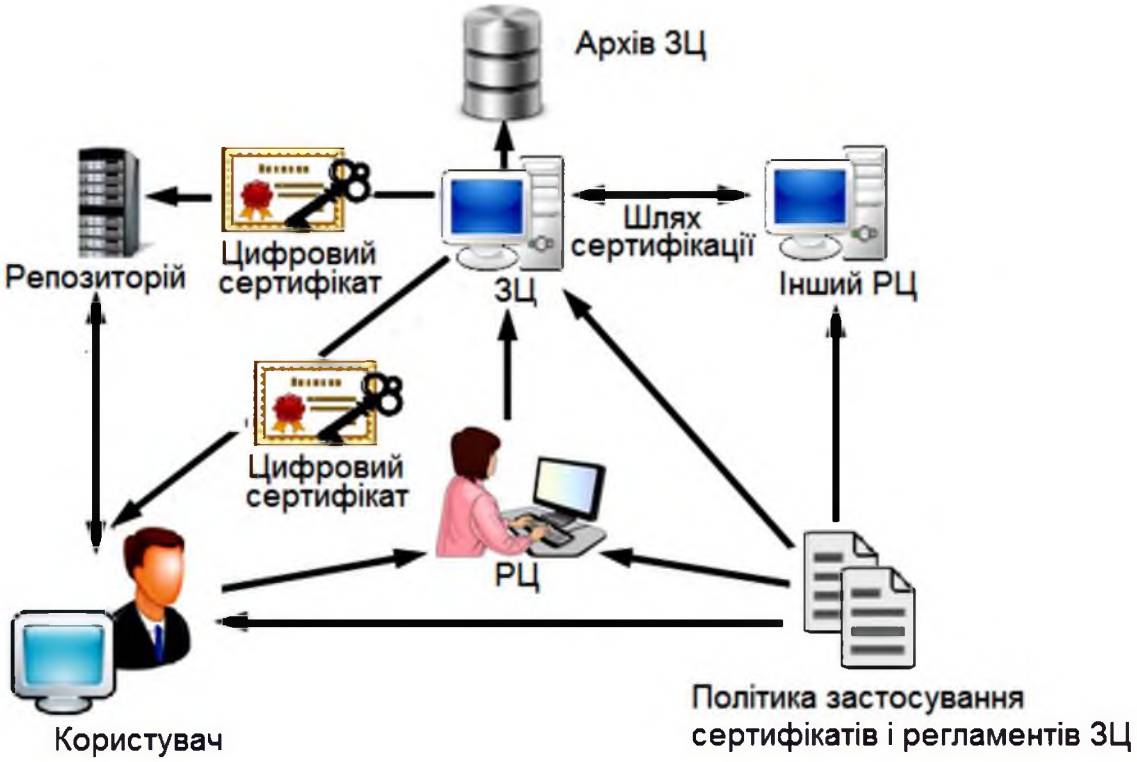

Рисунок 1.1 – Основні компоненти PKI

Наприклад, якщо користувач А бажає відправити конфіденційне повідомлення користувачу В, з яким він раніше не зустрічався, то для шифрування повідомлення він повинен мати можливість з'єднати будь-яким чином користувача В і його відкритий ключ. Для співтовариства потенційних користувачів, об'єднуючого сотні тисяч або мільйонів суб'єктів, найбільш практичним способом зв'язування відкритих ключів та їх власників є організація довірених центрів. Цим центрам велика частина співтовариства або, можливо, все співтовариство довіряє виконання функцій зв'язування ключів та ідентифікаційних даних (ідентичності) користувачів.

Такі довірені центри в термінології PKI називаються засвідчувальними (ЗЦ); вони сертифікують зв'язування пари ключів з ідентичністю, запевняючи цифровим підписом структуру даних, яка містить деяке уявлення ідентичності та відповідного відкритого ключа. Ця структура даних називається сертифікатом відкритого ключа (або просто сертифікатом). По суті сертифікат являє собою якесь зареєстроване посвідчення, яке зберігається у цифровому форматі і визнається спільнотою

користувачів PKI законним і надійним. Для запевнення електронного сертифіката використовується електронний цифровий підпис ЗЦ – у цьому сенсі засвідчувальний центр уподібнюється нотаріальній конторі, бо підтверджує дійсність сторін, що беруть участь в обміні електронними повідомленнями або документами.

Хоча ЗЦ не завжди входить до складу PKI (особливо невеликих інфраструктур або тих, які оперують у закритих середовищах, де користувачі можуть самі ефективно виконувати функції управління сертифікатами), він є критично важливим компонентом багатьох великомасштабних PKI. Безпосереднє використання відкритих ключів вимагає додаткового їх захисту та ідентифікації для встановлення зв'язку з секретним ключем. Без такого додаткового захисту зловмисник може видавати себе як за відправника підписаних даних, так і за одержувача зашифрованих даних, замінивши значення відкритого ключа або порушивши його ідентифікацію. Засвідчувальний центр об'єднує людей, процеси, програмні та апаратні засоби, задіяні для безпечного зв'язування імен користувачів і їх відкритих ключів. Засвідчувальний центр відомий суб'єктам PKI за двома атрибутам: назвою і відкритому ключу. ЗЦ включає своє ім'я в кожен випущений ним сертифікат і в список анульованих сертифікатів (CAC) і підписує їх за допомогою власного секретного ключа. Користувачі можуть легко ідентифікувати сертифікати на ім'я ЗЦ і переконатися в їх достовірності, використовуючи його відкритий ключ.

Засвідчувальний центр – головний керуючий компонент PKI – виконує такі основні функції:

– формує власний секретний ключ; якщо є головним ЗЦ, то видає і підписує свій сертифікат, званий самовиданим або самопідписаним;

– випускає (тобто створює і підписує) сертифікати відкритих ключів підлеглих засвідчувальних центрів та кінцевих суб'єктів PKI; може випускати крос -сертифікати, якщо пов'язаний відносинами довіри з іншими PKI;

– підтримує реєстр сертифікатів (базу всіх виданих сертифікатів) і формує списки відкликаних сертифікатів (CBC) з регулярністю, визначеною регламентом ЗЦ;

– публікує інформацію про статус сертифікатів та списків CAC.

При необхідності ЗЦ може делегувати деякі функції інших компонентів PKI. Випускаючи сертифікат відкритого ключа, ЗЦ тим самим підтверджує, що особа, зазначена у сертифікаті, володіє особистим ключем, який відповідає цьому відкритому ключу. Включаючи в сертифікат додаткову інформацію, ЗЦ підтверджує її приналежність цьому суб'єкту. Додаткова інформація може бути контактною (наприклад, адреса електронної пошти) або містити відомості про типи програм, які можуть працювати з даними сертифікатом. Коли суб'єктом сертифіката є інший ЗЦ, видавець підтверджує надійність випущених цим центром сертифікатів.

Дії ЗЦ обмежені політикою застосування сертифікатів (ПЗС), яка визначає призначення та зміст сертифікатів. ЗЦ виконує адекватний захист свого секретного ключа і відкрито публікує свою політику, щоб користувачі могли ознайомитися з призначенням і правилами використання сертифікатів. Ознайомившись з політикою застосування сертифікатів і вирішивши, що довіряють ЗЦ і його діловим операціями, користувачі можуть покладатися на сертифікати, випущені цим центром. Таким чином, у PKI засвідчувальні центри виступають як довірена третя сторона.

1.1.2 Реєстраційний центр та репозиторій сертифікатів

Реєстраційний центр (РЦ) є необов'язковим компонентом PKI. Зазвичай РЦ отримує від засвідчувального центру повноваження реєструвати користувачів, забезпечувати їх взаємодію з ЗЦ і перевіряти інформацію, яка заноситься в сертифікат. Сертифікат може містити інформацію, яка надана суб'єктом, що подає заявку на сертифікат і пред'являє документ (паспорт, водійські права, чекову книжку і т.п.) або третьою стороною (наприклад, кредитним агентством – про кредитний ліміт пластикової карти). Іноді у сертифікат включається інформація з відділу кадрів або дані, що характеризують повноваження суб'єкта в компанії (наприклад, право підпису документів певної категорії). РЦ агрегує цю інформацію і надає її ЗЦ.

ЗЦ може працювати з декількома реєстраційними центрами, в цьому випадку він підтримує список акредитованих реєстраційних центрів, тобто тих, які визнані надійними. ЗЦ видає сертифікат РЦ і відрізняє його по імені та відкритому ключу. РЦ виступає як об'єкт, підлеглий ЗЦ, і повинен адекватно захищати свій секретний ключ. Перевіряючи підпис РЦ на повідомленні або документі, ЗЦ покладається на надійність наданої РЦ інформації.

РЦ об'єднує комплекс програмного і апаратного забезпечення та людей, що працюють на ньому. У функції РЦ може входити генерація та архівування ключів, повідомлення про анулювання сертифікатів, публікація сертифікатів і СВС в каталозі LDAP (Lightweight Directory Access Protocol) [2]. Але РЦ не має повноважень випускати сертифікати та списки анульованих сертифікатів. Іноді ЗЦ сам виконує функції РЦ.

Репозиторій – спеціальний об'єкт інфраструктури відкритих ключів, база даних, в якій зберігається реєстр сертифікатів. Репозиторій значно спрощує управління системою і доступ до ресурсів. Він надає інформацію про статус сертифікатів, забезпечує зберігання і розповсюдження сертифікатів і СВС, управляє внесеннями змін до сертифікатів. До репозиторію пред'являються такі вимоги:

– простота і стандартність доступу;

– регулярність оновлення інформації;

– вбудована захищеність;

– простота управління;

– сумісність з іншими сховищами (необов'язкова вимога).

Репозиторій зазвичай розміщується на сервері каталогів, організованих згідно з міжнародним стандартом X.500 і його підмножиною. Більшість серверів каталогів і прикладне програмне забезпечення користувачів підтримують спрощений протокол доступу до каталогів LDAP. Такий уніфікований підхід дозволяє забезпечувати функціональну сумісність додатків PKI і дає можливість сторонам отримувати інформацію про статус сертифікатів для верифікації цифрових підписів.

На архів сертифікатів покладається функція довготривалого зберігання (від імені ЗЦ) та захисту інформації про всі видані сертифікати. Архів підтримує базу даних, використовувану при виникненні спорів з приводу надійності електронних цифрових підписів, якими в минулому завірялися документи. Архів підтверджує якість інформації на момент її отримання і забезпечує цілісність даних під час зберігання. Інформація, яку надає ЗЦ архіву, повинна бути достатньою для визначення статусу сертифікатів та їх видавця. Архів повинен бути захищений відповідними технічними засобами і процедурами.

Кінцеві суб'єкти PKI, або користувачі, діляться на дві категорії: власники сертифікатів та сторона, що довіряє. Вони використовують деякі сервіси та функції PKI, щоб отримати сертифікати або перевірити сертифікати інших суб'єктів. Власником сертифіката може бути фізична або юридична особа, додаток, сервер і т.д. Сторони, що довіряють, запитують і покладаються на інформацію про статус сертифікатів і відкриті ключі для підписів своїх партнерів по діловому спілкуванню.

1.1.3 Фізична топологія

Система PKI, крім виконання цілого ряду функцій − випуску сертифікатів, генерації ключів, управління безпекою, аутентифікації, відновлення даних, − повинна забезпечувати інтеграцію із зовнішніми системами. PKI необхідно взаємодіяти з безліччю найрізноманітніших систем і додатків − це і програмне забезпечення групової роботи, і електронна пошта, і системи управління доступом, і каталоги користувачів, і віртуальні приватні мережі, і різноманітні операційні системи, і служби безпеки, і web додатки, і широкий спектр корпоративних систем [3]. Рис. 2 ілюструє взаємодію користувачів з серверами PKI.

Функціональні компоненти PKI (ЗЦ, РЦ тощо) можуть бути реалізовані програмно і апаратно різними способами, наприклад, розташовуватися на одному або кількох серверах. Системи, що виконують функції засвідчувального та реєстраційного центрів, часто називають серверами сертифікатів та реєстрації відповідно.

1.1.3.1 Серверні компоненти PKI

Основними серверними компонентами PKI є сервер сертифікатів, сервер каталогів і сервер відновлення ключів, опціональними компонентами − сервер реєстрації, OCSP-сервер, обслуговуючий запити користувачів за онлайновим протоколом статусу сертифіката Online Certificate Status Protocol, і сервер проставлення міток часу.

На сервер сертифікатів покладаються функції випуску та управління сертифікатами, захищеного зберігання секретного ключа засвідчувального центру, підтримки життєвого циклу сертифікатів і ключів, відновлення даних, ведення контрольного журналу та реєстрації всіх операцій, засвідчених центром.

Сервер каталогів містить інформацію про сертифікати і атрибути суб'єктів сертифікатів відкритих ключів. Через протокол LDAP додатки стандартним чином звертаються до записів каталогів, наприклад, до адрес електронної пошти, номерів телефонів, повноважень та сертифікатів користувачів. Взаємодія користувачів з серверами PKI показана на рисунку 1.2.

Сервер каталогів повинен забезпечувати:

− мережеву аутентифікацію через IP- адреси або DNS-імена і аутентифікацію кінцевих суб'єктів за іменами і паролями або за сертифікатами відкритих ключів;

− управління доступом суб'єктів до інформації залежно від їх прав на виконання операцій читання, запису, знищення, пошуку або порівняння;

− конфіденційність (за допомогою протоколу SSL) і цілісність повідомлень для всіх видів зв'язку [4].

Рисунок 1.2 – Взаємодія користувачів з серверами PKI

Сервер відновлення ключів підтримує створення резервних копій і відновлення ключів шифрування кінцевих суб'єктів. Серед усіх компонентів PKI сервер відновлення ключів повинен бути найбільш захищений і забезпечувати сильну аутентифікацію адміністратора і користувачів, підтримку конфіденційності та цілісності повідомлень, безпечне зберігання всіх компонентів ключів.

PKI управляє ключами і сертифікатами, використовуваними для реалізації криптографічних операцій у web-браузерах, web-серверах, додатках електронної пошти, електронного обміну повідомленнями і даними, у додатках, що підтримують захищені мережні транзакції і сеанси зв'язку через World Wide Web або у віртуальних приватних мережах на базі протоколів S/MIME, SSL і IPsec, а також для запевнення цифровим підписом електронних документів або програмного коду [5]. Поряд з перерахованими вище додатками, PKI-сумісними можуть бути і корпоративні додатки, розроблені всередині організації.

Програми електронної пошти та обміну повідомленнями використовують пари ключів для шифрування повідомлень і файлів і засвідчення їх цифровими підписами. Системи електронного обміну даними підтримують транзакції, що

вимагають аутентифікації сторін, забезпечення конфіденційності і цілісності даних. Браузери та web-сервери використовують шифрування для аутентифікації, забезпечення конфіденційності, а також у додатках електронної комерції та онлайнового надання банківських послуг. Шифрування і аутентифікація застосовуються також для створення віртуальних приватних мереж (Virtual Private Networks – VPN) на основі мереж загального користування, для захисту комунікацій між сайтами або віддаленого доступу (клієнт-сервер). Засвідчення цифровим підписом програмних кодів і файлів дає можливість користувачам підтвердити джерело одержуваних по Інтернету програм і файлів і цілісність їх змісту, це важливо і для контролю вірусного зараження.

1.1.3.2 Клієнтське програмне забезпечення

Як відомо, технологія " клієнт-сервер" передбачає обслуговування клієнта тільки за його запитом, такий саме принцип справедливий і для PKI. Клієнтське програмне забезпечення (ПЗ) користувача повинно запитувати сервіси сертифікації та обробляти інформацію про анульовані сертифікати, розуміти історії ключів і відстежувати своєчасне оновлення або відновлення ключів, аналізувати необхідність проставлення міток часу. Клієнтському ПЗ необхідно розпізнавати ідентифікатори політики застосування сертифікатів, вчасно визначати статус сертифіката та правильно виконувати обробку шляху сертифікації.

Клієнтське ПЗ – істотний компонент повнофункціональної PKI. Важливо відзначити, що клієнтське ПЗ не є ні програмним забезпеченням програми, ні PKI-сумісним кодом, який розміщується всередині програмного забезпечення, подібного браузеру, або програми електронної пошти. Така архітектура фундаментально порушувала б концепцію PKI як інфраструктури, що узгоджено забезпечувала б безпеку всім додаткам і платформам, що її використовують. Навпаки, клієнтське ПЗ – це код, який існує поза будь-яких додатків і реалізує необхідну клієнтську сторону PKI. Додатки зв'язуються з клієнтським ПО через стандартні точки входу, їм не доводиться самостійно взаємодіяти з різними

серверами PKI. Таким чином, додатки використовують інфраструктуру, а не є частиною інфраструктури [6].

Компонент клієнтської сторони PKI може бути:

– відносно великим ("товстий" клієнт), виконуючим більшу частину операційної роботи PKI, у тому числі обробку шляхів сертифікації та валідацію;

– відносно невеликим ("тонкий" клієнт), що просто викликає зовнішні сервери для виконання PKI-функцій;

– Java-аплетом або аналогічним мобільним кодом, які за необхідністю завантажуються у режимі реального часу, а потім видаляються після завершення роботи, що викликла додатки (подібні web-браузеру);

– бібліотекою (Dynamically Linked Library – DLL), що динамічно підключається або аналогічною, яка розміщується резидентно на клієнтській платформі.

Існує багато можливостей реалізації та виклику клієнтського ПЗ, але головною вимогою є незалежність цього компонента від додатків, що використовують PKI.

Кожен компонент, щоб бути частиною PKI, повинен задовольняти критерієм безпеки. Цей критерій характеризує необхідний для цілей бізнесу рівень захищеності в межах допустимого рівня ризику [3]. Механізми безпеки, що забезпечують заданий рівень захищеності, зазвичай поділяють на механізми захисту апаратних засобів, комп'ютерної платформи, мережі і додатків. PKI-сумісні програми не дозволяють забезпечити повну безпеку корпоративної мережі і повинні бути доповнені іншими засобами захисту, наприклад, міжмережевими екранами, сервісами аутентіфіціруемих імен (службами імен) та суворим контролем адміністратора мережі.

1.2 Проектування і впровадження PKI

1.2.1 Проектування PKI

Ключовим аспектом розгортання PKI є вибір архітектури та проектування. PKI допускає гнучкість проектування незалежно від обраної технології. Етап проектування займає тривалий час, оскільки на цьому етапі має бути сформована

політика PKI і регламент, задана архітектура PKI, визначені апаратні і програмні засоби підтримки інфраструктури, обрані її компоненти, сервіси, режими роботи, протоколи та базові стандарти [7].

1.2.2 Формування правової політики PKI

Проектування PKI неможливо без розгляду правових аспектів її функціонування: ППС та регламенту, відповідальності, страхування та ін. Багато додатків PKI так чи інакше потребують правової підтримки, оскільки працюють з документами, завіреними цифровим підписом, або, наприклад, вимагають відновлення секретних ключів через процес депонування. Організації необхідно оцінити необхідність розробки власних юридичних документів; якщо в штаті є юристи, то ним може бути доручена розробка таких документів, в іншому випадку організація може запозичити політику відомого ЗЦ, який надає послуги аутсорсингу. Хоча цей спосіб і не забезпечує великої гнучкості у розробці юридичних документів замовника, але він простий і економічний. Проектування PKI повинно починатися зі збору еталонних політик і використання їх як шаблонів для розробки політики даної PKI [8]. Цифрові сертифікати базисом довіри при комунікації між сторонами. Політика має розроблятися з урахуванням усіх можливих проблем безпеки в даному середовищі, неадекватність і нечіткість політики веде до помилок при реалізації системи безпеки і може загрожувати цілісності всієї PKI. При формуванні політики необхідно орієнтуватися на стандарти в області PKI, що дозволяють забезпечити функціональну сумісність різних інфраструктури відкритих ключів.

1.2.3. Основні правові документи

Якщо організація вирішує самостійно сформувати правову політику, то повинна розробити такі документи:

– політику застосування сертифікатів та регламент ЗЦ;

– політику аутентифікації;

– політику конфіденційності (щодо відомостей, наданих користувачами в цілях аутентифікації).

Організація, яка експлуатує PKI, повинна укласти зі своїми внутрішніми і зовнішніми користувачами угоди, що закріплюють відповідальність сторін. Правове регулювання PKI передбачає укладання трьох видів угод:

– угода ЗЦ з РЦ;

– угода між кінцевими суб'єктами та РЦ;

– угода між передплатниками / кінцевими суб'єктами та ЗЦ (причому як кінцевий суб'єкта може виступати людина або пристрій).

1.2.4 Політика застосування сертифікатів та регламент ЗЦ

Як правило, архітектура PKI еволюціонує від поодиноких ізольованих засвідчувальних центрів, до більш складних форм, що встановлюють відносини довіри між різнорідними центрами. Ці відносини закріплюються сертифікатами. Кожній політиці застосування сертифікатів у своєму домені довіри присвоюється ідентифікатор об'єкта. Ідентифікатор політики – це унікальний зареєстрований ідентифікатор об'єкта (політики застосування сертифікатів), який аналізується при ухваленні рішення про довіру сертифікату і можливості його використання для певної мети. Ідентифікатори політик характеризують набір додатків, для яких придатний даний сертифікат. Сертифікат формату X.509 v.3 в доповненні certificatePolicy може містити один або більше ідентифікаторів політики залежно від числа політик застосування сертифікатів даного ЗЦ.

У тому випадку, якщо засвідчувальні центри випускають сертифікати відповідно до загальних політик, у доповненні certificatePolicy вказуються ідентифікатори цих політик, і немає необхідності використовувати інші доповнення та обмеження. Коли засвідчувальні центри працюють в різних доменах політики, то процедури узгодження політик стають більш складними [8] і потрібен ретельний аналіз відповідності політики кожного ЗЦ політикам інших засвідчувальних центрів. Відносини між політиками фіксуються в доповненні відповідності політик policyMappings. Це доповнення сертифіката дозволяє

засвідчувальним центрам задавати обмежений набір прийнятних політик і відхиляти сертифікати, випущені відповідно до неприйнятною для даного ЗЦ політикою. Крім того, функціональна сумісність доменів може досягатися у результаті укладення формальних угод між корпоративними доменами, охочими взаємодіяти відповідно з однією або декількома міждоменними політиками.

ПЗС забезпечує певний рівень довіри довіряє боку до сертифікату, виданому на умовах, описаних у цій політиці. Якщо, наприклад, організація передає функції ЗЦ на аутсорсинг і їй необхідний дуже надійний сертифікат, то вона може запросити від ЗЦ сертифікат високого рівня безпеки. У цьому випадку ЗЦ, перш ніж випустити сертифікат, буде виконувати величезну кількість перевірок. Іншою крайністю може бути видача сертифікатів, перед випуском яких виконується мінімальна перевірка, наприклад, правильності адреси електронної пошти майбутнього власника сертифіката.

Регламент описує процеси та процедури виконання ЗЦ операцій з сертифікатами. ППС характеризує надійність конкретного сертифіката, а регламент − надійність самого ЗЦ. ППС розробляється на досить тривалий термін і повинна задовольняти суворим вимогам, зазвичай вона викладається відповідно з форматом опису політики, який задає документ RFC 2527 Certificate Policy and Certification Practices Framework [9]. Цей документ містить стандартний ієрархічний набір положень, згрупований у 8 основних розділів і 185 підрозділів другого і третього рівнів. Примірний перелік положень служить орієнтиром при описі політики застосування сертифікатів та розробці регламенту ЗЦ і допомагає розробникам політики та регламенту не упустити важливі моменти.

1.2.5 Угода між ЗЦ і РЦ

Ця угода охоплює всі сторони відносин між ЗЦ і РЦ. Якщо ЗЦ і РЦ є компонентами моделі інсорсінга, то угода між ними спрощується і набуває статусу внутрішньої юридичної угоди між ЗЦ (зазвичай працюють під управлінням IT-штату) і РЦ (зазвичай функціонуючим під управлінням штату, що займається

адміністративною та операційною роботою). У будь-якому випадку ця угода обов'язково має проходити процедуру затвердження і містити такі положення:

– розмір компенсації РЦ засвідчувальному центру;

– фінансові гарантії безперервності функціонування ЗЦ;

– розмір компенсації ЗЦ сторонам-довірителям у разі випуску фальшивого сертифіката.

Угода між кінцевим суб'єктом і РЦ описує стосунки між користувачем сертифіката та РЦ тієї організації, яка випустила даний сертифікат. Угода повинна включати зобов'язання користувача:

– надавати правдиву інформацію, яка застосовується при випуску сертифіката;

– використовувати сертифікат відповідно до регламенту ЗЦ;

– звертатися із заявою про анулювання сертифікатів, якщо відповідні секретні ключі втрачені або скомпрометовані;

– припиняти використання всіх пар ключів (відкритий / секретний), термін дії яких закінчився, і не намагатися видати їх за діючі ключі.

Угоду між кінцевим суб'єктом і ЗЦ можна назвати угодою з стороною-довірителем. Воно містить такі положення:

– зобов'язання з боку довірителя перевіряти статус сертифіката перед його використанням, тобто переконуватися в тому, що сертифікат не прострочений і не анульований;

– зобов'язання сторони-довірителя використовувати сертифікат тільки за призначенням, тобто у цілях, встановлених ППС і регламентом ЗЦ;

– розміри компенсації РЦ або ЗЦ у разі заподіяння шкоди стороною-довірителем.

У моделях аутсорсингу всі ці угоди вже існують. У моделях інсорсінга потрібне ретельне складання таких угод.

1.2.6 Модель довіри та архітектура PKI

Фундаментом довіри PKI є надійні сертифікати відкритих ключів. Надійність сертифікатів відкритих ключів залежить від надійності центрів, що засвідчують підписи. Це допущення формує відносини довіри між різними сторонами-учасниками системи PKI і дозволяє кінцевим суб'єктам рахувати свої транзакції надійними.

Широкомасштабне розгортання PKI може втягувати в інфраструктуру багато засвідчувальних центрів, які випускають різноманітні сертифікати, створюючи множинні відносини довіри залежно від галузі застосування сертифікатів, типів використовуваних додатків, користувачів сертифікатів та видів ділових операцій. Для забезпечення функціональної сумісності компонентів PKI повинні бути визначені відносини між засвідчувальними центрами і задана архітектура PKI.

Відносини між взаємодіючими засвідчувальними центрами формують один або кілька шляхів сертифікації, у результаті верифікації яких приймається рішення про довіру до сертифіката учасника системи PKI. Організації, що розгортає PKI, необхідно визначити, як будувати шляхи сертифікації та підтверджувати надійність сертифікатів. У PKI закритої корпоративної системи всі власники сертифікатів працюють в одній організації, довіряють одному й тому ж ЗЦ, і шлях сертифікації будується на базі кореневого сертифікату цього центру.

При розгортанні PKI складної структури організація повинна визначити, чи буде вона довіряти сертифікатам користувачів і додатків тільки свого домену довіри чи інших доменів теж. Як уже згадувалося раніше, домен довіри, або домен політик, характеризується набором політик, відповідно до яких випускає сертифікати даний ЗЦ. Якщо приймається рішення про довіру обмеженого набору доменів, то повинні бути випущені крос-сертифікати і тим самим впроваджена в інші домени модель довіри даної організації. Якщо організація планує використовувати, наприклад, додаток глобальної захищеної електронної пошти, то буде потрібно більш складна структура крос-сертифікації всіх вхідних до складу PKI засвідчувальних центрів, здатна забезпечити побудову шляхів сертифікації між будь-якими двома власниками сертифікатів з будь-яких доменів довіри.

Модель довіри важлива для визначення відносин не тільки з зовнішніми сторонами, але й між учасниками PKI всередині організації. Так, деяким організаціям властива складна корпоративна ієрархія, тому в складі їх PKI можуть бути один головний ЗЦ і безліч підлеглих йому засвідчувальних центрів відділів і підрозділів, тобто модель довіри базуватиметься на традиційних для конкретної компанії правилах ведення бізнесу та відносинах між підрозділами. В інших випадках модель довіри PKI організації може будуватися на основі підписаних угод про політику застосування сертифікатів і відповідальності засвідчувальних центрів, пов'язаних відносинами довіри, – тоді мають бути розглянуті питання про ступінь відповідальності організації і користувачів сертифікатів в умовах крос-сертифікації.

На сьогодні великомасштабні корпоративні PKI базуються як на ієрархіях, так і на розподілених моделях довіри. Розподілена модель є більш гнучкою, оскільки дозволяє приєднувати і видаляти засвідчувальні центри, мінімально втручаючись в систему взаємодії з іншими засвідчувальними центрами, як усередині організації, так і зовні.

В ієрархічній PKI збиток від виходу з ладу конкретного ЗЦ (наприклад, через компрометації секретного ключа підпису ЗЦ) залежить від того, на якому рівні ієрархії він знаходиться. Чим ближче ЗЦ до верху ієрархії, тим більш руйнівні для всієї PKI наслідки його виходу з ладу. Очевидно, що для захисту більш високих рівнів ієрархії, особливо головного ЗЦ, необхідні додаткові заходи безпеки, наприклад, використання ключа підпису більшої довжини та / або зберігання матеріалу секретних ключів за допомогою апаратного модуля.

На даний час ієрархічна модель, як правило, використовується в web-середовищі, деякі корпоративні домени також адаптують її. Вважається, що ієрархічна модель є гарним механізмом контролю політики підлеглих засвідчувальних центрів, але насправді аналогічні можливості контролю існують і у крос-сертифікованих засвідчувальних центрів [6].

1.2.7 Вибір програмного продукту або постачальника сервісів PKI

При виборі програмного продукту повинні бути враховані можливості функціональної сумісності з іншими програмними продуктами / постачальниками послуг, легкість адаптації до відкритих стандартам, зручність розробки, гнучкість адміністрування, масштабованість і переносимість інсталяції [8]. Крім того, важливим критерієм є наявність інтерфейсів прикладного програмування (Application Program Interface − API) і підтримка поширених додатків (наприклад, віртуальних приватних мереж, управління доступом, захищеної електронної комерції, управління смарт-картами, сервісів каталогів, захищеної електронної пошти тощо).

1.2.8 Вибір основних засобів та обладнання

1.2.8.1 Апаратне і програмне забезпечення ЗЦ і РЦ

Успіх розгортання PKI в чому залежить від навколишнього і підтримуючої інфраструктури. Під інфраструктурою розуміються основні засоби, обладнання та персонал, необхідні для функціонування PKI.

При проектуванні PKI насамперед необхідно вибрати програмне і апаратне забезпечення ЗЦ і РЦ. Вибір більшою мірою залежить від постачальників програмних та апаратних засобів, а також від наміру організації створити власний ЗЦ або передати ці функції на аутсорсинг, але можна виділити деякі основні моменти, не пов'язані з постачальником або варіантом розгортання, які повинна гарантувати організація:

− апаратне забезпечення для захисту ключа підпису, призначеного для функцій РЦ, повинно відповідати вимогам принаймні мінімального рівня безпеки, який здатний забезпечити криптографічний модуль, що використовується усередині системи безпеки для захисту несекретної інформації;

– апаратне забезпечення захисту ключа підпису, призначеного для функцій ЗЦ, повинно відповідати вимогам більш високого рівня безпеки, який передбачає аутентифікацію суб'єктів на основі ролей;

– компоненти РЦ мають бути відокремлені від компонентів ЗЦ, знаходитися на різних серверах і, можливо, у різних центрах обробки даних. Оскільки в PKI постійно підтримується взаємодія багатьох користувачів з ЗЦ, фізичне розділення функцій ЗЦ і РЦ забезпечує захист від потенційних загроз з боку порушників усередині організації [6].

Сервери, призначені для PKI, повинні володіти високою продуктивністю, значними системними ресурсами і можливостями. При виборі серверів повинні оцінюватися точний обсяг оперативної пам'яті і дискового простору. Масштабованість системи PKI може забезпечити апаратне забезпечення типу SMP-систем (з симетричною мультипроцесорной обробкою).

Такі компоненти PKI, як ЗЦ, РЦ і репозиторій сертифікатів, теоретично можна розмістити на одному сервері, але для розподілу робочого навантаження і з метою безпеки рекомендується використовувати декілька серверів. Поділ функцій трохи знижує продуктивність системи, але підвищує захищеність компонентів і дозволяє розподілити обов'язки щодо їх підтримки між кількома підрозділами. Для захисту та зберігання секретного ключа ЗЦ, який найчастіше є об'єктом внутрішніх і зовнішніх атак, повинно використовуватися криптографічне апаратне забезпечення.

1.2.8.2 Периферійні пристрої

Для зберігання секретних ключів і сертифікатів кінцевих суб'єктів PKI доцільно використовувати такі портативні криптографічні пристрої, як смарт-карти або токени безпеки. У деяких середовищах необхідна багатофакторна аутентифікація, коли може знадобитися зберігання секретних ключів у периферійному модулі, а не на персональних комп'ютерах кінцевих користувачів – з цією метою іноді застосовують біометричні пристрої на додаток або до апаратних токенів, або смарт-карток, або замість них.

Компактність смарт-карт робить зручним їх використання у персональних і мережевих комп'ютерах, кіосках, зчитувачах жетонів доступу і т.д. залежно від конкретних PKI-додатків, але при цьому виникає необхідність у додаткових периферійних пристроях-зчитувачах смарт-карток. У ряді PKI-продуктів для зберігання ключів та сертифікатів реалізовані віртуальні смарт-карти, що імітують поведінку фізичних аналогів і забезпечують доступ користувачів без зчитувачів смарт-карток.

Не усі постачальники технології підтримують периферійні пристрої в однаковій мірі. Але якщо постачальники пропонують підтримку периферійних пристроїв, то вони повинні дотримуватися стандартних інтерфейсів прикладного програмування.

1.2.9 Безпека компонентів PKI

Багато організацій вважають, що PKI сама по собі створює захищену інфраструктуру. Це, звичайно, не так – крім PKI, необхідні такі засоби безпеки, як міжмережеві екрани, антивірусне програмне забезпечення і т.д. Усі критично важливі компоненти PKI мають бути адекватно захищені. Найбільш суворі вимоги пред'являються до фізичної безпеки систем ЗЦ, іноді потрібно у тій же мірі запобігати несанкціонованому доступу і до системи РЦ. Рекомендується фізично розділяти функції ЗЦ і РЦ за допомогою міжмережевих екранів.

Система РЦ має бути добре захищена фізично і логічно від атак зовнішніх і внутрішніх порушників. Оскільки доступ до сервера реєстрації повинен підтримуватися для великої групи користувачів (неважливо, внутрішніх або зовнішніх, для організації), доцільно його встановлювати в демілітаризованій зоні з системою виявлення вторгнень і можливостями контролю доступу. У зв'язку з тим, що реєстрація зазвичай виконується за допомогою web-сервера (провідні постачальники PKI забезпечують таку функціональність), організація повинна мати відповідний комп'ютер для розміщення на ньому web-сервера реєстрації.

Функції будь-якого РЦ повинні бути захищені зовнішніми пристроями типу смарт-карток, які вимагають двофакторної аутентифікації. З метою мінімізації

лазівок безпеки слід застосовувати пристрої безпеки – прості апаратні модулі з однією або двома функціями. Міжмережеві екрани і антивірусні засоби мають пристрої безпеки, які дозволяють швидко розгортати й приводити у стан готовності захищені системи.

Сервери PKI повинні розміщуватися в окремому закритому приміщенні, доступ до якого дозволений тільки обслуговуючому персоналу, ретельно контролюється і реєструється. Сервери мають бути підключені до джерела безперебійного живлення, а на час його відключення сервери повинні автоматично створювати резервні копії даних і завершувати роботу у штатному режимі. Сегмент мережі з серверами PKI повинен бути захищений принаймні за допомогою брандмауера, прозорого тільки для трафіку PKI.

Кожній організації слід визначити, де компоненти PKI розміщуватимуться і яким чином захищатимуться. Якщо організація не має коштів для адекватного захисту, то вона або повинна їх придбати, або вдатися до послуг довіреної третьої сторони. Очевидно, що придбання потребують значних капіталовкладень, тому варіант аутсорсінгу може у ряді випадків виявитися економічно більш вигідним.

1.2.10 Вибір персоналу для обслуговування PKI

Персонал, який обслуговує PKI, складає частину інфраструктури. Незважаючи на те, що криптографія з відкритими ключами з'явилася три десятиліття то-му, вона стала широко застосовуватися тільки недавно. Оскільки з точки зору реалізації та впровадження, ця технологія досить нова, поки явно не вистачає знаючих фахівців у цій області, більш того – їх важко залучити до роботи й утримати.

Для розгортання PKI необхідні не тільки адміністратори зі знанням технології цифрових сертифікатів, а й фахівці, здатні брати участь у розробці правових документів та угод, таких як політики застосування сертифікатів та угоди про крос-сертифікації (по суті, про функціональну сумісність між доменами PKI).

Більш того, важливо, щоб сама стратегія розгортання PKI була добре продумана і оформлена у вигляді документа, що також неможливо здійснити без

досвідченого і знаючого персоналу. Звичайно, у разі використання аутсорсінгової моделі ці функції можуть передаватися постачальнику послуг, але при самостійному розгортанні PKI організації необхідний кваліфікований персонал. Їй слід визначити кількість і рівень кваліфікації необхідного персоналу, які залежать від масштабу PKI, а також від того, якою мірою інфраструктура підтримується власними силами організації [6].

Для успішної реалізації проекту необхідні розробники програмного забезпечення, яке здатне виконати інтеграцію системи з діючими системами і PKI-сумісними програмами і налаштування системи на конкретні вимоги замовника. Підрозділ інформаційних технологій забезпечує роботу за наступними напрямками:

– інсталяція програмного продукту;

– конфігурація системи;

– системне адміністрування;

– теорія і практика PKI;

– криптографія з відкритими ключами;

– інформаційна безпека.

Персонал підрозділу підтримки операційної роботи системи повинен мати базові знання технології PKI, займатися постановкою завдань і експлуатацією системи. Співробітники підрозділу авторизації повинні мати уявлення про концепцію PKI і системне адміністрування. Підрозділ аудиту відповідає за правове забезпечення системи PKI (політика, відповідальність), його персонал має володіти знаннями в галузі права та інформаційної безпеки.

Одна з найбільш важких проблем розгортання та успішного використання PKI полягає у залученні до цієї роботи на постійній основі кваліфікованого штату професіоналів з цієї галузі. При наймі фахівця на роботу (постійно або тимчасово для консультацій) важливо враховувати:

– наявність сертифіката авторитетної організації, що підтверджує кваліфікацію у сфері IT-безпеки;

– підготовку в галузі інформаційної безпеки;

– досвід розробки програмного забезпечення (якщо необхідна інтеграція);

– можливість бути доступним або принаймні оперативно взаємодіяти з IT-штатом, щоб гарантувалася щоденна цілодобова робота PKI-системи.

При розгортанні PKI повинні бути визначені й оформлені у вигляді інструкцій посадові обов'язки персоналу, що займається управлінням та адмініструванням системи PKI, а при необхідності організовано додаткове навчання службовців, що забезпечують безпеку системи. Залежно від масштабу PKI і конкретних умов допускається суміщення посад. У список посад, необхідних для підтримки системи PKI, входять:

– системний адміністратор;

– системний оператор;

– адміністратор ЗЦ;

– адміністратор РЦ;

– адміністратор каталогу;

– фахівець служби допомоги;

– менеджер з політики безпеки;

– аудитор безпеки або головний адміністратор.

Системний адміністратор відповідає за функціонування системи безпеки в цілому і звичайно залучається до роботи з розгортання PKI на самих ранніх стадіях. Особливо важлива участь системного адміністратора в складанні плану проекту, бо що він здатний оцінити, скільки часу потребують різні види активності системи. Якщо організація планує роботу свого власного ЗЦ, то системний адміністратор відповідає за підбір, інсталяцію та конфігурування необхідного програмного забезпечення, а також за його підтримку і внесення змін. Крім того, обов'язки системного адміністратора полягають у привласненні повноважень і профілів користувачам системи і підтримці паролів.

Системний оператор повинен стежити за операційною роботою системи PKI, реагувати на помилки та дотримуватися встановлених регламентом процедур. До додаткових функцій операторів можна віднести відновлення

колишнього стану системи та підтримку електронних документів. Залежно від масштабу PKI до щоденної роботи залучаються від одного до декількох операторів.

Адміністратор ЗЦ відповідає за підтримку всіх функцій засвідчувального центру, генерацію ключів, випуск і підписання сертифікатів, а також обробку запитів на крос-сертифікацію й авторизацію послуг з відновлення ключів. Якщо до складу PKI входить реєстраційний центр, то на його адміністратора покладаються обов'язки обробки заявок на сертифікати та прийняття рішення про видачу сертифіката заявнику.

Адміністратор каталогу відповідає за створення структури, організацію та підтримку каталогу (LDAP), що містить інформацію про сертифікати, а також управління правами доступу до каталогу внутрішніх і зовнішніх для PKI користувачів. Адміністратор каталогу забезпечує реалізацію угоди про використовувані у каталозі імена відповідно до вимог промислових або корпоративних стандартів, а також зберігання даних аутентифікації і сертифікації у репозиторії.

Фахівці служби допомоги мають реагувати на звернення клієнтів системи, керуючись відповідними документами, що описують процедури обслуговування користувачів.

Для підтримки захищеного та ефективного функціонування PKI повинна регулярно переглядатися політика безпеки, за її оновлення відповідає менеджер з політики безпеки.

Функції аудиту системи у цілому та підготовки звітів для керівництва покладаються на аудитора безпеки або головного адміністратора. Аудитор безпеки повинен мати спеціальну підготовку у галузі інформаційної безпеки та криптографії і відповідати за реалізацію корпоративної політики безпеки, у тому числі політики застосування сертифікатів, регламенту та політики управління ключами, і документальне оформлення всіх політик і процедур. На аудитора безпеки покладається відповідальність за розробку та удосконалення процедур управління та адміністрування системою безпеки, процедур відновлення колишнього стану системи та відновлення після аварії, а також процедур, яких

повинні дотримуватися треті сторони при їх обслуговуванні PKI-системою. Аудитор зобов'язаний виконувати регулярні та незаплановані перевірки контрольних журналів і відстежувати відповідність усіх компонентів і процедур системи безпеки PKI промисловим та корпоративним стандартам.

У процесі розгортання PKI також можуть знадобитися послуги досвідчених консультантів та юрисконсультів для розробки та/або аналізу ППС і регламенту ЗЦ. Витрати на оплату праці персоналу можуть істотно вплинути на сукупну вартість володіння PKI і повинні розглядатися поряд з іншими витратними факторами.

1.2.11 Завершення етапу проектування

Після документального оформлення політики застосування сертифікатів, вибору програмного продукту або постачальника послуг, апаратних засобів підтримки PKI і фізичного середовища, формулювання вимог з управління та адміністрування системою, повинен бути розроблений регламент ЗЦ. На цьому ж кроці визначаються процедури оперування та управління, які необхідні для перевірки ефективності системи безпеки на базі PKI, і розробляється методика супроводу та підтримки готової системи [7].

1.3 Проблеми реалізації PKI

Хоча варіанти реалізації PKI можуть відрізнятися компонентами і деталями, існують деякі головні критерії прийняття рішень:

– призначення PKI;

– час, необхідний для підготовки до функціонування PKI;

– можливість контролю середовища користувачів;

– експертиза під час і після розгортання;

– фінансові можливості.

Трьома ключовими областями реалізації PKI є:

– підготовка системи PKI до роботи;

– управління сертифікатами і ключами;

– реагування на інциденти під час функціонування PKI.

1.3.1 Підготовка системи PKI до роботи

На етапі підготовки системи PKI до роботи виконується установка програмного й апаратного забезпечення ЗЦ/РЦ, клієнтських коштів користувачів, а також реєстрація та ідентифікація користувачів для отримання сертифікатів.

Підготовка системи PKI до роботи залежить від обраної моделі розгортання: аутсорсінгу або інсорсінгу. Як відомо, у моделі аутсорсінгу головні функції ЗЦ контролюються третьою довіреної стороною. Найпростіші аутсорсінгові сервіси забезпечують доступ до всіх функцій управління життєвим циклом сертифікатів через web-сторінку та Інтернет-з'єднання, не вимагаючи від організації установки спеціального апаратного та програмного забезпечення.

У моделі інсорсінгу функції PKI виконуються під контролем організації, а підлеглі кореневого ЗЦ засвідчують центри та сертифікати, створені всередині корпоративного домена. Це забезпечує велику гнучкість, але пред'являє більш суворі вимоги до рівня безпеки процедур випуску та зберігання кореневого сертифікату.

Частиною процесу підготовки до роботи є реєстрація користувачів для отримання сертифікатів. Організація повинна вирішити, яка інформація достатня для аутентифікації користувача. Існують два основні методи аутентифікації:

– на основі персональної інформації (відомої тільки РЦ і користувачеві);

– через схему парольного коду, коли секретний код генерується до початку реєстрації і видається суб'єкту для виконання процедури реєстрації.

У великих організаціях виникає проблема реєстрації великої кількості суб'єктів. Кожен користувач може проходити реєстрацію 2-3 рази на рік, якщо йому необхідно мати кілька сертифікатів. Реєстрація вручну, коли кожен запит потрапляє до черги до адміністратора РЦ, а потім приймається або відкидається, забезпечує більший контроль, але досить трудомістка. Автоматизація процедур порівняння інформації, що надається користувачем у процесі реєстрації, та інформації, що зберігається у надійній базі даних, спрощує реєстрацію, тому для

масштабних проектів рекомендується автоматична реєстрація, хоча вона є менш керованою.

Процес реєстрації кінцевих суб'єктів включає два важливих кроки: обробку запиту на сертифікат і аутентифікацію суб'єкту. Для встановлення ідентичності суб'єкта використовуються звичайні питання про ім'я та адресу заявника. Вимоги до персональних даних заявника залежать від типу запитуваного сертифіката. В одних випадках для прийняття рішення про випуск сертифіката відкритого ключа достатньо інформації, надісланої суб'єктом електронною поштою, в інших випадках, коли власник сертифіката наділяється особливими повноваженнями, необхідна особиста присутність заявника і пред'явлення документів, що підтверджують його особу. Якщо ЗЦ створюється для службовців однієї організації, то від заявника може знадобитися тільки обґрунтування свого запиту на сертифікат, бо персональні дані всіх службовців є у відділі кадрів.

Аутентифікація суб'єкта сертифіката передбачає підтвердження персональних даних, що надаються заявником при зверненні до реєстраційного центру чи засвідчуються центром із запитом про видачу сертифіката. Ретельність перевірки ідентичності суб'єкта визначається типом запитуваного сертифіката. Зазвичай взаємодія між заявником і центром будується на основі угоди з передплатником,

закріпленого регламентом ЗЦ. Угода може містити пункти, що передбачають включення до ціни сертифіката або надання за окрему плату великих гарантій захисту та додаткового страхування збитку.

1.3.2 Управління сертифікатами і ключами

Управління сертифікатами і ключами − істотний аспект успішної реалізації PKI. Проблеми управління особливо актуальні для масштабних PKI з великою кількістю власників сертифікатів і користувачів [10]. До найбільш важливих проблем управління сертифікатами і ключами відносяться:

− вибір способу управління списками CAC;

− порядок поновлення сертифікатів;

– пошук інформації про статус сертифікатів;

– вибір способу генерації пари ключів;

– порядок поновлення ключів;

– вибір способу зберігання секретних ключів.

1.3.3 Вибір способу управління списками CAC

Для функціонування PKI критично важливо правильне управління списками CAC: саме вони забезпечують перевірку статусу використовуваного сертифіката, оскільки дата закінчення терміну дії, що вказується у сертифікаті, не може служити підтвердженням того, що даний сертифікат є дійсним.

У PKI може підтримуватися один центральний сервіс каталогів, що надає інформацію про статус сертифікатів, або кілька пунктів розповсюдження сертифікатів та списків CAC. Організація, що використовує PKI, може відокремити сервіси аутентифікації від сервісів управління сертифікатами – у цьому випадку вона, діючи як РЦ, самостійно виконує аутентифікацію користувачів і підтримує захищеність бази даних про своїх службовців, а частина функцій PKI з видачі сертифікатів, оновленню ключів і поновленню сертифікатів передає на аутсорсінг тре-

тій стороні. У цьому випадку відбувається передача відповідальності за виконання цих функцій PKI, і також організація мінімізує свою активність з адміністрування інфраструктури.

1.3.4 Порядок поновлення сертифікатів

Оскільки більшість сертифікатів діють протягом обмеженого періоду часу, система PKI повинна підтримувати оновлення сертифікатів. Сертифікат зазвичай оновлюється одним із двох способів:

– випускається сертифікат з новим терміном дії, але з тими ж відкритим ключем і реєстраційною інформацією, які містилися у старому сертифікаті;

– випускається сертифікат з новим терміном дії і новим відкритим ключем, але з тією ж реєстраційною інформацією, яка містилася у старому сертифікаті.

Стратегії оновлення повинні будуватися таким чином, щоб забезпечити безперервну роботу користувачів. Зазвичай сертифікати випускаються з періодом перекриття термінів їх дії від 4 до 6 тижнів, щоб забезпечити плавний перехід від старого сертифіката до нового. Своєчасність поновлення сертифікатів часто залежить від підготовки і кваліфікації користувачів. Хоча в більшості PKI-систем існує режим налаштування на автоматичне оновлення сертифікатів після закінчення строку їх дії, але часто сертифікати оновлюються за запитами користувачів. Тому для відновлення сертифіката користувачеві необхідно у певний момент часу підтвердити ЗЦ свої ідентифікаційні дані і відправити відповідний запит.

Деяку проблему представляє оновлення подвійної пари ключів, коли користувач для роботи з однією програмою застосовує два сертифікати: сертифікат ключа шифрування і сертифікат ключа підпису. У цьому випадку на момент оновлення користувач повинен отримати два нових сертифікати. При переході від старих сертифікатів до нових кількість сертифікатів, якими оперує користувач, може збільшуватися до чотирьох (для однієї програми), у цей період одночасно діють пара сертифікатів із терміном дії, що закінчуються, і пара нових сертифікатів. Якщо враховувати, що користувач може працювати з декількома додатками, стає ясно, що кількість сертифікатів, які необхідно оновлювати, постійно зростає. На жаль, немає простого способу розв'язання цієї проблеми, крім навчання користувачів, технічної підтримки та документування процесів оновлення ключів.

Ряд постачальників PKI пропонують клієнтське програмне забезпечення з функціями управління процесом оновлення сертифікатів. У цьому випадку клієнтське програмне забезпечення формує і відправляє ЗЦ підписаний запит (відповідний тому сертифікату, який оновлюється). Цифровий підпис на запиті верифікується за допомогою відкритого ключа, що міститься у копії сертифіката відправника запиту. Якщо підпис підтверджується, то вважається, що користувач, на правивший запит, є законним власником вихідного сертифіката. У цьому випадку ЗЦ випускає новий сертифікат з тими ж саме даними користувача і відкритим ключем, але новим терміном дії.

1.3.5 Пошук інформації про статус сертифікатів

Під час роботи в системі PKI користувачам доводиться ідентифікувати інших користувачів і використовувати їх сертифікати. Більшість організацій зберігають сертифікати у загальнодоступному каталозі, у репозиторії. Користувачі звертаються із запитами до сховища, щоб знайти сертифікати, що належать певній людині або пристрою. Проблема, пов'язана з пошуком, полягає у тому, що коли доступ до каталогу може отримати кожен бажаючий, то інформація про користувачів, розміщена у каталозі, також доступна кожному. Очевидно, що багато організацій не прагнуть розкривати інформацію про своїх службовців.

Додаток Microsoft Outlook автоматично прикріплює сертифікат користувача до повідомлення із завіреним цифровим підписом. Це дозволяє одержувачеві перевіряти електронну пошту, маючи необхідні сертифікати і не виконуючи жодної зайвої дії. Надіслані поштою сертифікати інших користувачів потім зберігаються одержувачем локально і використовуються для майбутніх перевірок. Поки не всі програми надають подібний сервіс, тому сторони-довірителі змушені виконувати пошук інформації про статус сертифікатів самостійно.

1.3.6 Вибір способу генерації пари ключів

Генерація ключів може здійснюватися централізовано (ЗЦ або за його дорученням РЦ) або індивідуально (кінцевим суб'єктом). У більшості випадків пари ключів створюються кінцевими суб'єктами, які повинні мати програмні або апаратні засоби для створення надійних ключів. Цей спосіб дозволяє суб'єкту забезпечити більшу конфіденційність у відносинах з іншими сторонами, оскільки власник сам зберігає секретний ключ і ніколи його не пред'являє. На жаль, більшість користувачів не вживає достатніх заходів для захисту своїх секретних ключів, збільшуючи ризик їх компрометації.

До переваг централізованої генерації можна віднести швидкість створення ключів, використання спеціалізованих засобів генерації високоякісних ключів, контроль відповідності алгоритмів генерації встановленим стандартам, а також

зберігання резервних копій секретних ключів на випадок їх втрати користувачами. Якщо ключі генеруються централізовано, то політикою безпеки PKI мають бути передбачені засоби їх захищеного транспортування до інших компонентів PKI, а також гарантії того, що паралельно не здійснюватиметься несанкціоноване копіювання секретних ключів.

1.3.7 Порядок поновлення ключів

Політикою PKI повинен бути визначений порядок дій у разі поновлення пар ключів. Пари ключів можуть оновлюватися вручну й автоматично. При ручному оновленні відповідальність за своєчасне формування запиту про оновлення покладається на кінцевого суб'єкта, який повинен пам'ятати дату закінчення терміну дії сертифіката. Якщо запит про оновлення не буде вчасно направлений в ЗЦ, суб'єкт позбудеться сервісів PKI. При автоматичному оновленні система PKI сама відслідковує дату закінчення терміну дії сертифіката та ініціює запит про оновлення ключа відповідного ЗЦ.

Політика безпеки організації може передбачати, наприклад, щоб усі документи, зашифровані старими ключами, розшифровувалися і знову зашифровувалися за допомогою нових ключів або щоб будь-які документи, підписані раніше старим ключем, перепідписувалися за допомогою нового ключа. Раціональна політика управління ключами допускає п'ятирічний (і навіть більше) термін дії пари ключів, але може обмежувати період дії ключів шифрування строго конфіденційних даних кількома місяцями. Іноді конкретний термін дії ключів не встановлюється, а ключі замінюються у разі потреби, наприклад, при втраті секретного ключа. У цьому випадку слід повторно оцінювати рівень захищеності використовуваної пари ключів після закінчення п'яти років або при появі нових криптографічних алгоритмів чи інших технологічних досягнень.

1.3.8 Вибір способу зберігання секретних ключів

При проектуванні PKI повинен бути вибраний спосіб зберігання криптографічних ключів − він, як правило, залежить від специфіки діяльності

конкретної організації. Згідно з [11] для обмеження доступу до секретних ключів застосовуються такі механізми:

– захист за допомогою пароля. Пароль або PIN -код використовуються для шифрування секретного ключа, який зберігається на локальному жорсткому диску. Цей метод вважається найменш безпечним, так як проблема доступу до ключа вирішується підбором пароля.

– карти PCMCIA. Ключ захищено зберігається на карті з мікрочіпом, але при введенні в систему "залишає" карту, отже, стає вразливим для розкрадання;

– пристрої зберігання секрету. Секретний ключ зберігається у зашифрованому вигляді у спеціальному пристрої і витягується тільки за допомогою одноразового коду доступу, наданого пристроєм. Цей метод безпечніший, ніж згадані вище, але вимагає доступності пристроїв зберігання кінцевого суб'єкту і не виключає втрати пристрою;

– біометричні засоби. Ключ захищається біометричними засобами аутентифікації власника ключа, при цьому забезпечується той саме рівень захисту, що й у попередньому випадку, але суб'єкт позбавляється необхідності мати при собі пристрій зберігання секрету;

– смарт-карти. Ключ зберігається на смарт-карті з чіпом, який забезпечує можливість виконувати операції шифрування і цифрового підпису. Ключ ніколи не покидає карту, тому ризик його компрометації низький. Однак власник ключа повинен носити смарт-карту з собою і піклуватися про її збереження. При втраті смарт-карти зашифровані за допомогою секретного ключа дані можуть виявитися невідновними.

1.3.9 Реагування на інциденти під час функціонування PKI

Більшість систем PKI не потребують якоїсь особливої підтримки, що вимагає великих технічних зусиль. Найбільш важлива роль відведена адміністраторам ЗЦ і РЦ. Підтримка нормального функціонування системи PKI потребує планування і регулярного аудиту безпеки апаратних і програмних засобів, керуючих системою. Незважаючи на заходи безпеки і аудит, системи PKI повинні мати адекватні засоби

захисту і підготовлений персонал для реагування на виявлені інциденти. Системи PKI мають бути доступні щодня у цілодобовому режимі, бо вони не тільки випускають сертифікати, а й беруть участь в онлайновій валідації сертифікатів. Найбільш критичними є анулювання кореневого сертифіката або інциденти порушення безпеки кореневого ключа ЗЦ, оскільки саме на ньому базується довіра суб'єктів PKI.

Для аутсорсінгових систем PKI це не є проблемою, бо про безпеку кореневого ключа піклується сторонній ЗЦ. У інсорсінгових системах PKI повинні підтримуватися надзвичайні заходи безпеки, що гарантують захист кореневого сертифіката, або робитися негайні кроки у разі компрометації кореневого ключа (анулювання всіх сертифікатів і повторний їх випуск за допомогою нового кореневого ключа).

1.3.10 Анулювання цифрових сертифікатів

Анулювання цифрових сертифікатів по суті схоже на анулювання громадянських паспортів. Бувають випадки, коли громадянин продовжує користуватися анульованим паспортом, й іноді йому навіть вдається пройти паспортний контроль на кордоні та виїхати з країни, якщо офіцер прикордонної служби припускається помилки при перевірці списку номерів анульованих паспортів. Що стосується сертифікатів, то інколи їх буває необхідно анулювати перш, ніж закінчиться термін їх дії. У цих випадках РЦ повинен повідомити ЗЦ про те, які сертифікати повинні мають бути анульовані.

У PKI є кілька можливостей виявлення та перевірки анульованих сертифікатів:

– валідація у режимі реального часу (за протоколом OCSP), яка необхідна при виконанні найбільш важливих транзакцій, наприклад фінансових;

– перевірка з запізненням, яка підходить для менш важливих транзакцій, таких як доступ до корпоративних порталів інтрамережі або екстрамережі (у цьому випадку CAC оновлюється протягом доби).

1.3.11 Порядок обробки запитів про анулювання

При формуванні політики та розгортанні PKI має бути встановлено порядок обробки запитів про анулювання і позначено коло осіб, які мають право звертатися з такими запитами. Зазвичай запит про анулювання сертифіката направляє його власник при втраті або компрометації секретного ключа. У деяких випадках із запитом про анулювання може звертатися не власник сертифіката, а інша особа. Наприклад, при звільненні службовця з компанії запит про анулювання його сертифіката може надійти від начальника підрозділу, в якому працював службовець. Крім того, запит про анулювання сертифіката може бути спрямований від ЗЦ, який випустив сертифікат, або від іншого ЗЦ з мережі крос-сертифікації, якщо виявляється, що власник сертифіката порушив вимоги політики безпеки або регламенту.

Після отримання запиту про анулювання сертифіката та аутентифікації особи, який направив запит, ЗЦ вносить зміни в CAC. Для управління сертифікатами у відносно невеликий PKI зазвичай застосовується пряма публікація анульованих сертифікатів в CAC і забезпечується доступ до нього додатків, що перевіряють статус сертифіката. Деякі програми зберігають у пам'яті комп'ютера останню версію списку, що дозволяє їм працювати в автономному режимі і підвищує їх продуктивність. Збільшення масштабу PKI і необхідність керувати сертифікатами з декількох доменів породжує проблеми зберігання й обробки великих списків анульованих сертифікатів. У процесі вироблення політики і проектування PKI повинні бути враховані ці обставини, а також обрано спосіб публікації, пункти розповсюдження і тип CAC.

1.3.12 Вибір способу публікації CAC

Вибираючи спосіб публікації CAC, організація повинна оцінити переваги та недоліки кожного з трьох можливих способів (публікація з опитуванням наявності змін, примусова розсилка змін і онлайнова верифікація), характер PKI-транзакцій і ступінь операційного ризику.

Публікація САС з опитуванням наявності змін ("pull") виконується у певні заплановані моменти часу і може привести до ситуації, коли анульований сертифікат деякий час не включається до САС, а користувачі продовжують покладатися на нього. Даний спосіб придатний у більшості випадків, але піддає серйозному ризику клієнтів, які використовують критично важливі для ведення бізнесу додатки, навіть якщо плановані поновлення виконуються досить часто.

Спосіб примусової розсилки змін ("push") САС підходить для PKI невеликих організацій, що використовують обмежену кількість PKI-додатків, і не підходить для PKI, обслуговуючих велику спільноту користувачів і численні додатки. Поширення списку цим способом вимагає вирішення проблем розпізнавання додатків, яким розсилається інформація про оновлення САС, синхронізації випуску списку, а також відкладеного отримання зазначеної інформації додатками, якщо останні були недоступні на момент розсилки.

Важливою перевагою способу онлайнової верифікації є своєчасність доставки (у реальному часі) інформації про анулювання сертифікатів. Цей спосіб кращий для обслуговування додатків, що вимагають обов'язкової перевірки сертифікатів до виконання транзакції. Спосіб онлайнової верифікації встановлює жорсткі вимоги постійної захищеності OCSP-сервера і засвідчення всіх запитів до ЗЦ цифровими підписами, що може створити "вузькі місця" при обробці запитів.

Проблеми поширення САС можуть бути вирішені шляхом комбінування різних способів публікації САС: онлайнової верифікації для сертифікатів, які використовуються у додатках, критичних для ведення бізнесу (наприклад, в електронній комерції), і "pull"-способу – для сертифікатів інших типів.

1.3.13 Відновлення, резервне копіювання та зберігання ключів в архіві

Організація повинна оцінити необхідність підтримки сервісу відновлення ключів, який полягає в захищеному зберіганні та розповсюдженні ключів, використаних для шифрування корпоративних даних. Сервіс відновлення ключів може надаватися ЗЦ, а може бути реалізований як окремий компонент [6]. Організації слід ретельно зважити варіанти, якщо вона дійсно потребує цього

сервісу. Деякі постачальники ПЗ для PKI вже підтримують відновлення ключів, але не завжди можуть запропонувати обидва варіанти реалізації.

Дуже важливими аспектами управління ключами є створення резервних копій і відновлення ключів, бо суб'єктам будь-якої PKI властиво втрачати свої секретні ключі. У разі втрати секретного ключа кінцевого суб'єкта ЗЦ повинен анулювати відповідний сертифікат відкритого ключа, після цього повинна бути згенерована нова пара ключів і створений новий сертифікат відкритого ключа. Сервер відновлення ключів забезпечує копіювання секретних ключів у момент їх створення, для того щоб вони могли бути згодом відновлені. В екстремальній ситуації при втраті ключа підпису самого ЗЦ стають неможливими випуск сертифікатів та підписання CAC, тобто компрометується весь домен довіри. Політикою безпеки резервного копіювання і відновлення повинен бути визначений формат резервних копій ключів (звичайний текст, зашифрований текст або ключ по частинах) і визначений порядок роботи з персоналом, відповідальним за процедури резервного копіювання і відновлення, ведення контрольних журналів, матеріалів архіву, підтримки секретних ключів ЗЦ, РЦ і кінцевих суб'єктів.

При розробці процедур зберігання ключів та іншої інформації в архіві повинні бути обрані об'єкти, що підлягають зберіганню, період зберігання та особи, відповідальні за архів і мають доступ до нього, детально описані події, що фіксуються у контрольних журналах, способи пошуку й захисту від спотворень архівної інформації, процедури датування. Через однотипність операцій створення резервних копій, архівування та копіювання, до будь-яких копій даних мають застосовуватися ті ж суворі правила, які поширюються на сам оригінал.

1.3.14 Депонування копій секретних ключів

Організація може депонувати, тобто зберігати копії секретних ключів, пов'язаних з відкритими ключами шифрування. Тоді у випадку втрати секретного ключа або звільнення його власника можна відновити дані, зашифровані цим ключем. Втрата ключа підпису не має серйозних наслідків, тому що може бути випущений сертифікат нового ключа підпису. Оскільки ключі підпису

підтверджують приналежність електронного документа особі, що його підписала, і не використовуються для шифрування інформації, немає необхідності їх депонувати.

Будь-яка організація, що використовує PKI для критично важливих цілей бізнесу, повинна забезпечувати випуск подвійних сертифікатів (шифрування й підпису) та депонування ключів шифрування [3]. Більшість систем PKI (навіть аутсорсінгових) підтримують депонування секретних ключів шифрування та їх зберігання у власній мережі організації. Типовим способом підтримки неспростовності є використання симетричного ключа для шифрування секретного ключа, а потім шифрування симетричного ключа за допомогою відкритого ключа ЗЦ. Якщо РЦ звертається із запитом про відновлення депонованого ключа, то ЗЦ повинен розшифрувати симетричний ключ і відправити його РЦ. Тільки у цьому випадку РЦ може відновити необхідний секретний ключ. Сам ЗЦ не може відновлювати депоновані ключі, бо не має доступу до бази даних ключів шифрування і здатний тільки розшифрувати симетричний ключ.

Поділ функцій РЦ і ЗЦ у процесі відновлення депонованих ключів забезпечує більшу захищеність і контроль за тим, як і чому відновлювалися секретні ключі шифрування. Деякі ЗЦ не допускають масового відновлення депонованих ключів і вимагають створення індивідуального запиту для кожного ключа, обмежуючи доступ адміністратора відразу до всіх секретних ключів шифрування організації.

1.3.15 Вибір способу і агента депонування ключів

При розгортанні PKI на додаток до функцій резервного копіювання і відновлення ключів може бути запланована підтримка депонування ключів. Під депонуванням ключів розуміється надання копій секретних ключів третій стороні і дозвіл користуватися ними за певних обставин, в якості третьої сторони найчастіше виступають урядові установи і правоохоронні органи. Депонування ключів може бути покладено на незалежний підрозділ усередині організації, що розгортає PKI, або на зовнішнє агентство. Один із способів депонування ключів і підтримки високого рівня безпеки полягає у шифруванні секретних ключів відкритим ключем

агента депонування та передачі їх на локальне зберігання під контроль власників ключів або іншої уповноваженої особи. Коли з'являється необхідність відновити секретний ключ, зашифрований ключ знову передається агенту депонування для розшифрування за допомогою секретного ключа останнього.

Альтернативним способом депонування всередині організації є поділ ключа на дві частини, шифрування кожної частини відкритими ключами різних осіб (наприклад, офіцерів безпеки) і локального зберігання під контролем власників ключів або уповноваженої особи. Крім того, для депонування і роздільного зберігання двох частин секретного ключа підпису користувача іноді застосовуються смарт-картки.

Вибір способу й агента депонування здійснюється з урахуванням фінансових можливостей, вимог безпеки і особливостей діяльності організації, що розгортає PKI.

1.3.16 Плани реагування на катастрофи та відновлення роботи системи

Хоча ретельне складання планів реагування на катастрофи та реалізація зайвих компонентів може мінімізувати ризик, пов'язаний з багатьма причинами катастроф, організації важливо розглянути найгірші сценарії і гарантувати, що мається оптимальний план забезпечення безперервної роботи і відновлення функціонування PKI. Це прискорить відновлення, якщо катастрофа дійсно відбудеться.

Однією з найбільш серйозних катастроф, які становлять загрозу для PKI, є компрометація ключа ЗЦ (або підозра, що він скомпрометований). Організації слід гарантувати, що вжиті відповідні заходи безпеки, щоб мінімізувати ризик катастрофи, і що постачальник технології розуміє цю проблему і може надати рекомендації і засоби, які допоможуть прискорити відновлення, якщо така подія дійсно відбудеться.

1.3.17 Проблеми інтеграції PKI

Важливий фактор адаптації PKI – вирішення проблем інтеграції та забезпечення роботи додатків. PKI може бути інтегрована кількома способами:

– з додатками (наприклад, клієнтськими додатками електронної пошти);

– з даними третьої сторони (наприклад, з базою даних аутентифікації);

– з системами сильнішою аутентифікації (біометрією або смарт-картками);

– з існуючими системами організації.

Великі труднощі при розгортанні інфраструктури відкритих ключів викликає інтеграція відповідних PKI функцій у знову створювані додатки, а також у вже наявні прикладні системи. PKI повинна взаємодіяти з безліччю різноманітних систем та програм, серед яких можуть бути системи управління доступом, каталоги користувачів, віртуальні приватні мережі, операційні системи, сервіси безпеки, додатки захищеної електронної пошти та web-додатки [12]. Налагодження зв'язку між новою інфраструктурою і всіма цими додатками і системами є складним завданням, для її вирішення важлива наявність інтерфейсів прикладного програмування, які забезпечують взаємодію існуючих корпоративних додатків з PKI та використання її сервісів. Деякі програмні засоби підтримки PKI надають інтерфейси прикладного програмування високого рівня для поширених додатків. Вибір програмного продукту такого типу полегшує інтеграцію PKI і скорочує час розгортання інфраструктури.

1.3.17.1 Інтеграція з додатками

Щоб використовувати програмне забезпечення, що оперує від імені кінцевих користувачів, процесів або пристроїв, PKI має підтримувати такі функції, як шифрування та розшифрування, генерацію та верифікацію цифрових підписів, а також забезпечувати доступ до функцій управління життєвим циклом сертифікатів і ключів, тобто бути PKI-сумісним.

Очевидно, що не всі програми сумісні з PKI, наприклад, популярний додаток Microsoft Word не здатна використовувати можливості PKI. Для того щоб запевнити цифровим підписом договір, підготовлений в MS Word, і переслати його

партнеру з гарантією дотримання цілісності, користувачеві необхідно отримати сертифікат ключа підпису і скористатися додатком, що забезпечує виконання криптографічних функцій.

Існує кілька способів додання додатком функцій PKI. Найчастіше для цього використовуються інструментальні засоби постачальника PKI. Інструментальний набір дозволяє додавати основні функції PKI, наприклад, генерацію ключів. Розробники повинні потім адаптувати інтерфейс користувача для виклику специфічних функцій PKI, таких як формування запиту на сертифікат. Приклад розширеного web-запиту сертифіката показано на рис. 1.3.

Крім того, останні версії більшості web-серверів істотно розширили можливості web-адміністратора створювати запити на сертифікати з консолі адміністратора. Для інтеграції PKI деякі постачальники пропонують програмне забезпечення проміжного рівня.

На даний час список PKI-сумісних програмних засобів зростає, і можна очікувати, що ця тенденція збережеться. Деякі найбільш популярні системи електронної пошти та електронного документообігу є PKI-сумісними. Багато постачальників ринку віртуальних приватних мереж також реалізують технологію відкритих ключів (наприклад, ті, які орієнтуються на стандарт IKE [13]), крім того, web-технологія може розглядатися як частково PKI-сумісна.

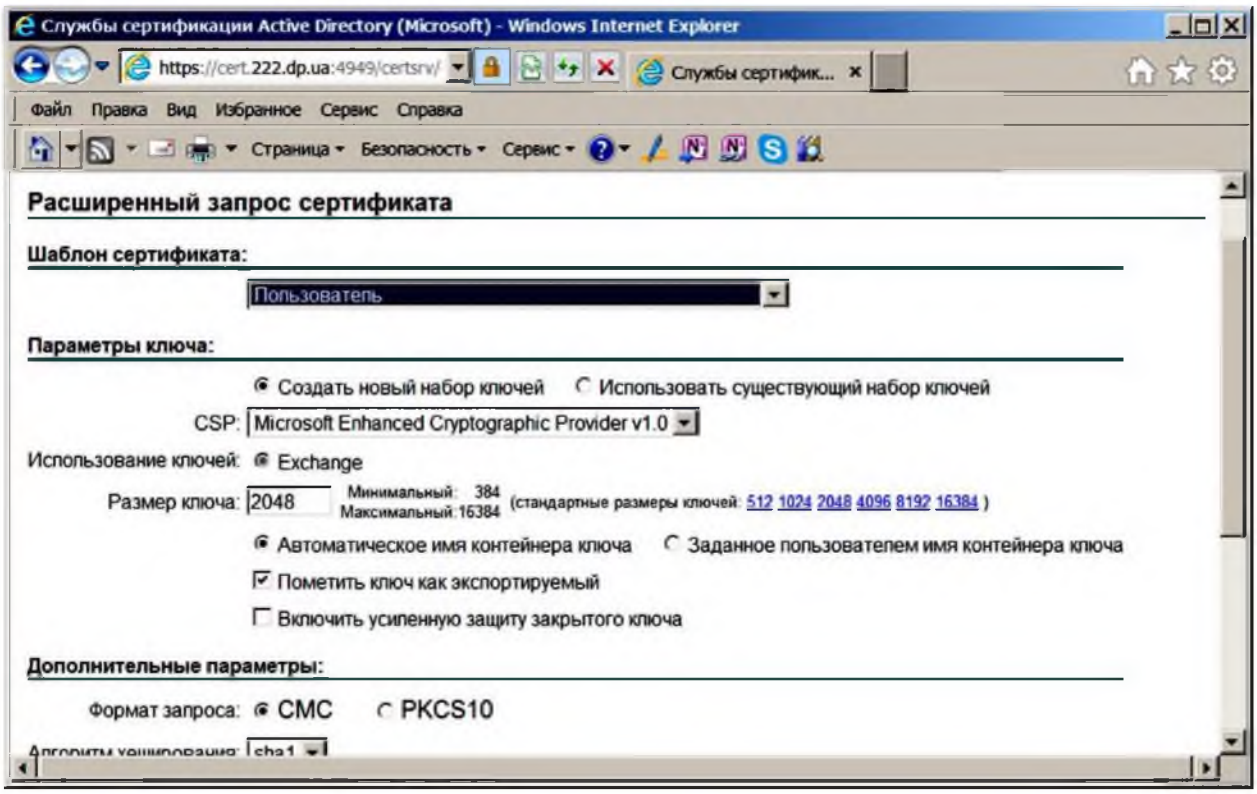

Рисунок 1.3– Розширений web-запит сертифіката

1.3.17.2 Інтеграція з даними третьої сторони

Основою моделі розгортання якісної PKI є сильна аутентифікація, яка, в свою чергу, залежить від інтеграції з надійним джерелом даних. Системи PKI зазвичай забезпечують доступ до ODBC - і LDAP-сумісних баз даних та інтеграцію з цими даними, а також з даними на базі текстових файлів. У багатьох корпоративних системах виконується інтеграція з базою даних персоналу. У системах PKI, призначених для масового ринку, часто необхідна інтеграція з даними третьої сторони, наприклад, бюро кредитних історій. Деякі постачальники даних надають також і інструментальні засоби інтеграції.

1.3.17.3 Інтеграція з системами сильнішою аутентифікації

Як тільки організація починає усвідомлювати необхідність сильної аутентифікації, вона переходить до використання біометрії і смарт-карток. Зазвичай велика частина роботи з інтеграції з біометричними пристроями покладається на постачальника пристроїв, а не на постачальника PKI, тому

важливий правильний вибір постачальника, який підтримує партнерські програми, або постачальника незалежного програмного забезпечення, що пропонує готові рішення.

Застосування біометричних пристроїв вимагає установки клієнтського програмного забезпечення для контролювання доступу до середовища зберігання сертифікатів на кожному персональному комп'ютері, а також реєстрації і збереження на комп'ютері біометричних характеристик користувачів для процедур порівняння.

Застосування смарт-карток та управління їх життєвим циклом також пов'язане з використанням спеціального клієнтського програмного забезпечення та встановлення додаткових драйверів. Постачальники смарт-карток можуть використовувати звичайні стандарти типу CAPI (Cryptographic Application Programmer Interface) [14] і PKCS#11 [15]. Слід враховувати, що інтеграція з системами сильнішою аутентифікації вимагає додаткових фінансових витрат і витрат часу.

1.3.17.4 Інтеграція з існуючими системами

Оскільки існуючу IT-інфраструктуру може використовувати будь-яка організація, часто виникають проблеми інтеграції PKI з уже діючими системами. Звичайно передбачається, що PKI обслуговуватиме тільки системи на базі персональних комп'ютерів і PKI-сумісні програми. Більшість програмних продуктів для PKI не призначена для роботи в системах на базі UNIX або мейнфреймів. Для інтеграції PKI з великими обчислювальними системами необхідно програмне забезпечення проміжного шару або передача даних вручну.

1.3.17.5 Інтеграція з інтерфейсом користувача

Важливим аспектом PKI, який часто упускається з виду, є зручність роботи користувача. Користувач повинен мати простий і зрозумілий засіб формування запитів на видачу, оновлення та анулювання сертифікатів. Більшість постачальників PKI пропонують деякий інтерфейс користувача, але, як правило,

він є додатком, що базуються на клієнтському програмному забезпеченні, і не завжди пристосований для роботи на різних комп'ютерних платформах (PC, UNIX, Mac) або різних версіях.

1.3.18 Проблеми функціональної сумісності продуктів різних постачальників

Крім проблеми стандартів, існує також проблема функціональної сумісності продуктів різних постачальників [16]. Не всі програмні засоби підтримки каталогу мають однакову функціональність, більш того – одні й ті ж функції у різних продуктах реалізуються по-різному, навіть якщо і базуються на одних і тих же стандартах. Але проблема з часом буде вирішуватися, оскільки постачальники каталогів прагнуть до цього, працюючи разом не тільки зі своїми технологічними партнерами й клієнтами, але навіть з конкурентами.

Постачальники програмних засобів можуть законно заявляти про відповідність своїх продуктів стандартам, але через низку причин функціональна сумісність продуктів кількох постачальників реально може досягатися не завжди. Для організації дуже істотні розуміння цих причин і гарантії, що обрані постачальники будуть спільно вирішувати проблеми функціональної сумісності.

1.3.19 Формат X.509 або альтернативні формати сертифікатів

Окрім формату X.509 існують й альтернативні формати сертифікатів. Не дивно, що є прихильники кожного формату. Так, наприклад, прихильники формату SPKI стверджують, що сертифікати SPKI дозволяють фіксувати ролі і права авторизації, не розкриваючи ідентичність суб'єктів. Прихильники формату PGP або Open PGP вважають важливою перевагою більшу гнучкість сертифікатів PGP у порівнянні з сертифікатами відкритих ключів X.509 v3 і, отже, велику придатність для встановлення відносин довіри між суб'єктами. Однак поки більшість постачальників PKI підтримують тільки сертифікати X.509.

У майбутньому, можливо, отримають поширення формати сертифікатів, засновані на мові розмітки XML (eXtensible Markup Language) [17], який все частіше застосовується як формат для обміну інформацією між різними додатками

в Інтернеті [6]. Нові формати сертифікатів, затверджені технічним комітетом по сервісам безпеки OASIS (у специфікації мови SAML – Security Assertion Markup Language) [18], ймовірно, будуть використовуватися спільнотою розробників бізнес-додатків на базі XML. Такі формати можуть замінити сертифікати X.509 на рівні XML-додатків, але, швидше за все, будуть співіснувати разом з ними на іншому рівні, для того щоб здійснювалася взаємодія з іншими діючими інфраструктурами. Середа для такої взаємодії може базуватися на специфікації управління ключами XML Key Management Specification [19], щоб, як визначено Консорціумом World Wide Web Consortium (W3C), приховувати від XML-додатки деталі базової PKI стандарту X.509.

1.3.20 Профілі сертифікатів та списки CAC

Навіть коли адаптуються технології, засновані на стандартах, реалізації PKI варіюються залежно від типу домену довіри. Це стосується сертифікатів та списків CAC формату X.509. Для задоволення специфічних вимог різних доменів створюються різні профілі сертифікатів та списків CAC. Для розгортання PKI важливо вибрати постачальника технології, який пропонує процедуру генерації сертифікатів та списків CAC, що дає можливість враховувати вимоги багатьох профілів сертифікатів та списків CAC.

Щоб додаток міг використовувати необхідні сервіси безпеки й функції управління життєвим циклом ключів і сертифікатів, воно має бути PKI-сумісним. Постачальники технології повинні пропонувати стандартні PKI-сумісні програми, а також певні інструментальні засоби, призначені для інтеграції в PKI інших додатків.

Багато корпоративних доменів використовують онлайновий репозиторій для своєчасного і надійного розповсюдження сертифікатів, інформації про їх статус, а також іншої інформації, що має відношення до PKI (наприклад, інформації про політику). Досвід розгортання PKI свідчить про те, що надання послуг репозиторію не обходиться без проблем, які пов'язані з відсутністю єдиних стандартів, прийнятих в індустрії, і сумісністю продуктів PKI різних постачальників [20].

1.3.21 Вибір репозиторія

У PKI може бути реалізовано кілька варіантів поширення сертифікатів кінцевих суб'єктів, інформації про їх анулювання та інших релевантних даних; є ряд постачальників, які підтримують один або кілька подібних сервісів. Як і у випадку вибору постачальника технології PKI, для організації важливі гарантії, що постачальник репозиторія пропонує гнучку функціональність і забезпечує сумісність з продуктами багатьох постачальників.

Одна з проблем, пов'язаних з сервісами каталогу, полягає у відсутності єдиного стандарту на ці послуги. Деякі сегменти ринку адаптували стандарти каталогу X.500, але одночасно існує і розробляється велика кількість стандартів, що мають відношення до сховища. Наприклад, відомий спрощений протокол доступу до каталогу LDAP, розроблений організацією IETF, з точки зору технічної перспективи знаходиться у прямій конкуренції з протоколом DAP, що базується на стандарті X.500. Є ще ряд невирішених проблем обміну інформацією та взаємодії "клієнт-сервер" і "сервер-сервер". Робоча група LDAPext організації IETF розробляє ряд стандартів, таких як механізми управління доступу та моделі контролю доступу, в стадії розробки знаходиться протокол LDUP [21], який, ймовірно, буде конкурувати зі своїм двійником − протоколом DISP (Directory Information Shadowing Protocol) стандарту X. 500. Крім того, поширення інформації PKI виконується й у інші способи. Хоча будь-яке з цих рішень може цілком відповідати вимогам конкретної організації, при взаємодії систем PKI різних організацій можуть виникнути проблеми функціональної сумісності різних рішень.

Нарешті, з розгортанням сервісу репозиторія пов'язані потенційні проблеми масштабованості та продуктивності. Очевидно, що необхідна кількість серверів залежить від кількості кінцевих користувачів, а також від строку дії списків CAC (у припущенні, що допускається кешування) та інших обставин реалізації (наприклад, від того, чи підтримуються дельта-списки CAC). Також треба враховувати і додаткове навантаження на репозиторій, оскільки він часто використовується не тільки для цілей PKI, але й для інших потреб організації.

1.4 Висновок. Постановка задачі

В даному розділі визначені особливості розгортання PKI у інформаційно-комунікаційної системі підприємства, що забезпечить:

– можливість одержання e-mail повідомлень у ручному й автоматичному режимі для базових мобільних користувачів;

– можливість віддаленого та мобільного доступу до сервісів сучасної інформаційній системи по захищеному каналу та шифруванням трафіку на всіх етапах передачі інформації;

– організацію захищеного каналу, що блокує можливість перехоплення і дешифрування даних;

– швидке, якісне та надійне забезпечення бізнес-процесів і створення загального робочого простору для віддалених та мобільних користувачів інтрамережі підприємства у будь якому місці, де є доступ до Інтернету;

– можливість створення системи захисту та управління використання документу, що містить впроваджений відео потік.

Для цього необхідно вирішити наступні задачі:

– визначити проблеми безпеки при доставці відео контенту віддаленим та мобільним користувачам інформаційно-комунікаційної системи підприємства;

– розробити алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, яка підвищить рівень захищеності електронного документа, що містить відео для віддалених та мобільних співробітників;

– розробити алгоритм створення, зберігання, доставки документа з впровадженим відео потоком;

– розробити алгоритм використання документа віддаленими та мобільними співробітниками підприємства;

– розробити архітектуру інформаційно-комунікаційної системи підприємства, що реалізує наведені вище алгоритми;

– вибрати програмні елементи інфраструктури, що реалізуватимуть наведені вище алгоритми;

– розробити рекомендації щодо політики видачі, відкликання та відновлення сертифікатів для віддалених та мобільних користувачів;

– провести експериментальну перевірку отриманих результатів.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Технічне завдання

2.1.1 Мета та вихідні дані для проведення роботи

Об'єкт досліджень – інформаційна система підприємства-виробника, зберігача і постачальника мультимедійного контенту для співробітників, що перебувають за межами контрольованої зони.

Предмет досліджень – рівень захисту інформації при доступі співробітників, що перебувають за межами контрольованої зони до документів, що містять відео.

Мета – підвищити рівень захищеності електронного документа, що знаходяться за межами контрольованої зони підприємства і містить технічне відео

Ідея роботи – використовувати потокове відео у форматі електронного документа і захистити його за допомогою інфраструктури відкритих ключів (PKI), інтегрованих в сучасні мережеві операційні системи

Вихідні дані для проведення роботи:

- державні стандарти України в галузі інформаційної безпеки, нормативні документи з технічного захисту інформації та закони України;
- міжнародні стандарти в галузі інформаційної безпеки.

2.1.2 Очікувані наукові результати

Наукова новизна роботи полягає у:

- розробці алгоритму створення інфраструктури корпоративної інформаційної системи, яка підвищує рівень захищеності електронного документа, що містить відео, за межами контрольованої зони підприємства;
- розробці алгоритму створення, зберігання, доставки документа з впровадженим відео потоком;
- розробці алгоритму використання документа співробітником поза контрольованої зони підприємства.

Практична цінність роботи полягає в тому, що:

- отримані результати можуть бути використані для подальшого та поглибленого вивчення інформаційних систем, які мають користувачів поза контрольованої зони;
- розроблені алгоритми щодо підвищення рівня захисту інформації в системах при використанні технічного відео, можуть бути використані на підприємствах різної форми власності.

2.1.3 Вимоги до результатів виконання роботи

Результати повинні відповідати вимогам Закону України «Про інформацію», Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», «Положення про технічний захист інформації в Україні», що затверджено указом Президента України від 27 вересня 1999 р. №1229/99, НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», «Про вищу освіту», Закону України «Про освіту», «Положення про організацію навчального процесу у вищих навчальних закладах», що затверджено наказом Міністерства освіти України від 2 червня 1993 р. №161, нормативних документів з технічного захисту інформації, державних стандартів України в галузі інформаційної безпеки та інших законів України, що стосуються забезпечення безпеки інформації.

Результати досліджень мають бути подано у вигляді, що дозволяє безпосереднє використання для створення засобів захисту інформації в системах хмарних обчислень.

2.1.4 Реалізація результатів та ефективність

Економічний ефект від реалізації результатів роботи очікується позитивним

завдяки зменшенню вірогідності збитків підприємства за рахунок підвищення рівня захищеності електронного документа, що знаходяться за межами контрольованої зони підприємства і містить технічне відео.

Соціальний ефект від реалізації результатів роботи очікується позитивним завдяки створенню умов для реалізації можливостей працівникам підприємства підвищити продуктивність праці та її комфортність.

2.2 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

Відповідно до документу: «НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» встановимо критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу при використанні мультимедійного контенту для співробітників, що перебувають за межами контрольованої зони підприємства.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

- порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах;
- базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

2.3 Критерії конфіденційності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого

ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного

об’єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об’єкт.

Права доступу до кожного захищеного об’єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту і імпорту.

Цілісність при обміні

Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об’єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об’єкті, який передається.

Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити

особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму.

Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ,

повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

В ідеальному випадку вище перераховані критерії оцінки захищеності інформації, при використанні мобільного доступу, мають допомогти визначити вимоги з захисту інформації в комп'ютерних системах від несанкціонованого доступу, створити захищені комп'ютерні системи, оцінити придатність комп'ютерних систем для обробки критичної інформації при використанні мобільних технологій. Але, враховуючи особливості функціонування систем що мають мобільних користувачів можна передчасно зробити висновок, що забезпечити деякі критерії буде досить складно, а іноді неможливо.

2.4 Архітектура інформаційної системи підприємства яка має користувача поза контрольованої зони підприємства

Архітектура інформаційної системи підприємства яка має користувача поза контрольованої зони показана на рисунку 2.1. Система має такий алгоритм функціонування :

- зовнішній користувач ініціює зв'язок з Інтернет провайдером, а мобільний з оператором мобільного зв'язку, або Wi-Fi;
- після цього інформація через сервер-шлюз надходить в Інтернет і досягає брандмауера інтрамережі підприємства;
- перевіривши сертифікат зовннішнього користувача, міжмережевий екран починає сесію з серверами інтрамережі, що перебувають у зоні периметру;

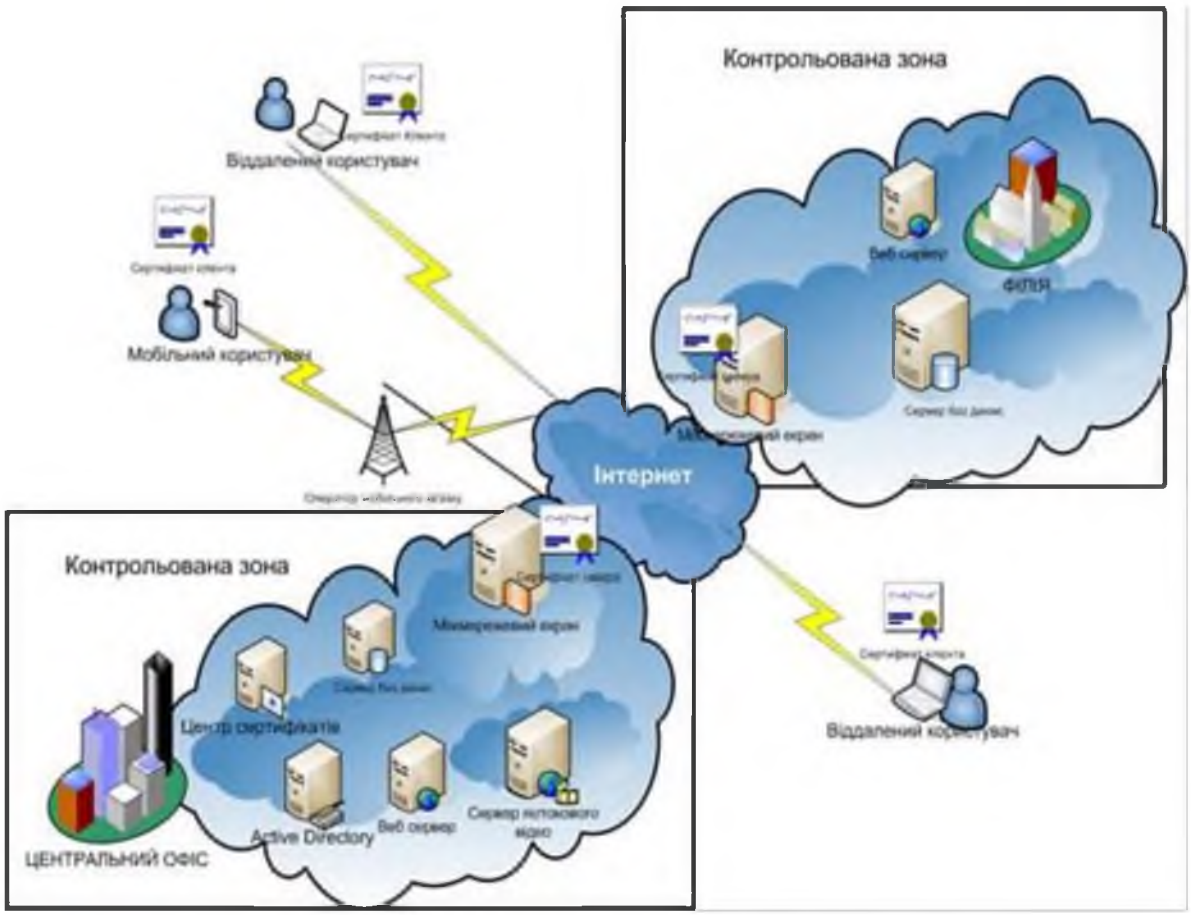

Рисунок 2.1 – Архітектура інформаційної системи підприємства яка має користувача поза контрольованої зони підприємства

- перевіривши дійсність сертифіката у Центрі Сертифікатів, сервери дозволяють почати обмін інформацією з пристроєм зовнішнього користувача, так як якби користувач фізично перебував у інтрамережі підприємства.

2.5 Сервіси, що надаються віддаленим та мобільним користувачам в середовищі сучасної інформаційної системи підприємства

Віддаленим та мобільним користувачам в середовищі сучасної інформаційної системи підприємства надаються такі сервіси:

- Web доступ до внутрішніх і зовнішніх сайтів;
- доступ до потокового відео;
- корпоративна електронна пошта та відео конференції;

- дистанційні корпоративні додатки (RemoteApps);
- Web доступ до віддалених робочих столів (термінальний сервіс);
- доступ до файлових серверів по VPN.

2.6 Проблеми безпеки при підключенні мобільних користувачів до інформаційної системи підприємства

При підключенні мобільних користувачів до інформаційної системи підприємства виникають проблеми:

- як віддалено керувати мобільними пристроями?
- чи є можливість заборонити запуск небажаних програм?
- як вибірково заборонити деякі інтерфейси і функції пристрою (камера, Bluetooth, Wi-Fi)?
- як забезпечити безпечну доставку, зберігання та видалення конфіденційної інформації на пристроях?
- чи є спосіб розповсюдження ПЗ на мобільні пристрої?
- як запобігти доступу пристроїв в Інтернет або до деяких сайтів?
- як заборонити підключення до корпоративної інфраструктурі певних пристроїв?
- чи можна віддалено знищити інформацію на мобільному пристрої?
- що робити, якщо пристрій вже втрачено або вкрадено?
- чи є можливість відключити некорпоративні поштові та користувальницькі додатки і сервіси?

2.7 Модель загроз при підключенні користувачів, що знаходяться поза межами контрольованої зони

Модель загроз при підключенні користувачів, що знаходяться поза межами контрольованої зони наведена в таблиці 2.2.

Таблиця 2.2 – Модель загроз

№ п/п	Джерело загрози	Інформація, що порушується				Вірогідні збитки
		К	Ц	Д	С	
1	Загроза перехоплення даних при при завантаженні документа з серверів підприємства	Так	Так	Так	Так	Суттєві
2	Загроза перехоплення потоку відео при проходженні його через Інтернет	Так	Так	Так	Так	Суттєві
3	Загроза неавторизованного перегляду документа на пристрої віддаленого чи мобільного співробітника	–	–	Так	Так	Середні
4	Загроза шляхом аналізу HTML коду визначити URL джерела потокового відео для організації на нього DDOS атаки	Так	Так	Так	Так	Середні
5	Загроза перенесення і перегляду мультимедійного контенту на інших пристроях	–	–	Так	Так	Низькі
6	Загроза витягання відео з тимчасових файлів і кеша пристрої для подальшого неавторизованого перегляду	–	–	Так	Так	Низькі

2.8 Алгоритм створення інфраструктури корпоративної інформаційної системи

Алгоритм створення інфраструктури корпоративної інформаційної системи складається з таких етапів:

1 Розгортання Active Directory і як основи авторизації співробітників підприємства;

2 Розгортання Центру Сертифікації підприємства, що забезпечує функції PKI;

3 Розгортання веб сервера IIS, що забезпечує створення веб вузла для отримання особистих сертифікатів співробітників;

4 Розгортання веб порталу на основі Windows Sharepoint Service як основи для створення депозитарію відкритих ключів співробітників і бібліотек документів, що містять потокове відео;

5 Розгортання сервера потокового відео, що підтримує протоколи передачі контенту в зашифрованому вигляді (наприклад протокол RTMPE). Це забезпечить конфіденційність і цілісність при трансляції потоку через Інтернет;

6 Розгортання корпоративного брандмауера, інтегрованого з Active Directory і забезпечує перевірку автентичності (аутентифікацію) за допомогою сертифіката користувача і з фомощью форм;

7 Отримання сертифікатів для зовнішніх веб серверів з Центру Сертифікації і установка їх на міжмережевому екрані;

8 Публікація сервера потокового відео в середу Інтернет за допомогою міжмережевого екрану;

9 Створення груп зовнішніх користувачів, що мають доступ до відеопотоку;

10 Публікація за допомогою брандмауера депозитарію відкритих ключів та бібліотек документів в середу інтернет. Перевірка справжності здійснюється за допомогою сертифіката користувача, отриманого в Центрі Сертифікатів підприємства;

11 Розгортання служби терміналів.

12 Установка на сервері терміналів програмного пакета Adobe Acrobat, що дозволяє автору документа у форматі PDF реалізацію таких функцій:

– упаковування потокового відео в документ;

– призначати користувачів документа;

– застосовувати до нього політику використання.

2.8.1 Рекомендації щодо розгортання центру сертифікації підприємства

Інфраструктура відкритих ключів (PKI) - це система цифрових сертифікатів, центрів сертифікації й центрів реєстрації, які перевіряють і підтверджують дійсність кожного об'єкта, що приймає участь в електронній транзакції з

використанням криптографії з відкритими ключами. Стандарти для PKI усе ще розвиваються, незважаючи на те, що вони широко реалізовані як необхідний елемент електронної торгівлі

Інфраструктура PKI підтримує ієрархічну модель центрів сертифікації, що є масштабованою та забезпечує погодженість із безліччю, що збільшується, комерційних і інших продуктів для центрів сертифікації.

У найпростішій формі ієрархія сертифікації складається з одного центра сертифікації. Але ієрархія часто містить кілька центрів сертифікації з чіткими відносинами "батько-нащадок". У цій моделі дочірній підлеглий центр сертифікації сертифікується за допомогою сертифікатів, виданих його батьківським центром сертифікації й прив'язують відкритий ключ до його посвідчення. Центр сертифікації, що перебуває на вершині ієрархії, називається кореневим центром сертифікації. Дочірній центр сертифікації кореневого центра сертифікації називається підлеглим центром сертифікації.

Якщо користувач довіряє кореневому центру сертифікації (його сертифікат перебуває в сховище користувача для сертифікатів довірених кореневих центрів сертифікації), він довіряє й всім підлеглим центрам сертифікації ієрархії, що володіє дійсним сертифікатом центра сертифікації. Отже, кореневий центр сертифікації є дуже важливою крапкою довіри в організації й повинен бути відповідним чином захищений.

Існує кілька практичних причин для створення декількох підлеглих центрів сертифікації, у тому числі:

– використання. Сертифікати можуть бути видані для декількох цілей, наприклад для захищеної електронної пошти й для перевірки дійсності в мережі. Політика видачі для цих застосувань може бути різної, і це розходження є основою для адміністрування цих політик;

- підрозділи організації. Політики видачі сертифікатів можуть відрізнятися залежно від ролі об'єкта в організації. І знову можна створити підлеглі центри сертифікації для поділу й адміністрування цих політик;

- географічні підрозділи. Об'єкти організацій можуть перебувати в

багатьох фізичних місцях. Для мережної взаємодії між цим місцями можуть знадобитися окремі підлеглі центри сертифікації для багатьох або для всіх площадок;

- балансування навантаження. Якщо інфраструктура PKI буде використовуватися для видачі великої кількості сертифікатів і керування ними, використання тільки одного центра сертифікації може привести до помітного мережного навантаження для цього єдиного центра сертифікації. Використання декількох підлеглих центрів сертифікації для видачі сертифікатів того самого виду ділить мережне навантаження між центрами сертифікації;

- резервне копіювання й відмовостійкість. Кілька центрів сертифікації підвищують імовірність постійної наявності в мережі працюючих центрів сертифікації, готових відповісти на запити користувачів;

Ієрархія центрів сертифікації може також надати ряд переваг з погляду адміністрування, у тому числі:

- гнучка конфігурація середовища безпеки центрів сертифікації для настроювання балансу між безпекою й зручністю використання. Наприклад, можна використовувати спеціальне криптографічне устаткування на кореневому центрі сертифікації, використовувати кореневий центр сертифікації у фізично захищеній області або автономно. Такий підхід може бути неприйнятним для підлеглих центрів сертифікації через міркування вартості або зручності;

- можливість "виключити" конкретну частину ієрархії центрів сертифікації, не впливаючи на встановлені довірені відносини. Наприклад, можна легко завершити роботу й відкликати виданий сертифікат, пов'язаний з конкретним підрозділом, не впливаючи на інші частини організації.

2.8.2 Політика та процедура видачі сертифікатів

У корпоративних мережах підтримується кілька методів видачі сертифікатів користувачам і комп'ютерам: одержання сертифіката через web-інтерфейс, запит сертифіката за допомогою Майстра, автоматичне розгортання й одержання

сертифіката через агента.

Одержання сертифіката через web-інтерфейс (web-enrollment). Цей метод може застосовуватися для одержання комп'ютерних і користувальницьких сертифікатів. Щоб цей метод був доступний, перед установкою на сервер Служби сертифікації необхідно спочатку встановити веб сервер. Для одержання сертифіката клієнт повинен набрати в рядку браузера адресу веб-інтерфейсу центра сертифікації і додержуватися інструкцій Майстра. Для мобільних користувчів звертатися двічі − один раз для відправлення запиту на одержання сертифіката, а другий раз − для установки сертифіката (якщо запит був успішно підтверджений адміністратором).

Запит сертифіката за допомогою Майстра (Request New Certificate wizard) може застосовуватися для одержання комп'ютерних і користувальницьких сертифікатів

Автоматичне одержання комп'ютерних сертифікатів (Automatic certificate request). Цей метод розгортання застосовувався в мережах Windows для автоматичної видачі тільки комп'ютерних сертифікатів.

Для настроювання автоматичного одержання комп'ютерних сертифікатів застосовується групова політика видачи сертифікатів для домена.

Автоматичне розгортання (Autoenrollment). За допомогою цього методу можна організувати автоматичну видачу комп'ютерних і користувальницьких сертифікатів, якщо в якості клієнтської операційної системи використовується Windows (Windows 7, 8, 10, 11) або Windows Server (2008, 2012, 2022).

Можна визначити, чи буде автономний центр сертифікації втримувати вхідні запити сертифікатів на очікуванні або видавати сертифікат автоматично. У більшості випадків з міркувань безпеки всі вхідні запити сертифікатів, адресовані ізольованому центру сертифікації, позначаються як очікуючи.

Можна настроїти модуль політики на автоматичне підтвердження всіх запитів на сертифікати або на приміщення запитів у чергу доти, поки адміністратор не перегляне ці запити й не почне необхідні дії. Вибір буде залежати від вимог до безпеки при видачі сертифікатів, від одержувачів сертифікатів і від ряду інших

факторів.

2.8.3 Рекомендації щодо політики видачі, відкликання та відновлення клієнтських сертифікатів для мобільних користувачів

Рекомендується така політика видачі, відкликання та відновлення клієнтських сертифікатів для мобільних користувачів:

- сертифікат не експортується і встановлюється тільки на пристрій, з якого прийшов запит;
- запит на видачу через веб-інтерфейс можливий тільки інтрамережі філіалу, яка має фіксовану публічну IP-адресу;
- термін дії та оновлення сертифікату визначається посадовою інструкцією служби безпеки підприємства (від 1 години до 1 місяця);
- миттєве відкликання сертифікату та блокування облікового запису користувача згідно команди уповноваженої персони служби безпеки підприємства (офіцера безпеки);
- для повторної видачі або відновлення сертифікату треба аудіовізуальне підтвердження уповноваженої персони служби безпеки з інтрамережі філії, з якої користувач отримав попередній сертифікат.

2.8.4 Політика та процедура відкликання сертифіката

Кожний сертифікат видається з конкретним періодом дії. Відкликаний сертифікат стає непридатним для використання в системі безпеки до витікання вихідного строку його дії. Існує декілька причин, по яких сертифікат може стати недостовірним у якості облікових даних безпеки до витікання його строку. Наприклад:

- компрометація або можлива компрометація закритого ключа суб'єкта сертифіката;
- компрометація або можлива компрометація закритого ключа центра сертифікації;

- виявлення того, що сертифікат був отриманий шахрайським образом;
- зміна статусу суб'єкта сертифіката як довіреного суб'єкта;
- зміна ім'я суб'єкта сертифіката.

Не завжди можна зв'язатися із центром сертифікації або з іншим довіреним сервером, щоб одержати відомості про дійсність сертифіката.

Для ефективної підтримки перевірки статусу сертифікатів у клієнта повинна бути можливість доступу до даних відкликання, щоб визначити, чи діє сертифікат або він був відкликаний. Для підтримки різних сценаріїв служба сертифікатів підприємства підтримує методи відкликання сертифікатів, що є галузевим стандартом. Серед них публікація списків відкликаних сертифікатів (CRL) і різницевих CRL, які могли бути доступні клієнтам з різних місць, включаючи служби сертифікатів, веб-сервери та загальні файлові мережні ресурси.

CRL являють собою повні і захищені цифровим підписом списки сертифікатів, які були відкликані. Ці списки публікуються періодично й можуть витягати й кешуються клієнтами (на основі настроєного часу життя CRL), а потім використовуватися для перевірки статусу відкликання сертифіката.

Тому що CRL можуть бути більшими, залежно від кількості сертифікатів, виданих і відкликаних центром сертифікації, проміжні CRL називаються різницевими CRL. Різницеві CRL містять тільки сертифікати, відкликані з моменту публікації останнього регулярного CRL. Це дозволяє клієнтам одержувати різницеві CRL меншого розміру й швидше створювати повний список відкликаних сертифікатів. Використання різницевих CRL також дозволяє частіше публікувати дані про відкликання, тому що завдяки малому розміру різницевого CRL для його передачі звичайно не потрібно так багато часу, як для повного CRL.

Сертифікати можуть бути відкликані з багатьох причин, включаючи наступні:

- ключ був скомпрометований;
- центр сертифікації, що видав сертифікат, був скомпрометований;
- сертифікат більше не є дійсним для своєї мети або був замінений іншим сертифікатом;

- клієнт більше не має права на цей сертифікат.

Кожний сертифікат має термін дії. По закінченні терміну дії сертифікат більше не розглядається як прийнятне посвідчення особи. Оснащення «Сертифікати» дозволяють за допомогою майстра відновлення сертифікатів обновляти сертифікат, виданий центром сертифікації підприємства під керуванням Windows, перед закінченням або після закінчення строку його дії.

Можна обновити сертифікат з тим же набором ключів, що використовувався раніше, або з новим набором ключів. Вибір конкретного варіанта залежить від декількох факторів, включаючи термін дії сертифіката, довжину існуючого або майбутнього ключа, значення даних, захищених парою ключів, а також імовірність захвата закритого ключа зловмисником.

Перед відновленням сертифіката необхідно знати наступне.

- центр сертифікації, що видає сертифікат;
- (необов'язково.) постачальників служби криптографії (CSP), якого варто використовувати для створення пари ключів, якщо для сертифіката необхідна нова пара з відкритого ключа й закритого ключа.

Windows видає попередження, якщо термін дії сертифікатів користувачів або комп'ютерів минув або близький до закінчення. У більшості випадків функція автоматичної реєстрації обновляє такі сертифікати при наступному підключенні до мережі й вході в систему.

Відновлення сертифіката з тим же ключем забезпечує максимальну сумісність із попереднім використанням відповідної пари ключів, але не підвищує безпеки сертифіката або пари ключів. Керування сертифікатами користувачів можуть здійснювати відповідний користувач або адміністратор. Управляти сертифікатами, виданими комп'ютеру або службі, може тільки адміністратор або користувач, якому були надані відповідні дозволи.

Відновлення сертифіката з новим ключем дозволяє продовжити використання існуючого сертифіката й зв'язаних даних, одночасно підвищивши надійність ключа сертифіката. Це доцільно в тому випадку, якщо застосування нового сертифіката може привести до порушення роботи й, якщо, існуючий

сертифікат не був скомпрометований.

Для виконання цієї процедури необхідно бути, як мінімум, членом групи Користувачі або Адміністратори локальної системи.

2.9 Алгоритм створення, зберігання, доставки та використання документа з впровадженим відео потоком

Згідно технічного завдання був розроблений алгоритм створення, зберігання, доставки та використання документа з впровадженим відео потоком.

1 Автор документа по внутрішній інтрамережі підключається до сервера потокового відео для отримання коду вставки RTMPE потоку для вставки в HTML сторінку.

2 У будь-якому текстовому або спеціалізованому HTML редакторі створюється сторінка з впровадженим кодом.

3 Після цього автор документа підключається до сервера терміналів, де розташована програма Adobe Acrobat.

4 За допомогою цієї програми і створеної попередньо веб сторінкою автор починає створювати документ в PDF форматі. У процесі формування політики застосування документа автор повинен надати певні повноваження користувачам, що мають доступ до документа. Для цього йому необхідні додатково відкриті ключі.

5 Автор підключається до депозитарію відкритих ключів співробітників, що перебувають на веб порталі підприємства (наприклад до стандартного списку контактів співробітників SharePoint) і завантажує відкритий ключ передбачуваного користувача документа PDF.

6 Маючи відкриті ключі користувачів, автор в інтерфейсі Adobe Acrobat створює і застосовує політику використання документа.

7 Після цього автор поміщає документ в одну з бібліотек порталу, де у користувачів є права на завантаження.

2.10 Алгоритм використання документа співробітником поза контрольованої зони підприємства

Алгоритм використання документа співробітником поза контрольованої зони підприємства містить такі позиції.

1 Залежно від політики безпеки предприяти співробітник може отримати особистий сертифікат як в експортованому так і в неекпортіруемом вигляді. У другому випадку закритий ключ буде жорстко прив'язаний до комп'ютера співробітника.

2 Для завантаження документа з веб порталу підприємства співробітник повинен пройти перевірку автентичності на міжмережевим екрані за допомогою особистого сертифіката.

3 Якщо сертифікат відповідає політиці видачі і відкликання Центру Сертифікації підприємства і співробітник входить до групи, що має доступ до серверу потокового відео, то запит направляється на портал підприємства, де у відповідній бібліотеці можна знайти і завантажити документ, що цікавить.

4 Після завантаження документ може бути відкритий на компьтере тільки при наявності закритого ключа і з правами використання сконфігурованими автором при його створенні.

5 Після відкриття документа (наприклад в Adobe Reader версії 9 і молодші) користувач отримує доступ до потоку відео по протоколу RTMPE. У цьому випадку потік шифрується , не кешируется на комп'ютері користувача, не залишається в тимчасових файлах і не може бути записаний за допомогою програм «граббер». Розкрити джерело (URL) потоку при шифруванні PDF документа алгоритмом AES 256 практично неможливо.

2.11 Визначення програмних елементів інфраструктури, що реалізують мету роботи

Згідно технічного завдання були визначені елементи інфраструктури, що реалізують мету роботи. Результати наведені в таблиці 2.3.

Таблиця 2.3 – Програмні елементи інфраструктури

Функція елемента	Найменування елемента
Операційна система комп'ютерної мережі підприємства	Windows Server
Авторизація користувачів	Служба Active Directory Windows Server
Інфраструктура відкритого ключа (PKI)	Кореневий Центр Сертифікації Windows Server
Веб сервери підприємства	Internet Information Server, Apache
Веб портал підприємства	Windows SharePoint
Протокол потокового відео	Real Time Message Protocol Enscription (RTMPE)
Сервер потокового відео	Adobe Media Server
Формати відео	mp4 та flv
Міжмережевий екран	Microsoft Forefront Server
Аутентифікація користувачів, що знаходяться за межами контрольованої зони	За допомогою сертифіката користувача
Протоколи шифрування трафіку від веб серверів підприємства до віддаленим користувачам	SSL 3.0, TLS 1.0
Депозитарій відкритих ключів користувачів комп'ютерної мережі підприємства	Вкладення відкритого ключа у форматі *. cer в список контактів на порталі підприємства
Сервер баз даних для зберігання контенту порталу	MS SQL Server 2022
Програмне забезпечення для створення захищеного документа з впровадженим потоковим відео	Adobe Acrobat
Тип захисту документа	Шифрування AES 128 біт , електронний підпис автора документа

Програмне забезпечення для читання документа	Adobe Acrobat Reader

2.12 Рекомендації налаштування міжмережевого екрану та серверів для доступу інформаційної системи підприємства віддалених та мобільних користувачів

Міжмережевій екран захищає периметр одного або декількох мережевих сегментів. Між захищеним мережевим сегментом і зовнішнім периметром знаходяться прикордонні системи, наприклад балансувальники навантаження, які направляють трафік в так звану "демілітаризовану зону" (DMZ), захищену іншим брандмауером. У цій зоні розташовуються сервери додатків, які направляють запити до баз даних через третій брандмауер у внутрішню захищену мережу, де знаходяться внутрішні бази даних, що зберігають конфіденційну інформацію.

У такій структурі для отримання доступу до даних за зростанням рівня секретності організовуються кілька рівнів (або периметрів) мережевого захисту за допомогою брандмауерів. Основною перевагою такої архітектури є те, що навіть якщо правила брандмауера, що захищає внутрішню мережу, сформульовані погано, вони не обов'язково відкривають її для доступу ззовні, за винятком тих випадків, коли демілітаризована зона теж вже скомпрометована. На додаток, загальна тенденція полягає в тому, що зовнішні сервіси сильніше захищені від вразливостей Інтернету, у той час як внутрішні сервіси менш орієнтовані на Інтернет. Слабкість же цієї інфраструктури полягає в тому, що компрометація будь-якого з внутрішніх серверів в межах конкретного сегмента автоматично надає повний доступ і до інших серверів в цьому мережевому сегменті.

Всі сервери знаходяться в мережі на одному рівні, а управління трафіком здійснюється за допомогою визначення груп безпеки. Членство в одній і тій же групі безпеки не надає привілейованого доступу до інших серверів, що належать до тієї ж групи безпеки, за винятком того випадку, коли явно визначені правила надають привілейований доступ. Нарешті, окремий сервер може бути членом

кількох різних груп безпеки. Правила, визначені для конкретного сервера, являють собою об'єднання правил для всіх груп, до яких цей сервер належить.

Якщо система безпеки не дозволяє обмежувати доступ через порти при визначенні правил доступу з однієї групи безпеки в іншу, можна імітувати цю можливість за рахунок визначення правил на основі вихідної IP-адреси для кожного сервера у вихідній групі.

Доступ до серверів, що належать до вашої внутрішньої групі безпеки, можна отримати лише тоді, коли попередньо буде скомпрометована спочатку прикордонна група, потім - DMZ, і, нарешті - один з внутрішніх серверів. На відміну від традиційного захисту периметра, тут існує можливість того, що випадково буде надано глобального доступу до внутрішньої зони і, таким чином, вона буде відкрита для вторгнень.

Така архітектура системи безпеки надає дві основні переваги:

– оскільки можна віддалено керувати правилами брандмауера, атакуючий не має єдиної мішені для своєї атаки, як у випадку з фізичним брандмауером;

– відсутність можливості випадково зруйнувати правила захисту мережі і таким чином назавжди блокувати будь-який доступ в даний мережевий сегмент.

Рекомендується скористатися підходом, який імітує традиційний захист мережевого периметра, тому що цей підхід до управління мережевим трафіком добре вивчений і простий для розуміння. Якщо скористатися цим підходом, важливо розуміти, що створюються тільки віртуальні еквіваленти фізичних мережевих сегментів традиційної фізичної інфраструктури. Справжніх рівнів мережевої безпеки, які є у традиційній конфігурації, немає.

Рекомендації по найбільш ефективної організації мережевої системи безпеки в інформаційній системі підприємства, що мають в у своєму середовищі віртуальні машини:

– на кожній віртуальній машині слід запускати тільки один мережевий сервіс (плюс всі сервіси, необхідні для адміністрування). Кожен новий мережевий сервіс, присутній в системі, являє собою вектор атаки. Якщо зосередити на одному сервері безліч сервісів, то створиться безліч векторів атаки, які потенційно

дозволяють отримати доступ до даних, що зберігаються на цьому сервері або для використання цього сервера для отримання прав доступу до іншої мережі;

- не слід надавати відкритого доступу до даних, які мають вищий рівень секретності. Якщо отримання несанкціонованого доступу до клієнтської бази даних вимагає компрометації балансувальника навантаження, сервера додатків і сервера бази даних (і при цьому ви впроваджуєте рекомендації запускати тільки один сервіс на кожному з серверів), зловмисникові потрібно реалізувати цілих три різних вектора атаки перш, ніж він зможе дістатися до цих даних;
- слід відкривати тільки ті порти, які є абсолютно необхідними для підтримки сервісу, що надається конкретним сервером, і не більше того. Зрозуміло, захист кожного з серверів повинен бути посилений таким чином, щоб на ньому працював тільки один сервіс – той, який спочатку був призначений для роботи на ньому. Іноді буває й так, що на сервері запускаються ті сервіси, які спочатку не призначалися для роботи на даному сервері. Також може бути, коли в складі сервісу виявляється експлойт, що не вимагає доступу від імені root (nonroot exploit), але дозволяє атакуючому запустити ще один сервіс за допомогою експлойтів, що вимагають доступ від імені root. Блокуючи доступ до всього, за винятком цільового сервісу, можна запобігти використанню цих типів експлойтів;
- слід обмежити доступ до сервісів, надаючи його тільки тим клієнтам, які дійсно їх потребують. Природно, що балансувальники навантаження повинні відкривати Web-порти 80 і 443 для всього трафіку. У відкритому доступі потребують тільки ці два протоколи і конкретний сервер. Для будь-якого іншого сервісу трафік повинен бути обмежений конкретними вихідними адресами;
- слід використовувати зворотний проксі. Зворотний проксі – це проксі-сервер, який, на відміну від прямого, ретранслює запити клієнтів із зовнішньої мережі на один або декілька серверів, логічно розташованих у внутрішній мережі. Зазвичай зворотні проксі-сервери встановлюються перед Web-серверами. Часто використовується для балансування мережного навантаження між декількома Web-серверами і підвищення їх безпеки, граючи при цьому роль брандмауера на прикладному рівні. Як правило, зворотний проксі представляє собою Web-сервер,

наприклад Apache, який маршрутизує трафік від клієнта до сервера. За рахунок використання проксі-сервера можна ускладнити для зловмисника атаку на вашу інфраструктуру. По-перше, Apache і IIS набагато краще справляються з завданнями щодо відображення мережевих атак, ніж будь-який з серверів додатків, які ви можете використовувати. У результаті ймовірність проникнення експлойта буде значно знижена, а ймовірність його знешкодження та швидкість випуску поліпшення істотно підвищаться. По-друге, при використанні експлойта на проксі-сервер атакує не отримає доступ, йому в будь-якому випадку доведеться шукати додаткову уразливість на самому вашому сервері додатків.

Отже, виходячи з вищевикладенного необхідно:

- обмежити доступу до до вебінтерфейсу Центра сертифікації (тільки з публічних IP адресів філій підприємства);
- сконфігурувати політику сервера сертифікатів домена щодо перевірки довірених издателей;
- сконфігурувати групи безпеки міжмережевіх екранів, щодо серверів, віртуальних машин та груп безпеки домена;
- для організаційного підрозділу мобільних користувачів дозволити тільки необхідні порти;
- встановити сертіфікати на усі вебсервери підприємства;
- налаштувати аутентифікацію мобільних користувачів до веб сервісів підприємства тільки з обов'язковим пред'явленням сертифіката користувача.

2.13 Експериментальна перевірка отриманих результатів

Мета експерименту – створити документ із впровадженим у нього захищеним відео потоком, який можуть переглядати співробітники підприємства. Творцем документа є автор-співробітник. При цьому співробітники можуть переглядати документ на будь-яких комп'ютерах, підключених до локальної мережі підприємства, а користувач гість тільки з єдиного строго визначеного комп'ютера, підключеного до локальної мережі підприємства.

Послідовність проведення експерименту.

1 За допомогою стандартного відео плеєра автор підключається до сервера за протоколом RTMP.

2 Одержує HTML код для вставки в будь-яку Web сторінку.

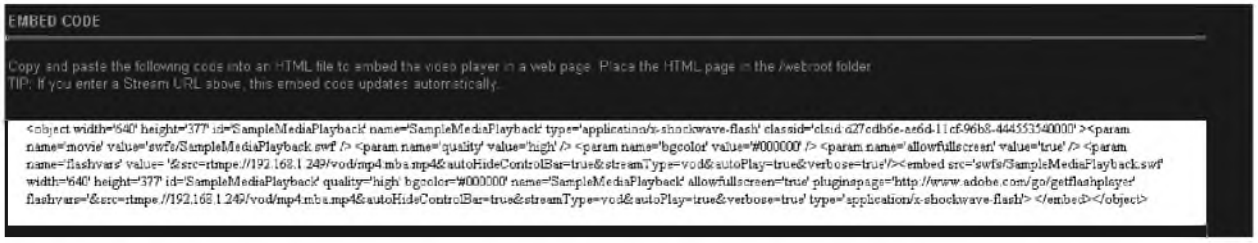

Рисунок 2.2 – Одержання HTML коду для вставки в Web сторінку

3 У будь-якому текстовому редакторі створює HTML сторінку й вставляє отриманий вище код (рисунок 2.3).

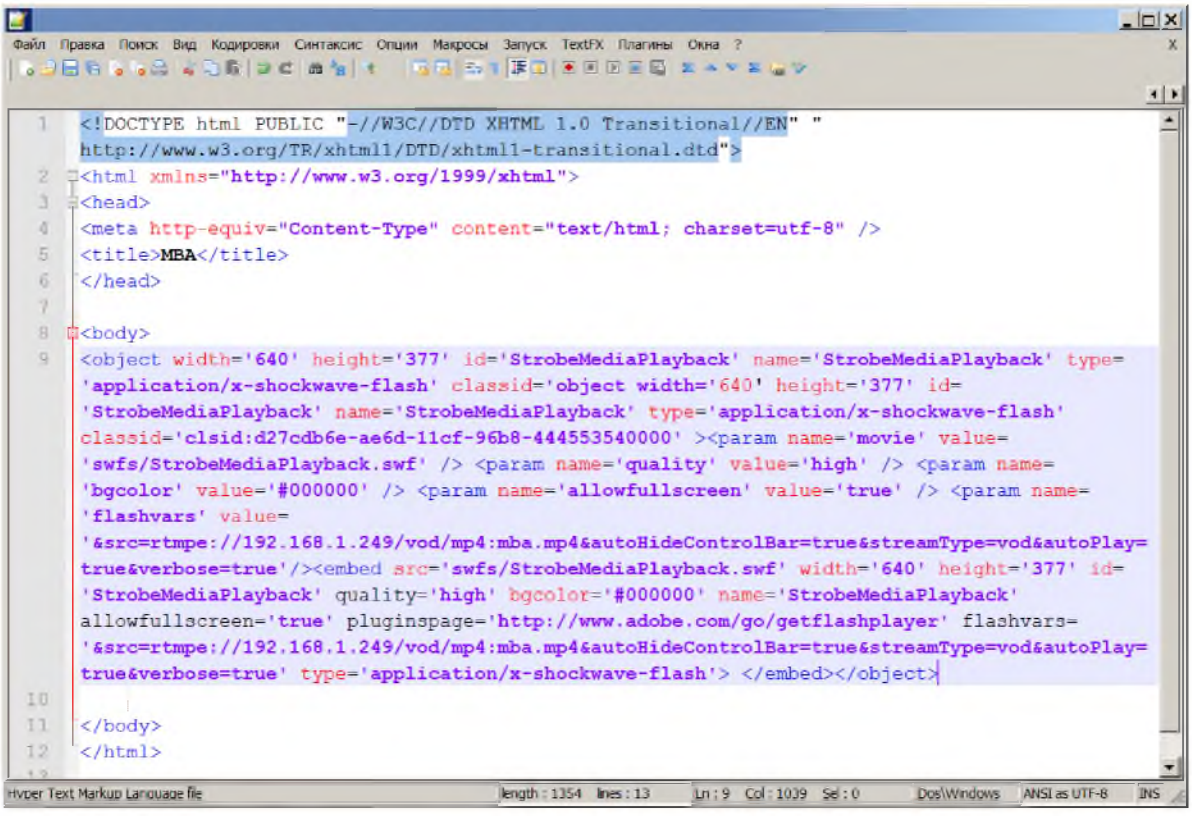

Рисунок 2.3 – Створення HTML-сторінки й вставлення отриманого коду

4 При наявності облікового запису в Active Directory одержує свій сертифікат користувача на сайті засвідчувальний центр підприємства (рисунок 2.4).

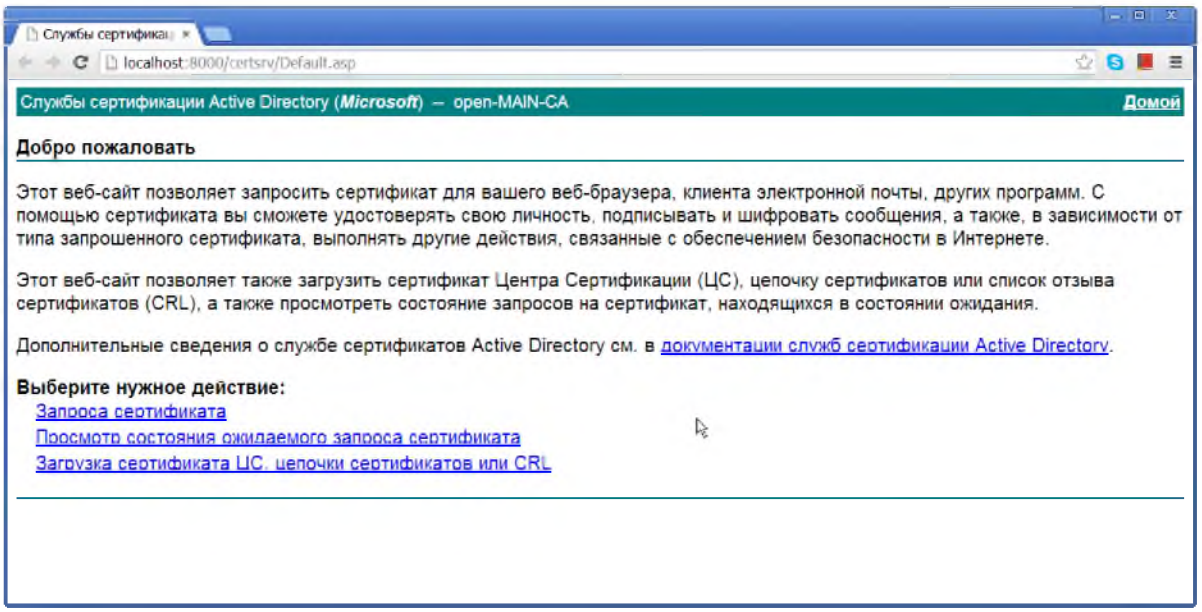

Рисунок 2.4– Одержання сертифікату користувача на сайті Центра сертифікації підприємства

5 Підключається до депозитарію відкритих ключів і отримує відкриті ключі (рисунок 2.5).

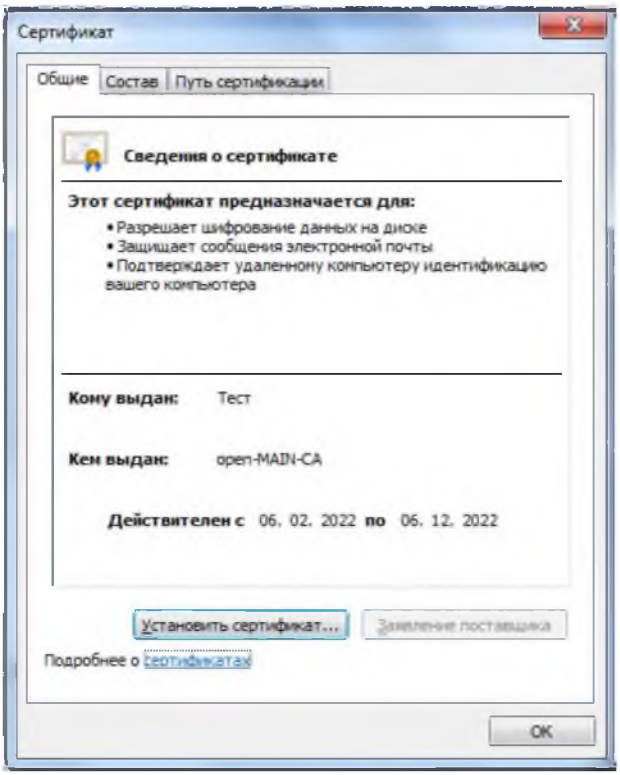

Рисунок 2.5 – Підключення до депозитарію відкритих ключів і отримання відкритих ключів респондентів

6 Відкриває створену сторінку в додатку Adobe Acrobat.

7. Переходить на вкладку «Tools» і в розділі «Enscript» формує (або обирає готову) стратегію захисту документа, яка передбачає тип шифрування й можливості використання документа користувачами.

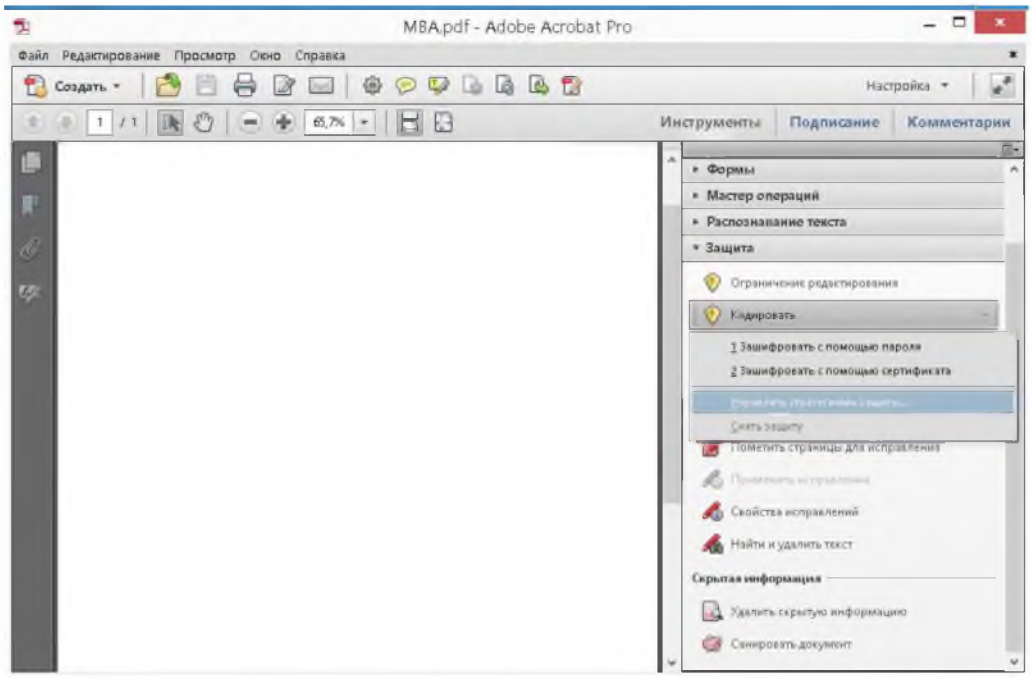

Рисунок 2.6 – Перехід на вкладку «Tools» і формування стратегії захисту документа

8. У процесі створення стратегії захисту обирає її параметри (рисунок 2.7).

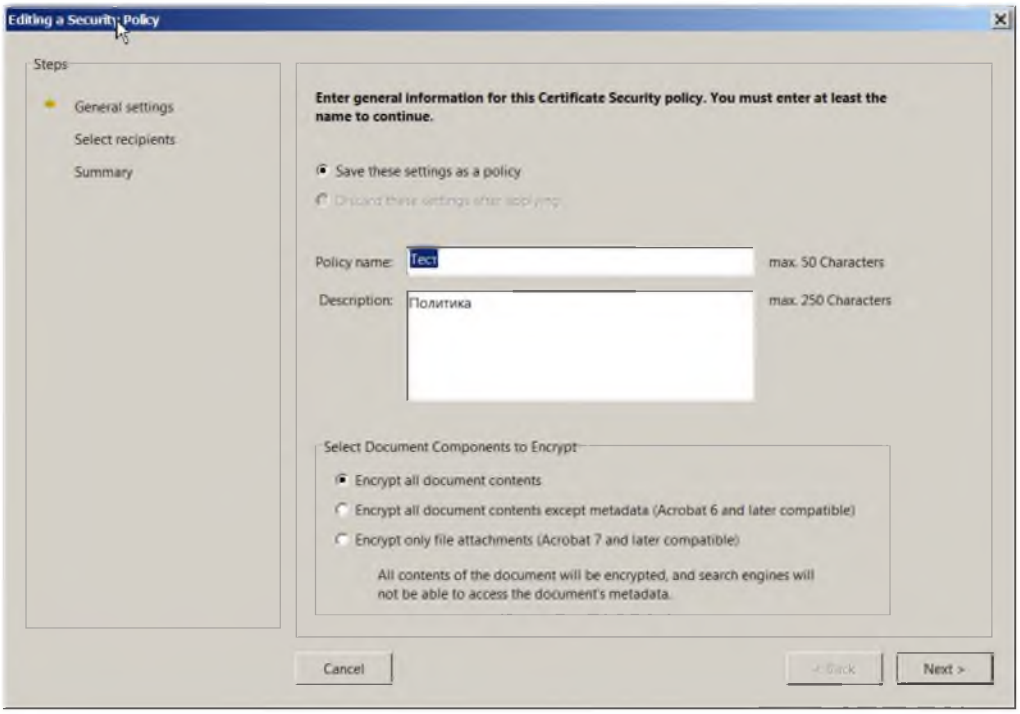

Рисунок 2.7 – Вибір параметрів стратегії захисту

9. Після створення стратегії захисту вона застосовується до документа. Документ може бути відкритий у безкоштовному додатку Adobe Reader (рисунок 2.8).

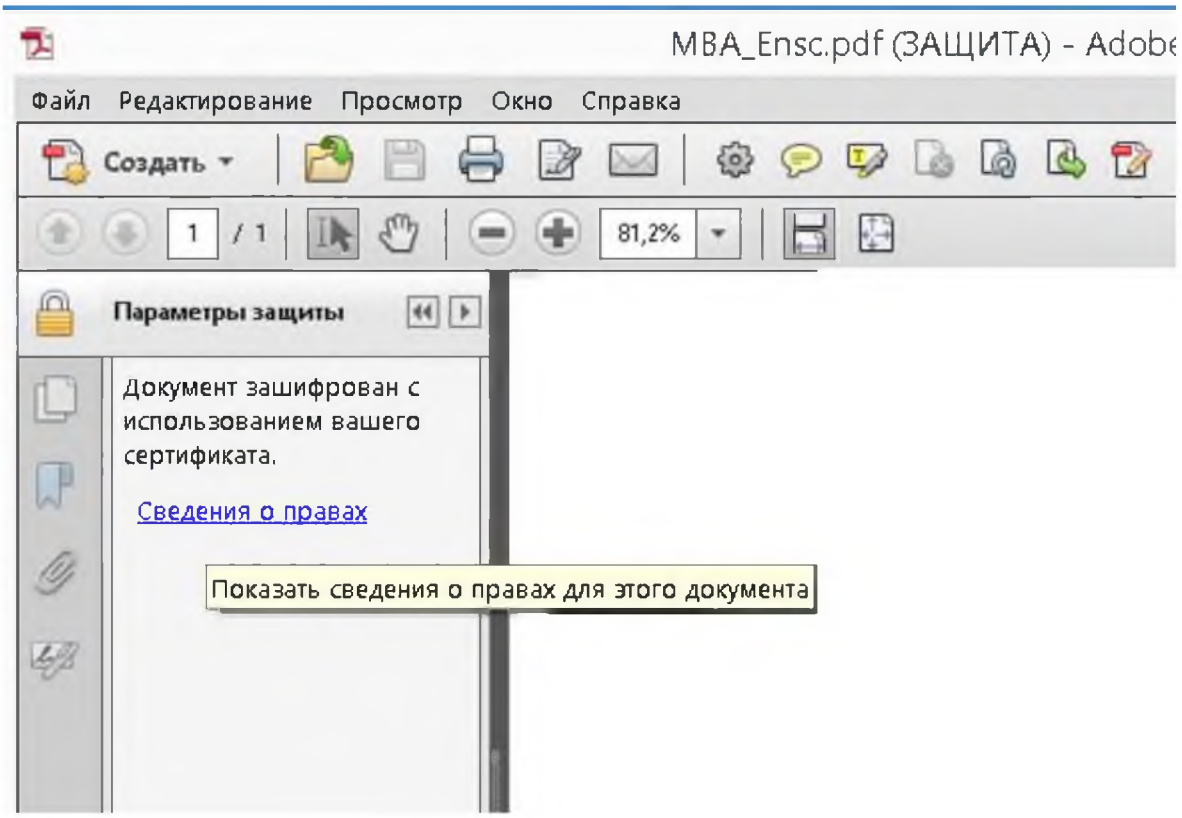

Рисунок 2.8 – Відкриття документу респондентом після створення стратегії захисту у додатку Adobe Reader

2.14 Висновки

1 Багато організацій, які все ще не наважуються впроваджувати у себе системи з віддаленими та мобільними користувачами, виправдовують таку свою поведінку побоюваннями за безпеку своїх даних. У сфері безпеки організації найбільше стурбовані такими факторами, як захист даних, що знаходяться поза контрольованої зони;

2 При розгортанні в інформаційній системі сервісів для доставки відео для віддалених та мобільних користувачів організація повинна замислитися над дотриманням вимог забезпечення інформаційної безпеки даних. Репрезентовані у

роботі рішення обґрунтовують:

- можливість безпечного віддаленого доступу по захищеним каналом до сучасних послуг корпоративної інформаційної системи процесів типу сайти, відеоконференції, потоку відео тощо, із шифруванням трафіка на всіх етапах передачі інформації;
- визначення проблеми безпеки при доставці відео контенту користувачів інформаційної системи підприємства, які знаходяться за межами контрольованої зони, розробку алгоритму створення інфраструктури, розробку алгоритму створення, зберігання, доставки документа з впровадженим відео потоком, розробку алгоритму використання документа, вибір програмних елементів інфраструктури, проведення експериментальної перевірки отриманих результатів.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Визначення трудовитрат на науково-технічну розробку алгоритму

Визначення трудомісткості проекту дозволяє оцінити необхідні трудові ресурси, а також тривалість роботи. У загальному випадку, вона визначається як сума трудомісткості кожного алгоритму, що розробляється.

Розраховуємо трудомісткість для кожного етапу проведення дослідження по таких основних частинах:

t_n – витрати праці на підготовку і опис поставленого завдання;

t_a – витрати праці на дослідження алгоритмів;

t_o – витрати праці на оптимізацію методик з дослідження алгоритмів;

t_p – витрати праці на проведення розрахунку параметрів і критеріїв алгоритмів;

$t_м$ – витрати праці на аналіз отриманих результатів;

$t_д$ – витрати праці на підготовку документації по завданню.

Оцінка витрат праці на підготовку й опис завдання залежить від конкретних умов. У нашому випадку t_n по кожному алгоритму буде становити 1 людино-годину.

Оцінка витрат праці на інші складові трудомісткості проекту визначаємо на підставі підрахунку умовної кількості параметрів і характеристик систем, що обробляються, у тому числі й параметрів та критеріїв, які необхідно буде розрахувати у процесі дослідження.

Розраховуємо витрати праці на алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, здатної підвищити рівень захищеності електронного документа, що містить потік відео для віддалених та мобільних співробітників.

Умовна кількість параметрів при розрахунку становить:

$$Q = q \cdot c \cdot (1 + p), \qquad (3.1)$$

де q – кількість параметрів, що обробляються;

c = 1,25...2,0 – коефіцієнт складності алгоритму;

p = 0,05...0,1 – коефіцієнт корекції алгоритму в процесі його обробки, що відповідає внесенню 3...5 корекцій, які спричиняють переробку 5-10% готового розрахунку.

Приймаємо q = 250;

c = 1,5;

p = 0,065.

Тоді за формулою (3.1)

$$Q = 250 \cdot 1{,}5\ (1 + 0{,}065) = 400.$$

Витрати праці на вивчення опису завдання визначаються з урахуванням уточнення опису й кваліфікації виконавця роботи з формули (3.2):

$$t_a = \frac{Q \cdot B}{(75...85) \cdot k} = \frac{400 \cdot 1{,}3}{75 \cdot 1} = 6{,}9 \text{ людино-годин}, \qquad (3.2)$$

де B = 1,2...1,5 – коефіцієнт збільшення витрат праці в наслідок недостатнього опису завдання;

k–коефіцієнт кваліфікації працівника, що визначається залежно від стажу роботи за профілем. При стажі роботи від 2 до 3 років k = 1.

Витрати праці на обробку методики рішення завдання знаходимо з формули (3.3):

$$t_o = \frac{Q}{(20...25) \cdot k} = \frac{400}{20 \cdot 1} = 20 \text{ людино-годин}. \qquad (3.3)$$

Витрати праці на розрахунок параметрів і критеріїв відповідності завданню за обраною методикою знаходимо з (3.4):

$$t_p = \frac{Q}{(20...25)\cdot k} = \frac{400}{20\cdot 1} = 20 \text{ людино-годин.} \qquad (3.4)$$

Витрати праці на аналіз отриманих результатів розраховуються за наступною формулою (3.5):

$$t_m = 1{,}5\cdot\frac{Q}{(4...5)\cdot k} = 1{,}5\cdot\frac{400}{4{,}5\cdot 1} = 133 \text{ людино-години.} \qquad (3.5)$$

Витрати праці на підготовку документації за завданням визначаються за формулою (3.6):

$$t_д = t_{др} + t_{до}, \text{ людино-годин,} \qquad (3.6)$$

де $t_{др}$ – трудомісткість підготовки матеріалів до запису проведених розрахунків;

$t_{до}$ – трудомісткість редагування, печатання й оформлення документації знаходимо за виразами (3.7)... (3.9)

$$t_{др} = \frac{Q}{(15...20)k} = \frac{400}{20\cdot 1} = 20 \text{ людино-годин;} \qquad (3.7)$$

$$t_{до} = 0{,}75 t_{др} = 0{,}75\cdot 20 = 15 \text{ людино-годин;} \qquad (3.8)$$

$$t_д = 20 + 15 = 35 \text{ людино-годин.} \qquad (3.9)$$

За таким ж принципом розраховано витрати праці для двох наступних алгоритмів.

Розрахунок трудомісткості за обраною методикою наведений у таблиці 3.1.

Таблиця 3.1 – Розрахунок трудомісткості

Стадія проведення НДР	Трудомісткість, чол.-г
1	2
1 Підготовка та опис поставленого завдання t_n:	
1.1 Алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, здатної підвищити рівень захищеності електронного документа, що містить потік відео для віддалених та мобільних співробітників	1
1.2 Алгоритм створення, зберігання, доставки документа з впровадженим відео потоком	1
1.3 Алгоритм використання документу віддаленим та мобільним співробітником підприємства	1
2 Аналіз існуючих алгоритмів t_a	
2.1 Алгоритми створення інфраструктури інформаційно-комунікаційної системи підприємства, здатної підвищити рівень захищеності електронного документа, що містить потік відео для віддалених та мобільних співробітників, визначення ступіні відповідності алгоритмів вимогам ТЗ	6,9
2.2 Алгоритм створення, зберігання, доставки документа з впровадженим відео потоком, визначення ступіні відповідності алгоритмів вимогам ТЗ	5,6
2.3 Алгоритм використання документу віддаленими та мобільними співробітниками підприємства, визначення ступіні відповідності алгоритмів вимогам ТЗ	2,8
3 Оптимізація існуючих методик (розробка алгоритомів) t_o	
3.1 Алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, здатної підвищити рівень захищеності електронного документа, що містить потік відео для віддалених та мобільних співробітників	20

Продовження таблиці 3.1

1	2
3.2 Алгоритм створення, зберігання, доставки документа з впровадженим відео потоком	16
3.3 Алгоритм використання документу віддаленими та мобільними співробітниками підприємства	8
4 Опрацьовування t_p	
4.1 Алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, здатної підвищити рівень захищеності електронного документа, що містить потік відео для віддалених та мобільних співробітників. Витрати розробника на виготовлення й тестування програмного забезпечення	20
4.2 Алгоритм створення, зберігання, доставки документа з впровадженим відео потоком. Витрати розробника на виготовлення й тестування програмного забезпечення	16
4.3 Алгоритм використання документу віддаленими та мобільними співробітниками підприємства. Витрати розробника на виготовлення й тестування програмного забезпечення	8
5 Аналіз отриманих результатів $t_м$	
5.1 Алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, здатної підвищити рівень захищеності електронного документа, що містить потік відео для віддалених та мобільних співробітників. Витрати на імітаційне моделювання й проведення комплексного аналізу протікання процесу	133,3
5.2 Алгоритм створення, зберігання, доставки документа з впровадженим відео потоком. Витрати на імітаційне моделювання й проведення комплексного аналізу протікання процесу	106,7
5.3 Алгоритм використання документу віддаленими та мобільними співробітниками підприємства. Витрати на імітаційне моделювання й проведення комплексного аналізу протікання процесу	53,3
6 Підготовка документації $t_д$	

6.1 Алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, здатної підвищити рівень захищеності електронного документа, що містить потік відео для віддалених та мобільних співробітників	35
6.2 Алгоритм створення, зберігання, доставки документа з впровадженим відео потоком	28
6.3 Алгоритм використання документу віддаленими та мобільними співробітниками підприємства	14
Усього	476,6

3.2 Розрахунок витрат на НДР

Витрати на створення алгоритмів визначаються на основі годинної тарифної заробітної плати розробника й машинного часу з урахуванням спожитої електроенергії й використаного програмного забезпечення знаходимо згідно з (3.9) [31].

$$K_{пз} = З_{зп} + З_{мч}. \quad (3.9)$$

Заробітна плата виконавця враховує мінімальну заробітну плату, а також відрахування на соціальні потреби (єдиний соціальний внесок 22%) і визначається за формулою (3.10):

$$З_{зп} = t \cdot З_{пр} = 476,6 \cdot 40,46 = 19283,24 \text{ грн}, \quad (3.10)$$

де t = 476,6 – загальна тривалість створення розробки, годин;

$З_{пр}$ = 40,46 грн/год – мінімальна заробітна плата в Україні на 01.10.2022 з нарахуваннями.

Вартість машинного часу знаходимо з (3.11):

$$C_{мч} = C_{мг} \cdot t = 14{,}17 \cdot 476{,}6 = 6753{,}42 \text{ грн}, \quad (3.11)$$

де $C_{мг}$ – вартість 1 години машинної години ПК, грн./час.

Вартість 1 години машинної години ПК визначається за формулою (3.12):

$$C_{мч} = PtP_e + \frac{Ф_{зал} H_a}{F_p} + \frac{K_{лпз} H_{амз}}{F_p}; \quad (3.12)$$

$$C_{мч} = 0{,}8 \cdot 1 \cdot 1{,}44 + \frac{9000 \cdot 0{,}5}{1920} + \frac{82000 \cdot 0{,}25}{1920} = 14{,}17 \text{ грн/рік},$$

де $P = 0{,}8$ – встановлена потужність ПК, кВт;

P_e =1,44 грн/кВт·год – тариф на електричну енергію;

$Ф_{зал}$ = 9000 грн – залишкова вартість ПК на поточний рік;

H_a = 0,5 – річна норма амортизації на ПК, частки одиниці;

$H_{апз}$ = 0,25 – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ = 82000 грн, вартість ліцензійного програмного забезпечення, грн. згідно з таблицею 3.2;

F_p = 1920 год – річний фонд робочого часу (за 40-годинним робочим тижнем).

Таблиця 3.2 – Вартість необхідного програмного забезпечення

Програмне забезпечення	Вартість, грн
Adobe Acrobat	7000
Adobe Media Server	19000
Microsoft Forefront Server	15000

MS SQL Server 2022	41000
Усього	82000

Таким чином, капітальні (фіксовані) витрати на проектування розроблених алгоритмів будуть становити (3.13):

$$К = З_{зп} + С_{мч} = 19283,24 + 6753,42 = 26036,66 \text{ грн.} \quad (3.13)$$

3.3 Висновок

Практична цінність роботи визначається створенням готових до безпосереднього застосування й реалізованих для виконання практичних вимог до діючої УЦ оригінальних моделей і алгоритмів, що дозволяють розробити рекомендації з керування сертифікатами ключів.

ВИСНОВКИ

Відповідно з метою роботи та технічним завданням у даній кваліфікаційній роботі були виконані такі завдання:

– визначено проблеми безпеки при доставці відео контенту віддаленим та мобільним користувачам інформаційно-комунікаційної системи підприємства;

– розроблено алгоритм створення інфраструктури інформаційно-комунікаційної системи підприємства, яка підвищує рівень захищеності електронного документа, що містить відео для віддалених та мобільних співробітників;

– розроблено алгоритм створення, зберігання, доставки документа з впровадженим відео потоком;

– розроблено алгоритм використання документа віддаленими та мобільними співробітниками підприємства;

– розроблена архітектура інформаційно-комунікаційної системи підприємства, що реалізують наведені вище алгоритми;

– вибрано програмні елементи інфраструктури для реалізації наведених алгоритмів;

– розроблені рекомендації щодо політики видачі, відкликання та відновлення сертифікатів для віддалених та мобільних користувачів;

– проведена експериментальна перевірка отриманих результатів.

Все це створює можливість підвищення рівня захищеності електронного документа, що містить відео потік для віддалених та мобільних співробітників підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1 Raina K, PKI Security Solutions for Enterprise: Solving HIPAA, E-Paper Act and Other Compliance Issues.: Wiley Publishing Inc., 2003.

2 RFC2559 LDAP V2 Operational Protocols.

3 CCITT. Recommendation X.800: Security Architecture for Open Systems Interconnection for CCITT Applications. Geneva, 1991.

4 Kiran S., Lareau P., Lloyd S. PKI Basics – A Technical Introduction // A PKI Forum Note. November 2002.

5 Adams C., Lloyd S. Understanding PKI. Concepts, Standards and Deployment Consideration. Second Edition. Addison-Wesley, 2003.

6 Kuhn D.R., Hu Vincent C., Polk W.T, Chang Shu-Jen. Introduction to Public Key Technology and the Federal PKI Infrastructure // National Institute of Standards and Technology – February, 2001.

7 RFC2527. Certificate Policy and Certification Practices Framework.

8 Jarupunphol P., Mitchell C. PKI implementation issues in B2B e-commerce EICAR // Conference Best Paper Proceedings, 2003.

9 Рапоза Д. Незнакомая PKI, PC Week/RE, январь 2001.

10 Security Service API: Cryptographic API Recommendation Second Edition, NSA Cross Organization CAPI Team July 1, 1996.

11 PKCS#11 Cryptographic Token Interface (Cryptoki).

12 PKI Interoperability Framework. PKI Forum White Paper.

13 Extensible Markup Language (XML) 1.0 (Third Edition).

14 OASIS Security Services (Security Assertion Markup Language – SAML) TC.

15 XML Key Management Specification (XKMS 2.0).

16 Raina K, PKI Security Solutions for Enterprise: Solving HIPAA, E-Paper Act and Other Compliance Issues.: Wiley Publishing Inc., 2003.

17 Татарчук М.І. Корпоративні інформаційні системи. Навчальний посібник. – К.: КНЕУ, 2005. – 291 с.

18 Управление сертификатами (Электрон. Ресурс)/Способ доступа: URL: http://technet.microsoft.com/ru-ru/library/cc771377%28WS.10% 29.aspx - Загол. з екрану.

19 Шаблоны сертификатов (Электрон. Ресурс)/Способ доступа: URL: http://technet.microsoft.com/ru-ru/library/cc730705%28WS.10% 29.aspx - Загол. з екрану.

20 Обзор PKI предприятия (Электрон. Ресурс)/Способ доступа: URL: http://technet.microsoft.com/ru-ru/library/cc771026%28WS.10%29.aspx - Загол. з екрану.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	4	
4	А4	Вступ	2	
5	А4	1 Розділ	46	
6	А4	2 Розділ	30	
7	А4	3 Розділ	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу магістра на тему:
Підвищення рівня захищеності мультимедійного контенту в інформаційно-телекомунікаційній системі підприємства
Ляш Данила Вячеславовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 102 сторінках та містить 11 рисунків, 5 таблиць, 20 джерел та 4 додатка.

Об'єкт розробки: інформаційно-комунікаційна система підприємства, що виробляє, зберігає і постачає мультимедійний контент віддаленим та мобільним співробітникам.

Мета роботи: підвищення рівня захищеності електронного документа, що містить потік відео, для віддалених та мобільних користувачів.

У спеціальній частині дана характеристика предмету досліджень; визначені проблеми безпеки та розроблено алгоритм розгортання інфраструктури доставки відео контенту віддаленим та мобільним співробітникам підприємства; розроблено алгоритми створення, зберігання, доставки та використання документа; розроблено архітектуру інформаційно-комунікаційної системи, що здатна реалізувати ці алгоритми.

У роботі наведені програмні елементи інфраструктури для реалізації алгоритмів та рекомендації щодо політики видачі, відкликання і відновлення сертифікатів для віддалених та мобільних користувачів; проведена експериментальна перевірка отриманих результатів.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник