ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Систем захисту електронного документообігу в корпоративних мережевих каналах»

на здобуття освітнього ступеня магістра
зі спеціальності __125 - _Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ 61
КАЛІШ Владислав

Керівник:__ІВАНЧЕНКО Ігорь_____
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент:_____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

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

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___125-Кібербезпека та захист інформації_____
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр Туровський

«____» _____ 2024 р.

ЗАВДАННЯ
НАКВАЛІФІКАЦІЙНУРОБОТУ

_____Калішу Владиславу В`ячеславовичу_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Систем захисту електронного документообігу в корпоративних мережевих каналах»
керівник кваліфікаційної роботи: ____ІВАНЧЕНКО Ігорь к.т.н., доцент_____

затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
__Загрози витоку інформації матеріально-речовим каналом.
__Технічна система охорони для протидії витоку інформації матеріально-речовим каналом.
__Надійність захисту інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.__Дослідження систем електронного документообігу_____
2.__Аналіз ефективності алгоритмів та стандартів захисту систем електронного документообігу____
3.__Розробка заходів підвищення захисту систем електроного документообороту_____
5. Перелік графічного матеріалу: ___Презентаційний матеріал на 15 слайдах_____

6. Дата видачі завдання _____20.10.2024 ___ _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ _Владислав КАЛІШ___
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ __Ігорь ІВАНЧЕНКО_
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина бакалаврської (магістерської) кваліфікаційної роботи: стор., рис., табл., джерел.

Об'єкт дослідження – Процес захисту систем в електронному документообороту.

Предмет дослідження – Захист інформації від витоку в мережевих каналах передачі інформації.

Мета роботи– Підвищити надійність захисту електронного документообороту в в мережевих каналах.

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

У роботі проаналізовано загрози інформації, що передається через мережеві канали. Розглянуто можливість використання системи шифрування даних та засобів мережевої безпеки для захисту інформації в системі електронного документообігу.

Ґрунтуючись на проведеному дослідженні, розроблено рекомендації щодо підвищення надійності захисту інформації від несанкціонованого доступу та витоку під час передачі даних мережевими каналами.

Галузь використання – захист інформації в системах електронного документообігу організацій.

Апробація:

Каліш В,В,, Котенко А.М. Порівняння криптографічних алгоритми хешування sha-3 та sha-256. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.90 - 91.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

МЕРЕЖЕВІ КАНАЛИ, ЗАГРОЗИ ІНФОРМАЦІЇ, ШИФРУВАННЯ ДАНИХ, МЕРЕЖЕВА БЕЗПЕКА, ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ІНФОРМАЦІЙНИЙ ЗАХИСТ.

ABSTRACT

The text part of the bachelor's (master's) qualification work: pages, figures, tables, sources.

Object of research is the process of protecting systems in electronic document circulation.

Subject of research is protection of information from leakage in network channels of information transmission.

Purpose is to increase the reliability of electronic document flow protection in network channels.

Research methods is system analysis, numerical methods, study of literature on this topic.

The paper analyzes the threats of information transmitted through network channels. The possibility of using the data encryption system and network security tools to protect information in the electronic document management system is considered.

Based on the study, recommendations have been developed to improve the reliability of information protection against unauthorized access and leakage during data transmission over network channels.

Branch of use - information protection in electronic document management systems of organizations.

Kalish VV, Kotenko A.M. Comparison of cryptographic hashing algorithms sha-3 and sha-256. All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 3, 2024, Kyiv: RVC DUIKT. – 024. P.90 - 91.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

NETWORK CHANNELS, INFORMATION THREATS, DATA ENCRYPTION, NETWORK SECURITY, ELECTRONIC DOCUMENT MANAGEMENT, UNAUTHORIZED ACCESS, INFORMATION PROTECTION.

Зміст

ВСТУП 8
1.ДОСЛІДЖЕННЯ СИСТЕМ ЕЛЕКТРОНОГО ДОКУМЕНТООБІГУ 10
1.1. Дослідження систем електронного документообігу 10
1.2. Загрози системам електронного документообігу 13
1.3 Загрози для інформації в мережевих каналах передачі даних. 15
1.4 Методи забезпечення безпеки мережевих каналів для систем електронного документообігу. 18
1.5 Аналіз міжнародного досвіду з підвищення безпеки систем електронного документообігу. 22
Висновки до першого розділу. 26
2. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ ТА СТАНДАРТІВ ЗАХИСТУ 27
2.1 Оцінка надійності та швидкодії криптографічних алгоритмів. 27
2.2 Аналіз алгоритмів хешування. 31
2.3. Використання алгоритмів хешування, криптографії та різних систем безпеки в системах електронного документообігу. 35
Висновки до другого розділу 37
3.АНАЛІЗ СИСТЕМ ДЛЯ РОБОТИ З ЕЛЕКТРОНИМИ ДОКУМЕНТАМИ 39
3.1.Використання ІІТ-Користувач 39
3.2 Використання центрального засвідчуваного органа. 40
3.3.Порівняння аналізів досліджених систем для роботи з електронними документами. 43
Висновки до третього розділу 44
4.ПІДВИЩЕННЯ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОНОГО ДОКУМЕНТООБОРОТУ 46
4.1.Шифрування даних електронних документів 46
4.2.Використання систем авторизації 50
4.3. Захист мережних з'єднань TCP\IP 54
4.4.Використання блокчейну для захисту систем електронного документообороту 57
Висновки до четвертого розділу 60
ВИСНОВКИ 62
ПЕРЕЛІК ПОСИЛАНЬ 62
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СДО– системи електронний документообіг

AES – Advanced Encryption Standard

MFA– багатофакторна авторизація

ЦЗО– центральний засвідчуваний орган

БД-база даних

ЕЦП – електронний цифровий підпис

IV – вектор ініціалізації

VPN – віртуальна приватна мережа

ВСТУП

Актуальність дослідження: У сучасному світі питання інформаційної безпеки набувають все більшого значення, особливо в контексті електронного документообігу та поширення мережевих технологій. Керівництво компаній та організацій активно шукає рішення для забезпечення безпеки інформації, що передається мережевими каналами, впроваджуючи новітні технології захисту та інструменти управління безпекою даних. З розвитком цифрових технологій зростає ризик несанкціонованого доступу, втручання в роботу систем та витоку інформації під час передачі даних мережами.

Мережевий канал передачі інформації є одним з найважливіших елементів системи електронного документообігу. Тому важливо оцінювати рівень їх захищеності, проводити регулярний аналіз загроз, впроваджувати нові засоби криптографічного захисту та постійно контролювати їх безпеку. Несанкціонований доступ або порушення безпеки під час передачі даних може призвести до значних фінансових втрат і репутаційних збитків для компанії.

Захист мережевих каналів вимагає використання таких технологій, як шифрування, брандмаузери, системи виявлення вторгнень та інші інструменти мережевої безпеки. З огляду на постійно зростаючі кіберзагрози, важливо адаптувати сучасні рішення, які підвищують надійність захисту даних під час передачі.

Тому необхідність підвищення безпеки систем електронного документообігу в мережевих шляхах передачі інформації є актуальною і потребує поглибленого дослідження та впровадження новітніх технологічних рішень. Тому тема магістерської роботи, присвячена підвищенню безпеки систем електронного документообігу в мережевих каналах передачі інформації, є доречною.

Об’єкт дослідження – Процес захисту систем в електронному документообороту.

Предмет дослідження – Захист інформації від витоку в мережевих каналах передачі інформації.

Мета роботи– Підвищити надійність захистуелектронного документообороту в мережевих каналах.

Наукові завдання:

дослідити загрози витоку інформації в мережевих каналах передачі даних;
встановити сутність захисту інформації в мережевих каналах передачі;
проаналізувати технічні засоби захисту інформації в мережевих каналах;
розробити систему захисту інформації в мережевих каналах передачі для підвищення безпеки електронного документообігу.

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

Практичне значення одержаних результатів полягає у розробці системи захисту інформації в мережевих каналах передачі даних, а також у формуванні рекомендацій щодо підвищення безпеки інформації під час електронного документообігу.

Розділ 1.

ДОСЛІДЖЕННЯ СИСТЕМ ЕЛЕКТРОНОГО ДОКУМЕНТООБІГУ

1.1.Дослідження систем електронного документообігу

Багато країн відчувають значні зміни у своєму підході до СДО. Традиційно ці системи розглядаються в першу чергу як інструменти для документування організаційної діяльності та полегшення співпраці. Але в сучасному висококонкурентному і швидко мінливому бізнес-середовищі керівники організацій намагаються вийти за рамки традиційної квартальної або щомісячної звітності. Існує зростаюча потреба в реальному часі видимості прогресу до цілей, і СДО має важливе значення для сучасних бізнес-операцій.

СДО є важливим для оптимізації робочого процесу вашої організації та покращення можливостей керування документами. Вони надають співробітникам надійні інструменти для моніторингу та управління станом завдань в режимі реального часу. Основною перевагою цих систем є універсальні можливості працювати самостійно або без зайвих проблем інтегрувати у власну цифрову екосистему, яка включає управління проектами, управління відносинами з клієнтами та різні функції управління.

Однією з основних особливостей СДО є можливість управління розподіленими документами, що полегшує співпрацю і обмін між співробітниками незалежно від географічного положення. Цей функціонал дозволяє членам команди отримувати доступ, редагувати та працювати з документи на декількох пристроях, значно знижуючи витрати які пов'язані з друком та розповсюдженням фізичних копій. Ця гнучкість полегшує більш повне та динамічне робоче середовище, роблячи можливим співробітництво в реальному часі з будь-якого місця.

Крім того, інтеграція електронних підписів в рамках СДО зробила революцію в процесі затвердження документів. Співробітники можуть швидко підписати важливі документи, затвердити завдання і призначити обов'язки

всього за декілька кліків. Ця інновація спрощує робочі процеси, зменшує затримку та підвищує загальну продуктивність в організаціях. Швидкість, що забезпечується за допомогою СДО, не тільки підвищує операційну ефективність, але також сприяє культурній співпраці, яка дозволяє організаціям більш ефективно реагувати на завдання та виклики.

СДО відіграють важливу роль у сучасних організаціях шляхом значного підвищення ефективності та забезпечення відповідності різним нормативним стандартам. Хоча багато СДО мають спільний інтерфейс і базову функціональність.Але є помітні відмінності в вартості реалізації та обслуговування. Основним фактором, що відрізняє ці системи один від одного є особливості, які адаптовані до унікальних потреб різних організацій.

Значення СДО в сучасному цифровому середовищі неможливо переоцінити. Ці системи необхідні для поліпшення як доступності, так і безпеки важливих документів. Ці системи забезпечують централізоване зберігання документів, оновлення в режимі реального часу і дозволяє співробітникам отримувати доступ до важливих файлів з різних місць. Ця доступність полегшує гнучкі бізнес-процеси та підвищує прозорість всередині команди. Окрім цього, менеджери можуть відстежувати історію документів, відстежувати зміни та аналізувати активність користувачів, що необхідно для підтримки підзвітності та розвитку позитивної організаційної культури.

СДО особливо цінні, так як допомагають організаціям дотримуватися різних нормативних та законодавчих вимог. Це особливо важливо в таких областях, як охорона здоров'я, фінанси та уряд, де важливо приймати швидкі рішення та дотримуватися суворих правил щодо збереження документів та конфіденційності. Автоматизуючи критичні процеси, такі як зберігання документів, класифікація та архівація, організації можуть краще відповідати стандартам відповідності, таким як загальний регламент захисту даних та закон про портативність та підзвітність медичного страхування.

СДО пропонують кілька переваг, які значно підвищують операційну ефективність, але організації повинні бути в курсі і готові до деяких потенційних

проблем, які можуть виникнути під час впровадження. Однією з таких є вартість, оскільки вартість може сильно відрізнятися залежно від конкретної функціональності та вимог до масштабованості вибраноїСДО. Організації повинні провести комплексний аналіз витрат і вигод, щоб визначити, яка система найкраще відповідає їх потребам і бюджетам.

Ще однією з важливий проблем є інтеграція СДО з існуючою інфраструктурою. Це може бути дуже складно, особливо для організацій, які покладаються на застарілі системи, які можуть бути несумісні з останніми цифровими інструментами. Успішна інтеграція часто вимагає значної кількості часу, а також спеціалізованих технічних навичок, які не легко доступні всередині компанії. Організаціям може знадобитися участь у додатковому тренінгу для співробітників компанії та IT-персоналу для забезпечення плавного переходу.Навчання та підбір персоналу також є важливими факторами для успішної реалізації СДО. Це може включати в себе багатогранний підхід, такий як живі демонстрації, практичні заняття та комплексні посібники користувача, які можуть бути використані для підвищення якості цифрових інструментів на різних рівнях персоналу. Його пристосували до грамотності.

Існує ще більш складний транспортний рівень даних. Перехід від традиційних паперових систем і застарілих цифрових платформ до редагувань - це не просто перетворення документів у цифрові формати. Необхідний ретельний і системний підхід для того, щоб всі дані були точно оцифровані без втрат. Крім того, необхідно здійснити заходи щодо захисту цілісності даних під час процесу міграції.

На додаток до цих технічних проблем, організаціям необхідно посилити заходи безпеки для захисту конфіденційних даних під час і після переходу. Це включає в себе реалізацію надійних протоколів захисту даних, таких як шифрування, контроль доступу та періодичний аудит безпеки, щоб запобігти несанкціонованому доступу та зменшити ризик витоку даних. У сучасному цифровому середовищі де кіберзагрози стають все більш складними, підготовка до потенційних вразливостей особливо важлива.

1.2. Загрози системам електронного документообігу

Загрози для СДО можуть бути розділені на три основні характеристики безпеки:

- Загроза конфіденційності;
- Загрози цілісності;
- Загроза доступності.

ЕфективнаСДОскладається з трьох ключових компонентів:

- Сервери;
- Робочі станції;
- Канали зв'язку.

Загроза конфіденційностістановлять серйозний ризик несанкціонованого доступу до конфіденційної інформації. Як проявляються ці загрози, показано нижче:

- Фізичний несанкціонований доступ до робочих станцій дозволяє зловмиснику, який отримав критичні облікові дані, такі як логіни та паролі, отримати доступ до документів користувача. Якщо адміністративні повноваження скомпрометовані, зловмисник може отримати доступ до всіх документів СДОбез виявлення;
- Операційна система (ОС) серверних загроз:Доступ до сервера ОС дозволяє встановлювати шкідливе програмне забезпечення (віруси, шпигунські програми) і виступає в якості шлюзу для проникнення СДО. Зловмисники можуть легко створювати робочі станції, замінювати законні робочі станції або отримувати доступ до баз даних, потенційно надаючи їм повний контроль над всією системою;
- Загроза сервера СДО: зловмисник може підключитися безпосередньо до СДО, обійти сервер ОС та обійти ключові механізми безпеки;

- Контролюючи сервер БД, зловмисник може отримати безперешкодний доступ до збережених документів;
- загрози каналу зв'язку: Шляхом прослуховування ліній зв'язку зловмисник може перехоплювати пакети даних, що обмінюються між робочими станціями і серверами; реалізація зашифрованого протоколу типу HTTPS значно знижує ймовірність успішного перехоплення.

Загрози цілісності - виникають, коли дані втрачають первісну форму або якість. Вони включають в себе наступне:

- Пошкодження документів, що зберігаються на серверах баз даних або резервних копій. Це дуже важливо, оскільки ці документи часто містять конфіденційну інформацію, яка повинна бути захищена;
- Пошкодження сервера бази даних, операційної системи або сервера СДОпорушить інформаційні транзакції, але не знищить збережені документи;
- Апаратний збій, що впливає на канали зв'язку або брандмауери, тимчасово порушує доступ, але не ставить під загрозу цілісність збережених даних;

Загрози доступності не підлягають обговоренню, оскільки забезпечують постійний доступ до інформації. Такі загрози часто виникають через помилки користувача або адміністратора, які створюють вразливості, які можна використовувати.

Розуміння цих загроз дозволяє класифікувати потенційних нападників на кілька категорій

- Хакери;
- Конкуренти;
- Злочинні організації;
- Колишні співробітники;
- Техніки без доступу до СДО;

- Корпоративна система користувачів;
- Користувачі СДО;
- ІТ-адміністратори;
- Адміністратори СДО;
- Адміністратори інформаційної безпеки.

1.3 Загрози для інформації в мережевих каналах передачі даних.

Загрози обміну інформацією через мережі є однією з найбільш актуальних проблем сучасного цифрового суспільства. Оскільки інформаційні технології прогресують, а кількість даних, якими обмінюються мережі, зростає з кожним днем все більше, так само пов'язані з цим ризики безпеки. Мережеві канали діють як основне середовище для передачі даних, що робить їх основною метою для зловмисників, які прагнуть вкрасти, змінити або знищити інформацію. Розуміння цих загроз і навчання, як їх запобігти, має вирішальне значення для захисту як окремих осіб, так і організацій у взаємопов'язаному світі.

Однією з найпоширеніших загроз для мережевої інформації є несанкціоноване перехоплення даних. Це відбувається, коли зловмисники відстежують або «підслуховують» мережевий трафік для отримання конфіденційної інформації, такі як:

- Паролі;
- Фінансові дані;
- Особисті дані.

Несанкціоноване перехоплення даних часто використовує вразливості в мережевих протоколах, які недостатньо захищають шлях передачі інформацій. Цей тип атаки є особливо проблематичним, оскільки він часто залишається непоміченим, не даючи користувачам знати, що їх інформація була викрадена. Зловмисники можуть використовувати такі інструменти, як підміну пакетів, щоб захопити пакети даних, коли вони передаються мережею та витягують цінну

інформацію. Несанкціоноване прослуховування може мати серйозні наслідки, особливо в критичних для конфіденційності середовищах, таких як фінансові, медичні та урядові організації.

Поширена форма перехоплення даних відома як атака «man-in-the-middle» (MITM). У цьому типі атаки зловмисник може потрапити між двома комунікаційними сторонами для перехоплення і потенційно змінити обмін даними. Атаки MITM особливо небезпечні, оскільки вони можуть бути непоміченими. Ці атаки можуть націлюватися на різні типи з'єднань, включаючи незашифровані HTTP-запити та більш безпечні з'єднання SSL/TLS. Специфічною технікою, що використовується в таких атаках, є видалення SSL, де зловмисник змушує безпечне HTTPS-з'єднання знижуватися до небезпечного HTTP-з'єднання. Це зниження може піддавати конфіденційну інформацію несанкціонованому доступу.

Протокол SSL/TLS призначений для захисту від такого підслуховування, але зловмисники можуть обійти цей захист, якщо використовувана версія застаріла або неправильно налаштована. Наприклад, старі протоколи SSL мають вразливості, які можна використовувати для взлому систем, тому організаціям важливо регулярно оновлювати свої заходи безпеки.Крім прослуховування, підробка даних є ще одним серйозним ризиком. Зловмисники можуть змінювати або вводити фальшиву інформацію під час передачі даних, що може мати руйнівні наслідки. Це може статися шляхом прямого злому системи, яка обробляє або передає дані, або шляхом втручання в сам мережевий протокол. Така підміна даних може обдурити осіб, які приймають рішення, які покладаються на точність отриманої інформації, що призводить до стратегічних помилок, економічних втрат і втрати довіри користувачів. [19]

Наприклад, фальсифікація фінансових звітів, переданих між банками, може спотворити фінансові ринки. У сфері охорони здоров'я фальсифікована інформація може поставити під загрозу життя пацієнтів, якщо медичні працівники приймають рішення про лікування на основі неточних даних. Ці

потенційні наслідки підкреслюють, що фальсифікація даних є серйозною загрозою цілісності важливої галузі.Одним з найбільш ефективних заходів проти мережевих загроз є шифрування. Шифрування створює сильний бар'єр для перехоплення даних шляхом перетворення інформації у формат, який не може бути зрозумілим неавторизованим користувачам; протоколи, такі як SSL/TLS, створюють зашифроване з'єднання між користувачем і сервером, так що навіть якщо дані перехоплюються, воно не може бути прочитано неавторизованими сторонами. Однак ці протоколи не є досконалими, особливо якщо використовуються старі версії або ключ шифрування був скомпрометований. Експерти з безпеки рекомендують регулярно оновлювати методи шифрування та оцінювати силу шифрування, щоб запобігти потенційним порушенням. На додаток до шифрування, сильні механізми аутентифікації також необхідні для підвищення безпеки. Наприклад, багатофакторна аутентифікація вимагає ідентифікації за допомогою двох або більше методів, таких як пароль і одноразова комбінація коду, відправлена на мобільний пристрій; MFA додає важливий рівень захисту і значно ускладнює зловмисникові отримання доступу, навіть якщо пароль вкрадено. Впроваджуючи MFA, організації можуть зменшити ризик несанкціонованого доступу та краще захищати конфіденційні дані.

Доступність системи - ще одна сфера занепокоєння. Зловмисники часто намагаються закрити мережеві системи за допомогою атак відмови в обслуговуванні (DOS) і розподілених атак відмови в обслуговуванні (DDoS). Ці атаки переповнюють мережу надмірними запитами на отримку інформації, напружуючи ресурси та викликаючи перебої в обслуговуванні та значні затримки. Як результат, підприємства та громадські організації зазнають серйозного впливу, не в змозі ефективно працювати або надавати критичні послуги населенню. Цими діями робота сервісів порушується, що може призвести до значних фінансових втрат. Значні DDoS-атаки зазвичай спрямовані на фінансові установи, постачальників онлайн-послуг і навіть державні

відомства, підкреслюючи необхідність надійних оборонних механізмів для забезпечення доступності системи.

Іншою важливою технікою атаки є соціальна інженерія. На відміну від чисто технічних методів, соціальна інженерія передбачає маніпулювання людьми для отримання несанкціонованого доступу до конфіденційної інформації. Класичним прикладом цього є фішинг, де зловмисники надсилають фальшиві електронні листи або повідомлення, обманюючи одержувачів, щоб вони розкрили свої облікові дані для входу або інші особисті дані. Фішингові кампанії дуже ефективні, тому що вони вміло використовують людську психологію, щоб змусити людей повірити, що вони спілкуються з законною організацією. Такі атаки націлені на людський елемент безпеки і часто можуть обійти навіть найсучасніші технічні заходи.

Вразливості програмного забезпечення також становлять значний ризик для мережевої безпеки. Багато програм для керування мережею та передачі даних містять помилки та помилки, які можуть бути використані зловмисниками. Такі вразливості можуть бути результатом помилок програмування, поганої конфігурації безпеки або неадекватного тестування перед випуском продукту. Застарілі протоколи, такі як старі версії SSL, є особливо привабливими цілями для нападників і можуть бути легко скомпрометовані. Оскільки нові вразливості виявляються регулярно, постачальники програмного забезпечення повинні швидко випускати оновлення та патчі. Однак організації, які не застосовують ці оновлення, піддаються відомим вразливостям. Важливість управління патчами очевидна, враховуючи, що неперевірені вразливості призвели до деяких найбільших порушень даних у новітній історії.

1.4 Методи забезпечення безпеки мережевих каналів для систем електронного документообігу.

Оскільки організації переходять до цифрового обміну інформацією, забезпечення безпеки мережевих каналів СДО стало головним пріоритетом. Така еволюція документообігу спрощує різні задачі обробки, скорочує як часові, так і ресурсні витрати, значно підвищує операційну ефективність. Однак, оскільки ситуація з СДО продовжує розвиватися, пов'язані загрози також розвиваються, особливо пов'язані з несанкціонованим доступом до даних та перехопленням. В результаті захист інформації, що передається через ці мережеві канали, має вирішальне значення для захисту безпеки та конфіденційності вашої організації.

Одним з найважливіших компонентів забезпечення безпеки СДО є надійна реалізація технології шифрування. За своєю суттю шифрування даних - це процес перетворення конфіденційної інформації у формат, незрозумілий будь-кому, хто не має права доступу до неї. Цей захід захисту має важливе значення, оскільки він захищає дані, навіть якщо сторонні особи блокують дані під час передачі.

Для того, щоб досягти ефективного шифрування, важливо прийняти безпечні та надійні алгоритми шифрування. Ці алгоритми служать основою для перетворення зчитуваних даних в складний код. Розблокувати та прочитати вихідну інформацію можуть лише ті, хто має відповідний дозвіл, оснащений власними ключами для розшифрування.

Сучасні протоколи, такі як Secure Sockets Layer і Transport Layer Security, відіграють важливу роль у захисті передачі даних через Інтернет. Ці протоколи встановлюють безпечне розшифроване з'єднання між сервером і кінцевим користувачем. Це створює захисний бар'єр, який запобігає перехопленню або доступу до конфіденційної інформації між окремими особами та системами.

Важливість шифрування зростає ще більше, коли ви думаєте про такі загрози, як атаки «людина посередині» (MITM). У цих сценаріях зловмисник намагається підслуховувати повідомлення або розшифровувати повідомлення, що надсилаються між користувачами. СДО не тільки захищає від таких вторгнень, вживаючи суворі заходи шифрування, але також зміцнює довіру та

довіру до користувачів щодо безпеки їхніх конфіденційних документів та повідомлень.

Крім того, автентифікація користувача є ще одним важливим елементом безпеки мережі. Важливо, щоб доступ до системи був обмежений тільки авторизованими особами. Однією з найбільш ефективних стратегій підвищення безпеки є реалізація MFA. MFA додає рівень безпеки, який виходить за рамки традиційних комбінацій імені користувача та пароля. Цей метод вимагає від користувача отримати тимчасовий код на мобільному пристрої або забезпечити біометричну автентифікацію, таку як відбиток пальця або розпізнавання обличчя. Ці різні методи перевірки значно знижують ризик несанкціонованого доступу і роблять облікові записи користувачів більш стійкими до кіберзагроз. Ці інструменти дозволяють організаціям призначати різні рівні доступу для окремих користувачів або груп відповідно до їх конкретних ролей і обов'язків. Наприклад, одному користувачеві може бути надано дозвіл на перегляд документа, а іншому дозвіл на редагування або видалення файлів. Прийнявши чітко визначену структуру контролю доступу, організації можуть ефективно мінімізувати ризик несанкціонованих змін документів і в кінцевому підсумку запобігти втраті важливої інформації.

Крім того, захист мережевих каналів також включає забезпечення безпеки всієї мережевої інфраструктури від цілеспрямованих атак. Основні компоненти цієї системи захисту включають брандмауери, системи виявлення вторгнень, системи запобігання вторгнень та інструменти моніторингу трафіку. Брандмауери призначені для обмеження зовнішнього доступу до вашої мережі, блокуючи потенційно шкідливі дії та певні типи вхідного трафіку. З іншого боку, технологія системи виявлення вторгнень та системи запобігання вторгнень допомагає виявляти нові загрози і швидко реагувати на їх нейтралізацію не завдаючи шкоди функціонуванню системи та зберіганню даних. Ці системи необхідні для забезпечення захисту від спроб злому мережі та зовнішніх загроз, таких як відмова в обслуговуванні та розподілені атаки відмови в обслуговуванні.

Крім того, надійна інфраструктура СДО вимагає постійного моніторингу та контролю мережевої активності. Регулярний моніторинг не тільки забезпечує своєчасне виявлення аномальної поведінки, але і полегшує аналіз вразливостей і здійснення профілактичних заходів від несанкціонованого доступу. Важливо провести аудит безпеки, щоб переконатися, що ваша мережева інфраструктура відповідає встановленим стандартам безпеки і дозволяє швидко виявляти можливі загрози. Автоматизовані системи моніторингу можуть значно скоротити час реагування на інциденти та попередження менеджерів у реальному часі аномалій та спроб вторгнення.

Регулярні оновлення програмного забезпечення та своєчасне впровадження патчів безпеки також важливі для підтримки безпечного середовища. Вразливості програмного забезпечення часто забезпечують шлюз для зловмисників для використання системи, тому для організацій, які залежать від безпеки СДО. Важливо захистити всі системи включаючи операційні системи, програми та мережеве обладнання, щоб зменшити ризики, пов'язані з відомими вразливостями програмного забезпечення. Важливо переконатися, що всі компоненти оновлюються і вдосконалюються послідовно. Прийняття політики, яка вимагає оновлення на регулярному графіку має вирішальне значення для зміцнення захисту мережі.

Нарешті, необхідні ефективні заходи щодо резервного копіювання та відновлення даних для захисту систем СДО. Регулярно резервуючи дані та документи, організації можуть швидко відновити функціональність системи у разі кібератак або втрати даних. Багато організацій використовують стратегії резервного копіювання Multi-Decker, які зберігають дані між різними фізичними та хмарними платформами. Цей підхід забезпечує безперервність роботи бізнесу та цілісність конфіденційної інформації шляхом ефективного мінімізації ризику втрати інформації, викликаної технічними збоями та атаками шкідливих програм.

1.5 Аналіз міжнародного досвіду з підвищення безпеки систем електронного документообігу.

Аналіз міжнародного досвіду підвищення безпеки СДО важливий для розуміння кращих практик, які можуть бути застосовані до кожної країни. Оскільки електронний документообіг стає все більш поширеним у бізнесі та державних установах, захист цих систем має важливе значення для забезпечення конфіденційності, цілісності та доступності інформації. Вивчаючи міжнародні практики, ми можемо визначити успішні стратегії та способи зниження ризику та підвищення інформаційної безпеки.

Швеція стала лідером у сфері безпеки СДО встановлюючи помітні стандарти, яких повинні дотримуватися інші країни. Центральним у шведському підході є інтеграція передової системи електронного документообігу та надійної національної системи ідентифікації та сертифікації під назвою BankID. Ця інноваційна система підвищує надійність і безпеку цифрових взаємодій і дозволяє користувачам впевнено аутентифікувати себе при доступі та управлінні електронними документами. Крім того, зусилля Швеції щодо захисту електронних документів підтримуються комплексними правовими заходами щодо контролю за використанням цих електронних документів. Одним з ключових аспектів цієї нормативно-правової бази є юридичне визнання електронних підписів, що гарантує їх збереження тієї ж дійсності, що і традиційні рукописні підписи. Ця юридична гарантія сприяє підвищенню довіри між користувачами та бізнесом, полегшуючи навігацію цифровими транзакціями.Створена структура не тільки сприяє безпечному обміну документами між державними та приватними компаніями, а й сприяє розвитку та розширенню електронних сервісів по всій країні. Забезпечуючи міцну правову основу та передову технологічну інфраструктуру, Швеція заохочуватиме інновації та прийняття цифрових рішень, прокладаючи шлях до більш ефективного та безпечного майбутнього електронного документообігу.

Великобританія придбала ключовий досвід у сфері безпеки СДО через ініціативу Government Digital Services (GDS). Ця комплексна програма встановлює надійні стандарти безпеки, розроблені спеціально для прийняття та використання державних цифрових послуг.[38]

В основі ініціативи GDS лежать чітко визначені стандарти цифрових послуг та базова безпека, якої повинні дотримуватися всі цифрові послуги. Ці вимоги включають такі важливі аспекти, як захист даних, ефективне управління ризиками та доступність послуг для всіх користувачів. Впроваджуючи ці стандарти, уряд Великобританії прагне створити безпечне середовище для обробки конфіденційної інформації та гарантувати, що всі цифрові взаємодії є безпечними та надійними. Ключовим елементом підходу GDS до захисту цифрових послуг є передова безпека, включаючи технологію шифрування даних, яка захищає конфіденційні дані як в стані спокою, так і в дорозі. Крім того, GDS вимагає використання MFA для посилення процесу автентифікації користувачів, значно знижуючи ризик несанкціонованого доступу до критичних систем.Досвід Великобританії в ініціативі GDS підкреслює важливу роль стандартизації та нормативної бази в підвищенні безпеки та цілісності СДО. Встановлюючи чіткі рекомендації та дотримуючись суворих протоколів безпеки, ініціатива може не тільки захистити публічні дані, але й підвищити довіру суспільства до цифрових можливостей уряду. Ця модель служить цінним прикладом для інших країн, які прагнуть посилити власну практику електронного документообігу та безпеки.

Німецький підхід до безпеки СДО є особливо важливим і багатогранним. В основі цієї системи лежить вимога до кваліфікованих електронних підписів, які мають таку ж юридичну силу, як і традиційні рукописні підписи. Це положення гарантує, що електронні договори та документи зберігаються в правовому контексті та сприяє довірі до цифрових транзакцій.Згідно з німецьким законодавством, ці кваліфіковані електронні підписи видаються тільки сертифікованими постачальниками послуг електронного підпису. Ці постачальники проходять суворий процес сертифікації, який перевіряє заходи

безпеки та надійність роботи. В результаті користувачі можуть бути впевнені, що їх довірений підпис відповідає високим стандартам захисту від шахрайства та шахрайства.Крім того Німеччина робить сильний акцент на навчанні та навчанні користувачів, як ключовому елементі своєї стратегії безпеки СДО. Визнаючи, що лише технології не можуть запобігти порушенню безпеки, уряди та різні організації активно проводять інформаційні кампанії та тренінги. Ці ініціативи спрямовані на те щоб надати користувачам знання про потенційні загрози, такі як фішингові атаки та зловмисне програмне забезпечення, а також ефективні методи захисту в середовищі СДО. Завдяки такому комплексному підходу технології та користувачі сприяють безпечній системі електронного документообігу.

Скандинавські країни досягли значного прогресу у своєму підході до безпеки СДО і продемонстрували прихильність захисту конфіденційних даних. Одним з помітних прикладів є Норвегія, яка прийняла технологію блокчейн для підвищення цілісності даних.Блокчейн діє як децентралізований і розподілений реєстр, який записує транзакції між декількома комп'ютерами. Ця технологія забезпечує надійний рівень безпеки шляхом створення незмінних записів електронних документів. Це означає, що як тільки дані вводяться в блокчейн, вони не можуть бути змінені або видалені. Ця характеристика не тільки запобігає підробці, але і встановлює прозору історію всіх операцій пов'язаних з документом. На практиці використання блокчейна в СДО дозволяє ефективно відстежувати спроби модифікації документів. Кожного разу, коли робиться спроба зміни, слід залишається в книзі, що дозволяє легко визначити, хто і коли зробив зміну. Завдяки підвищенню простежуваності дій це сприяє на підзвітності та створює довіру між користувачами та зацікавленими сторонами у підтримці цілісності документів.Інтегруючи блокчейн в процес СДО, Норвегія створила прецедент для інших країн регіону, демонструючи потенціал інноваційних технологій для підвищення безпеки даних та оптимізації практики документообігу. як більш скандинавські країни аналогічним чином, зосередили

увагу на підвищенні безпеки СДО, що може призвести до більш стійких і безпечних систем в різних областях.

США мають великий досвід у сфері безпеки СДО. Основою цієї системи безпеки є широко прийняті методи шифрування, які захищають цілісність і конфіденційність даних під час передачі та зберігання. За допомогою цих протоколів шифрування забезпечуються захист конфіденційної інформації від несанкціонованого доступу. На додаток до шифрування ще є системи виявлення вторгнень, які відіграють важливу роль у моніторингу мережевого трафіку для підозрілої активності та порушень. Ці системи призначені для виявлення потенційних загроз в режимі реального часу і дозволяють швидко реагувати на ризики. Крім того, комплексна політика управління безпекою має важливе значення для встановлення надійного режиму безпеки у організації та окреслення найкращих методів обробки та захисту конфіденційної інформації.Важливою ініціативою, яку проводить уряд США, є Федеральна програма управління ризиками та схвалення (FedRAMP). [29]

Програма стандартизує вимоги безпеки, характерні для хмарних сервісів, які використовуються федеральними відомствами для забезпечення стабільного високого рівня безпеки на різних платформах. Передбачаючи суворі стандарти, FedRAMP допомагає мінімізувати ризики, пов'язані з обробкою та зберіганням конфіденційної інформації в електронних системах.Для підтримки цих стандартів FedRAMP вимагає ретельного аудиту, оцінки та остаточної сертифікації постачальників хмарних послуг. Цей процес включає в себе детальну оцінку контролю безпеки та заходів, що здійснюються цими постачальниками, які в кінцевому підсумку призводить до підвищення надійності та надійності використання систем електронного документообігу в рамках державних операцій. Завдяки цим заходам Сполучені Штати прагнуть покращити загальне середовище безпеки СДО та захистити конфіденційну інформацію від потенційних вразливостей та загроз.

Такі країни, як Австралія, зосередилися на інтеграції СДО з національними рамками управління ідентифікацією. Демонструючим прикладом цієї ініціативи є програма «myGov», яка виступає централізованою платформою для доступу громадян до широкого спектру електронних послуг, що надаються урядом. Цей комплексний підхід спрямований на оптимізацію користувацького досвіду та підвищення зручності громадян шляхом надання єдиної точки доступу до різних державних ресурсів. Крім того, ця інтеграція полегшує ефективний розподіл інформації між декількома службами, надаючи користувачам своєчасний доступ до критичних даних.[27]

Для пріоритезації безпеки даних та захисту конфіденційної особистої інформації платформа myGov включає надійні механізми автентифікації та шифрування. Це включає в себе багатофакторний процес автентифікації для перевірки особистості користувача та передових стандартів шифрування для захисту даних як під час транзиту через мережу, так і під час відновлення після поломки.

Висновки до першого розділу.

Огляд світових практик, спрямованих на підвищення безпеки систем електронного документообігу підкреслює важливу роль включення передових технологій таких як електронний документообіг. Доведено, що ключові фактори, такі як шифрування, багаторівнева аутентифікація та моніторинг загроз у реальному часі ефективно знижують ризики, які пов'язані з несанкціонованим доступом та порушеннями даних. Реалізація цих рішень не тільки забезпечує захист конфіденційних даних але і підвищує довіру користувача до системи. Шифрування, використання віртуальної приватної мережі і двофакторна аутентифікація мають важливе значення для захисту ваших даних під час передачі. Ці технології значно знижують ймовірність таких атак як перехоплення даних, атаки «людина посередині» та несанкціонований моніторинг трафіку.

Інтеграція в системи електронного документообігу забезпечує безпечну передачу даних і мінімізує вразливість до сучасних кіберзагроз.Постійні загрози інформації, такі як втручання в мережеві канали зв'язку, підробка даних і DDoS-атаки все ще залишаються критичними проблемами безпеки. Вирішення цих загроз вимагає постійного посилення, як технічних так і організаційних заходів. Це включає впровадження систем моніторингу та виявлення вторгнень для ефективної ідентифікації та реагування на можливі порушення безпеки.Основними загрозами з якими стикаються системи електронного документообігу є несанкціонований доступ, внутрішнє зловживання, втрата даних, викликана технічними збоями та вірусними атаками. Ці проблеми підкреслюють необхідність комплексної стратегії безпеки, яка включає в себе навчання користувачів з управління доступом, регулярне резервне копіювання даних і просування практики інформаційної гігієни.

2. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ ТА СТАНДАРТІВ ЗАХИСТУ

2.1 Оцінка надійності та швидкодії криптографічних алгоритмів.

Криптографічні алгоритми відіграють важливу роль у збереженні конфіденційності, цілісності та надійності даних в СДО. Оскільки організації все більше покладаються на цифрові документи та безперешкодний обмін інформацією між різними платформами, необхідність захисту цих даних досягла безпрецедентних рівнів. Постійно розвивається різні кіберзагрози, такі як порушення даних, несанкціонований доступ і методи взлому.Ці кіберзагрози створюють серйозні ризики для конфіденційної інформації організації, що зберігається і передається в цих системах. Це підкреслює важливість надійних криптографічних рішеньїх надійність і ефективність стали основою для безпечного управління інформаційними системами.

Ретельна оцінка різних алгоритмів шифрування має важливе значення для забезпечення найвищого рівня захисту. Ця ретельна оцінка дозволяє організаціям вибрати найбільш відповідний метод шифрування для вирішення унікальних проблем безпеки та забезпечити індивідуальні рішення, які покращують їх загальний захист від потенційних загроз безпеці.

Надійність криптографічних алгоритмів тісно пов'язана з їх стійкістю до різних видів атак. Ефективний алгоритм шифрування повинен забезпечувати високий рівень безпеки, особливо проти ворогів з сильними обчислювальними потужностями. Ця надійність залежить від двох важливих факторів:

- Математична складність алгоритму: Основна математична складність відіграє важливу роль у визначенні надійності алгоритму. Хоча алгоритми мають великі обчислювальні можливості, залишається неможливим вирішити математичні проблеми.
- Стійкість до крипто аналізу : Алгоритми повинні демонструвати стійкість до різних методів крипто аналізу, що використовуються для взлому криптосистеми, використовуючи її слабкі сторони. Сильна система захисту проти цих аналітичних методів має важливе значення для захисту цілісності криптосистем.

Захист від атак грубої сили особливо важливий при оцінці надійності криптографічних алгоритмів. У цих атаках зловмисники систематично пробують всі можливі ключі для виявлення правильного ключа. Важливо використовувати довгий ключ шифрування, щоб зменшити ризик пов'язаний з атаками грубої сили.

Для прикладу Розширений стандарт шифрування створює і перевіряє велику кількість можливих комбінацій, забезпечуючи довжину ключа в 128, 192 і 256 біт. Експоненціальне збільшення ключового простору з довшими ключами значно покращує безпеку, а атаки грубої сили стають все більш непрактичними. [14]

На рис.2.1 продемонстровано роботу алгоритму розширеного стандарту шифрування.

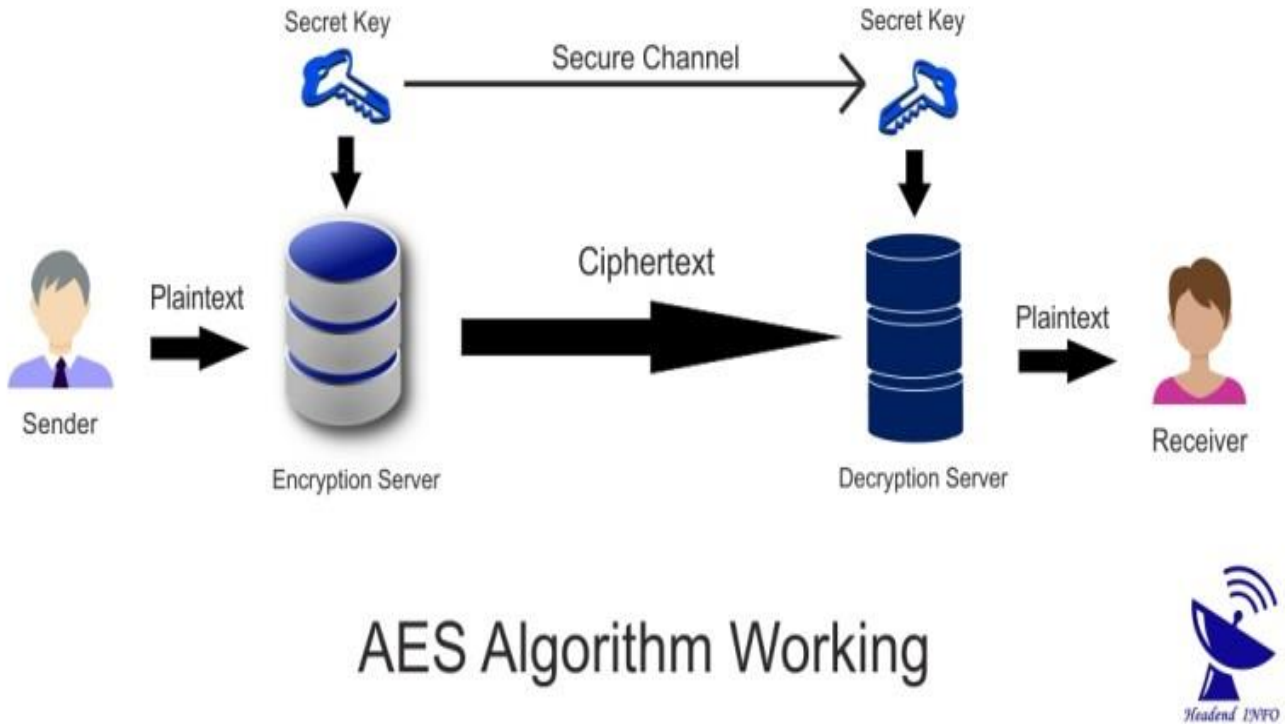


Рис.2.1.Робота алгоритму розширеного шифрування

Крім відомих загроз, пов'язаних з атаками грубої сили, криптографія являє собою значний і складний виклик цілісності криптографічних систем. Крипто аналіз включає в себе різні передові технології для виявлення вразливостей в криптографічних алгоритмах. Ці методи можуть значно зменшити обчислювальні ресурси та час необхідний для зловмиснику щоб розшифрувати конфіденційну інформацію, яка може бути особливо ризикованою для організацій.Для ефективного захисту від крипто аналізуважливо, щоб криптографічні алгоритми були ретельно розроблені шляхом розуміння потенційних векторів атак з самого початку розробки. Це включає в себе прогнозування слабкостей, які можуть бути використані і створення алгоритмів для пом'якшення цих ризиків.

Типовим прикладом цього є алгоритм RSA, який значною мірою базується на математичній складності ділення великих складених чисел на прості множники. Безпека RSA в основному базується на використанні дуже великих

розмірів ключів і вимагає мінімальної рекомендації 2048 біт для забезпечення надійного захисту від можливих атак. З розвитком технологій, включаючи розвиток обчислень, потреба в ще більших ключових вимірах стає все більш важливою для забезпечення безпеки алгоритмів проти загроз що розвиваються. Тому як обчислювальна потужність розвивається і нові криптографічні методи розробляються, криптографічні системи повинні постійно адаптуватися і для того, щоб підтримувати сильну безпеку системи.[10]

На рис.2.2 продемонстровано роботу алгоритму RSA.

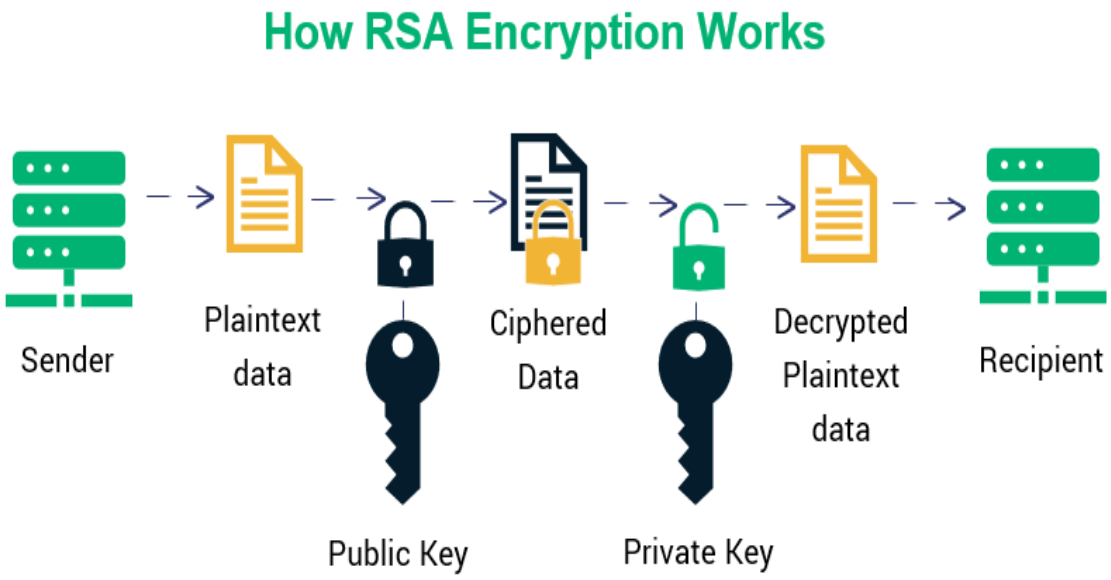


Рис.2.2.Робота алгоритму RSA

Іншим важливим аспектом надійності є те, наскільки ретельно алгоритм розглядається. Алгоритми які були ретельно перевірені крипто експертами протягом тривалого часу, як правило вважаються більш надійними. Такі як AES, RSA та криптографія еліптичних кривих довели свою надійність протягом багатьох років інтенсивних досліджень та практичних застосувань. Крипто експерти часто зацікавлені в перегляді та аналізі цих алгоритмів, щоб постійно вдосконалювати та адаптувати їх у відповідь на нові загрози. Важливість комплексного тестування не може бути переоцінена, оскільки це підвищує довіру в організаціях. Незалежні аудити, експертні оцінки та реальні тести значною мірою сприяють цьому процесу перевірки. Алгоритми які розроблені

під таким широким контролембудуть засновані як на відомих, так і на потенційних вразливостях, підкреслюючи важливість захисту конфіденційних даних.

При оцінці криптографічних алгоритмів продуктивність є ключовим фактором у визначенні придатності для конкретного застосування. Важливо, щоб ці алгоритми полегшували швидкий процес шифрування та дешифрування, не викликаючи жодних затримок у системі. Це особливо важливо для систем, які обробляють великі обсяги даних в режимі реального часу, таких як СДО.

2.2 Аналіз алгоритмів хешування.

Хеш-алгоритми є важливою складовою цифрової безпеки та відіграють ключову роль у забезпеченні конфіденційності, цілісності та автентифікації даних у системах електронного документообігу. Вони складають основу цифрового підпису та криптографічних систем, підкреслюючи їх важливість у цій галузі. Щоб алгоритм хешування вважався корисним, надійним і безпечним, він повинен відповідати певним критеріям, які дозволяють йому ефективно захищати конфіденційну інформацію.

Властивості хеш-функцій:

- Детерміновані: хеш-функції завжди повинні давати однакове значення хешу для одного вхідного повідомлення. Іншими словами, якщо обробляються одні й ті ж вхідні дані, виходить той самий вихід незалежно від того, скільки разів він виконується.
- Підтримка введення довільної довжини: хеш-функції повинні мати можливість обробляти вхідні повідомлення довільної довжини. Це дозволяє алгоритму ефективно працювати як з короткими, так і довгими повідомленнями, зберігаючи при цьому послідовну надійність і ефективність.

- Постійна довжина виводу: всі хеш-значення повинні мати однакову довжину, незалежно від довжини або вмісту вхідного повідомлення. Ця послідовність має вирішальне значення для різних криптографічних додатків, таких як цифрові підписи та автентифікація.
- Непередбачуваність: Результат алгоритму хешування не повинен бути легко передбачуваним без запуску алгоритму. Ключовою особливістю хорошого алгоритму хешування є «лавинний ефект», де невеликі зміни на вході (наприклад, перевертання одного біта) викликають значні та непередбачувані зміни у вихідному хеші, що робить його надзвичайно складним для передбачення.
- Однонаправлені: хеш-функції повинні бути однонаправленими. Це означає, що вихідне вхідне значення не може бути отримано з хеш-значення. Іншими словами, вихідне вхідне значення не може бути отримано з хеш-значення. Ця властивість робить хеші особливо корисними для безпечного зберігання паролів і даних автентифікації.
- Опір зіткнення: Ця властивість означає, що повинно дуже важко знайти два різних вхідних значень, які виробляють той же хеш. Ця властивість дуже важлива в таких додатках, як цифрові підписи, тому що зіткнення можуть викликати серйозні проблеми безпеки. У криптографії цю складність часто називають «парадоксом дня народження». Це свідчить про те, що ймовірність знаходження зіткнення значно вище очікуваної, навіть якщо є

Найкращим прикладом хеш-алгоритму є алгоритм безпечного хешування - SHA. Розроблений Національним інститутом стандартів і технологій США, SHA був покращений багато разів, включаючи SHA-0, SHA-1 і SHA-2, для підвищення безпеки та мінімізації вразливостей. Ці алгоритми використовують структуру Меркла-Демгарда для забезпечення опору зіткнень. На рис.2.3 показано загальну структуру конструкції Меркла-Дамгарда.

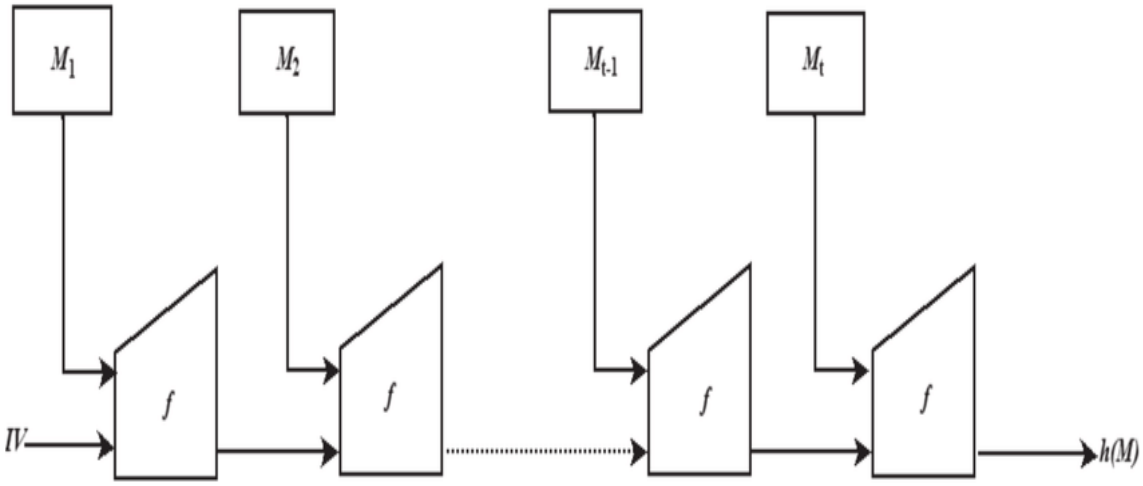


Рис.2.3. Зображення, що відображає загальну структуру конструкції МерклаДамгарда

SHA використовує структуру Меркла-Демгарда, яка є фундаментальною для забезпечення захисту даних. Ця структура починається з вектора ініціалізації, який є початковим блоком для першого хешу. Кожен блок даних обробляється через функцію стиснення з двома блоками як вхід для отримання вихідного блоку. Перший блок даних об'єднаний з вектором ініціалізації і кожен наступний блок виробляє новий хеш на основі результатів попереднього блоку.Тим не менш, деякі версії SHA, зокрема SHA-1 і SHA-2, були визнані уразливими для певних типів атак, таких як тривалі атаки. Для вирішення цих проблем SHA-3 був розроблений як новий хеш-стандарт і має унікальний дизайн, відомий як структура губки. [17]

Структура губки, що використовується в SHA-3, є найсучаснішим методом хешування, який обробляє вхідні дані довільної довжини і виробляє вихідні данні фіксованого розміру. Метод обробляє повідомлення в блоках і застосовує внутрішню перестановку до вхідних бітів після кожного блоку. Цей інноваційний метод роботи дозволяє SHA-3 залишатися гнучкими, одночасно підвищуючи безпеку, на рис 2.4 продемонстровано як працює структура губки в SHA-3.

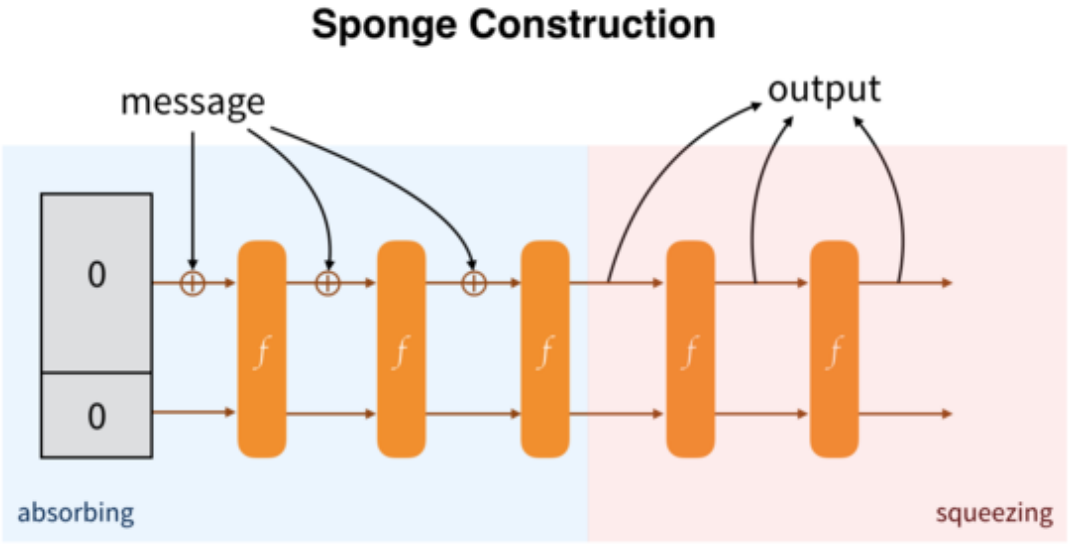


Рис.2.4 Робота структури губки в SHA-3

Прийнятий як стандарт у 2015 році, SHA-3 розроблений, щоб бути надійним проти різних атак, забезпечуючи високу надійність та продуктивність на різних платформах, SHA-3 є безпечною альтернативою традиційним схемам хешування, SHA-3 є безпечною схемою хешування з простою структурою та надійністю. Покращена стійкість до вразливостей робить його надійним вибором для широкого кола криптографічних додатків.

Важливість хеш-алгоритмів виходить за межі їх математичних властивостей. Вони відіграють ключову роль у захисті цілісності та безпеки даних у все більш цифровому світі. З розвитком кіберзагроз зростає і попит на надійні криптографічні рішення. Хеш-алгоритми захищають конфіденційну інформацію, діючи як перша лінія захисту від несанкціонованого доступу та підробки даних. Хеш-алгоритми мають застосування в різних областях, таких як захищені комунікації, цифрові підписи та технологія блокчейн. У захищених комунікаціях вони використовуються для перевірки цілісності повідомлень, що обмінюються між сторонами, і можуть швидко виявляти несанкціоновані зміни. Цифрові підписи використовують хеші, щоб створити унікальний відбиток повідомлення, який потім може бути перевірений одержувачем для перевірки його автентичності.

У сфері технології блокчейн алгоритми хешування є фундаментальними для роботи децентралізованих мереж. Кожен блок в блокчейні містить хеш попереднього блоку, який створює безпечний і незмінний ланцюжок даних. Ця взаємозв'язок забезпечує цілісність всього блокчейна, оскільки будь-яка модифікація блоку вимагає перерахунку всіх наступних хешів.

2.3. Використання алгоритмів хешування, криптографії та різних систем безпеки в системах електронного документообігу.

Важливим аспектом безпеки в системах електронного документообігу є автентифікація користувачів. Цей процес контролює доступ до документів та даних і є життєво важливим у середовищах, де конфіденційність та інформаційна безпека мають першорядне значення. Існують різні методи автентифікації, але багатофакторна автентифікація особливо ефективна.MFAпоєднує в собі різні методи автентифікації такі як паролі, біометричні дані (наприклад, відбиток пальця або розпізнавання особи) і одноразові коди, відправлені на мобільні пристрої. Такий багаторівневий підхід значно підвищує надійність доступу до системи.Багатофакторна автентифікація особливо ефективна, оскільки це ускладнює для зловмисних обхід декількох рівнів автентифікації. Гарантуючи, що користувачі можуть отримати доступ тільки до власних документів і даних, MFAне тільки запобігає несанкціонованому доступу, але також допомагає виявити підозрілу активність, наприклад, спроби входу з невідомих пристроїв або IP-адрес.

На додаток до традиційних методів автентифікації користувачів, важливо впровадити надійні протоколи безпеки. Ці протоколи можуть включати механізми реєстрації та моніторингу спроб доступу, забезпечуючи цінне розуміння потенційних порушень безпеки. Крім того, алгоритми машинного навчання можуть бути інтегровані в ці системи для виявлення незвичайних моделей поведінки користувачів і поліпшення виявлення потенційних загроз.

Наприклад, якщо користувач зазвичай звертається до системи з певного географічного розташування і раптово намагається увійти з іншої країни, система може вважати цю поведінку підозрілою і запросити додаткові кроки затвердження.

При створенні електронних документів також може бути корисно використовувати хешування або криптографічні методи для створення цифрового відбитка пальця. Коли документ створюється, система автоматично генерує хеш-код і цей код зберігається разом з документом. Це дозволяє системі пізніше перевірити, чи був документ підроблений під час зберігання або передачі. Якщо хеш-код документа не відповідає початково створеному коду, це вказує на можливе підроблення. Таким чином, хеш гарантує цілісність і справжність електронного документа.

Схеми шифрування відіграють важливу роль у створенні електронних документів шляхом захисту даних і збереження конфіденційної інформації. Наприклад, при підготовці фінансових звітів або контрактів, що містять конфіденційну інформацію, документи можуть бути зашифровані за допомогою асиметричного шифрування. Такий підхід гарантує, що тільки люди з відповідним приватним ключем можуть читати або змінювати документ. Цей додатковий рівень безпеки не тільки захищає дані, але і дає впевненість у цілісності документа, роблячи його придатним для транзакцій з високою вартістю.

Іншим важливим аспектом є використання цифрових підписів на основі криптографії. Ці підписи підтверджують, що документ був підписаний конкретною особою і гарантують його справжність. Коли користувач підписує документ, система використовує закритий ключ для створення цифрового підпису, який потім можна перевірити за допомогою відкритого ключа. Цей процес забезпечує надійний спосіб відслідковувати дії підписувача, тим самим збільшуючи відповідальність та відмову від нього та запобігаючи суперечкам щодо автентичності документа.

Технологія блокчейн спрощує перевірку документів. Наприклад, цифрові підписи, збережені в блокчейні, можна швидко і легко перевірити, оскільки вони використовують відкриті ключі для перевірки автентичності. Це просування відкриває шлях до автоматизації бізнес-процесів, оскільки контракти можуть автоматично виконуватися при виконанні певних умов, записаних на блокчейні.Крім того, технологія блокчейн дозволяє відстежувати всі зміни, внесені в документ гарантуючи його справжність і цілісність. Кожна зміна проходить перевірку часу, забезпечуючи чітку історію документа і захищаючи його від підробок. Блокчейн також може бути інтегрований в системи електронного документообігу для підвищення ефективності робочого процесу. Незмінність даних блокчейна означає, що після підписання та зберігання документа зберігається його цілісність. Це особливо вигідно в умовах, коли потрібно суворе дотримання правових і нормативних норм. Використовуючи блокчейн, організація може вести журнал всіх дій користувача, зроблених щодо документа, що є неоціненним у разі аудиту або юридичного запиту.

Висновки до другого розділу

Узагальнюючи викладене, криптографічні алгоритми та хеш-функції є невід'ємними компонентами систем електронного документообігу, забезпечуючи конфіденційність, цілісність та автентифікацію даних. Надійність алгоритмів, таких як AES, RSA та SHA-3, критично важлива для протистояння різноманітним атакам, включаючи методи грубої сили та крипто аналіз. Вибір правильного алгоритму залежить не лише від його безпеки, але й від продуктивності, що має значення для систем, які обробляють великі обсяги даних у реальному часі. Багатофакторна автентифікація, хешування та цифрові підписи є ключовими методами для підвищення безпеки доступу та виявлення підробок. Окрім цього, технології блокчейн відкривають нові горизонти для автоматизації бізнес-процесів, забезпечуючи перевірку документів та надійний

запис змін. Таким чином, впровадження цих технологій у системи електронного документообігу є критично важливим для забезпечення їх безпеки та ефективності.

3.АНАЛІЗ СИСТЕМ ДЛЯ РОБОТИ З ЕЛЕКТРОНИМИ ДОКУМЕНТАМИ

3.1.Використання ІІТ-Користувач

Програма ІІТ-Користувач є інноваційним і дуже складним інструментом, який був ретельно розроблений для складного процесу електронного підпису та шифрування транзакцій. Його основна мета це забезпечення високої безпеки даних у сфері систем електронного документообігу. Однією з найбільш помітних особливостей програми є використання сучасної технології шифрування, яка ефективно захищає конфіденційну інформацію від несанкціонованого доступу.

Коли користувач взаємодіє з програмою для підписання документа, система ретельно створює унікальний цифровий відбиток, який часто називають розшифровкою, і діє як цифровий підпис для документа, створюючи нерозривний зв'язок між підписувачем і документом. Процес підписання ще більше захищений шляхом шифрування цього хешу приватним ключем користувача, внесення змін після підписання документа практично неможливо. Ця двоетапна процедура не тільки гарантує незмінність документа, але й допомагає переконатися, що він підписаний законним користувачем і перевірити цілісність документа.

На додаток до розширених можливостей цифрового підпису, програма пропонує розширені можливості шифрування файлів, які захищають ваші файли від несанкціонованого доступу. Це досягається за рахунок використання асиметричних методів шифрування, при яких дані надійно шифруються за допомогою відкритого ключа одержувача. Тільки відповідний закритий ключ може розшифрувати цю інформацію і гарантує, що тільки вказаний одержувач включений в конфіденційний вміст, який він містить.

Основною задачею програми ІІТ-Користувач єсильні протокол безпеки під час підписання документів. Приватні ключі ретельно зберігаються в зашифрованому вигляді на надійних пристроях, таких як комп'ютери, смарт-

карти і апаратні токени, що значно знижує ризик крадіжки ключів і несанкціонованого використання. З іншого боку, відкритий ключ знаходиться в публічному реєстрі, контрольованому уповноваженим органом, і кожен може безпечно перевірити дійсність цифрового підпису.

Для подальшого підвищення безпеки користувачів програма включає надійний механізм аутентифікації на основі цифрових сертифікатів. Система забезпечує правильну ідентифікацію користувачів перед доступом до конфіденційних документів та ефективно вирішує загрозу можливого шахрайства з сертифікатами. Програма ІІТ-Користувач розроблена для безперебійної роботи як в урядовій так і в корпоративній інфраструктурі, та повністю інтегрована з національною інфраструктурою відкритих ключів. Часте оновлення сертифікатів і суворе дотримання міжнародних стандартів шифрування підвищують їх надійність і надійність.

Доступ до закритого ключа захищений за допомогою безпечного пароля або PIN-коду, додаючи додатковий рівень захисту від можливого шахрайства. Це значно знижує ймовірність отримання зловмисниками доступу до конфіденційних даних користувачів.

Ретельно розроблена відповідно до українських законів та міжнародних стандартів інформаційної безпеки, програма ІІТ-Користувач завоювала довіру як окремих користувачів, так і великих організацій, включаючи різні державні установи. Крім основною функції в захисті файлів, програма ІІТ-Користувач вміло запобігає перехопленню даних зловмисними третіми особами. Ця комплексна стратегія необхідна для програми ІІТ-Користувач для підтримки конфіденційності даних на всіх етапах її життєвого циклу, включаючи створення, підписання, передачу та зберігання. Це потужний інструмент, який дозволяє створювати та керувати своїми даними простим та простим у використанні способом.

3.2 Використання центрального засвідчуваного органа.

Портал ЦЗО є невід'ємною складовою національної цифрової інфраструктури України, відомої як платформа «Дія». Цей інноваційний портал відіграє важливу роль в рамках системи електронного документообігу та цифрового підпису країни. Його основна мета - забезпечити як громадянам, так і організаціям легкий доступ до різних послуг, що полегшують управління цифровими підписами та сертифікатами ключів. Використовуючи цей портал, користувачі можуть безпечно підписувати документи в Інтернеті та забезпечувати їх юридичну силу та цілісність відповідно до законодавства України.

Архітектура безпеки порталу ЦЗО заснована на новітній технології шифрування і встановлених стандартах, призначених для захисту особистої інформації користувачів і цифрових підписів від несанкціонованого доступу. В основі цієї системи лежить асиметричне шифрування, в якому використовується 1 пара ключів шифрування для кожного користувача. Ця пара складається з відкритого ключа, що зберігається в публічній книзі, і приватного ключа, що міститься в призначеному для користувача безпечному токені або смарт-карті. Цей багатошаровий дизайн безпеки зменшує ризик несанкціонованого підписання документів, обмежуючи доступ лише до закритого ключа власника ключа. Коли користувач починає процес підписання документа через портал ЦЗО, він повинен спочатку перевірити свою особу за допомогою закритого ключа. Потім система створює зашифрований хеш, що представляє унікальний цифровий відбиток документа, і підписує цей хеш закритим ключем користувача. Цей підписаний хеш додається до самого документа. Важливо відзначити, що зміни, внесені в документ, незалежно від того, наскільки малі, змінюють хеш, тим самим скасовуючи підпис і попереджаючи одержувача про будь-які можливі фальсифікації.

Щоб безпечно зберігати та керувати цими важливими приватними ключами, портал ЦЗО надає користувачам захищені апаратні пристрої, такі як USB-токени та смарт-карти. Ці пристрої спеціально розроблені для підвищення

загальної безпеки цифрових підписів. Навіть у випадках, коли токен може потрапити в чужі руки, токен не може бути використаний без правильного PIN-коду. Крім того, 10 травня ми внесли поліпшення, які включали біометричні методи автентифікації та додали ще один 1 важливий рівень безпеки для процесу автентифікації користувача.

Крім того, портал оснащений надійними механізмами перевірки автентичності цифрових підписів. Цей процес перевірки гарантує, що документ фактично підписаний уповноваженою особою і не зазнає жодних змін після підписання. Ця особливість особливо важлива для організацій, що займаються електронним документообігом, оскільки забезпечує перевірку підпису в режимі реального часу шляхом безперервного спілкування з офіційними органами сертифікації.

Для забезпечення цілісності надійного зберігання даних і передачі інформації портал використовує набір розширених протоколів дешифрування, які захищають обмін даними на всіх етапах між користувачем і серверною інфраструктурою. Захист конфіденційної інформації значно покращився завдяки використанню протоколу Transport Layer Security, який діє як грізний бар'єр від можливих перешкод та підробок, які можуть виникнути під час передачі даних.

Крім того, сертифікати ключів, що зберігаються у відкритому реєстрі підлягають періодичному оновленню та обширній перевірці. Цей поточний процес має вирішальне значення для підтримки ефективності та надійності систем цифрового підпису, що використовуються на порталі ЦЗО. Ця ретельна увага до деталей є важливою для створення основи безпечного середовища та підвищення довіри до електронних транзакцій по всій Україні. Ця комплексна стратегія не тільки зміцнює захист порталу але і гарантує користувачам, що дані обробляються з максимальною обережністю і безпекою.

3.3.Порівняння аналізів досліджених систем для роботи з електронними документами.

Порівняння програм ІІТ- Користувач та ЦЗО надає цінну інформацію про функції та можливості, необхідні для користувачів електронного цифрового підпису в Україні.

ІІТ- Користувач це надійний додаток, який пропонує широкий спектр функцій для роботи з ЕЦП. Однією з головних переваг ІІТ- Користувач є його універсальність, що дозволяє користувачам підписувати та шифрувати документи, керувати сертифікатами та створювати ЕЦП. Це робить його комплексним інструментом електронного документообігу. Крім того, програма підтримує різні пристрої зберігання даних, такі як токени та смарт-карти, що значно підвищує безпеку зберігання приватних ключів. Доступ до закритого ключа вимагає, щоб користувач був фізично присутнім на пристрої та вводив PIN-код, забезпечуючи таким чином захист даних користувача. Крім того, ІІТ-Користувач відповідає українському законодавству та міжнародним стандартам безпеки, що робить його надійним варіантом як для організацій, так і для окремих користувачів. Однак є деякі проблеми з використанням ІІТ- Користувач. Для користувачів, незнайомих з криптографією, інтерфейс може здатися складним. Крім того, для обробки закритих ключів потрібне спеціалізоване обладнання, яке може бути дорогим і незручним для користувачів, які не хочуть мати справу з налаштуванням і обладнанням.

На відміну від цього, ЦЗОнадає користувачам доступ до послуг управління ЕЦП через зручний інтерфейс та онлайн-платформу. Однією з основних переваг ЦЗОє їх інтеграція з державними системами, полегшення подання податків, реєстрація бізнесу та взаємодія з різними державними установами, полегшення взаємодії. Тому портал особливо корисний для користувачів, які часто взаємодіють з державними службами і потребують швидкого і легкого доступу.Крім того, ЦЗОможе перевірити справжність електронних підписів в режимі реального часу, тим самим допомагаючи

запобігти шахрайству через підроблені підписи. Однак, як і ІІТ- Користувач у ЦЗОтакож є недоліки. Портал вимагає стабільного підключення до Інтернету, що є проблематичним для користувачів у віддалених або погано підключених районах. Якщо доступ до інтернету перервано, користувачам може бути важко підписати документи або перевірити підписи.Хоча ЦЗОпропонують ряд корисних послуг, деякі функціональні можливості можуть бути менш ефективними ніж ті, які доступні в нативних додатках, таких як ІІТ- Користувач. Наприклад, складні маніпуляції з документами та розширені функції управління сертифікатами можуть бути обмежені.

Як результат, вибір між ІІТ- Користувач та ЦЗОзалежить від конкретних потреб та переваг користувача: ІІТ- Користувач може більше сподобатися користувачам, які надають перевагу універсальності та автономним можливостям, тоді як ЦЗОідеально підходить для користувачів, які активно беруть участь у державних послугах та хочуть зручності онлайн-доступу. Кожна програма має свої сильні і слабкі сторони, і остаточне рішення буде залежати від того, які аспекти використання електронного цифрового підпису є найбільш важливими для окремого користувача або організації.

Висновки до третього розділу

У даному аналізі розглянуто програму ІІТ-Користувач і Центр сертифікації ключів як ключові інструменти для електронного підпису та управління електронними документами в Україні. ІІТ-Користувач забезпечує комплексні функції, такі як підписання, шифрування документів та управління сертифікатами, при цьому акцентуючи увагу на безпеці через використання приватних ключів, що зберігаються на захищених пристроях. Натомість ЦЗОпропонує зручний онлайн-доступ до послуг, полегшуючи взаємодію з державними установами та перевірку підписів у реальному часі. Однак кожна система має свої недоліки: ІІТ-Користувач може бути складним для нових

користувачів, тоді як ЦЗОзалежить від стабільного Інтернет-з'єднання. Вибір між цими програмами залежить від потреб користувача: ІІТ-Користувач підходить для тих, хто цінує універсальність і автономність, тоді як ЦЗОє ідеальним для активних користувачів державних послуг, які шукають простоту та зручність в онлайн-інструментах.

4.ПІДВИЩЕННЯ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОНОГО ДОКУМЕНТООБОРОТУ

4.1.Шифрування даних електронних документів

Шифрування передбачає перетворення даних у безпечний формат, який може бути доступний або розшифрований лише тими, хто має відповідний ключ дешифрування. Ця трансформація спирається на складні алгоритми, які роблять оригінальний документ нечитабельним для неавторизованих користувачів, ефективно захищаючи конфіденційність. Історично шифрування використовувалося в різних формах протягом століть. Однак з появою сучасних обчислень алгоритми шифрування стали значно складнішими і включають розширені функції безпеки, адаптовані до цифрового середовища.

У цьому розділі розглядаються складності шифрування даних за допомогою Advanced Encryption Standard та RSA.

Advanced Encryption Standard,який зазвичай називають AES-256, який працює з сильною довжиною ключа 256 біт. Щоб проілюструвати, як цей стандарт шифрування працює в реальному світі, ми можемо припустити консольну програму, призначену для впровадження процесу шифрування та дешифрування конфіденційної інформації за допомогою AES-256. Цей приклад показує, як AES перетворює зчитувані дані в безпечний формат, доступ до якого можуть отримати тільки люди з відповідним ключем дешифрування.

Програма починається з простого сценарію, що включає шифрування конфіденційного повідомлення: процес шифрування даних за допомогою AES-256 спирається на два ключові елементи: по-перше, 256-бітний ключ, який виступає наріжним каменем безпеки; по-друге, ключ дешифрування, який є ключем, використовуваним для розшифрування даних. Велика кількість комбінацій клавіш, доступних в AES-256, сприяє його винятковій силі і робить його дуже стійким до атак грубої сили. Крім того, використання векторів ініціалізації додає процесу важливий рівень непередбачуваності. Це гарантує, що навіть якщо одні й ті ж дані шифруються кілька разів одним і тим же ключем,

результат кожного разу відрізняється. При цьому IV додатково зміцнює загальну цілісність і конфіденційність процесу шифрування, допомагаючи запобігти вразливості, які можуть виникнути внаслідок повторюваних шаблонів в зашифрованих даних.

Після створення вектора ключа та IV починається процес шифрування. Програма отримує відкритий текст (по суті оригінальне, читабельне повідомлення) і обробляє його за допомогою алгоритму шифрування Advanced Encryption Standard. У цьому методі дані діляться на 128-бітові блоки, кожен з яких зазнає ряд перетворень за кілька раундів шифрування. Ці перетворення складаються з декількох етапів. До них відносяться заміна (байти міняються місцями відповідно до попередньо визначеної таблиці), зміна рядка (перестановка даних), перемішування стовпців (подальше поширення даних для підвищення безпеки) і додавання ключа шифрування. Чотирнадцять раундів цієї послідовності збільшують складність зашифрованого виводу. Після завершення, відкритий текст перетворюється в зашифрованийтекст. Зашифрованийтекст знаходиться в безпечному і непорушному форматі, який неможливо розшифрувати без правильного ключа і IV.Після процесу шифрування програма витягує зашифрованийтекст. Зашифрованийтекст зазвичай представляється у вигляді Base64 рядка, так що дані байта можуть бути легко прочитані. Таким чином, якщо неавторизована особа перехопить це зашифроване повідомлення, повідомлення з'явиться у вигляді рядка незрозумілих символів, захищаючи таким чином оригінальне повідомлення від несанкціонованого доступу. Це узагальнює основні принципи шифрування AES. Без правильного ключа і IV дані ефективно блокуються і залишаються в безпеці.

Для розшифрування повідомлення програма використовує той самий ключ та IV, який використовується під час шифрування, зокрема AES-256. Враховуючи правильний ключ і IV, алгоритм успішно змінює і реорганізовує перетворення і обробляє кожен блок відповідно до його первісної структури. В результаті повідомлення відкритого тексту відновлюється правильно. Однак,

якщо ключ або IV не відповідає вихідному значенню, розшифрування зазнає невдачі і призводить до нечитабельності або помилкового виводу.

На рис.4.1 відображений приклад консольного додатка, який використовує AES-256 та забезпечує надійний захист конфіденційних даних, необхідних для безпечного обміну повідомленнями, Високий рівень безпеки, наданий AES-256, є встановленим глобальним стандартом захисту цифрової інформації. Він був встановлений як глобальний стандарт захисту цифрової інформації та гарантує, що вміст залишається конфіденційним, навіть якщо дані перехоплюються.

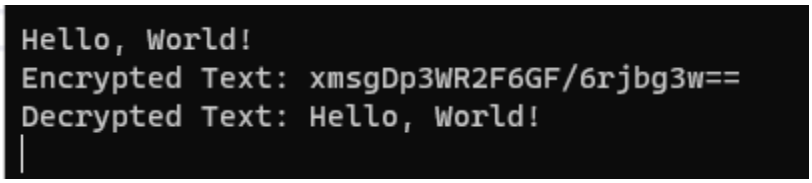


Рис.4.1. Приклад роботи алгоритму AES-256 в консольному додатку

Але також треба розглянути шифрування RSA, широко прийнятого методу шифрування з відкритим ключем. Важливу роль відіграє шифрування RSA в таких сферах як:

- Захист комунікації;
- Цифрові підписи;
- Системи захисту даних.

Щоб зрозуміти, як працює шифрування RSA, розглянемо, як працює шифрування RSA в консольному додатку, призначеному для шифрування і розшифрування повідомлень. Оскільки відкритий ключ відкритий і загальний, будь-хто може зашифрувати повідомлення для власника пари ключів. На відміну від цього, приватний ключ зберігається в таємниці і захищається власником ключа. Шифрування RSA особливо ефективне для захисту даних, оскільки дозволяє розшифровувати повідомлення, зашифровані відповідним відкритим ключем, тільки закритий ключ. Цей параметр створює безпечну односторонню функцію та підвищує цілісність та конфіденційність обмінюваної інформації.

Щоб проілюструвати процес шифрування, додаток-приклад спочатку отримує текстове повідомлення, яке є вихідними читабельними даними. Потім

програма шифрує це повідомлення за допомогою відкритого ключа одержувача; Шифрування RSA принципово базується на математичних концепціях, зокрема модульній арифметиці та факторизації великих простих чисел. На етапі шифрування повідомлення перетворюється в зашифрований текст за допомогою відкритого ключа. На відміну від алгоритмів симетричного шифрування, які використовують один ключ як для шифрування, так і для дешифрування, RSA використовує два ключа в структурі роботи. Цей поділ ключа підвищує безпеку, оскільки тільки людина з закритим ключем може розшифрувати повідомлення.Як тільки дані зашифровані, вони представлені у вигляді зашифрованого тексту, який не може бути зрозумілий нікому без доступу до закритого ключа. Зазвичай цей зашифрований текст виражається як базовий шістнадцятковий або Base64 закодований рядок, що полегшує читабельність і передачу в цифрових системах. Навіть якщо неавторизований користувач намагається розшифрувати цю інформацію, сила шифру RSA підтримується складністю факторизації простих чисел. Загалом, при використанні досить великих розмірів ключа, таких як 2048 або 4096 біт, стає обчислювально неможливим вирішити цю проблему в розумні терміни. Ця властива складність робить RSA складним механізмом захисту конфіденційності даних.

Щоб змінити процес шифрування, програма застосовує цей ключ для перетворення зашифрованого тексту в його вихідну форму відкритого тексту. Ця процедура дешифрування схожа на процедуру шифрування, але використовує унікальне математичне перетворення на основі секретного ключа. Якщо використовується правильний секретний ключ, оригінальне повідомлення можна точно відновити. Однак, якщо використовується неправильний або недійсний секретний ключ, розшифрування зазнає невдачі, що призводить до нечитабельності даних або повідомлення про помилку.

Цей приклад підкреслює ефективність шифрування RSA у захисті інформації в реальних сценаріях; RSA широко використовується в онлайн протоколах безпеки, таких як HTTPS, щоб гарантувати захист даних під час передачі між браузером користувача і сервером веб-сайту. Крім того, RSA

дозволяє відправнику «підписати» повідомлення за допомогою його приватного ключа. Цей процес підписання дозволяє одержувачу перевірити справжність та цілісність цифрового повідомлення за допомогою відкритого ключа відправника, гарантуючи, що повідомлення не було підроблено та підвищення надійності цифрових комунікацій. На рис.4.2 відображено приклад додатку з використанням RSA.

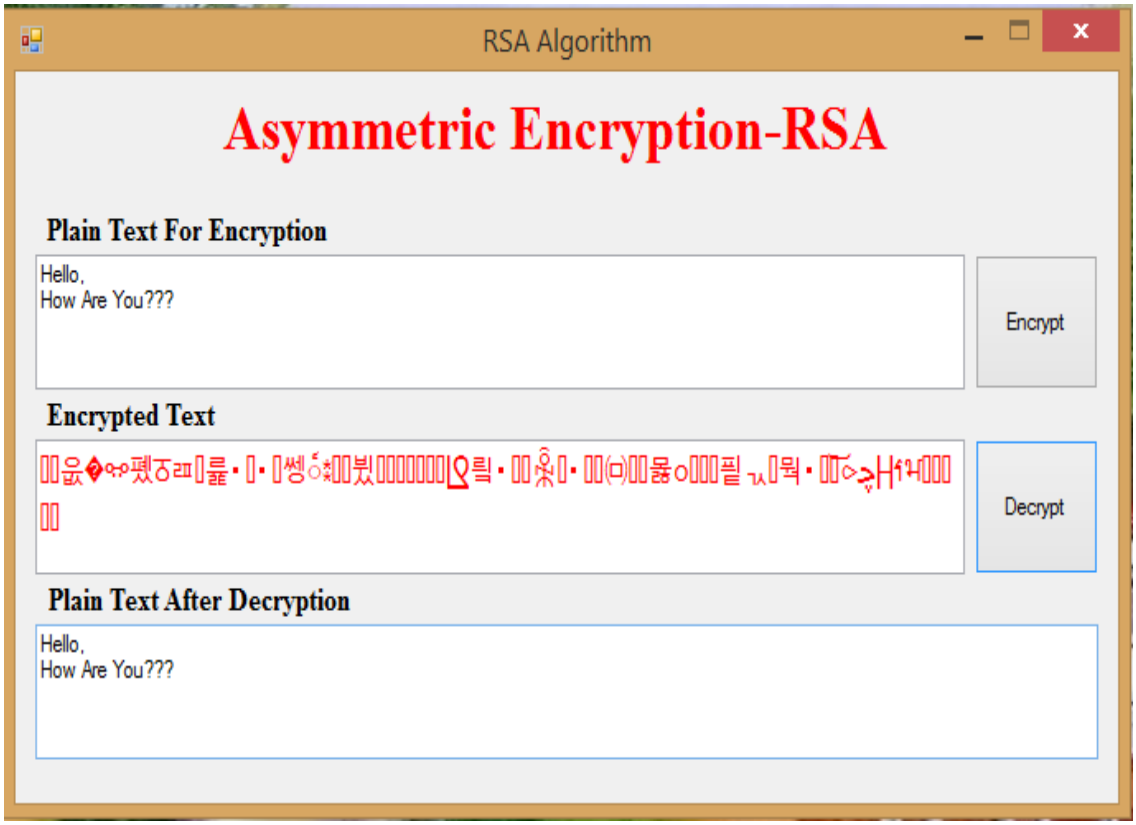


Рис.4.2.Приклад додатку з використанням RSAшифрування

4.2.Використання систем авторизації

Системи електронного документообороту особливо вразливі до несанкціонованого доступу через їх роль у сприянні обміну критичними даними та зберіганню конфіденційної інформації. Ця вразливість вимагає суворих заходів аутентифікації, щоб контролювати, хто може отримати доступ до цієї інформації та визначити обсяг їх авторизації.

Важливо визнати, що кожен метод аутентифікації має свої переваги і недоліки. Наприклад, біометричні системи призначені для високої безпеки, але може знадобитися спеціальне обладнання, а апаратні рішення, такі як Cristal-1, доступні користувачами, є надійними з точки зору безпеки, але можуть бути незручними через вимоги до фізичної присутності. BankID корисний і безпечний, але його ефективність залежить від надійності і доступності банківської мережі, а в деяких сценаріях можуть бути обмеження. Ці фактори мають значний вплив на загальну ефективність і валідність методу аутентифікації для конкретної системи документообігу.При виборі варіанту аутентифікації важливо враховувати конкретні вимоги, пов'язані з конфіденційною інформацією, яка потребує захисту і пов'язані з цим ризики. Такі системи, як Bankid разом з FaceID та Cristal-1, представляють різноманітний підхід до підвищення безпеки систем електронного документообігу та захисту конфіденційних даних у все більш складному цифровому середовищі.

*FaceID:*FaceID є одним із сучасних біометричних методів авторизації, що базується на розпізнаванні обличчя користувача. Суть роботи FaceID полягає у створенні тривимірного цифрового зображення обличчя користувача за допомогою інфрачервоних датчиків, що дозволяє уникнути помилок, характерних для двовимірних технологій. FaceID забезпечує високий рівень захисту, оскільки система здатна розрізняти навіть найдрібніші деталі обличчя, що робить підробку надзвичайно складною. Однак використання FaceID має й певні недоліки. Зокрема, система може працювати неефективно за умов поганого освітлення або при значних змінах у зовнішності користувача. Додатково, висока вартість впровадження цієї технології обмежує її застосування у певних системах документообігу. На рис.4.3 продемонстрований процес авторизації через FaceID.

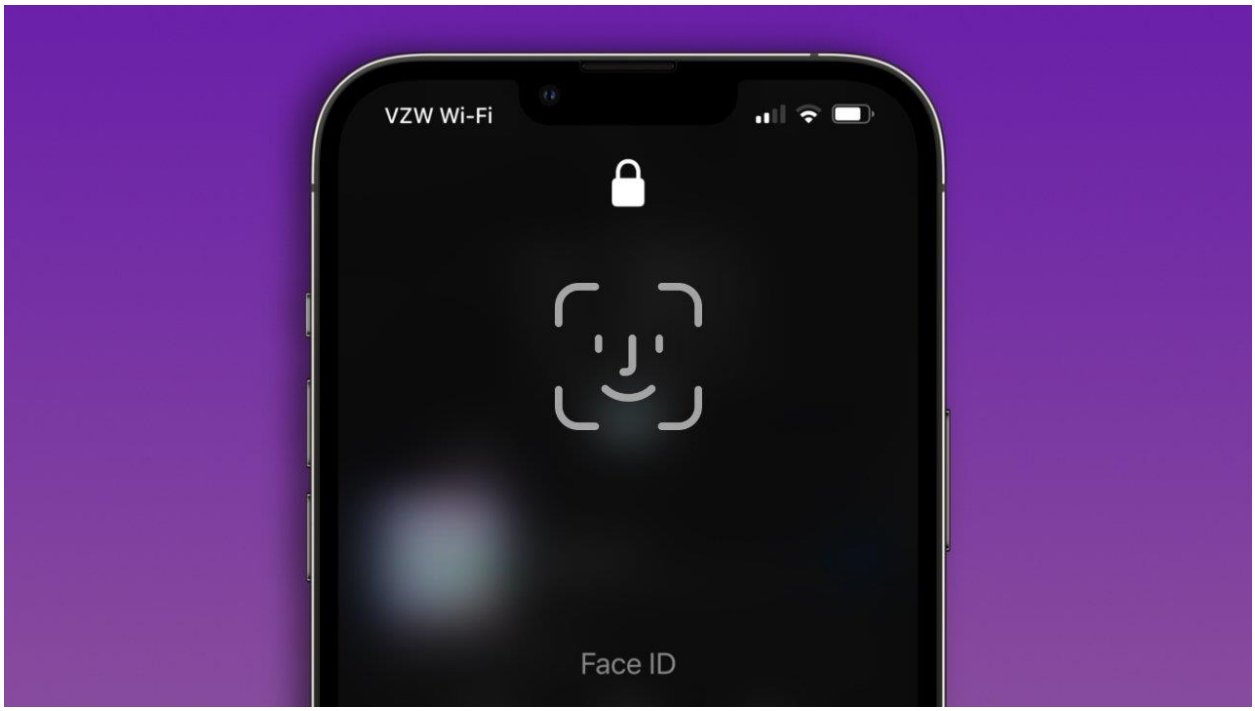


Рис.4.3. Процес авторизації через FaceID

*Cristal-1:*Пристрій включає в себе безліч криптографічних функцій, призначених для забезпечення високого ступеня захисту та забезпечення надійного рішення для інформаційної безпеки. Його основними цілями є аутентифікація користувачів для безпечного доступу до ключів, генерація приватних і відкритих ключів для електронних цифрових підписів (ЕЦП) і протоколів розподілу ключів, а також генерація криптографічних ключів для шифрування даних. Для подальшого підвищення безпеки система включає апаратний генератор випадкових чисел, який служить додатковим заходом захисту. Ключові дані надійно зберігаються у внутрішній пам'яті пристрою, запобігаючи несанкціонованому доступу та мінімізуючи ризик крадіжки особистих даних. Крім того, пристрій здатний генерувати і перевіряти цифрові підписи, тим самим гарантуючи достовірність і цілісність переданих документів.

Крім функцій підпису та шифрування, пристрій також підтримує розрахунки хеш-функцій для створення унікального відбитка цифрових даних, що значно підвищує безпеку даних. Ключові дані розподіляються за допомогою асиметричних протоколів, включаючи алгоритм Діффі-Геллмана, зменшуючи ризики, пов'язані з передачею інформації по мережі. Внутрішня пам'ять може

надійно зберігати будь-які дані, а всі файли на внутрішній флешці шифруються для додаткової безпеки.

Електронний ключ розроблений як компактний USB-пристрій з програмним інтерфейсом CCID разом з внутрішньою флешкою, що використовує протокол масового зберігання USB. Його конструкція має двошарову друковану плату, покриту захисним матеріалом і розміщену в міцному пластиковому або металевому корпусі, що забезпечує як стійкість, так і простоту використання. Прилад відповідає криптографічним стандартам ДСТУ ГОСТ 28147:2009 в різних режимах, реалізує цифрові підписи згідно ДСТУ 4145-2002 і підтримує всі довжини ключів, зазначені в ГОСТ 34.311-95 Протокол Діффі-Хеллмана, гарантує надійний розподіл даних ключів в групах еліптичних точок кривої з довжиною ключів до 571 біт.

Протокол Діффі-Хеллмана забезпечує ефективність за допомогою швидкого створення цифрового підпису та загальних секретних обчислень для задоволення потреб швидкої обробки інформації. Крім того, флеш-накопичувачі ємністю 4 Гб, 8 Гб, 16 Гб і 32 Гб доступні для шифрування даних зі швидкістю читання/запису 0.5MB/секунду. Внутрішня апаратна реалізація, орієнтована на криптографічне перетворення, гарантує, що приватні ключі захищені від несанкціонованого доступу як в апаратних, так і в програмних середовищах. Приватні ключі генеруються, зберігаються і використовуються тільки всередині пристрою, ефективно усуваючи ризик компромісу або витоку. Внутрішня енергонезалежна пам'ять забезпечує безпечне зберігання даних ключів, особливо закритих ключів.

*BankID:*Однією з найбільших переваг Bankid є його неймовірна зручність. Користувачі не встановлюють необхідність створювати або запам'ятовувати чіткі імена користувачів і паролі. Замість цього користувач можете легко використовувати існуючі банківські облікові дані для доступу до різних служб та спрощення процесу аутентифікації. Це не тільки покращує користувальницький досвід, але й знижує ризики пов'язаний зі слабкими паролями, яка є загальною вразливістю в більш традиційних системах

аутентифікації та ризиком повторного використання облікових даних на багатьох платформах. Крім того, банк прийняв складну багатофакторну модель аутентифікації, яка об'єднує аутентифікацію на основі інформації та аутентифікацію, щоб значно підвищити рівень безпеки. Але, незважаючи на безліч сильних сторін, система BankID не безмежна. Помітним недоліком є невід'ємна залежність від банківської інфраструктури, яка може відштовхнути фізичних осіб, які не мають доступу до банківських послуг. Крім того, на BankID, як і на багатьох централізованих системах, не впливають кіберзагрози. Якщо порушення відбувається в банківській мережі, вплив може вийти за рамки просто грошових втрат і поставити під загрозу цілісність всієї системи документообігу, яка спирається на банк для аутентифікації користувача.

Існують також побоювання щодо залежності користувача від однієї точки відмови. Якщо фінансова установа стикається з відключенням або технічною затримкою, користувач може не мати доступу до необхідних важливих послуг. Успішна реалізація BankID вимагає спільних зусиль між банками, постачальниками послуг та регуляторами і можуть виникнути логістичні проблеми, особливо в регіонах, де регуляторне середовище фрагментоване або непослідовне.

У контексті електронного документообігу BankID значно підвищує безпеку, значно знижуючи ризики, пов'язані з несанкціонованим доступом та крадіжкою особистих даних. Система мінімізує вразливості безпеки при передачі та зберіганні конфіденційної інформації та забезпечує перевірку ідентичності користувачів відповідно до високих стандартів, встановлених фінансовою індустрією. Крім того, включивши шифрування під час процесу аутентифікації, можна запобігти перехопленню та несанкціонованому обміну даними, що необхідно для захисту інформації, переданої між мережевими каналами.

4.3. Захист мережних з’єднань TCP\IP

Під час передачі інформації між клієнтом і серверними компонентами прикладного програмного забезпечення через TCP-з'єднання починається детальний і процес аутентифікації, як тільки користувач підключається до сервера для підтримки високого рівня конфіденційності та забезпечення цілісності даних. Цей процес складається з багатьох шагів починаючи з розшифровки облікових даних користувача та ретельної перевірки легітимності користувача або пристрою, який намагається підключитися. Тільки після успішного завершення цього шагу суворої аутентифікації може бути запущено безпечне з'єднання TCP і дані, що передаються по мережі, захищені від можливих загроз.Для досягнення такого високого рівня безпеки використовується передова технологія шифрування, яка ретельно захищає весь обмін даними через з'єднання від несанкціонованого доступу та можливого втручання в систему. Основною метою впровадження цих широких заходів є захист конфіденційності та цілісності переданих даних, отриманих за допомогою застосування передових методів шифрування, які захищають конфіденційну інформацію.

Стандартний протокол TCP/IP сприяє безперебійному зв'язку між клієнтською стороною і сервером, в той же час організовуючи таким чином захищені з'єднання без переривання безпечної передачі даних, підкреслює важливість збереження довіри і безпеки при обміні конфіденційною інформацією по мережі.

Операції з управління ключами в першу чергу делегуються сертифікаційним органам, які виконують ключові функції в забезпеченні цілісності та безпеки обробки зашифрованих даних. Загальна архітектура системи - високо інтегрована комбінація як програмних, так і апаратних компонентів, що працюють разом. Програмні компоненти мають різні обов'язкові функції, включаючи моніторинг різних операційних завдань, управління доступом користувачів і прийняття надійних заходів безпеки на різних етапах обробки даних.

Демонструючим прикладом є шлюз безпеки, який призначений для аутентифікації користувача і створення захищеного каналу зв'язку. Цей шлюз діє, як перша лінія захисту, гарантуючи, що тільки авторизовані користувачі можуть отримати доступ до системи. Він шифрує всі відправлені дані та забезпечує захист від можливих загроз і забезпечує надійну передачу інформації на сервер. Цей багаторівневий підхід не тільки покращує захист даних, та також підвищує впевненість у здатності всієї системи безпечно обробляти конфіденційну інформацію.Залежно від конкретної ролі в мережі, шлюз безпеки може функціонувати, як спеціальний окремий апаратний пристрій, або гнучкий програмний апаратний шлюз безпеки може зробити додатковий рівень безпеки, діючи як надійний інструмент захисту для мережевих з'єднань. Це також полегшує легку інтеграцію з іншими мережевими компонентами через стандартний інтерфейс зв'язку, забезпечуючи загальносистемну сумісність і функціональність.

Конфігурація цих апаратних пристроїв може зручно управлятися віддалено за допомогою спеціальних програмних засобів, що робить процес простіше для мережевих адміністраторів. Система призначена для автоматичного сповіщення адміністратора мережі, якщо помилка або проблема виникає в шлюзі. Ця функція оповіщення має вирішальне значення для забезпечення швидкого та ефективного реагування, своєчасного втручання та мінімізації можливих збоїв у безпеці мережі.

Крім того, система повинна бути продумана та розроблена, щоб включати проксі-сервер, який виступає посередником у процесі передачі даних. Проксі-сервер ще більше підвищую захист даних і безпеку шляхом маскування особистих даних користувачів і додавання ще одного бар'єру від несанкціонованого доступу.

Окрім основних можливостей захисту даних, система має надавати потужні інструменти для налаштування віртуальних приватних мереж, які відіграють ключову роль у захисті з'єднань, що надсилаються через зовнішні мережі. VPN шлюзи є важливим компонентом налаштування та підтримки цих

віртуальних мереж і вони керують маршрутизацією даних між різними клієнтами VPN. Ці шлюзи виконують критичні функції розшифровки конфіденційної інформації, одночасно реалізуючи різні протоколи безпеки, призначені для запобігання несанкціонованого доступу і з'єднань між клієнтами.Крім того, сам VPN-клієнт може створити спеціальний віртуальний мережевий інтерфейс і значно спростити підключення до захищеної мережі. Ця функція дозволяє забезпечити безперебійне та ефективне підключення до системи, що дозволяє безпечно передавати дані в різних географічних місцях. В результаті користувачі можуть безпечно обмінюватися інформацією та отримувати доступ до неї, знаючи, що їхні повідомлення захищені від потенційних загроз.

Для підтримки найвищих стандартів безпеки система використовує передові апаратні електронні ключі, спеціально розроблені для криптографічних транзакцій. Ключі відіграють важливу роль у захисті закритих ключів як користувача, так і шлюзу, створюючи бар'єр від несанкціонованого доступу. Система мінімізує ризик порушення даних і загроз гарантуючи, що всі дії шифрування відбуваються в контрольованому і безпечному середовищі. Інтеграція цих передових заходів безпеки не тільки захищає конфіденційні дані протягом усього життєвого циклу, але також покращує цілісність зв'язку в мережі та підтримує безпечне та надійне цифрове середовище.

4.4.Використання блокчейну для захисту систем електронного документообороту

Ключові особливості блокчейну це децентралізація, незмінність і прозорість. Ці особливості роблять блокчейн привабливим варіантом для організацій, які прагнуть ефективно управляти конфіденційною інформацією, для зберігання цілісності своїх цифрових документів. Впроваджуючи блокчейн, організації можуть створити надійну інфраструктуру для електронного документообігу, що призведе до більшої безпеки та операційної ефективності. Інтеграція технології блокчейн в СДО приносить великі переваги при створенні

незмінних реєстрів. Ця функція дозволяє зберегти всі транзакції або зміни, які внесені в документ та в інший блок, який криптографічно пов'язаний з попереднім блоком в черзі. В результаті, ця структура забезпечує автентичність та цілісність цифрового файлу шляхом створення постійного та захищеного запису всіх видів діяльності, пов'язаних з документом. На рис.4.4 предомонстраванно як працює блокчейн в системах СДО.

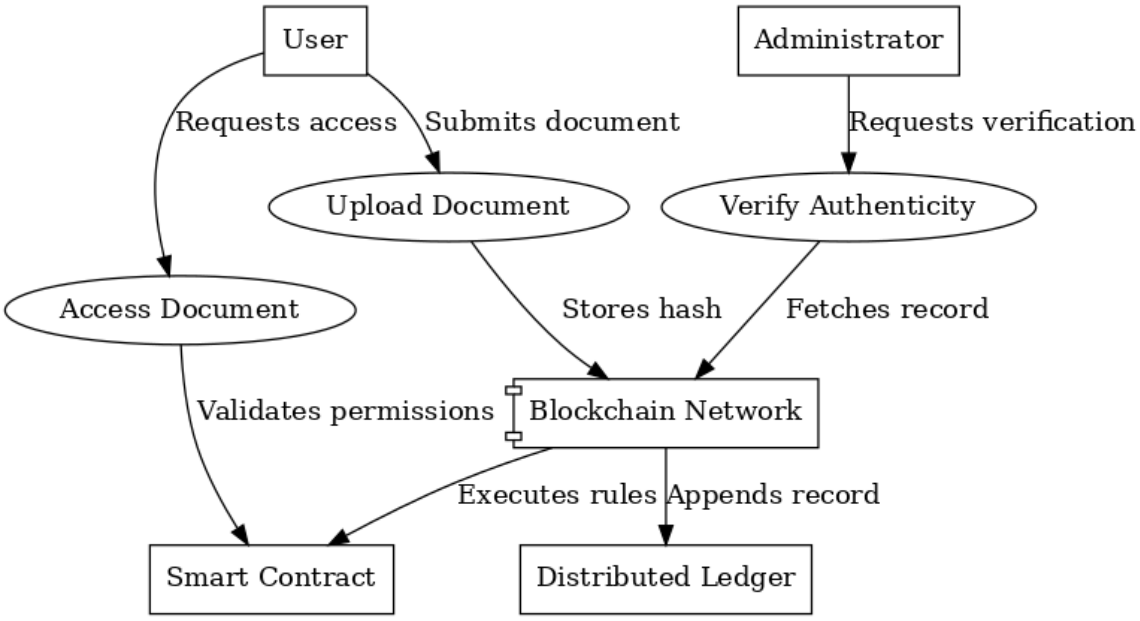


Рис.4.4. Робота блокчейну в системах СДО

Наприклад, юридичні документи, контракти та сертифікати, що зберігаються в блокчейні не можуть бути змінені без виявлення, а їх дійсність може бути перевірена швидко. Ця функція необхідна для підвищення надійності всього процесу документування і особливо цінна в галузях де рекордна надійність має вирішальне значення.

Прийняття технології блокчейн значно підвищує прозорість робочих процесів документообігу. Всі дії, пов'язані з документом такі як оновлення, спроби доступу та передачі –ці дій ретельно записуються з точними часовими мітками та унікальними ідентифікаторами шифрування. Цей комплексний рівень відслідковування дозволяє контролювати всі дії, які пов'язані з документом. Це

особливо важливо для галузей, які повинні відповідати суворим нормативним нормам відповідності.

Крім того, блокчейну підтримує реалізацію смарт-контрактів.Смарт-контракт є самостійним виконанням контракту, в якому терміни вбудовані безпосередньо в код. Ці розумні контракти зменшують залежність від ручного моніторингу, дозволяючи автоматизувати певні дії при виконанні визначених умов. Ця автоматизація мінімізує ризик людських помилок та забезпечує надійне та безпечне виконання критичних процесів, таких як затвердження документів та транзакції.

Для того, щоб ефективно захистити СДО на основі блокчейну від різних загроз безпеці, організаціям необхідно реалізувати комплексну багатошарову захисну стратегію. Технологія блокчейн в основному забезпечує певні функції безпеки, але можуть виникнути уразливості, які особливо виникають при взаємодіє з зовнішніми системами або обробляється людьми, які не мають достатнього досвіду. Одним з ключових елементів цієї стратегії безпеки є захист приватних ключів, які важливі для доступу та підписання транзакцій блокчейн. Щоб запобігти несанкціонованому доступу, важливо надійно зберігати ці ключі в середовищі високої безпеки, такому як апаратний гаманець або безпечний анклав. Такий підхід забезпечує більш надійний захист від можливих порушень безпеки.

На додаток до захисту приватного ключа, важливо захистити основну мережеву інфраструктуру, яка підтримує блокчейн-систему. Організації повинні впроваджувати стійкі протоколи кібербезпеки, які включають брандмауери, системи виявлення та запобігання вторгненням. А також періодичні перевірки безпеки для захисту від загроз, таких як розподілені атаки відмови в обслуговуванні. Своєчасні оновлення та патчі до протоколу блокчейна також важливі, оскільки невирішені вразливості можуть піддавати систему зловмисним експлойтам.

Застосування передових технологій шифрування значно покращує режим безпеки СДО на основі блокчейна. Документи, що зберігаються в блокчейні,

шифруються, і важливо, щоб тільки авторизовані користувачі тримали ключ дешифрування, необхідний для доступу до контенту. Цей додатковий рівень захисту означає, що навіть якщо кіберзлочинець успішно порушує інфраструктуру блокчейна. Фактичні дані залишаться зашифрованими і можуть бути доступні без належного ключа. Це означає, що ви не зможете отримати доступ до конфіденційності та захистити свою конфіденційність.

Висновки до четвертого розділу

Аналіз шифрування даних в електронних документах висвітлює комплексну взаємодію технологій, спрямованих на забезпечення безпеки та цілісності сучасних інформаційних систем, а також впровадження сучасних систем автентифікації та захисту мережевих з'єднань.

Методи шифрування даних, такі як AES і RSA, відіграють важливу роль у захисті конфіденційної інформації. AES відома тим, що балансує швидкість і безпеку і є основою процесу шифрування в реальному часі. На відміну від цього, RSA особливо ефективний для безпечної передачі даних, особливо в сценаріях, які вимагають безпечного обміну ключами. Інтеграція цих алгоритмів з дієвими програмними рішеннями підкреслює їх актуальність та адаптивність у вирішенні сучасних проблем безпеки.

Вивчення систем автентифікації, включаючи такі технології, як FaceID і Crystal-1, розкриває розвиток технології автентифікації. Ці системи підвищують безпеку, зменшуючи залежність від традиційних паролів і забезпечуючи безперешкодний користувальницький досвід. Хоча FaceID використовує біометрію для швидкої та надійної автентифікації, Crystal-1 демонструє різноманітний технічний підхід до контролю доступу. Його ефективність залежить від розумної практики та дотримання стандартів конфіденційності які гарантують, що заходи безпеки не порушують права користувачів.

Крім того, акцент на захисті мережевих з'єднань TCP/IP підкреслює необхідність захисту даних при транзиті в взаємопов'язаному середовищі. Багаторівнева архітектура протоколу TCP/IP підтримує зв'язок і сприяє шифруванню, безпечним протоколам рукостискання та уважному моніторингу мережі.

ВИСНОВКИ

Було оглянуто міжнародні практик, які спрямовані на підвищення безпеки систем електронного документообігу, та було підкреслено необхідність передових технологій захисту даних. Основні функції які включають розшифровку, багаторівневу аутентифікацію та постійний моніторинг загроз, щоб зменшити ризик несанкціонованого доступу та витоку даних. Основні технології безпеки, такі як методи шифрування, віртуальні приватні мережі та двофакторна аутентифікація, допомагають захистити дані на ходу та захистити їх від загроз викрадення даних. Поточні проблеми, включаючи мережеві перешкоди та DDoS-атаки, вимагають постійного оновлення технічних та організаційних заходів безпеки систем виявлення вторгнень.Основними загрозами для цих систем є несанкціонований доступ, внутрішня розшифровка, втрата даних і зловмисне програмне забезпечення. Для більшої безпеки системи потрібно включати такі заходи, як навчання користувачів, регулярне резервне копіювання та належну практику інформаційної гігієни.

Було проведено аналіз таких систем: Центральнийзасвідчуваний орган та ІІТ-Користувач.

У тексті підкреслюється необхідність сучасних алгоритмів шифрування, таких як AES і RSA для захисту електронних документів. Алгоритми шифрування, такі як AES, RSA і SHA-3, важливі для безпеки. Важливо збалансувати потреби безпеки з продуктивністю системи. Багатофакторна автентифікація та технологія блокчейн також можуть підвищити безпеку та ефективність систем електронного документообігу.

Було досліджено методи автентифікації, такі як FaceID і Crystal-1. Так як ці методипокращують контроль доступу і зменшують залежність від паролів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про електронні документи та електронний документообіг». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/85115/print1274774604685720#Text

2. Закон України «Про електронний цифровий підпис» [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/852-15#Text

3. U.S. Department of Homeland Security. Office of Biometric Identity Management. [Електронний ресурс] - Режим доступу: http://www.biometrics.gov/ReferenceRoom/FederalPrograms.aspx

4. U.S. Congress. Electronic signatures in global and national commerce act. [Електронний ресурс] - Режим доступу: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

5. EU Directive 1999/93/EC. [Електронний ресурс] - Режим доступу: http://data.europa.eu/eli/dir/1999/93/oj/eng

6. UN General Assembly. United nations convention on the use of electronic communications in international contracts. [Електронний ресурс] - Режим доступу: https://treaties.un.org/doc/Treaties/2005/11/20051128%2004-23%20PM/Ch_X_18p.pdf

7. Entrust Inc. Digital Signatures. Entrust: Securing Digital Identities & Information. [Електронний ресурс] - Режим доступу: https://www.entrust.com/digital-signatures/

8. КРИПТОГРАФІЧНИЙ АЛГОРИТМ “RSA”[Електронний ресурс] - Режим доступу:https://elartu.tntu.edu.ua/bitstream/123456789/9601/2/Conf_2013v1_Popivchak_V-Kryptohrafichnyi_alhorytm_103.pdf

9. Алгоритм шифрування RSA, види атак на нього. Реалізація мовою Python[Електронний ресурс] - Режим доступу:https://dou.ua/forums/topic/43026/

10. RSA Algorithm in Cryptography [Електронний ресурс] - Режим доступу: https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

11. Public Key Cryptography: An Overview of RSA Encryption[Електронний ресурс] - Режим доступу:https://www.rcdevs.com/glossary-rsa/

12. RSA Encryption[Електронний ресурс] - Режим доступу:https://brilliant.org/wiki/rsa-encryption/

13. Advanced Encryption Standard (AES)[Електронний ресурс] - Режим доступу:https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

14. Advanced Encryption Standard (AES)[Електронний ресурс] - Режим доступу:https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

15. What Is SHA Encryption? SHA-1 vs SHA-2[Електронний ресурс] - Режим доступу:https://www.sectigo.com/resource-library/what-is-sha-encryption

16. Secure Hash Algorithms[Електронний ресурс] - Режим доступу:https://brilliant.org/wiki/secure-hashing-algorithms/

17. SHA-256 vs. SHA-1: Which Is The Better Encryption?[Електронний ресурс] - Режим доступу:https://www.securew2.com/blog/what-is-sha-encryption-sha-256-vs-sha-1

18. What Is the TLS Protocol, How It Works, and What It Protects Against[Електронний ресурс] - Режим доступу:https://cityhost.ua/en/blog/scho-take-protokol-tls-yak-vin-pracyu-ta-vid-chogo-zahischa.html

19. What is an SSL/TLS Certificate?[Електронний ресурс] - Режим доступу:https://aws.amazon.com/what-is/ssl-certificate/?nc1=h_ls

20. Что такое SSL-сертификат и зачем он нужен[Електронний ресурс] - Режим доступу:https://ssl.com.ua/info/what-is-ssl/

21. Introduction to Secure Sockets Layer[Електронний ресурс] - Режим доступу:https://www.scribd.com/document/413471292/SSL-pdf

22. Електронний ключ "Кристал-1". [Електронний ресурс] - Режим доступу:https://iit.com.ua/index.php?page=itemdetails&p=3&gtype=1&type=1&id=50

23. Захист мережних з’єднань (TCP/IP)[Електронний ресурс] - Режим доступу:https://iit.com.ua/index.php?page=itemdetails&p=3&gtype=1&type=1&id=42

24. Програмний комплекс роботи з ключами користувача ЦСК[Електронний ресурс] - Режим доступу:https://ca.tax.gov.ua/korustyvach_csk

25. Про ЦЗО[Електронний ресурс] - Режим доступу:https://czo.gov.ua/about

26. About myGov[Електронний ресурс] - Режим доступу:https://my.gov.au/en/about

27. Government Digital Service[Електронний ресурс] - Режим доступу:https://www.gov.uk/government/organisations/government-digital-service

28. FedRAMP[Електронний ресурс] - Режим доступу:https://aws.amazon.com/compliance/fedramp/?nc1=h_ls

29. Swedish BankID: All You Need to Know[Електронний ресурс] - Режим доступу:https://www.criipto.com/blog/all-you-need-to-know-bankid-sweden

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ
ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА
КІБЕРНЕТИЧНОГ ЗАХИСТУ**

КВАЛІФІКАЦІЙНА РОБОТА НА ТЕМУ «ПІДВИЩЕННЯ ЗАХИСТУ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБОРОТУ В МЕРЕЖЕВИХ КАНАЛАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ»

Керівник: д.т.н
Котенко Андрій

Виконав: здобувач вищої освіти групи СЗДМ-61
Каліш Владислав

Об’єкт – Процес захисту систем в електронному документообороту.

Предмет – Захист інформації від витоку в мережевих каналах передачі інформації.

Мета – Підвищити надійність захисту електронного документообороту в в мережевих каналах.

Наукові завдання:

- проаналізувати правові аспекти функціонування цифрових підписів;
- дослідити алгоритми захисту даних в електронних документах;
- Дослідити захист електронних документів в мережевих каналах;
- Досліди платформи для роботи з електронними документами.

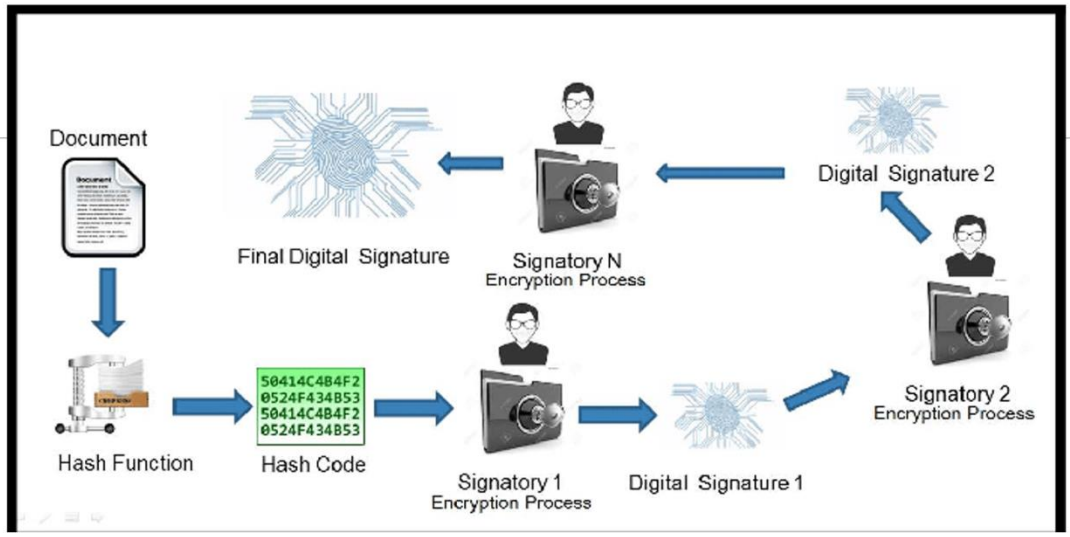


Рис.1. Послідовність реалізації цифрового підпису

Порівняння показників безпеки в програмах для роботи з електронними документами

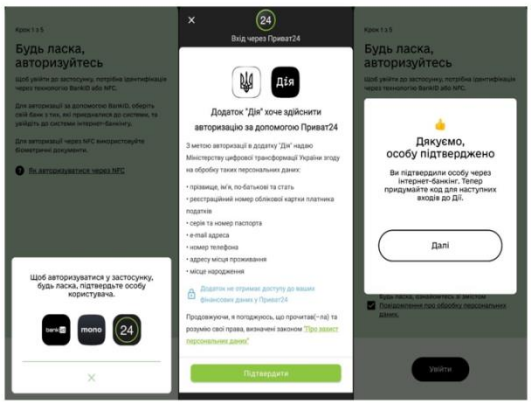


Рис.2.Процедура входу в BankID через ДІЯ

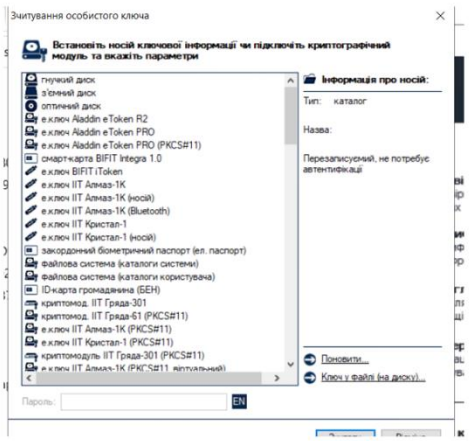


Рис.3. Процедура вибору електронного ключа в програмі ІІТ-Користувач

Рис.4. Приклад кодування даних за допомогою алгоритму AES

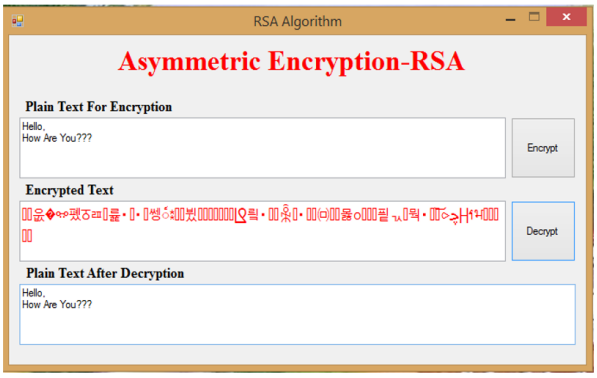


Рис.5. Приклад кодування даних за допомогою алгоритму RSA

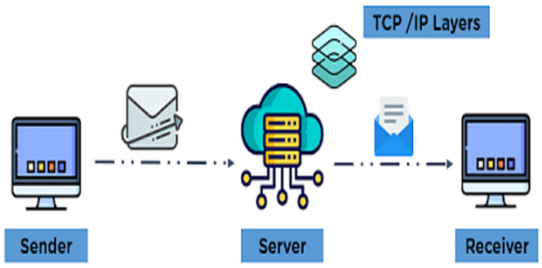


Рис.6. Приклад передачі даних через TCP\IP

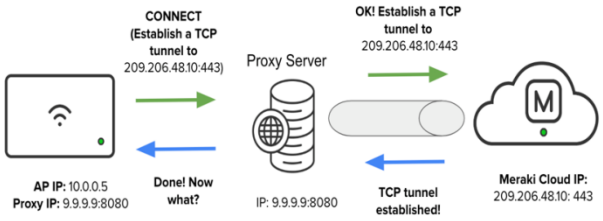


Рис.7. Приклад передачі даних через TCP\IP з використанням proxy

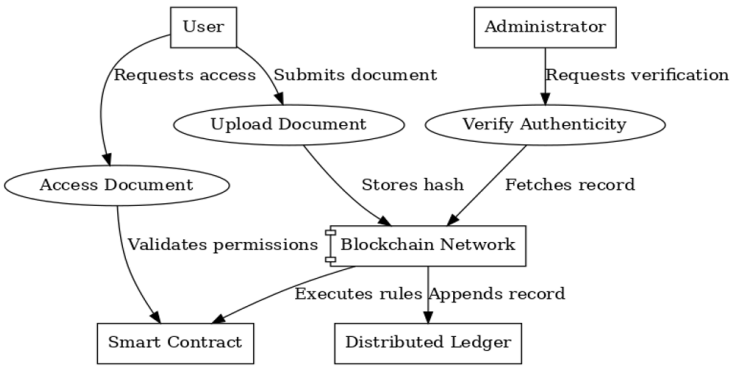


Рис 8. Робота блокчейну в системах СДО

Висновки

1. Аналіз міжнародних практик демонструє важливу роль передових технологій у підвищенні безпеки систем електронного документообігу.
2. Досліджено технології безпеки, які включаючи використання методів шифрування протоколів TCP/IP та проксі-серверів з використанням TCP/IP, що забезпечують безпечну передачу даних та запобігають несанкціонованому доступу та перешкодам.
3. Досліджено сучасні проблеми, такі як мережеві перешкоди та DDoS-атаки, що вимагають постійного оновлення технічних та організаційних заходів безпеки, зокрема систем виявлення вторгнень.
4. Основними загрозами для цих систем є несанкціонований доступ, внутрішня розшифровка, втрата даних і атаки шкідливих програм.
5. Для підвищення безпеки системи необхідно інтегрувати такі заходи, як навчання користувачів, регулярне резервне копіювання даних та дотримання практики інформаційної гігієни.
6. Сучасні алгоритми шифрування, такі як AES та RSA, є фундаментальними для захисту електронних документів, забезпечуючи баланс між безпекою та продуктивністю системи.
7. Багатофакторна аутентифікація та технологія блокчейн - це нові рішення, які мають потенціал для підвищення безпеки та ефективності систем електронного документообігу.
8. Проаналізовано системи, такі як Центральний Засвідчуваний Орган та ІІТ-Користувач, підкреслює важливість комплексної стратегії безпеки з урахуванням вимог конкретної системи.

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

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

СИСТЕМИ ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В КОРПОРАТИВНИХ МЕРЕЖЕВИХ КАНАЛАХ

Спеціальність: 125 - Кібербезпека та захист інформації
Виконав: Владислав КАЛІШ
Керівник: к.т.н., доц. Ігор ІВАНЧЕНКО

Київ - 2024

АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність роботи зумовлена зростанням ризиків несанкціонованого доступу, втручання в роботу систем електронного документообігу та витоку інформації під час передачі мережевими каналами.
- Об’єкт дослідження - процес захисту систем електронного документообігу.
- Предмет дослідження - захист інформації від витоку в корпоративних мережевих каналах передачі інформації.
- Мета роботи - підвищення надійності захисту електронного документообігу в мережевих каналах.
- Завдання: дослідити СДО, проаналізувати загрози та криптографічні алгоритми, розглянути системи роботи з електронними документами, сформувати заходи підвищення захисту.

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

- Проаналізовано роль систем електронного документообігу як інструменту організації, зберігання, маршрутизації та контролю електронних документів.
- Визначено загрози конфіденційності, цілісності та доступності документів у серверній, клієнтській і мережевій частинах СДО.
- Досліджено алгоритми AES, RSA, SHA-256, SHA-3 та напрями їх застосування для захисту документів, підписів і контрольних значень.
- Розглянуто засоби підвищення захисту: шифрування, авторизація, захист TCP/IP-з’єднань, VPN, TLS, цифровий підпис та блокчейн.

СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

- СДО забезпечують централізоване зберігання документів, спільну роботу користувачів, контроль версій і прискорення погодження документів.
- Основні компоненти СДО: сервери, робочі станції, бази даних, мережеві канали зв’язку та засоби електронного підпису.
- Критичними вимогами є доступність документів, цілісність змін, контроль прав користувачів і захист від зовнішніх та внутрішніх порушників.
- Під час впровадження необхідно враховувати вартість, інтеграцію з наявною інфраструктурою, міграцію даних і підготовку персоналу.

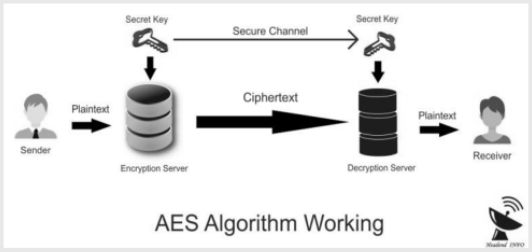
ЗАГРОЗИ СИСТЕМАМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

- Загрози конфіденційності пов’язані з несанкціонованим доступом до документів, компрометацією облікових даних і перехопленням мережевого трафіку.
- Загрози цілісності виникають у разі підміни, пошкодження або несанкціонованої зміни документів, баз даних і журналів подій.
- Загрози доступності включають DoS/DDoS-атаки, збої мережевого обладнання, відмови серверів і помилки адміністрування.
- Потенційними порушниками можуть бути хакери, конкуренти, колишні співробітники, адміністратори, користувачі СДО та злочинні групи.

ЗАГРОЗИ В МЕРЕЖЕВИХ КАНАЛАХ ПЕРЕДАЧІ ДАНИХ

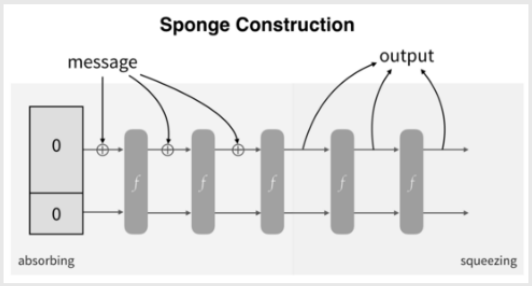
- Найбільш небезпечними є перехоплення даних, атаки типу «людина посередині», підміна пакетів, фішинг, соціальна інженерія та експлуатація вразливостей ПЗ.
- У мережевих каналах можуть передаватися паролі, фінансові дані, службові документи та інші конфіденційні відомості.
- Захист має базуватися на шифруванні, автентифікації, сегментації мережі, моніторингу трафіку та регулярному оновленні програмного забезпечення.
- Для зниження ризиків застосовують SSL/TLS, VPN, системи виявлення вторгнень, міжмережеві екрани та політики контролю доступу.

ОЦІНКА НАДІЙНОСТІ ТА ШВИДКОДІЇ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ



- Криптографічні алгоритми є базовим засобом забезпечення конфіденційності, цілісності та автентичності електронних документів.
- Для симетричного шифрування доцільно застосовувати AES, який поєднує високу швидкодію з достатньою криптографічною стійкістю.
- Для обміну ключами та цифрових підписів використовуються асиметричні алгоритми, зокрема RSA та пов’язані з ним механізми відкритого ключа.

АЛГОРИТМИ ХЕШУВАННЯ SHA-256 ТА SHA-3



- Хеш-функції забезпечують формування контрольного значення документа, яке використовується для перевірки його цілісності.
- SHA-256 базується на класичній структурі Меркла-Дамгарда, тоді як SHA-3 використовує губкову конструкцію Keccak.
- Порівняння SHA-256 та SHA-3 є важливим для вибору алгоритму в системах електронного документообігу, де критичні швидкодія та стійкість до колізій.

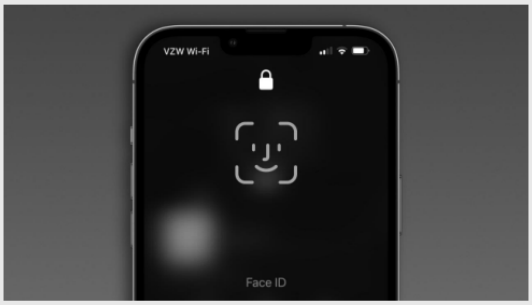
ВИКОРИСТАННЯ КРИПТОГРАФІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

- Криптографія застосовується для шифрування документів, формування цифрового підпису та підтвердження незмінності даних.
- Електронний цифровий підпис дозволяє встановити автора документа та виявити будь-які зміни після підписання.
- Комбінація хешування, шифрування та підпису створює комплексний механізм захисту документа на всіх етапах його життєвого циклу.

АНАЛІЗ СИСТЕМ ДЛЯ РОБОТИ З ЕЛЕКТРОННИМИ ДОКУМЕНТАМИ

- Розглянуто використання програмних засобів для створення, підписання, шифрування, перевірки та передавання електронних документів.
- Окремо враховано роль центрального засвідчувального органу як елементу інфраструктури відкритих ключів.
- Порівняння систем виконано за критеріями захищеності, зручності використання, підтримки ЕЦП, відповідності нормативним вимогам і можливості інтеграції.
- Надійна система має забезпечувати контроль доступу, журналювання дій, перевірку підпису, захист ключів та резервне відновлення документів.

ВИКОРИСТАННЯ СИСТЕМ АВТОРИЗАЦІЇ

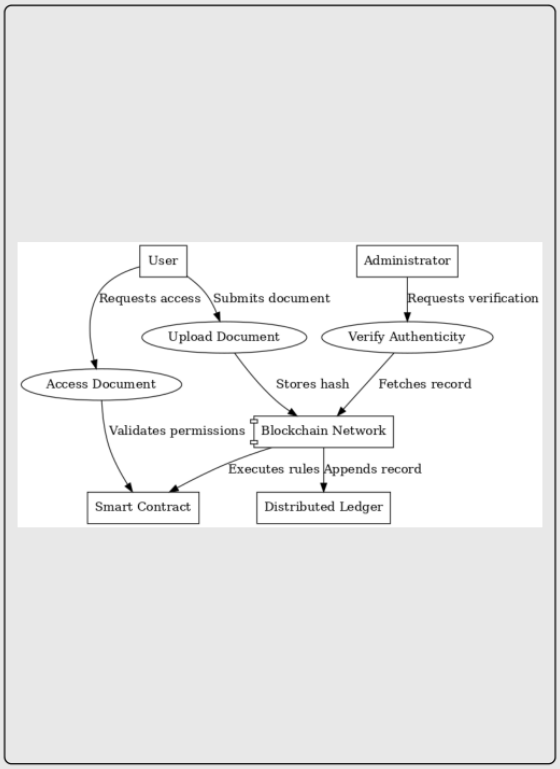


- Авторизація визначає, які дії користувач може виконувати після успішної автентифікації в системі електронного документообігу.
- Доцільним є застосування багатофакторної автентифікації, біометричних механізмів, одноразових кодів і політик ролей.
- Розмежування прав доступу зменшує ризик несанкціонованого перегляду, редагування або видалення електронних документів.

ШИФРУВАННЯ ДАНИХ ЕЛЕКТРОННИХ ДОКУМЕНТІВ


```
Hello, World!
Encrypted Text: xmsgDp3WR2F6GF/6rjbg3w==
Decrypted Text: Hello, World!
```

- Шифрування документів захищає їх зміст у сховищі, під час передавання мережею та у випадку компрометації носія.
- Для режимів блочного шифрування важливе коректне використання ключів і векторів ініціалізації, оскільки помилки в цих параметрах унеможливлюють коректне розшифрування.
- У практичній системі необхідно поєднати шифрування з керуванням ключами, контролем доступу та аудитом операцій користувачів.



- Блокчейн може застосовуватись як незмінний журнал подій, що фіксує операції з документами та контрольні хеш-значення.
- Такий підхід підвищує прозорість, ускладнює приховану зміну документів і забезпечує перевірку історії дій.
- Блокчейн доцільно розглядати як додатковий рівень контролю цілісності, а не як заміну класичним механізмам шифрування й авторизації.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Владислав КАЛІШ

Системи захисту електронного документообігу в корпоративних мережевих ка

Київ - 2024