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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до кваліфікаційної роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ»

Виконав студент 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Мешко Я.Ю.
(прізвище та ініціали)

Керівник Кожухівський А.Д.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтролер _____
(прізвище та ініціали)

КИЇВ - 2024

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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо підвищення захищеності систем електронного документообігу з використанням технології цифрового підпису»

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

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

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

_____ Ярослав МЕШКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
МЕШКО Ярослав
(прізвище, ім'я)

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

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

Київ 2024

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“ 04 ” березня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мешко Ярославу Юрійовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій щодо підвищення захищеності систем електронного документообігу з використанням технології цифрового підпису»
керівник кваліфікаційної роботи Кожухівський Андрій, д.техн.н., проф.
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 04 » березня 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.06.2024 р.

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

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз процесу захисту електронного документообігу організації.

2. Дослідження методів та засобів захисту електронного документообігу на базі платформи ПТАХ.

3. Розроблення рекомендацій щодо захисту електронного документообігу на базі платформи ПТАХ.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення проблеми захисту систем електронного документообігу з використанням технології цифрового підпису.	15.04.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	22.04.2024 р	
3.	Аналіз методів та засобів захисту систем електронного документообігу з використанням технології цифрового підпису	29.04.2024 р	
4.	Захисту електронних документів з використання технології електронного підпису	06.05.2024 р	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту систем електронного документообігу з використанням технології цифрового підпису	13.05.2024 р.	
6.	Оформлення результатів дослідження.	20.05.2024 р.	
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

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

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача МЕШКО Ярослава

на тему: «Дослідження шляхів та розробка рекомендацій щодо підвищення захищеності систем електронного документообігу з використанням технології цифрового підпису»

Актуальність: В сучасному світі електронний документообіг став невід'ємною частиною роботи багатьох організацій. Це дозволяє значно економити час та ресурси, покращити ефективність роботи та підвищити рівень обслуговування клієнтів. Однак широке використання електронного документообігу також призвело до зростання кількості кіберзагроз. Зловмисники можуть отримати незаконний доступ до електронних документів, змінити їх вміст або видалити їх взагалі.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту електронного документообігу з використанням технології цифрового підпису та визначено мету та завдання даного виду документообігу, а також його складові частини.
2. Досліджено методи та засоби електронного документообігу з використанням технології цифрового підпису.
3. Запропоновано варіант системи захисту електронного документообігу з використанням технології цифрового підпису та рекомендації щодо її застосування.
4. Чітко та змістовно сформовані висновки, які відображають суть проведеного дослідження. Графічні матеріали оформлені якісно та доповнюють текст, роблячи його більш зрозумілим та наочним. Список використаних джерел свідчить про глибоке розуміння теми кваліфікаційної роботи та вміння автора працювати з науково-технічною літературою.

Недоліки:

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

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент:

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

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

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

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

на тему: «Дослідження шляхів та розробка рекомендацій щодо підвищення захищеності систем електронного документообігу з використанням технології цифрового підпису»

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

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

Висновок кафедри про кваліфікаційну роботу

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: сторінок, рисунків, таблиця, джерел.

Об'єкт дослідження – захист систем електронного документообігу.

Предмет дослідження – методи та засоби захисту електронного документообігу з використанням технологій цифрового підпису.

Мета роботи розробити рекомендації щодо захисту систем електронного документообігу та рекомендації щодо захисту цифрового підпису.

Методи дослідження – опрацювання літератури за даною темою, аналіз програмних забезпечень та поточного стану систем. Аналіз документації щодо захисту системи .

Системи ведення електронного документообігу та забезпечення цифрового підпису відіграють провідну роль у підвищені захищеності електронних процесів на різних підприємствах. Дані технології, а саме: технологія цифрового підпису та системи електронного документообігу забезпечують ефективний моніторинг та реагування на можливі загрози.

В роботі досліджено проблеми, пов'язані із захистом електронного документообігу в організаціях. Проведено аналіз можливих методів та засобів захисту систем електронного документообігу. Визначено основні цілі та завдання заходів щодо підвищення безпеки електронного документообігу з використанням цифрового підпису.

На основі проведеного дослідження розроблено низка заходів, спрямованих на підвищення захищеності електронного документообігу, використовуючи технологію цифрового підпису.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ, ЦИФРОВИЙ ПІДПИС, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕД – Електронний документ

ОК – Особистий ключ

ВК – Відкритий ключ

ЕЦП – Електронний цифровий підпис

СЕД – Система електронного документообігу

SSL – Secure Sockets Layer (Захищений сокетний шар)

TLS – Transport Layer Security (Безпека транспортного рівня)

ЦСК – Центр сертифікації ключів

СВК – Сертифікати відкритого ключа

ЕДО – Електронний документообіг

VPN – Virtual Private Network (Віртуальна приватна мережа)

RBAC – Role-Based Access Control (Керування доступом на основі ролей)

СЕДО – Система електронного документообігу

ДССЗІ – Державна служба спеціального зв'язку та захисту інформації України

АЦСК – Акредитований центр сертифікаційних ключів

ПСВК – Персональний засіб підтвердження ключа

ВСТУП

Актуальність дослідження. Захист систем електронного документообігу важливий з наступних причин. По-перше, в контексті стрімкого розвитку сучасних технологій, системи електронного документообігу є основними інструментами для багатьох сфер діяльності, наприклад бізнес, урядові організації, освіта, тощо. Це створює потребу з ефективних засобах захисту конфіденційної інформації, яка забезпечує захищеність, запобігає витоку інформації та гарантує цілісність даних. По-друге, зростаюча кількість кібератак, які спрямовані на порушення безпеки електронних систем, свідчить про необхідність покращення захисних механізмів даних систем. Окрім цього, зі збільшенням обсягів електронного документообігу зростає і ймовірність вразливості цих систем перед інформаційними злочинцями.

По-третє, Україна активно впроваджує цифрові технології у галузі економіки, управління та адміністрування та загалом громадського життя, тому безпека електронного документообігу є вкрай важливою. Оскільки недостатня захищеність може призвести до серйозних наслідків, таких як крадіжка даних, фальсифікація документів, тощо. По-четверте, виникає необхідність у забезпеченості сумісності та інтеграції систем електронного документообігу із існуючими інформаційними та управлінськими платформами. Для цього є важливою задачею усунути недоліки у забезпечені сумісності та наполегливо розвивати практики інтеграції цифрових підписів у різноманітні програми.

Системи електронного документообігу відіграють значущу роль у забезпечені ефективної роботи та гарантуванні безпеки обміну документами. Ці системи спрощують процеси роботи з документами, економлять час на обробку цих документів, збільшують продуктивність працівників. Завдяки системам електронного документообігу відбувається автоматизація процесів створення, підписання, зберігання, обміну документами.

Системи електронного документообігу, які використовують технологію цифрового підпису набувають все більшої популярності серед різних компаній, установ та навіть фізичних осіб підприємців, оскільки дані системи забезпечують

надійний механізм перевірки цілісності документів. Завдяки технології цифрового підпису можна підтвердити авторство документа та забезпечити його недоторканість від впливу зовнішніх факторів.

Вищезазначене обґрунтовує актуальність теми даної кваліфікаційної роботи, оскільки основний зміст якої становлять дослідження методів та засобів захисту електронного документообігу з використанням технологій цифрового підпису.

Об'єкт дослідження – захист систем електронного документообігу.

Предмет дослідження – методи та засоби захисту електронного документообігу з використанням технологій цифрового підпису.

Мета роботи розробити рекомендації щодо захисту систем електронного документообігу та рекомендації щодо захисту цифрового підпису.

Наукові завдання:

дослідити сутність проблеми захисту електронного документообігу;

проаналізувати основні підходи до захисту електронного документообігу;

дослідити існуючі технології цифрового підпису для електронного документообігу;

проаналізувати методи та засоби захисту систем електронного документообігу;

запропонувати варіант захисту систем електронного документообігу з використанням технологій цифрового підпису;

розробити рекомендації щодо підвищення захищеності систем електронного документообігу з використанням технологій цифрового підпису.

Методи дослідження – опрацювання літератури за даною темою, аналіз програмних забезпечень та поточного стану систем. Аналіз документації щодо захисту системи .

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту систем електронного документообігу з використанням технології цифрового підпису.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ

1.1. Аналіз проблеми захисту систем електронного документообігу з використанням технології цифрового підпису

Електронний документ відіграє ключову роль у сучасних системах управління документообігом, що базуються на електронних технологіях. Він становить фундаментальний елемент цих систем, де кожен електронний документ є записом у базі даних. Така база даних забезпечує зберігання, організацію та обробку інформації, яка міститься в документах. Основною характеристикою електронного документа є його формат у вигляді електронних даних. У такому форматі інформація фіксується за допомогою комп'ютерних програм та засобів збереження. Важливою особливістю електронних документів є їхня спроможність зберігати різноманітні типи інформації, включаючи текст, зображення, відео, аудіо, таблиці та інші дані, що можуть бути створені або відображені у цифровому форматі.

Крім того, кожен електронний документ має визначені атрибути, які визначають його ідентифікацію та характеристики. Серед цих атрибутів можуть бути такі, як назва документа, дата створення, автор, категорія, ключові слова тощо. Одним із найважливіших атрибутів є електронний цифровий підпис, який забезпечує підтвердження автентичності та цілісності документа. Завдяки електронному цифровому підпису можна впевнитися, що документ не був змінений після його підписання, а також встановити особу, яка підписала документ. Це важливо для забезпечення безпеки та надійності документообігу в електронному форматі.

Таким чином, електронний документ виступає не лише як засіб передачі інформації, але й як важлива складова електронного документообігу, що дозволяє

забезпечувати збереження, обробку та обмін даними в цифровому середовищі. Закон України «Про електронні документи та електронний документообіг» [1] встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів, окрім цього регулює відносини, які пов'язані зі створенням, передачею, засвідченням та зберіганням електронних документів, а також використанням електронного документообігу в різних сферах діяльності. У статті 9 Закону України «Про електронні документи та електронний документообіг» подано таке визначення електронного документообігу (обіг електронних документів) – це «сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів».

Згідно з Законом «Про електронну ідентифікацію та електронні довірчі послуги» перевірка цілісності електронного документа здійснюється шляхом підтвердження електронного підпису або печатки, які можуть бути удосконалені або кваліфіковані. Якщо на електронний документ накладено інший вид електронного підпису або печатку, перевірка здійснюється з використанням інших методів захисту, які мають відповідати вимогам законодавства у сфері захисту інформації.

Електронний цифровий підпис — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Електронний цифровий підпис створюється шляхом криптографічного перетворення набору електронних даних. Він підтверджує надійність електронного документа, захищаючи його від несанкціонованого втручання або пошкодження під час передачі від відправника до отримувача. Якщо ЕЦП було засвідчено з використанням посиленого сертифіката ключа за допомогою перевірених засобів цифрового підпису, а під час перевірки використовувався діючий посилений сертифікат ключа, і особистий ключ підписанта відповідає відкритому ключу,

вказаному у сертифікаті, то ЕЦП дозволяє ідентифікувати підписанта й прирівнюється до особистого підпису.

Електронний цифровий підпис накладається за допомогою особистого ключа, який відомий лише власнику та перевіряється за допомогою відкритого ключа, який доступний всім учасникам електронного документообігу. Особистий ключ генерується за допомогою генератора випадкових чисел і складається з унікальної послідовності символів, що має довжину 264 біта. Підтвердження чинності відкритого ключа відбувається через видання документа, що називається сертифікатом відкритого ключа, центром сертифікації ключів. Сертифікат ключа включає в себе значну кількість інформації, яка надає важливі відомості про цифровий ключ та його власника. При розгляді сертифіката можна знайти детальні дані про центр сертифікації ключів, включаючи його назву та адресу. Крім того, сертифікат також містить інформацію про країну, в якій був виданий, що є важливим для визначення правового статусу сертифіката.

Один з ключових елементів сертифіката - це його унікальний номер, який служить для однозначної ідентифікації сертифіката та пов'язаних з ним даних. Також в сертифікаті містяться основні дані власника особистого ключа, такі як ім'я, прізвище, адреса, інформація про компанію чи організацію, до якої він належить, та інші релевантні відомості. Важливим аспектом сертифіката є дата початку та завершення терміну його дії. Ці дані вказують на період, протягом якого сертифікат є дійсним, що дозволяє контролювати його використання та вчасно продовжувати його термін дії. Крім того, сертифікат містить відкритий ключ, який є необхідним для перевірки цифрових підписів, а також вказує на криптографічний алгоритм, який використовується власником особистого ключа для створення підпису.

Цифровий підпис — дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації підписувача цих даних.

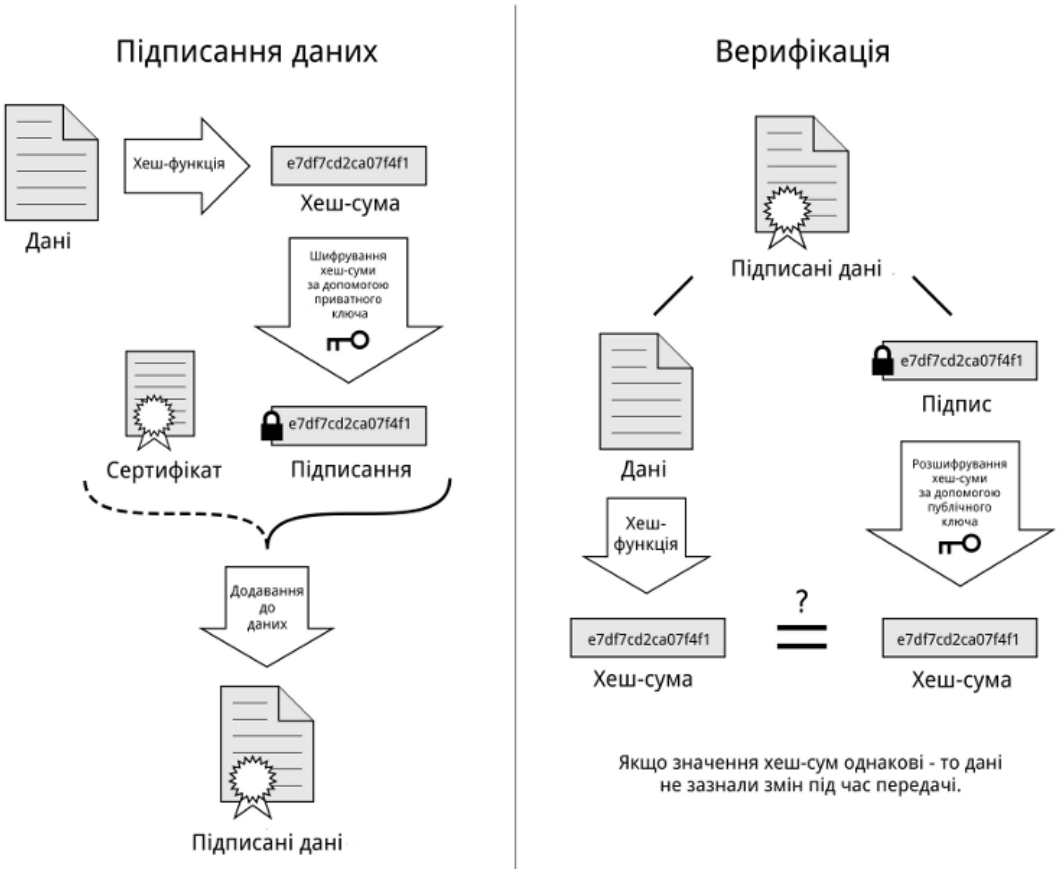

Рис. 1.1. Цифровий підпис даних

Посилаючись на дані Forrester Research [2, с. 103], для успішного ведення свого бізнесу 38% компаній зі списку Fortune 500 вважають придбання сучасних систем електронного документообігу досить важливим. Впровадження СЕД спрощує процес роботи з документами, зменшує час на їх обробку, підвищує ефективність співпраці між відділами та сприяє збереженню цінної інформації в цифровому форматі. Обсяг технічної роботи з документами іноді стає головним завданням для організацій. Згідно з дослідженням, проведеним Siemens Business Services [3] у ряді компаній, працівники витрачають 30% робочого часу на пошук та погодження документів, 6% документів втрачається, кожен внутрішній документ копіюється до 20 разів.

Впровадження системи електронного документообігу значно спрощує роботу з документами, але натомість з’являються певні ризики та проблеми.

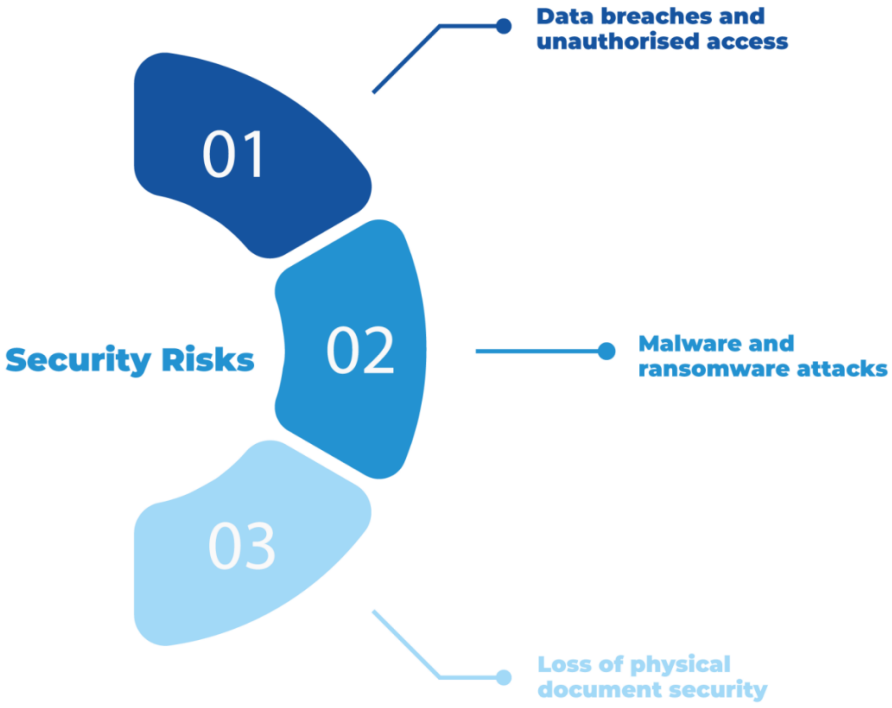

Рис. 1.2. Ризики безпеки під час міграції електронних документів [4]

Коли мова йде про безпечний документообіг, це означає не лише захист даних, які містяться у документах, від несанкціонованого доступу, але й гарантування безпеки в цілому. Це може включати в собі збереження працездатності системи, швидке відновлення після виникнення пошкоджень або збоїв, а навіть і після знищення. Оскільки безпека електронного документообігу повинна бути комплексною на всіх рівнях. У СЕД можна виділити загрози цілісності, загрози конфіденційності та загрози функціональності системи.

До загроз конфіденційності слід віднести проблему електронного документообігу, оскільки є ризик порушення конфіденційності даних та несанкціонованого доступу. Це можливо у випадку, якщо електронні документи не мають належного захисту або якщо працівники не дотримуються певних практик з безпеки. Наприклад, недостатньо складні паролі або відсутність шифрування інформації роблять документи більш уразливими для несанкціонованого доступу. Також важливим фактором є недостатня обізнаність персоналу щодо безпеки електронного документообігу та неналежне використання ресурсів, що можуть зробити СЕД менш уразливою.

Іншою потенційною проблемою безпеки електронного документообігу є ризик атак зловмисного програмного забезпечення та вимагання викупу. Це можна віднести до загроз цілісності, конфіденційності та функціональності. Ці загрози можуть призвести до крадіжки даних, пошкодження документів, або навіть знищення всієї інформації. В деяких випадках зловмисники можуть шифрувати дані і вимагати виплати для їх розшифрування. Для запобігання таких атак необхідно постійно оновлювати програмне забезпечення та встановлювати додаткове захисне програмне забезпечення.

Ще однією проблемою є втрата фізичного захисту документів, яка також може становити загрозу безпеці. Відмова від фізичних документів на користь електронних означає втрату фізичних заходів безпеки, притаманних традиційним паперовим системам. Фізичні документи можна зберігати в замкнених сейфах або шафах, а доступ до них можна суворо контролювати.

Зниження ризиків безпеки, пов'язаних з переходом від паперових до електронних документів, вимагає проактивного підходу та впровадження надійних заходів безпеки.

1.2. Аналіз підходів до захисту електронного документообігу з використанням технології цифрового підпису

Поглиблений та комплексний аналіз різноманітних стратегій та методик захисту, що використовуються у сфері електронного документообігу, ґрунтується на їх винятковій ефективності в гарантуванні твердої цілісності, повної достовірності та абсолютної недоступності для будь-яких незаконних чи несанкціонованих змінах в документах. Цей аспект має досить важливе значення у забезпеченні надійності та безпеки сучасних систем електронного документообігу, що перебувають у центрі уваги в умовах постійно зростаючого кількісного та якісного характеру цифрових загроз та атак.

Серед таких підходів можна зазначити найважливіші [5,6]:

законодавчі норми, законодавчі норми є найважливішим фактором забезпечення інформаційної безпеки, оскільки вони створюють правову основу для безпечного використання та захисту інформації від несанкціонованого доступу. Створення цілісної системи правових норм сприяє не лише контролю за обігом документів, але й забезпечує конфіденційність та цілісність інформації. Впровадження єдиної державної політики електронного документообігу дозволяє стандартизувати процеси, забезпечуючи їх сумісність та взаємодію між різними секторами економіки. Завдяки чіткій та стабільній правовій базі у сфері електронного документообігу, створюються умови для розвитку сучасного цифрового середовища, де інформація обмінюється ефективно, безпечно та з урахуванням вимог конфіденційності та захисту персональних даних. Такий підхід сприяє підвищенню довіри до цифрових технологій, що є важливим аспектом для сталого розвитку інформаційного суспільства;

шифрування, шифрування даних є важливим елементом забезпечення конфіденційності та цілісності інформації. В контексті систем електронного документообігу, де передаються чутливі або конфіденційні документи, застосування шифрування є незамінним. Воно забезпечує захист даних від несанкціонованого доступу та перегляду, навіть у випадку, якщо зловмисники отримають доступ до самого файлу. Інформація зашифрована за допомогою відповідних алгоритмів стає незрозумілою для будь-яких осіб, крім тих, хто має відповідний ключ розшифрування. Таким чином, шифрування даних є ефективним засобом забезпечення приватності та безпеки інформації в системах електронного документообігу;

резервне копіювання, резервне копіювання — важлива процедура, яка забезпечує захист інформації в разі непередбачених ситуацій, таких як випадкове видалення файлів, збій обладнання або кібератака. Резервні копії дозволяють відновити дані та швидко відновити нормальне функціонування системи. Переваги створення резервних копій полягають у тому, що вони забезпечують надійний метод збереження даних, допомагають у відновленні робочого стану системи та уникненні втрати важливих інформаційних ресурсів. Крім того, наявність

резервних копій дозволяє зменшити час та зусилля, необхідні для відновлення даних після подій, що можуть спричинити їх втрату;

управління метаданими, управління метаданими також є не менш важливим підходом до захисту електронного документообігу. Перед розповсюдженням або зберіганням електронних документів важливо використовувати програмне забезпечення, яке дозволяє переглядати та видаляти метадані з файлів. Багато програм, такі як редактори документів та конвертери PDF, мають вбудовані функції для видалення метаданих з документів перед їх зберіганням або розповсюдженням. Видалення метаданих перед розповсюдженням документів є важливим кроком у забезпеченні конфіденційності та захисту особистої інформації. Метадані можуть містити чутливу інформацію, таку як автора документа, дату та час його створення, а також редакційну історію. Ця інформація може бути небажаною для розповсюдження або може потенційно викликати конфлікти щодо конфіденційності;

Рис. 1.3. Способи захисту електронних документів

встановлення протоколів, встановлення протоколів, таких як SSL (Secure Sockets Layer) та TLS (Transport Layer Security), відіграє важливу роль у забезпеченні безпеки передачі даних через Інтернет. Ці протоколи забезпечують

захищене і шифроване з'єднання між користувачем та веб-сервером, що дозволяє передавати дані безпечно та надійно. Сертифікат SSL, що використовується у цих протоколах, є елементом, який гарантує автентичність веб-сайту та забезпечує шифрування даних, що передаються між браузером користувача і веб-сервером. Це дозволяє уникнути можливості перехоплення чутливої інформації, такої як паролі, особисті дані чи фінансові відомості, третіми сторонами під час їх передачі через мережу;

навчання персоналу, навчання персоналу є достатньо важливим підходом, оскільки більшість загроз безпеці організації походять від внутрішнього неправильного поводження чи маніпуляцій, надзвичайно важливо захистити документи від внутрішніх загроз. Зловмисники можуть захотіти отримати доступ до банківської інформації клієнта, або співробітники можуть навіть ненавмисно видалити або поділитися конфіденційними матеріалами. Навчання персоналу з питань кібербезпеки є критично важливим для будь-якої організації, оскільки вони стають першим ланцюгом оборони від потенційних загроз. Засвоєння персоналом навичок та знань з кібербезпеки також сприяє підвищенню ефективності та продуктивності в роботі, оскільки вони навчаються використовувати технології безпеки оптимальним чином.

налаштування користувацьких дозволів, налаштування користувацьких дозволів управління доступом до інформації в організації є не лише ефективним, але й надзвичайно важливим заходом забезпечення безпеки та конфіденційності даних. Цей процес передбачає створення та належне налаштування індивідуалізованих профілів доступу для кожного користувача, що працює в організації. Адміністратори системи мають можливість ретельно налаштовувати права доступу для кожного користувача з урахуванням його ролі та обов'язків. Це означає, що можна точно визначити, до якої інформації має мати доступ кожен працівник, забезпечуючи при цьому необхідний рівень обмежень та контролю.;

відстеження змін, відстеження редагувань є важливим інструментом в контексті підходу до забезпечення безпеки та ефективного управління документообігом в організації. Цей процес забезпечує системному адміністратору

можливість уважно відстежувати кожен етап обробки документів, реєструючи, хто має доступ до конкретних файлів, а також які саме зміни були внесені, якщо такі відбулися, до інформації у будь-якій з інтегрованих систем. Цей процес включає в себе детальне відстеження кожної дії, пов'язаної з документом, починаючи від моменту доступу до нього і закінчуючи будь-якими редагуваннями або модифікаціями, що здійснюються.

В кінцевому підсумку ліпше витратити час на те, щоб належним чином розробити структуру захисту та зберігання документів, щоб усе залишалося організованим і була можливість уникнути неприємні ситуації. Налаштуйте систему дозволів організації. Якщо використовується хмарна платформа потрібно обов'язково та регулярно робити резервні копії даних. Не слід зберігати більше даних, ніж потрібно для роботи, особливо якщо вони містять особисту інформацію або фінансові записи.

1.3. Аналіз існуючих рішень із захисту електронного документообігу з використанням технології цифрового підпису

Виконавши поглиблений аналіз існуючих рішень із захисту електронного документообігу з використанням технології цифрового підпису та оцінивши всі перспективи, можливо впевнено стверджувати, що інтеграція цифрового підпису в процес електронного документообігу є критичною для забезпечення цілісності, автентичності та конфіденційності документів. Ця технологія відіграє ключову роль у підвищенні безпеки документообігу, забезпечуючи надійний механізм перевірки підписувача та недопущення можливості зміни вмісту документів під час їх транспортування. Таким чином, впровадження цифрового підпису стане ефективним рішенням для забезпечення безпеки та надійності систем електронного документообігу.

Важливо зазначити що не тільки інтеграція цифрового підпису є важливим рішенням що до захисту електронного документообігу, вагому роль в захисті електронного документообігу беруть на себе системи електронного

документообігу (СЕД)[7], які надають можливість автоматизації процесів підписання документів за допомогою цифрового підпису. Ці системи забезпечують контроль доступу до документів та гарантують їх цілісність та конфіденційність.

Головне призначення СЕД - це організація збереження електронних документів, а також роботи з ними (зокрема, їх пошуку як за атрибутами, так і за змістом), СЕД можуть включати функціональні можливості для створення та перевірки цифрових підписів. Це означає, що користувачі можуть підписувати документи за допомогою свого цифрового ключа, що гарантує їх цілісність. Крім того, СЕД забезпечують контроль доступів до документу, що означає, що лише авторизовані користувачі мають доступ до конфіденційної інформації.

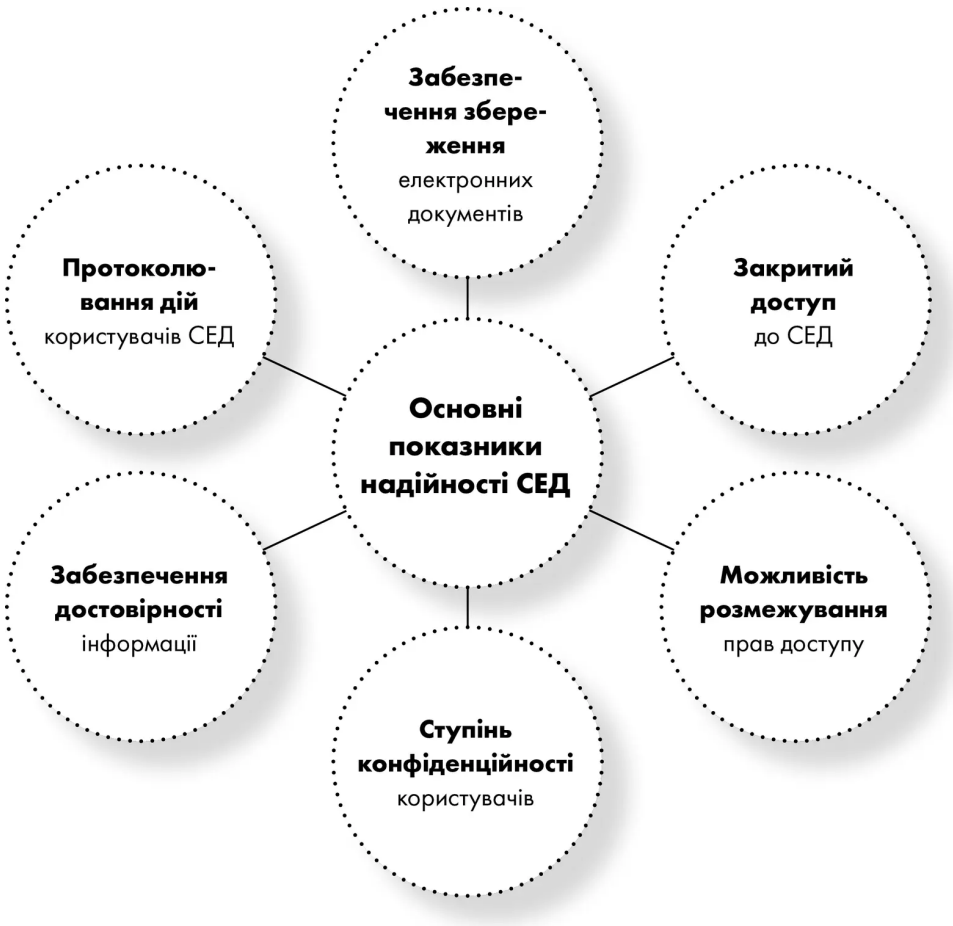

Рис. 1.4. Основні показники надійності СЕД

Також, СЕД можуть мати можливість автоматизованого управління над процесом підписання документів. Наприклад, система може автоматично надсилати запити на підписання документів до відповідних осіб та відстежувати статус підпису для кожного документа.

Відповідно до основних принципів електронного документообігу він повинен функціонувати на таких засадах:

1. Єдиноразова реєстрація документа;

2. Можливість паралельного виконання різних операцій з метою скорочення часу руху документів і підвищення оперативності їх виконання;

3. Безперервність руху документа;

4. Єдина база документальної інформації для централізованого зберігання документів і виключення можливості дублювання документів;

5. Ефективно організована система пошуку документа;

6. Розвинена система звітності за статусами і атрибутами документів, що дозволяє контролювати поетапний рух документів;

При усіх позитивних характеристиках згаданих систем автоматизації документообігу вони, як правило, високовартісні і більшість із них не є універсальними тобто розроблялися для виконання певних завдань підприємств і організацій певної галузі.

Окрім СЕД варто зазначити що використання блокчейн технології є досить важливим механізмом для забезпечення безпеки електронного документообігу. Використання блокчейн технології полягає в створенні розподіленої бази даних, яка забезпечує надійний, безпечний та непіддатний до втручання спосіб зберігання та обміну інформацією.

Блокчейн[8] — розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), який постійно довшає. Кожен блок містить часову позначку, хеш попереднього блоку та дані транзакцій, подані як хеш-дерево.

Кожен блок у блокчейні містить детальну інформацію про конкретну транзакцію або подію, яка може включаючи створення, підписання, зміну або будь-яку іншу операцію, пов'язану з документами чи іншими даними. Важливою

частиною кожного блоку є його хеш-значення, яке унікально ідентифікує цей блок та попередній блок у ланцюжку. Дана хеш-структура надає блокчейну виняткову надійність, оскільки навіть найменша зміна у попередньому блоку одразу виявляється в хеш-значенні наступного блоку. Такий механізм робить будь-яку спробу маніпулювання даними вкрай складною і легко виявляється.

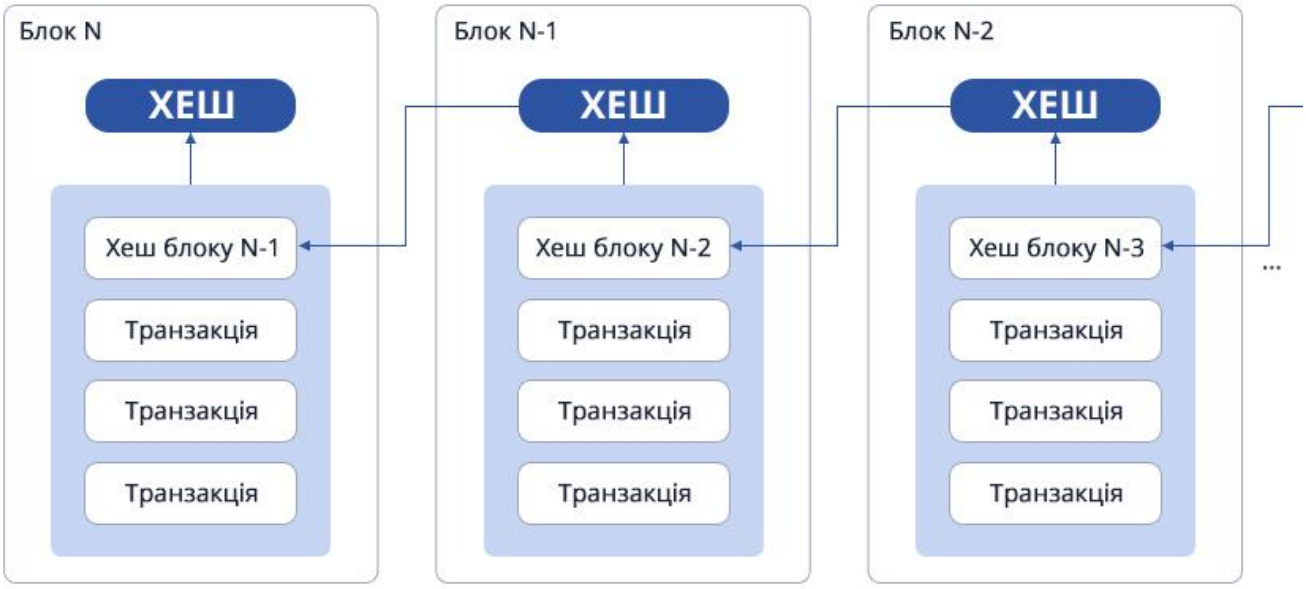

Рис. 1.5. Принцип роботи технології “Блокчейн”

У контексті електронного документообігу, можна розглянути кожен документ як окрему транзакцію у блокчейні. Зокрема, підписання документа в цифровому форматі може бути представлено як підписання транзакції у блокчейні, що дозволяє точно відстежувати кожну дію та забезпечує надійність та недоторканність даних в цифровому середовищі. Такий підхід використання блокчейну додає додатковий рівень захисту та достовірності до процесу обігу електронних документів, що стає надзвичайно важливим у сучасному цифровому світі, де зберігання та передача даних відбуваються в онлайн-середовищі.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ

2.1. Призначення та основні функції технології цифрового підпису в системах електронного документообігу

Розвиток глобальних комунікацій, науково-технічного прогресу та економіки, а також засвоєння нових територій та будівництво нових об'єктів, призвели до виникнення нової сфери взаємодії в діловому та повсякденному житті. Ця сфера стосується електронного обміну даними, у якому беруть участь державні органи, комерційні та некомерційні установи, а також громадяни у своїх офіційних і особистих відносинах. В електронному документі інформація, зафіксована за допомогою електронних даних, має включати обов'язкові реквізити документа, серед яких найважливішим є електронний підпис. Без електронного підпису згідно з певними вимогами документ втрачає юридичну силу та не може бути визнаний електронним документом.

Рис. 2.1. Формування електронного цифрового підпису

Для вирішення проблеми збереження електронних документів від копіювання, модифікації та підробки потрібно використовувати спеціальні засоби і методи захисту. Один з широко використовуваних інструментів захисту у світі - електронний цифровий підпис (ЕЦП). Він за допомогою спеціального програмного забезпечення підтверджує достовірність інформації в документі, його реквізитів і факту підписання конкретною особою.

Електронні документи, засвідчені електронним цифровим підписом, можуть бути передані до місця призначення протягом декількох секунд через швидкі телекомунікаційні системи, такі як Інтернет. Такі умови дозволяють усім учасникам обміну електронними документами, незалежно від відстані, мати однакові можливості в електронному інформаційному обміні.

Цифровий підпис дозволяє вирішити наступні завдання:

- здійснити аутентифікацію джерела повідомлення;
- встановити цілісність повідомлення;
- забезпечити неможливість відмови від факту підпису конкретного повідомлення

У практичній діяльності важливо не лише забезпечувати захист даних від несанкціонованого доступу, але й мати можливість перевірити достовірність та цілісність. І завдяки ЕЦП одержувач може переконатися, що документ не був змінений після його підписання, а також підтвердити автентичність відправника. Це один з факторів, який робить ЕЦП незамінним інструментом для надійного обміну даними, особливо в сферах, де важлива точність та конфіденційність, наприклад, в фінансовому секторі або сфері юридичних послуг.

Підписи, поставлені однією людиною під двома паперовими документами, візуально можуть здаватися схожими, але не ідентичними. Графологічна експертиза, за необхідності, може встановити, що ці підписи належать одній особі. Це може здатися парадоксальним, адже два електронні підписи (ЕЦП), створені однією людиною на двох електронних документах (ЕД) з використанням того ж ключа, завжди відрізняються один від одного. Два електронні підписи (ЕЦП), створені на основі одного й того ж коду для різних електронних документів (ЕД),

не ідентичні. Це пов'язано з тим, що ЕЦП ґрунтуються на криптографічних алгоритмах, які генерують унікальні значення для кожного підпису. Якщо припустити, що один ЕЦП буде використовуватися для множини ЕД, то його можна буде легко скопіювати або відтворити, що призведе до можливості підписання будь-якої кількості інших документів без згоди автора. Це може призвести до ситуації, коли автору нав'язують ЕД, з яким він не погоджується, але він все ж несе за нього юридичну відповідальність. У такому випадку використання електронного документообігу (ЕДО) з ЕЦП втрачає сенс, адже воно не гарантує автентичність та авторство документів.

Рис. 2.2. Перевірки справжності електронного цифрового підпису

Для вирішення завдань з перевірки автентичності було розроблено різноманітні алгоритми електронного цифрового підпису (ЕЦП) [9]. Більшість з них ґрунтуються на використанні односторонньої функції з секретним ключем FK для створення пари бінарних рядків (M, Q), де M - електронний документ, а Q - результат застосування функції FK до документу.

Виділимо наступні властивості ЕЦП:

1) при будь-якому K існує поліноміальний алгоритм обчислення значення FK(Q);

2) при невідомому K не існує поліноміального алгоритму для рішення рівняння FK(Q)=M відносно Q;

3) при відомому K існує поліноміального алгоритму для рішення рівняння FK(Q)=M відносно Q.

За першою властивістю завжди можна легко перевірити, чи відповідає підпис до повідомлення, і через другу властивість практично неможливо підробити підпис за достатньо великого ключа. Доказ цієї властивості дозволив би підписаним повідомленням надати юридичну силу. Секретний і відкритий ключі знаходяться у взаємно однозначній відповідності, і через третю вимогу не існує поліноміального алгоритму для обчислення секретної компоненти по відкритій компоненті.

Існує кілька методів побудови схем ЕЦП, а саме:

1) Шифрування електронного документа за допомогою симетричних алгоритмів включає у себе третю особу (арбітра), яка має довіру учасників обміну підписаними електронними документами. Взаємодія користувачів у цій системі відбувається наступним чином: учасник А шифрує повідомлення за допомогою свого секретного ключа КА, значення якого поділяється з арбітром, після чого шифроване повідомлення передається арбітру разом з інформацією про адресата. Арбітр розшифровує отримане повідомлення, виконує необхідні перевірки, і потім шифрує його на ключі учасника В (КВ). Зашифроване повідомлення надсилається учаснику В, разом із інформацією про відправника. Учасник В розшифровує повідомлення і переконується, що відправником є учасник А.

2) Використання асиметричних алгоритмів шифрування означає шифрування документа на секретному ключі його відправника. Ця схема використовується рідко через можливість критичної довжини електронного документа. Третя сторона не обов'язкова, хоча може виступати як сертифікаційний орган відкритих ключів користувачів.

3) Найпоширеніша схема ЕЦП полягає в шифруванні остаточного результату обробки електронного документа хеш-функцією за допомогою асиметричного алгоритму. Хеш-функція обчислює фіксоване значення для рядка будь-якої довжини, і це значення називається хеш-кодом або дайджестом.

Важливо зазначити, що особистий ключ (ОК), відкритий ключ (ВК) та електронний цифровий підпис (ЕЦП) - це компоненти, які використовуються у системах електронного документообігу для забезпечення безпеки та автентифікації. Зазвичай ці ключі формуються, представляються та зберігаються у вигляді електронних файлів з двійковими даними, які зберігаються в інформаційній системі та на персональних комп'ютерах користувачів.

Відповідно до постанови Кабінету Міністрів України “Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності” [10] справжність ЕЦП, накладеного на ЕД або інші електронні дані, та цілісність цього документа(електронних даних) перевіряється з дотриманням таких вимог:

– ЕЦП повинен бути підтверджений з використанням ПСВК за допомогою надійних засобів ЕЦП;

– під час перевірки повинен використовуватися ПСВК, чинний на момент накладення ЕЦП;

– ОК підписувача повинен відповідати ВК, зазначеному у ПСВК;

– на час перевірки повинен бути чинним ПСВК, сформований АЦСК та/або ПСВК відповідного засвідчувального центру.

Державний комітет з питань інформатизації та телекомунікацій (Держкомінформнаука) та Державна служба спеціального зв'язку та інформатизації України (ДССЗІ) спільним наказом затвердили " Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг" [11]. Ці Технічні специфікації є обов'язковими для надійних засобів електронного цифрового підпису (ЕЦП) та

програмно-технічних комплексів акредитованих центрів сертифікації ключів (АЦСК).

Щоб підтвердити правильність реалізації протоколу та форматів, описаних у Технічних специфікаціях, засоби ЕЦП повинні пройти сертифікацію та отримати відповідний сертифікат або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Користувач, відповідно до процедури, спочатку обчислює хеш-код (хеш-значення) електронного документа (ЕД). Цей код є проміжним етапом при створенні електронного цифрового підпису (ЕЦП), який накладається на ЕД. Далі користувач формує запит на створення позначки часу, який містить, зокрема, й обчислений хеш-код, і надсилає його до центру сертифікації ключів (ЦСК). ЦСК перевіряє правильність формату запиту, обробляє його, формує позначку часу та відповідь, яка містить цю позначку. У разі неможливості сформувати позначку часу, ЦСК надсилає відповідь з інформацією про відмову.

Після обробки запиту ЦСК надсилає користувачеві відповідь, яка містить засвідчену ЕЦП центру позначку часу. Позначка часу, створена за допомогою технічних засобів, являє собою сукупність електронних даних, що включає хеш-код ЕД (електронного документа), для якого було сформовано позначку, час її формування та серійний номер.

Отримавши відповідь від ЦСК, користувач перевіряє результат обробки запиту. У разі успішного обробки користувач перевіряє:

- Відповідність імені суб'єкта, який підписав позначку часу, власному імені ЦСК.
- Наявність у ЦСК права формувати позначки часу.
- Чинність сертифіката відкритого ключа (СВК) ЦСК.
- Справжність ЕЦП, накладеного на отриману від ЦСК позначку.

Після цього користувач порівнює попередньо обчислений ним хеш-код ЕД з хеш-кодом, записаним у позначці часу. Якщо порівняння успішне, позначка часу може бути додана до ЕД.

Перевірку позначки часу може виконати будь-яка особа (верифікатор) самостійно, без взаємодії з ЦСК, який її видав. Для цього верифікатор витягує позначку часу з електронного документа (ЕД), до якого вона прикріплена, і отримує з неї інформацію про ЦСК, що її сформував. Ця інформація використовується для отримання сертифіката відкритого ключа (СВК) ЦСК з центру сертифікації відкритих ключів (ЦЗО).

За допомогою чинного на момент формування позначки часу СВК ЦСК верифікатор перевіряє справжність електронного цифрового підпису (ЕЦП), накладеного на позначку часу. Потім, шляхом порівняння обчисленого хеш-коду ЕД з хеш-кодом, що зберігається у позначці часу, можна перевірити відповідність позначки часу та ЕД, до якого вона прикріплена. Наявність позначки часу, доданої до електронного документа (ЕД), може продовжити термін дії накладеного на нього електронного цифрового підпису (ЕЦП). Ця позначка (штамп) підтверджує, що ЕЦП був накладений на ЕД до того, як відповідний сертифікат відкритого ключа (СВК) був анульований (відкликаний).

Отже, для перевірки справжності ЕЦП, накладеного на ЕД до моменту відкликання СВК, можна використовувати відкритий ключ, який міститься у вже анульованому або відкликаному сертифікаті. Ланцюжок позначок часу робить можливим створення систем архівного зберігання ЕД, причому з гарантією збереження справжності ЕЦП, накладених на ці документи. Важливо зазначити, що для отримання позначки часу користувач не зобов'язаний надсилати до ЦСК сам електронний документ (ЕД) або накладений на нього електронний цифровий підпис (ЕЦП). Це означає, що процедура формування позначки часу не розкриває конфіденційного змісту ЕД. Таким чином, позначка часу може бути використана як один із механізмів для підтвердження авторства літературних творів, аудіовізуальних творів у цифровому форматі, баз даних, комп'ютерних програм та інших об'єктів інтелектуальної власності.

2.2. Методи та засоби захисту електронного документообігу з використанням технологій цифрового підпису

Як один з методів шифрування, який широко використовується, розглянемо шифрування інформації асиметричними ключами.

На відміну від симетричного шифрування, де використовується один ключ для шифрування та розшифрування, асиметричне шифрування використовує пару ключів: відкритий та закритий.

Відкритий ключ може бути доступний публічно, наприклад, на веб-сайті або у телефонній книзі. Закритий ключ, навпаки, повинен зберігатися в таємниці. Щоб надіслати зашифроване повідомлення, відправник використовує відкритий ключ одержувача. Розшифрувати таке повідомлення може лише одержувач, використовуючи свій секретний ключ. Головна перевага асиметричного шифрування полягає в тому, що немає необхідності конфіденційно передавати ключі.

Відкритий ключ можна вільно поширювати, не побоюючись, що треті особи зможуть його прочитати та розшифрувати повідомлення.

Це робить асиметричне шифрування ідеальним для таких завдань, як:

- Захист електронної пошти
- Захист онлайн-транзакцій
- Цифрові підписи
- Автентифікація

Важливо зазначити, що асиметричне шифрування, як і будь-який метод шифрування, не є абсолютно безпечним. Існують методи злому асиметричних алгоритмів шифрування, хоча вони й потребують значних ресурсів та обчислювальної потужності. Тому, при виборі асиметричного алгоритму шифрування, важливо враховувати рівень ризику та вибирати алгоритм з відповідним рівнем стійкості. Для спрощення шифрування та використання електронного цифрового підпису (ЕЦП) у корпоративних системах з великою кількістю користувачів застосовуються довідники відкритих ключів.

Кожен ключ у такому довіднику має два компоненти: тіло та номер. Номер ключа є однаковим як для секретної, так і для відкритої частин ключа, і він

унікальний для кожного користувача. При надсиланні зашифрованого документа або ЕЦП номер ключа передається у відкритому вигляді в заголовку. Одержувач, використовуючи цей номер, знаходить відповідний ключ у довіднику та застосовує його для розшифрування повідомлення або перевірки підпису.

Цей процес, як правило, виконується за допомогою спеціальних програм, і займає лише частки секунди.

Використання довідників відкритих ключів має ряд переваг:

1) Знижує навантаження на центр сертифікації ключів (ЦСК). ЦСК не потрібно видавати всім користувачам копії їхніх відкритих ключів, адже вони вже доступні в довіднику.

2) Збільшує безпеку. Відкриті ключі знаходяться лише у довіднику, до якого доступ мають лише авторизовані користувачі.

3) Спрощує роботу з ЕЦП. Користувачам не потрібно вручну шукати та передавати відкриті ключі, адже все це робиться автоматично.

Алгоритм RSA, розроблений у 1977-1978 роках Рональдом Ривестом, Аді Шаміром та Леонардом Адльманом, є найпоширенішим методом асиметричного шифрування. Цей алгоритм ґрунтується на принципі однобічних функцій з секретом, що робить його стійким до злому. Стійкість RSA базується на складності факторизації великих цілих чисел. У 1993 році RSA був стандартизований (PKCS #1: RSA Encryption Standard) та став широко використовуватися для шифрування та розшифрування даних, а також для генерації та перевірки електронно-цифрових підписів [12].

Таблиця 2.1.

Переваги та недоліки асиметричного шифрування

Переваги RSA:	Недоліки RSA:
Висока стійкість: RSA вважається одним із найстійкіших алгоритмів шифрування, завдяки чому він широко використовується для захисту конфіденційних даних.	Швидкість: RSA може бути повільнішим, ніж інші алгоритми шифрування, такі як AES.

Продовження таблиці 2.1.

Гнучкість: RSA може використовуватися як для шифрування, так і для підпису даних.	Розмір ключа: RSA використовує довгі ключі, що може призвести до проблем з їх зберіганням та обміном.
Широке поширення: RSA стандартизований та підтримується багатьма програмними забезпеченнями та бібліотеками.	Незважаючи на деякі недоліки, RSA залишається одним із найнадійніших та найпоширеніших алгоритмів асиметричного шифрування.

Альтернативою RSA може слугувати криптосистема Ель-Гамаля [13]. Дана система є альтернативою RSA і при рівному значенні ключа забезпечує ту ж криптостійкість. На відміну від RSA, метод Ель-Гамаля ґрунтується на проблемі дискретного логарифма, подібно до алгоритму Діфі-Хелмана. У цьому методі піднесення числа до степеня в кінцевому полі є простим завданням, але знайти аргумент за значенням (тобто знайти логарифм) дуже складно. Основу для системи складають параметри p і g - числа, перше з яких - простої, а друге - ціле.

Наприклад *Особа1* генерує секретний ключ a та обчислює відкритий ключ $y = g^a \bmod p$. Якщо *Особа2* хоче послати *Особі1* повідомлення m, то він вибирає випадкове число k, менше p і обчислює

$$y_1 = g^k \bmod p \quad \text{і}$$

$$y_2 = m \oplus y^k,$$

де $\oplus$ являє собою побітове додавання по модулю 2. Згодом *Особа2* надсилає (y_1,y_2) *Особі1*. *Особі1*, одержавши зашифроване повідомлення, відновлює його:

$$m = (y_1^a \bmod p) \oplus y_2.$$

Попри все алгоритм Ель-Гамаля не запатентований, отже не потребує сплати ліцензійних внесків. Важливо зазначити, що відсутність патенту не гарантує безкоштовність використання алгоритму. Можуть існувати інші обмеження, пов'язані з його застосуванням.

Ще однією альтернативою для стандарту асиметричного шифрування RSA є

алгоритм DSA. У 1991 році в США було опубліковано проєкт федерального стандарту цифрового підпису DSS (Digital Signature Standard, [DSS91]). Цей стандарт описує систему цифрового підпису DSA (Digital Signature Algorithm), яка була розроблена з урахуванням принципу "патентної чистоти", тобто без використання запатентованих технологій [14].

DSA, подібно до RSA, ґрунтується на теорії чисел і використовує модифікований варіант криптографічної системи Ель-Гамаля, про яку йшла мова раніше, відомий як схема Шнора. Стійкість DSA базується на практичній нерозв'язності певного випадку задачі обчислення дискретного логарифма. Сучасні методи розв'язання цієї задачі мають приблизно таку ж ефективність, як і методи розв'язання задачі факторизації. Тому для DSA рекомендується використовувати ключі довжиною від 512 до 1024 біт, що забезпечує рівень надійності, аналогічний RSA. Важливою перевагою DSA є менший розмір підпису порівняно з RSA. Довжина підпису в DSA становить 320 біт, що робить його більш компактним та економним у використанні.

Після публікації проект DSS отримав чимало зауважень, багато з яких були враховані під час його доопрацювання. Одним з головних аргументів проти DSA є те, що використаний в ньому частковий випадок задачі обчислення дискретного логарифма, на відміну від загальної задачі, недостатньо досліджений і може мати значно меншу стійкість до злому. Крім того, стандарт не описує метод генерування псевдовипадкових чисел, які використовуються при формуванні цифрового підпису, не підкреслює, що цей елемент алгоритму є одним із найважливіших для криптографічної стійкості.

Функціональність DSA обмежується лише цифровим підписом, і система не призначена для шифрування даних. За швидкістю генерування підпису DSA порівнянна з RSA, але значно поступається їй (у 10-40 разів) при перевірці підпису.

Що до генерації ЕЦП зазвичай використовують параметри трьох груп: загальні параметри, секретний ключ та відкритий ключ. Система ЕЦП потребує двох типів ключів: загальних параметрів та секретного ключа. Загалом, загальні параметри слугують для функціонування системи, секретний ключ

використовується для створення ЕЦП, а відкритий ключ для перевірки ЕЦП. Прості числа g, q, p, є загальними параметрами системами, що задовольняють наступним умовам:

g: так називаний генератор, що задовольняє рівності:

$$g = h^{((p-1)/q)} \, mod \, p > 1$$

q: простий дільник числа (p-1), що задовольняє умові:

$$q: 2^{159} < q < 2^{160}$$

Наведенні вище параметри публікуються для всіх учасників електронного документообігу з використанням технологій цифрового підпису, а секретний ключ обирається рандомно з діапазону *[1,q]* та тримається в секреті.

Після отримання повідомлення виконується перевірка умов на їх виконання *0<r1<q, 0<s1<q,* і у разі якщо хоча б одна умова не виконана – підпис не проходить перевірку.

2.3. Процеси функціонування електронного документообігу

Створення систем електронного документообігу потребує використання криптографічних методів захисту інформації та апарату електронного цифрового підпису (ЕЦП). Електронний цифровий підпис дає можливість однозначно підтвердити автентичність (авторство) відправника електронного документа та забезпечити контроль незмінності документа після його підписання.

В цілому система ЕЦП ґрунтується на використанні асиметричних криптографічних ключів. Для кожного користувача системи електронного документообігу створюється пара ключів ЕЦП:

- Секретний ключ: Цей ключ тримається в таємниці власником і використовується для генерування ЕЦП.
- Відкритий ключ: Цей ключ публікується та доступний всім учасникам системи. Він використовується для перевірки ЕЦП та ідентифікації відправника.

Секретний ключ дозволяє користувачеві підписувати електронні документи. ЕЦП гарантує, що документ не був змінений після підписання, а також підтверджує

авторство відправника, а відкритий ключ використовується для перевірки ЕЦП. Це дозволяє одержувачу документа переконатися, що документ не був підроблений і дійсно відправлений тим, ким зазначено.

Існує два основних способи поширення відкритих ключів ЕЦП між учасниками електронного документообігу корпоративна та відкрита технологія поширення ключів.

Зазвичай корпоративний метод використовує централізований орган, який називається "Адміністрація системи ЕЦП". Адміністрація відповідає за створення та ведення довідників відкритих ключів учасників системи, розповсюдження цих довідників серед усіх учасників та відновлення ключів у разі їх втрати або пошкодження. Ця технологія добре підходить для закритих корпоративних мереж, де можна гарантувати надійність Адміністрації.

Що до відкритої технології поширення, то цей метод ґрунтується на використанні цифрових сертифікатів, які є "цифровими підписами" користувачів. Кожен учасник має свій особистий цифровий сертифікат, який містить, ідентифікаційні дані користувача та відкритий ключ ЕЦП користувача. Кожен сертифікат підписується ЕЦП сертифікаційного центру - незалежного органу, який гарантує його автентичність та цілісність. Відкритий ключ Сертифікаційного центру є загальнодоступним і відомий всім учасникам системи.

Таблиця 2.2.

Переваги та недоліки відкритої технології

Переваги відкритої технології	Недоліки відкритої технології
Більш високий рівень безпеки: Сертифікаційні центри проходять суворі перевірки та мають високий рівень довіри	Витрати: Отримання сертифіката від авторитетного Сертифікаційного центру може бути платним
Простота використання: Не потрібна централізована Адміністрація, що спрощує адміністрування	Складність: Використання сертифікатів потребує додаткових знань та програмного забезпечення

При надсиланні електронного документа користувач додає до нього свій

цифровий підпис та підписує документ своєю ЕЦП.

При отриманні документа отримувач перевіряє дійсність та цілісність цифрового підпису, для цього він перевіряє ЕЦП сертифікаційного центру, яка знаходиться під підписом. З цифрового підпису витягується відкритий ключ відправника. Використовуючи відкритий ключ відправника, одержувач перевіряє ЕЦП відправника, яка знаходиться під документом.

Відкрита схема поширення відкритих криптографічних ключів має ряд переваг, які роблять її більш перспективною:

1) Простота керування ключами

1.1) Не потрібно створювати та підтримувати довідники відкритих ключів.

1.2) Користувачі самостійно отримують та зберігають свої ключі.

2) Масштабованість:

2.1) Відсутність довідників робить цю схему більш масштабованою.

2.2) Вона може використовуватися в системах з великою кількістю учасників.

3) Універсальність:

3.1) Користувачі з одним цифровим підписом та одним секретним ключем ЕЦП можуть брати участь у різних системах електронного документообігу.

3.2) Це спрощує використання ЕЦП для громадян.

Наприклад, один цифровий підпис може використовуватись для:

- Подання податкової декларації.
- Отримання пенсійних виплат.
- Сплати комунальних послуг.
- Здійснення покупок в онлайн-магазинах.

Важливу роль у функціонуванні ЕДО в Україні відіграло Положення про міжбанківські розрахунки, затверджене Постановою Правління Національного Банку України 08.10.1998 року № 414. Цей документ офіційно запровадив практику використання електронних документів у банківській системі, що стало значним кроком вперед.

Сьогодні ЕДО використовується у найрізноманітніших сферах. Наприклад, в

системах електронного урядування, Громадяни можуть отримувати та подавати документи онлайн, не виходячи з дому. Це економить час, кошти та спрощує взаємодію з державними органами. Також з допомогою ЕДО можна вести бізнес, електронний документообіг значно спрощує документообіг між компаніями та клієнтами. Ще однією сферою для ЕДО є медицина. Електронні документи та записи дають змогу лікарям мати швидкий доступ до історії хвороб та записів.

Таблиця 2.3.

Можливості та функції систем електронного документообігу

Функції	Можливості
Нормативно-довідкова інформація	
Контроль виконання	ведення контрольних завдань; перенесення терміну виконання завдань; ведення стану виконання; зняття завдань з контролю згідно із звітами; визначення результату виконання завдань; підтримка завдань централізованого і децентралізованого рівня
Реєстрація документів	реєстрація і облік документів; ведення журналів реєстрації та обліку. ведення номенклатури справ
Колективна робота	ведення електронних версій документів
Маршрутизація об'єктів документообігу	реєстраційних карток; контрольних карток; електронних версій документів; звітів щодо виконання контрольних завдань

Продовження таблиці 2.3.

Пошук	пошук об'єктів документообігу за атрибутами та повнотекстовий пошук документів
Звітність	журнали реєстрації та обліку; контрольні картки; аналіз виконання завдань; аналітичні і статистичні довідки
Адміністрування	розмежування повноважень; управління технологічними процесами; налагодження системи

В сучасних організаціях значна частина інформації має гриф конфіденційності, адже вона визначає напрямки діяльності та розвитку компанії. Для ефективного керування такою інформацією, окрім впровадження електронних систем управління, необхідний високий рівень інформаційної безпеки, як на організаційному, так і на технічному рівні. Зазвичай, захист даних на серверах ґрунтується на контролі доступу та шифруванні. Якщо вся корпоративна мережа знаходиться в межах однієї локальної обчислювальної системи, такі заходи можуть бути достатніми для прийнятного рівня захисту.

Однак у разі розгалуженої структури з філіями, підрозділами, представництвами та віддаленими співробітниками питання захисту інформації під час обміну конфіденційними даними стає більш гострим. Для повсякденної роботи користувачів такі засоби, як VPN (віртуальна приватна мережа) та просте шифрування даних, не завжди є зручними та практичними. VPN забезпечує безпеку передачі інформації через загальнодоступні мережі за допомогою шифрування, створюючи закритий канал для обміну даними. Завдяки клієнт-серверній технології VPN декілька географічно віддалених мереж або користувачів об'єднуються в єдину мережу з використанням захищених каналів для зв'язку. Однак VPN та шифрування не завжди є оптимальними рішеннями для всіх ситуацій.

Є ряд проблем, з якими можна зіткнутися:

- Складність налаштування та використання: VPN може бути складно налаштувати та використовувати, особливо для нетехнічних користувачів.
- Зниження продуктивності: VPN може призвести до зниження продуктивності, особливо при підключенні до мережі з низькою пропускною здатністю.
- Несумісність з деякими програмами та веб-сайтами: Деякі програми та веб-сайти можуть бути несумісні з VPN.
- Ризик обходу: Зловмисники можуть обійти VPN, якщо їм вдасться отримати доступ до ключа шифрування або іншої конфіденційної інформації.

Для вирішення цих проблем існує ряд альтернативних рішень, таких як:

- Хмарні служби: Хмарні служби зберігання та обміну даними можуть забезпечити високий рівень безпеки та зручності використання.
- Системи управління доступом на основі ролей (RBAC): RBAC дозволяють надавати користувачам доступ до даних лише на основі їхніх ролей та обов'язків.
- Захист даних на кінцевих пристроях: Захист даних на кінцевих пристроях може допомогти захистити дані на ноутбуках, планшетах та смартфонах.

Вибір найкращого рішення для захисту конфіденційної інформації залежить від конкретних потреб та вимог організації. Важливо провести ретельний аналіз та обрати рішення, яке забезпечить оптимальний баланс між безпекою, зручністю та практичністю.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЦИФРОВОГО

3.1. Варіанти захисту систем електронного документообігу з використанням технологій цифрового підпису

На сьогоднішній день система електронного документообігу (СЕДО) відіграє важливу роль у діяльності будь-якої установи, і Збройні Сили України не є винятком. Ефективність функціонування СЕДО напряму впливає на успішне виконання поставлених завдань. В умовах, в яких перебувають ЗСУ на даний момент, швидкість передачі інформації є критично важливою для успішного виконання бойових задач. Інформація, яка циркулює в СЕДО, може містити дані з обмеженим доступом. Для захисту такої інформації від несанкціонованого доступу необхідно впровадити надійну систему захисту електронних документів (ЕД). Однак важливо зважити, що впровадження захисту може призвести до ускладнення роботи системи та зниження її ефективності. Тому, рішення про впровадження системи захисту ЕД повинно бути обґрунтованим та доцільним. При прийнятті такого рішення необхідно врахувати наступні фактори:

- Рівень конфіденційності інформації, яка циркулює в СЕДО.
- Можливі ризики несанкціонованого доступу до інформації.
- Вартість впровадження та експлуатації системи захисту.
- Вплив системи захисту на продуктивність СЕДО.

Важливо знайти оптимальний баланс між безпекою інформації та зручністю роботи з СЕДО.

Для цього можна використовувати різні підходи, такі як:

- Впровадження багаторівневої системи доступу до інформації.
- Використання криптографічних методів захисту даних.
- Застосування програмних та апаратних засобів захисту інформації.

В Збройних Силах України вже вживаються заходи для вдосконалення СЕДО та підвищення рівня її захищеності. Так, наприклад, розробляються нові стандарти та регламенти роботи з СЕДО, проводяться навчання персоналу, впроваджуються нові програмні та апаратні засоби захисту інформації.

Інформація, яка циркулює в системі електронного документообігу (СЕДО), може бути піддана різним загрозам, які можна класифікувати наступним чином:

1. Загроза цілісності:

- Ненавмисне пошкодження, знищення або спотворення інформації: Це може статися через помилки користувачів, збої в роботі програмного забезпечення або апаратні проблеми.
- Навмисне пошкодження, знищення або спотворення інформації: Це може бути зроблено зловмисниками з метою крадіжки інформації, саботажу або вимагання.

2. Загроза конфіденційності:

- Несанкціонований доступ до інформації: Зловмисники можуть отримати доступ до конфіденційної інформації, зламавши систему або перехопивши дані під час їх передачі.
- Розголошення конфіденційної інформації: Авторизовані користувачі можуть ненавмисно або навмисно розголосити конфіденційну інформацію не уповноваженим особам.

3. Загроза працездатності системи:

- Навмисні атаки: Зловмисники можуть атакувати систему СЕДО з метою її виведення з ладу або крадіжки інформації.
- Помилки користувачів: Ненавмисні дії користувачів можуть призвести до збоїв у роботі системи.
- Збої в обладнанні та програмному забезпеченні: Технічні проблеми можуть призвести до тимчасової або постійної непрацездатності системи.

4. Неможливість підтвердження авторства:

- Відсутність електронного цифрового підпису: Якщо документи не підписані електронним цифровим підписом, неможливо довести, хто саме їх

створив.

- Підробка електронного цифрового підпису: Зловмисники можуть підробити електронний цифровий підпис, щоб видати себе за іншу особу.

5. Загроза доступності:

- Відмова в доступі до інформації: Авторизовані користувачі не можуть отримати доступ до інформації, яка їм необхідна, через збої в роботі системи, технічні проблеми або помилки в налаштуваннях доступу.
- Затримка в доступі до інформації: Користувачі змушені чекати занадто довго, щоб отримати доступ до необхідної інформації.

Для захисту інформації в СЕДО від цих загроз необхідно вживати комплексних заходів, таких як:

- Впровадження системи контролю доступу.
- Використання криптографічних методів захисту даних.
- Резервне копіювання інформації.
- Регулярне оновлення програмного забезпечення.
- Навчання персоналу питанням інформаційної безпеки.

Важливо також мати чіткий план дій на випадок виникнення інцидентів інформаційної безпеки, тому що вдосконалення системи захисту інформації в СЕДО є постійним процесом, який потребує постійного оновлення та адаптації до нових загроз.

3.2. Розробка конкретного плану впровадження системи електронного документообігу з урахуванням термінів, відповідальних осіб та ресурсів на підприємстві

В сучасному динамічному світі, де час та ефективність відіграють ключову роль в успіху будь-якого бізнесу, впровадження системи електронного документообігу (СЕДО) стає не просто опцією, а й нагальною потребою. СЕДО здатна трансформувати роботу вашого підприємства, оптимізуючи процеси, економлячи ресурси та виводячи його на новий рівень продуктивності.

Цей детальний план покликаний стати вашим путівником у захоплюючій трансформації документообігу на вашому підприємстві. Він описує чіткі кроки, необхідні для успішного впровадження СЕДО, з урахуванням індивідуальних потреб, термінів, відповідальних осіб та ресурсів вашої компанії.

Варто зазначити такі переваги впровадження СЕДО як [15]:

- Економія часу та ресурсів: Автоматизація рутинних завдань, пов’язана з обробкою документів звільняє час та ресурси для зосередження на більш стратегічних напрямках діяльності.
- Підвищення ефективності: Швидкий доступ до інформації, прозорість документообігу та оптимізовані процеси значно підвищують загальну ефективність роботи.
- Краща співпраця та комунікація: СЕДО полегшує обмін документами, спільну роботу над проектами та комунікацію між співробітниками, що веде до кращого розуміння та узгоджених дій.
- Підвищення безпеки та надійності: Захист даних за допомогою сучасних методів криптографії та резервне копіювання гарантують безпеку та конфіденційність інформації.
- Зменшення витрат на папір та друк: Перехід до електронного документообігу значно скорочує витрати на папір, тонери та друковані послуги.
- Покращення екологічності: Зменшення використання паперу позитивно впливає на довкілля, роблячи ваш бізнес більш екологічно відповідальним.

План впровадження системи електронного документообігу має містити чіткі цілі та завдання впровадження СЕДО, поточний стан документообігу на вашому підприємстві, чіткий графік впровадження з урахуванням термінів, безперебійний перехід до СЕДО, підтримка та оновлення СЕДО для її безперебійної роботи.

Рис.3.1. Шляхи вирішення можливих проблем впровадження СЕДО

Перш ніж впроваджувати СЕДО, важливо детально ознайомитися з існуючою системою документообігу на вашому підприємстві слід визначити які типи

документів використовуються. Це можуть бути бухгалтерські звіти, договори, рахунки, кадрові документи, технічна документація тощо, відстежити який життєвий цикл документів. Як вони створюються, узгоджуються, підписуються, архівуються та знищуються, які канали зв’язку використовуються для роботи з документами. Це може бути електронна пошта, паперові носії або спеціалізоване програмне забезпечення, перевірити хто має доступ до документів, Це можуть бути співробітники певних відділів, керівництво, клієнти, партнери, які проблеми виникають з поточним документообігом. Це можуть бути затримки в обробці документів, втрата інформації, недотримання норм конфіденційності, складність пошуку та обміну даними.

Після аналізу поточного документообігу потрібно визначити проблемні моменти та сфери, які потребують вдосконалення.

Таблиця 3.1.

Можливі та функції систем електронного документообігу

Ефективність та швидкість документообігу	**Безпека та конфіденційність**	**Доступність та пошук інформації**	**Витрати**	**Задоволеність працівників**
Затримках при узгодженні документів	Фізична втрата або пошкодження документів	Складність структури документообігу	Витрати на папір та друк	Відсутність технічної підтримки
Довгому пошуку потрібної інформації	Можливий несанкціонований доступ до документів	Неактуальна інформація	Заробітну плату співробітників, які обробляють документи вручну	Повільна робота системи

Продовження таблиці 3.1.

Дублюванні завдань	Ненавмисний або зловмисний витік інформації	Відсутність інструментів пошуку	Витрати на програмне забезпечення та обслуговування паперового архіву	Ненадійність системи

Для більш детального аналізу слід провести опитування користувачів системи та на основі їх відгуків сформувати план.

3.3. Рекомендації щодо застосування методів та засобів захисту електронного документообігу

Електронний документообіг стає все більш поширеним явищем і несе за собою значні переваги для організацій, оптимізуючи процеси, економлячи час та ресурси. Проте, подібно до будь-якої системи, що використовує дані, ЕДО потребує надійного захисту від кіберзагроз та інших ризиків. З метою мінімізації ризиків та забезпечення надійного захисту ЕДО рекомендується проведення комплексного аналізу загроз та ризиків для визначення найбільш ймовірних та критичних загроз для вашої системи ЕДО та впровадження багаторівневої системи захисту.

Захист ЕДО - це безперервний процес, який потребує постійного вдосконалення та адаптації до нових загроз. Захист даних в системах електронного документообігу ґрунтується на чіткій ідентифікації та аутентифікації користувачів.

Захист від загроз повинна реалізовувати будь-яка система електронного документообігу. Відповідно, в комплекс захисту електронної документації повинні входити наступні заходи:

1. Контроль фізичного доступу:

- Обмежити доступ до приміщень, де розміщено обладнання та дані

системи.

- Використовувати пропуски, карти доступу, охорону або інші методи для контролю доступу.
- Встановити камери відеоспостереження для фіксації подій.

2. Контроль доступу до інформації:

- Надати користувачам доступ лише до тих даних, які їм необхідні для роботи.
- Використовувати паролі, ключі або інші методи аутентифікації для захисту даних.
- Шифрувати конфіденційні дані.

3. Забезпечення авторства та цілісності документів:

- Використовувати електронні підписи для підтвердження авторства документів.
- Застосовувати методи контролю версій для відстеження змін документів.
- Використовувати хеш-функції для перевірки цілісності документів.

4. Забезпечення конфіденційності:

- Шифрувати дані під час зберігання та передачі.
- Обмежувати доступ до конфіденційних даних.
- Проводити навчання персоналу з питань конфіденційності.

5. Забезпечення юридичної сили електронних документів:

- Використовувати сертифіковані електронні підписи.
- Відповідно до законодавства оформлювати електронні документи.
- Зберігати електронні документи протягом визначеного періоду часу.

6. Забезпечення надійності роботи системи:

- Використовувати надійне обладнання та програмне забезпечення.
- Регулярно оновлювати програмне забезпечення.
- Проводити резервне копіювання даних.
- Тестувати систему на наявність помилок і вразливостей.

7. Захист від збоїв зв'язку:

- Використовувати резервні канали зв'язку.
- Встановлювати джерела безперебійного живлення.
- Розміщувати обладнання в різних місцях.

8. Захист від вірусів:

- Встановлювати антивірусне програмне забезпечення.
- Регулярно оновлювати антивірусні бази даних.
- Навчати персонал правилам комп'ютерної безпеки.

9. Захист від кібератак:

- Використовувати брандмауери та інші засоби захисту мережі.
- Шифрувати дані під час передачі.
- Навчати персонал правилам кібербезпеки.

ВИСНОВКИ

У роботі проведено дослідження шляхів підвищення захищеності систем електронного документообігу з використанням технології цифрового підпису, визначено мету та завдання цього дослідження. Сьогодні існують серйозні проблеми захисту електронного документообігу від нових і все більш витончених загроз. Спостерігається зростання ризиків для безпеки систем електронного документообігу, що ускладнюється їх недостатньою підготовленістю до протидії новим загрозам за допомогою наявних методів захисту.

Проведено аналіз існуючих технологій захисту систем електронного документообігу. Технологія цифрового підпису виконує функції забезпечення цілісності, автентичності та невідмовності документів, що є ключовими аспектами для захисту від кіберзагроз у реальному часі. Тому, цифровий підпис відіграє визначальну роль у загальній системі забезпечення безпеки електронного документообігу організації.

Впровадження технології цифрового підпису стало ключовим аспектом сучасної кібербезпеки, оскільки організації стикаються з дедалі складнішими кібератаками. Електронний цифровий підпис є комплексним рішенням для захисту електронного документообігу, яке забезпечує перевірку справжності підписів у реальному часі та реагування на загрози. Крім того, воно включає автоматизоване реагування на інциденти та можливості цифрового розслідування, що дозволяє оперативно реагувати на будь-які порушення та загрози.

Розширене впровадження технології цифрового підпису також відкриває нові можливості для інтеграції з іншими системами та сервісами, які використовуються в організаціях. Це включає синхронізацію з системами управління документами, обліковими системами, а також платформами для співпраці та обміну інформацією. Використання цифрового підпису може значно підвищити ефективність роботи, скоротити час на обробку документів і знизити витрати, пов’язані з фізичним зберіганням та обробкою паперових документів. Крім того, така інтеграція

дозволяє забезпечити більш високий рівень контролю та відстеження доступу до інформації, що є важливим аспектом для дотримання регуляторних вимог та внутрішніх політик безпеки. Таким чином, цифровий підпис не тільки підвищує рівень безпеки, але й сприяє загальному підвищенню ефективності та продуктивності організації, роблячи її більш конкурентоспроможною в сучасному цифровому світі.

Дана кваліфікаційна робота може допомогти організаціям скористатися останніми рекомендаціями, забезпечуючи комплексну безпеку електронного документообігу. Вона також сприяє автоматизації процесів реагування на інциденти та спрощує впровадження найкращих практик безпеки. Застосування сучасних технологій цифрового підпису дозволяє створити надійну систему захисту, яка відповідає вимогам сучасних стандартів кібербезпеки та ефективно протидіє новим загрозам.

Таким чином, правильна реалізація технології цифрового підпису в системах електронного документообігу організації має сприяти ефективному захисту корпоративних інформаційних ресурсів у цілому. Це забезпечує не лише захист документів, але й підвищує загальний рівень безпеки інформаційної системи організації, дозволяючи мінімізувати ризики втрати чи несанкціонованого доступу до конфіденційних даних. Впровадження цифрового підпису сприяє зміцненню довіри до електронного документообігу, підвищуючи його надійність та безпеку у сучасному цифровому середовищі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Моделювання та проектування приватного мережево-серверного середовища з використанням технології opennebula / А. В. Антоненко та ін. Таврійський науковий вісник. Серія: технічні науки. 2023. № 3. С. 3–19. URL: https://doi.org/10.32782/tnv-tech.2023.3.1 (дата звернення: 18.03.2024).

2. Про електронний цифровий підпис : Закон України від 22.05.2003 р. № 852-IV : станом на 7 листоп. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення: 16.03.2024).

3. «Про електронні документи та електронний документообіг» : Закон України від 22.05.2003 р. № 36 : станом на 31 груд. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 12.03.2024).

4. Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг : Постанова Каб. Міністрів України від 07.11.2018 р. № 992 : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/992-2018-п#Text (дата звернення: 21.03.2024).

5. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності : Постанова Каб. Міністрів України від 01.08.2023 р. № 798. URL: https://zakon.rada.gov.ua/laws/show/798-2023-п#Text (дата звернення: 17.03.2024).

6. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Каб. Міністрів України від 29.03.2006 р. № 373 : станом на 21 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 15.03.2024).

7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента

України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 16.03.2024).

8. Binance Academy. Що таке криптографія з публічним ключем?. Binance Academy. URL: https://academy.binance.com/uk/articles/what-is-public-key-cryptography (дата звернення: 21.03.2024).

9. Digital signature algorithm (DSA) - geeksforgeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/digital-signature-algorithm-dsa/ (дата звернення: 23.03.2024).

10. EDMS implementation: benefits and key steps. Assai. URL: https://www.assai-software.com/edms-implementation-benefits-and-key-steps/ (дата звернення: 26.03.2024).

11. Schmidt B., Shukla D. Essential windows workflow foundation. Pearson Education, 2021. 480 с.

12. Siemens business services. URL: https://www.siemens.com/ua/uk.html 28.05.2024(дата звернення: 25.05.2024).

13. The Economist. The great chain of being sure about things. The Economist. URL: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (дата звернення: 16.03.2024).

14. Vanstone S. A., Menezes A. J., Oorschot P. C. v. Handbook of applied cryptography. Taylor & Francis Group, 2018. 810 с.

15. Workflo Solutions ®. From paper to pixels: navigating the security risks of electronic document migration. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/from-paper-pixels-navigating-security-risks-electronic (дата звернення: 15.03.2024).