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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

на тему: «Технологія захисту систем електронного документообігу»

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
_____ Богдан ЗЕРНИЦЬКИЙ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти групи СЗДМ-61
_Богдан ЗЕРНИЦЬКИЙ_____
Ім'я, ПРІЗВИЩЕ

Керівник:_____Андрій КОТЕНКО_____
к.т.н., доцент Ім'я, ПРІЗВИЩЕ

Рецензент:_____
доцент Ім'я, ПРІЗВИЩЕ

Київ 2025

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ
_____Зерницькому Богдану Миколайовичу_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Технологія захисту систем електронного документообігу»_
керівник кваліфікаційної роботи _КОТЕНКО Андрій к.т.н., доцент_____
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи: Загрози в системах електронного документообігу, покращення захисту в системах електронного документообігу, протидія загрозам в системах електронного документообігу.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Аналіз електронного документообігу;_____
2. Проблематика систем електронного документообігу;_____
3. Вдосконалення безпеки на основі СЕДО Paperless._____

5. Перелік графічного матеріалу: ___Презентаційний матеріал на 14 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 _____ Богдан ЗЕРНИЦЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Андрій КОТЕНККО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи містить 90 сторінок, 7 рисунків, 4 таблиці, 31 джерело.

Актуальний захист систем електронного документообігу є надзвичайно важливим для забезпечення безпеки інформаційних ресурсів організації. Оскільки СЕДО зберігає та обробляє критично важливі документи, зокрема конфіденційні дані, їх несанкціонований доступ чи втрата можуть призвести до фінансових збитків, витоку інформації або зупинки робочих процесів.

Об'єкт дослідження – методи захисту, можливі для реалізації захисту систем електронного документобігу.

Предмет дослідження – технології захисту, які забезпечують безпеку в системах електронного документообігу там можуть бути реалізовані в організаціях.

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

Мета роботи – підвищити надійність захисту систем електронного документообігу.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз функціонування електронного документообігу;
- аналіз роботи та функціонування систем електронного документообігу;
- аналіз загроз в системах електронного документообігу;
- розробка рекомендацій щодо вдосконалення безпеки в системах електронного документообігу на прикладі СЕДО Paperless.

Апробація:

Б.М. Зерницький Методи захисту систем електронного документообігу. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.33 - 35.
https://duikt.edu.ua/uploads/p_2661_93669247.pdf

КЛЮЧОВІ СЛОВА: ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ, СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ, МЕТОДИ ЗАХИСТУ, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, БІОМЕТРІЯ. ЗАГРОЗИ ЗАХИСТУ ІНФРОРМАЦІЇ, ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС.

ABSTRACT

The text part of the master's qualification work contains 90 pages, 6 figures, 4 tables, and 30 references.

The protection of electronic document management systems is extremely important for ensuring the security of an organization's information resources. Since EDMS stores and processes critically important documents, including confidential data, unauthorized access or loss may lead to financial damage, data leaks, or disruption of operational processes.

Object of research – protection methods that can be implemented to secure electronic document management systems.

Subject of research – protection technologies that ensure security in electronic document management systems and can be implemented in organizations.

Research methods – system analysis and literature review on the given topic.

Purpose of the work – to improve the reliability of protection in electronic document management systems.

To achieve the specified purpose, the following main tasks are carried out:

- analysis of electronic document management functionality;
- analysis of the operation and functioning of electronic document management systems;
- analysis of threats in electronic document management systems;
- development of recommendations for improving security in electronic document management systems using the example of the Paperless EDMS.

Approbation:

B.M. Zernytskyi Methods of protecting electronic document management systems. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 3, 2024, Kyiv: RVC DUIKT. – 024. P.33 - 35.

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

KEYWORDS: ELECTRONIC DOCUMENT MANAGEMENT, ELECTRONIC DOCUMENT MANAGEMENT SYSTEM, PROTECTION METHODS, MULTIFACTOR AUTHENTICATION, BIOMETRICS, INFORMATION SECURITY THREATS, DIGITAL SIGNATURE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8

ВСТУП 9

РОЗДІЛ 1. АНАЛІЗ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ 11

1.1. Електронний документ 11

1.1.1. Переведення документа у електронну форму 16

1.1.2. Формати файлів електронного документу 18

1.2. Визначення електронного документообігу 21

1.3. Переваги ЕДО 23

1.4. Висновки до першого розділу 25

РОЗДІЛ 2. ПРОБЛЕМАТИКА СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ27

2.1. Система електронного документообігу 27

2.1.1. Характеристики СЕДО 29

2.1.2. Функціональні особливості СЕДО 35

2.1.3. Система WorkFlow 37

2.2. Хмарні технології в СЕДО 39

2.3 Класифікація СЕДО 43

2.3.1. Види систем електронного документообігу 47

2.3.2. Класифікація функціоналу та компонентів СЕДО 51

2.4. Основні загрози для СЕДО 54

2.4.1. Криптографічні методи захисту в СЕДО 57

2.4.2. Забезпечення автентичності документів 60

2.4.3 Перевірка правильності ключів ЕЦП 63

2.4.4 Надійність ЕЦП 64

2.5. Висновки до другого розділу 67
РОЗДІЛ 3. ВДОСКОНАЛЕННЯ БЕЗПЕКИ НА ПРИКЛАДІ СЕДО PAPERLESS 69
3.1. Характеристика СЕДО Paperless 69
3.1.1. Призначення та основні функціональні можливості 70
3.1.2. Архітектура та технічні особливості 71
3.2. Аналіз переваг та недоліків СЕДО Paperless з точки зору безпеки 71
3.2.1. Недоліки та потенційні вразливості 72
3.3. Рекомендації щодо вдосконалення захисту Paperless 73
3.3.1. Захист від несанкціонованого доступу 74
3.3.2. Модернізація криптографічних механізмів захисту 78
3.3.3 Додавання дозволених IP-адрес для доступу в СЕДО Paperless 79
3.3.4. Покращення моніторингу та аналізу подій безпеки 80
3.3.5. Посилення захисту від людського фактору 81
3.6. Висновки до другого розділу 83
ВИСНОВОК 84
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 85
ДОДАТОК А 89

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ECM (Enterprise Content Management) – управління корпоративним контентом

EDMS – Electronic Document Management Systems

IaaS (Cloud Infrastructure as a Service) – Інфраструктура як послуга

MFA (Multi-Factor Authentication) – Багатофакторна автентифікація

PaaS (Cloud Platform as a Service) – Платформа як послуга

PDM (Product Data Management) – Система управління даними

SaaS (Cloud Software as a Service) – Програма як послуга

VPN (Virtual Private Network) – Віртуальна приватна мережа

WF (WorkFlow) – Потік робіт

ЕД – Електронний документ

ЕДО – Електронний документообіг

ЕЦП – Електронний цифровий підпис

ІТ – Інформаційні технології

ОК – Особистий ключ

ПЗ – Програмне забезпечення

СЕДО – Система електронного документообігу

ВСТУП

Актуальність дослідження. В умовах глобальної цифровізації та зростання обсягів інформації, що обробляється в електронній формі, системи електронного документообігу стали невід'ємною частиною роботи сучасних організацій. Однак одночасно з розвитком таких систем посилюються і загрози їхній безпеці.

У сучасному світі кількість кібератак на інформаційні системи, включаючи СЕДО, зростає з кожним роком. Зловмисники постійно вдосконалюють свої методи, використовуючи фішинг, атаки типу «брутфорс» та інші методи для отримання несанкціонованого доступу до систем. СЕДО, як середовище, що обробляє конфіденційні документи, фінансову інформацію та персональні дані, є привабливою мішенню для хакерів. Несвоєчасний захист цих систем може призвести до витоку даних, фінансових втрат та репутаційних збитків для організації.

Розвиток віддаленої роботи створив нові виклики для безпеки СЕДО. Співробітники часто підключаються до систем через ненадійні мережі або пристрої, що збільшує ймовірність несанкціонованого доступу чи інфікування системи шкідливим програмним забезпеченням. В таких умовах, захист даних у СЕДО вимагає додаткових заходів, таких як багатофакторна автентифікація.

Однією з найактуальніших проблем для СЕДО є внутрішні загрози, що походять від самих співробітників. Це може бути як навмисне завдання шкоди організації, так і випадкові дії через низький рівень обізнаності у питаннях інформаційної безпеки. Наприклад, використання слабких паролів, нехтування політиками доступу або збереження конфіденційних документів на незахищених пристроях.

Саме тому, організації, які не приділяють достатньої уваги захисту СЕДО, ризикують втратити конкуретні переваги через можливий витік стратегічно важливих даних. Сучасний бізнес залежить від швидкого, надійного та безпечного документообігу. Будь-яка вразливість системи може бути використана зловмисниками для отримання несанкціонованого доступу до внутрішньої інформації, що може спричинити значні збитки для бізнесу та негативно позначитися на його репутації.

Об'єкт дослідження – методи захисту, можливі для реалізації захисту систем електронного документобігу.

Предмет дослідження – технології захисту, які забезпечують безпеку в системах електронного документообігу там можуть бути реалізовані в організаціях.

Мета роботи – підвищити надійність захисту систем електронного документообігу.

Наукові завдання:

проаналізувати електронний документообіг;

проаналізувати роботу та функціонування систем електронного документообігу;

проаналізувати загроз в системах електронного документообігу;

розробити рекомендації щодо вдосконалення безпеки в системах електронного документообігу на прикладі СЕДО Paperless.

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

Практичне значення одержаних результатів полягає у розробці рекомендацій щодо вдосконалення безпеки в системах електронного документообігу на прикладі СЕДО Paperless.

РОЗДІЛ 1. АНАЛІЗ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1.1. Електронний документ

В наш час, робота з документами є невід'ємною частиною будь-якої організації чи установи, оскільки це забезпечує ефективне управління інформацією, підтримує прозорість процесів, допомагає в зберіганні важливих даних та полегшує комунікацію між співробітниками та відділами. Завдяки сучасним технологіям, організації можуть автоматизувати роботу з документами, зменшуючи кількість паперової роботи, а також підвищувати рівень безпеки даних та забезпечувати легкий доступ до потрібної інформації.

Документи використовуються в різних галузях для управління інформацією, організації процесів та забезпечення належного рівня комунікації. Від юридичних і фінансових документів у банківській сфері до медичних карток і записів у охороні здоров'я, документи є важливими інструментами, що фіксують, зберігають та передають дані. В освітній сфері документи допомагають у веденні обліку успішності студентів та розкладів занять, в той час як, на виробництві —управління постачанням, плануванні та контролі якості. У державному секторі документи підтримують процеси прийняття рішень, ведення обліку громадян та надання послуг, що забезпечує ефективну роботу адміністративних установ.

В Законі України «Про інформацію» зазначено, що **документом** є матеріальний носій, який містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі [1].

З розвитком сучасних інформаційних технологій, почали виникати дискусії щодо того, які відмінності має електронний документ, порівняно з документом на паперовому носії.

В Україні, такий термін як «електронний документ», вперше з'явився в 2003 році, після прийняття Закону України «Про електронні документи та електронний документообіг» та Закону України «Про електронний цифровий підпис».

Електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа. Оригіналом електронного документа вважають електронний примірник документа з обов'язковими реквізитами, утому числі з електронним цифровим підписом його автора, накладанням якого й завершується створення документа. Якщо електронний документ надсилається декільком адресатам, то кожен з його примірників вважається оригіналом електронного документа. Оригінал електронного документа має довести його цілісність та справжність у порядку, визначеному законодавством [2].

В свою чергу, електронний документ бере свій початок після «зародження» в бінарному виді та призначений для «читання» людиною, лише з використанням технічних засобів.

Особливості електронних документів:

– матриця документу існує в формі, що не може сприйматися людиною без використання технічних засобів і яка відмінна від її відтворення, безпосередньо на екрані монітора;

– можливість об’єднання різних форм подання інформації в одному документі, таких як текст, звук, зображення, включаючи анімацію та відео;

– можливість перенесення інформації з одного носія інформації, на інший не зазнаючи змін, а також здатність одного й того ж тексту існувати в різних форматах;

– здатність багаторазово перекодовувати вихідний текст, використовуючи різні методи його збереження та відтворення;

– динамічний характер певних типів електронних документів, який надає можливість його авторам вносити в них зміни;

– можливість багатоканального та одночасного доступу до одного й того ж примірника документа;

– відсутність окремого фізичного носія для масивів документів, збережених на жорсткому диску комп’ютера;

– електронні документи можуть мати посилання, які не контролюються авторами.

Електронний документ може бути створений, переданий, збережений і перетворений у візуальну форму за допомогою електронних засобів. Візуальна форма подання електронного документа полягає в відображенні його інформації за допомогою технічних засобів (таких як комп'ютерна техніка та програмне забезпечення) або на папері (через переведення в друковану форму за допомогою сучасних пристроїв) у вигляді, зручному для сприйняття людиною.

Основними елементами, що виділяються в структурі електронного документа є його зміст, реквізити і носій.

1) **Зміст** ЕД – текстові та графічні складові документа, які формують інформаційне наповнення, включаючи основний текст, таблиці, малюнки, графіки, діаграми та інші візуальні елементи, що допомагають проілюструвати або доповнити представлену інформацію. Вони сприяють кращому розумінню змісту документа, роблять його більш привабливим і легким для сприйняття. Зміст також може включати різні шрифти, кольори та стилі форматування, які підкреслюють важливі моменти або структурні елементи документа, такі як заголовки, підзаголовки та списки [3].

2) **Реквізит** електронного документа - інформація, зафіксована в електронному документі та реєстраційно-моніторинговій картці для його ідентифікації, організації обігу та надання йому юридичної сили [4].

Реквізити документа виконують кілька важливих функцій, які забезпечують його ефективність і правову значущість. По-перше, вони сприяють ідентифікації документа, що дозволяє швидко зрозуміти його зміст та призначення. По-друге, реквізити забезпечують правильне оформлення, відповідно до встановлених стандартів, що підвищує юридичну силу документа. Реквізити також важливі для ведення обліку документів, що є необхідним для їх управління та архівування. Нарешті, певні реквізити підтверджують автентичність документа, що є критично важливим у юридичних і фінансових справах. Таким чином, реквізити є невід'ємною складовою електронного документа, що сприяє його правильному використанню та збереженню.

Обов’язкові реквізити які повинні мати електронні документи [5]:

- назва документа;
- дата складання;

- назва підприємства, від імені якого складений документ;
- зміст, обсяг та одиниця виміру господарської операції;
- посади і прізвища осіб, які відповідальні за впровадження господарської операції та правильність її оформлення;
- особистий підпис або інші дані, які дозволяють ідентифікувати особу, яка брала участь у господарській операції.

Крім того, саме електронні документи повинні мати дані, які дозволяють встановити:

- походження;
- призначення документа;
- дату і час його отримання.

3) **Носій** електронного документа – це матеріальний або віртуальний об'єкт, на якому зберігається інформація електронного документа. Носії можуть бути різними, залежно від формату та технології зберігання. Основні типи носіїв включають:

- Жорсткі диски – які використовуються в комп'ютерах для зберігання великих обсягів даних;
- Флеш-накопичувачі – портативні пристрої, що дозволяють легко переносити інформацію;
- Оптичні диски – CD, DVD або Дискети, які використовуються для запису та зберігання даних;
- Хмарні сховища – віртуальні платформи, які забезпечують зберігання даних в Інтернеті;
- Системи електронного документообігу – спеціалізоване програмне забезпечення, що забезпечує зберігання, організацію та доступ до електронних документів.

В свою чергу, електронні документи, які створені за допомогою технічних засобів мають такі загальні властивості:

- неможливість відтворення документу без використання технічних засобів;
- наявність одного спільного носія для групи документів;

- необхідність кодування для збереження та перекодування, щоб відтворити зміст;
- можливість багаторазового запису різних текстів на одному й тому ж носії.

Окрім цього, електронні документи мають певні специфічні властивості, до них можна віднести:

- доступна загальна система кодування (двійковий код), вона однакова для запису документів усіх знакових систем тексту, звуку, зображення, графіки тощо;
- деякі електронні документи практично неможливо витягти із програмної оболонки або загальних масивів даних, наприклад, у базі даних.
- незалежність інформаційної складової (таблиця, текст, зображення) від конкретного матеріального носія;
- для кожного документа не існує окремого носія, розміщеного на певному комп'ютері або сервері;
- «інтерактивність» документа, тобто можливість втручання користувача в його текст або структуру, надалі з можливістю доповнення або зміни вмісту фалу.

Якщо поглянути на останньою специфічну властивість електронного документа, а саме на інтерактивність, то виникає закономірне питання його цілісності. Однак, крім цього, відомо, що під час передачі документа через канали зв'язку він розбивається на дрібні складові, які потім знову з’єднуються в єдиний об'єкт на комп'ютері одержувача. Однак, при цьому можливі технічні збої, які можуть призвести до деформації документа.

Хоча всі електронні документи й містять програмне забезпечення, проте критичність впливу цього фактору варіюється в залежності від їх використання. Деякі документи можуть бути без проблем прочитані, практично на будь-яких системах, тоді як для роботи з іншими необхідне встановлення спеціальних додатків, без яких електронний документ не зможе функціонувати.

Електронний документ супроводжується специфічними метаданими – інформацією, що описує його соціальну спрямованість, зміст, структуру та призначення. Метадані слугують підтвердженням цілісності й автентичності документа та є невід'ємним елементом його збереження.

Характерні риси електронного документа:

1. Автентичність – підтвердження авторства документа та його справжності за допомогою електронних підписів, сертифікатів чи інших методів ідентифікації.

2. Достовірність – гарантія того, що інформація в документі відповідає дійсності та відображає реальні дані без спотворень.

3. Цілісність – захист від несанкціонованих змін або пошкоджень документа, забезпечення збереження його початкового змісту з моменту створення.

1.1.1. Переведення документа у електронну форму

Через стрімкий розвиток технологій у світі, розпочалося перетворення паперових документів в електронну форму для впровадження електронного документообігу.

Процес перетворення документа на електронний формат складається з наступних етапів:

1. Сканування документа та створення його копії у електронному вигляді, такого як зображення. Під час сканування, виконується візуальний контроль якості.

2. Розпізнавання сканованих документів – переведення зображення у текстовий документ, що дозволяє редагувати і обробляти текстову інформацію.

На рис. 1.1 зображено класифікацію документів з точки зору їх переведення у електронну форму.

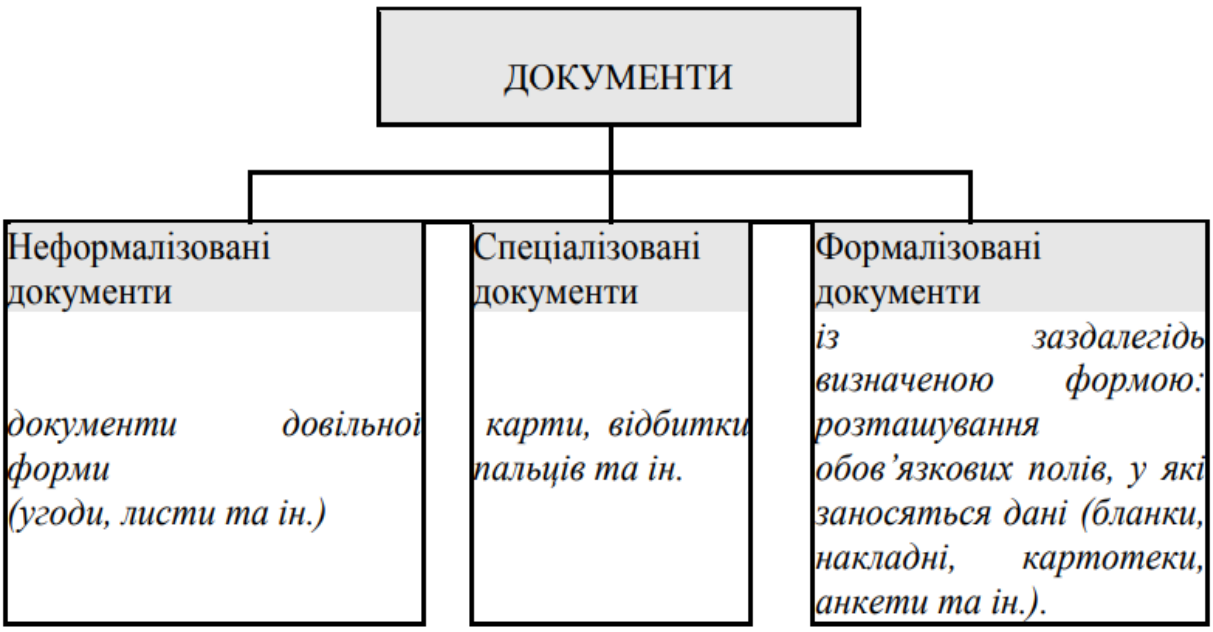


Рис. 1.1 — Класифікація документів з точки зору переведення у електронну форму

Зберігання документа, який був переведений в електронну форму, має свої переваги та недоліки. В Таблиці 1.1 детально описано переваги та недоліки способів зберігання інформації.

Таблиця 1.1

Переваги та недоліки способів зберігання інформації

Спосіб	Переваги	Недоліки
Лише текст	Потребує незначної кількості вільного простору на цифровому носії; Доступний повнотекстовий пошук документа; Можливе повторне використання тексту при підготовці документів у відповідь;	Рукописні документи скануються; Можливе не зовсім точне відтворення зовнішнього виду; Необхідний час на верифікацію документа;
Лише образ	Доступне сканування текстів та документів поганої якості; Економія часу на верифікації;	Неможливе здійснення пошуку по тексту;
Текст та образ	Доступний повнотекстовий пошук; Можливе повторне використання тексту; Доступне сканування всіх типів документів.	Збільшені вимоги до апаратного забезпечення, яке необхідне для зберігання великих обсягів інформації.

Перетворення документів у електронну форму, для кожного з видів - має такі особливості:

– для фотографій - достатньо цифрового зображення без додаткової обробки;

– для текстових документів - необхідно провести розпізнавання тексту та, за потреби, відновити його форматування;

– при введенні анкет, бюлетенів для голосування та ін., як правило, не потрібно зображення власне документа, а достатньо інформації про те, за кого віддано голос.

1.1.2. Формати файлів електронного документу

Електронні документи зберігаються та обробляються в різних форматах файлів, що забезпечують різні можливості для користувачів. Вибір формату файлу залежить від типу документу, вимог до його зберігання, обробки, захисту та доступності.

Отже, можна зробити висновок, що існує велика кількість форматів файлів, які можуть бути використані для створення електронного документу. Тому в 2014 році, було видано наказ: Наказ міністерства юстиції України № 1886/5 від 11.11.2014 (зареєстрований 11 листопада 2014 р. за № 1422/26199), згідно з цим наказом - для тривалого зберігання та розповсюдження документів, рекомендовано формати, що представлено у ДОДАТКУ А.

Формати файлів:

1) В першому пункті у ДОДАТКУ А зазначений формат для зберігання електронних документів, а саме **PDF/A-1** (Portable Document Format/Archival-1) — це стандарт для довгострокового архівного зберігання електронних документів у форматі PDF. Він був розроблений Міжнародною організацією зі стандартизації (ISO) як спеціалізована версія формату PDF, має розширення *.pdf , а також дозволяє зберігати документи таким чином, щоб забезпечити їхню цілісність, читабельність та доступність протягом тривалого часу. Стандарт забезпечує відкриття архівних файлів навіть через тривалий час, накладаючи певні обмеження на складові частини документа для досягнення від-

повідності. Формат зараз широко поширений в багатьох підприємствах. Програми перегляду PDFA/A-1, такі як Adobe Acrobat Reader, гарантують, що файли, збережені в цьому форматі, можна буде відкрити навіть у майбутньому відповідно до інформації, наданої цим стандартом.

Деякі функції PDF 1.4, такі як прозорість або інтеграція аудіо- та відеоконтенту, не допускаються стандартом PDF/A-1. Деякі опції, зазначені в PDF 1.4, є обов'язковими в PDF/A-1: наприклад, усі шрифти, що використовуються, повинні бути вбудовані в документ. По суті, стандарт PDF/A-1 лише конкретно ідентифікує окремі характеристики PDF Reference 1.4 і вказує, чи кожна з них є абсолютно необхідною, рекомендованою, обмеженою або недопустимою.

2) Для фото-електронних документів рекомендується використовувати формат TIFF (Tagged Image File Format) — це один із найбільш розповсюджених форматів для зберігання растрових зображень високої якості. Його розробником є компанія The Aldus and the Microsoft Corporations, він має розширення *.tif . Кольорова модель яку використовує даний формат RGB. Він розроблений для надійного зберігання сканованих документів, зокрема для архівування та обробки графічної інформації, яка потребує збереження всіх деталей. Даний формат широко використовується у сферах, де важливе точне відтворення зображень, таких як сканування документів, фотографія, видавництво та медична візуалізація. Цей формат може описувати дані дворівневих зображень, зображень у відтінках сірого, палітрованих кольорів і повнокольорових зображень у різних колірних просторах. Він підтримує як стиснення з втратами, так і без втрат, дозволяючи обирати між економією простору та швидкістю для програм, що працюють із цим форматом. Формат є незалежним від технічних платформ, операційних систем та файлових систем.

3) Для аудіоданих аудіовізуальних електронних документів рекомендується використовувати формат FLAC — це формат, який широко використовується для збереження високоякісних аудіофайлів без втрат якості. Це означає, що при стисненні аудіоданих у FLAC не втрачаються деталі звуку, які б втрачаються у інших форматах. Він був розроблений некомерційним фондом Xiph.Org Foundation та має розширення *.flac.

FLAC-файли популярні у сфері відтворення аудіо без втрат. У цифровому аудіо, кодек без втрат — це кодек, який не втрачає важливої сигнальної інформації про оригінальну аналогову музику під час стиснення файлу. Багато популярних кодеків використовують алгоритми стиснення з втратами — наприклад, стандарти MP3 та Windows Media Audio, — які втрачають певну автентичність звуку під час рендерингу.

4) Для інкапсуляції даних аудіовізуальних електронних документів рекомендується використовувати формат Matroska — це універсальний контейнерний формат для зберігання мультимедійного контенту, зокрема відео, аудіо, зображень і субтитрів в одному файлі. Він був розроблений як відкритий стандарт і отримав популярність завдяки своїй гнучкості та розширюваності. Формат Matroska часто використовується для зберігання високоякісних відео та аудіо матеріалів, що робить його хорошим варіантом для використання.

5) Для створення відеоданих аудіовізуальних електронних документів рекомендується використовувати стандарт відеокодування MPEG-4 AVC/H.264 — це блочно-орієнтований стандарт стиснення відео, який широко використовується для запису, стиснення і розповсюдження відео з високою якістю. Його назва складається з трьох частин:

- MPEG-4: це стандарт стиснення відео та аудіо, розроблений групою Moving Picture Experts Group. Він включає в себе кілька різних кодеків і стандартів для обробки мультимедіа, і його мета — забезпечити високоякісне стиснення аудіо та відео при зниженні розміру файлів.
- AVC: це інша назва для H.264, яка підкреслює його здатність ефективно стискати відео. AVC використовується в MPEG-4 для досягнення більш високого ступеня стиснення, зберігаючи якість відео. Він забезпечує набагато кращу якість при меншому розмірі файлів порівняно з попередніми стандартами, такими як MPEG-2.
- H.264: це стандарт, розроблений групою фахівців з організації Міжнародної спілки електрозв’язку або ITU. Даний стандарт став одним із найбільш популярних форматів стиснення відео завдяки своїй здатності забезпечувати високу якість зображення за низької пропускної здатності, що робить його популярним для потокового відео, Blu-ray дисків, відеоконференцій та багато іншого [6].

1.2. Визначення електронного документообігу

Електронний документообіг, також відомий як обіг електронних документів – 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 [2].

Основне завдання електронного документообігу полягає у скороченні часу на виконання рутинних операцій, підвищенні точності обробки документів та покращенні контролю за документообігом у рамках організації. З розвитком інформаційних технологій ЕДО поступово замінює традиційний паперовий документообіг, що сприяє збільшенню ефективності управління інформацією в державних установах та бізнесі.

На даний момент ЕДО можна класифікувати за різними критеріями, однак виділяють два основних види:

1) **Внутрішній документообіг** – це обіг документів у межах компанії, тобто передача документів між різними відділами та працівниками однієї організації. Основною метою внутрішнього документообігу є забезпечення точності та оперативності у виконанні задач. За допомогою СЕДО процеси, що стосуються контролю завдань і сповіщення про порушення регламентів, стають автоматизованими, що дозволяє значно зменшити ризик людських помилок і дублювання даних. Такий документообіг також передбачає контроль доступу до конфіденційної інформації та архівування завершених документів, забезпечуючи зручний доступ до них у разі потреби. Окрім цього, автоматизовані системи дозволяють керівництву організації отримувати оперативні звіти про стан виконання завдань і загальну продуктивність підрозділів, що підтримує обґрунтованість управлінських рішень і підвищує загальну ефективність діяльності компанії.

2) **Зовнішній документообіг** – це обмін документами поза межами компанії, який здійснюється з клієнтами, партнерами, державними установами та іншими зовнішніми організаціями. Зовнішній документообіг включає всі процеси обміну докумен-

тами між компанією та її зовнішніми партнерами, з якими вона співпрацює. Він є важливою частиною ділових комунікацій, оскільки забезпечує формалізацію взаємин і гарантує юридичну силу документів, що надсилаються або отримуються. У цьому процесі особливо важливими є стандарти безпеки та надійності, адже документи, що передаються зовнішнім суб'єктам, можуть містити конфіденційну інформацію, фінансові звіти або комерційні пропозиції. Завдяки системам електронного документообігу компанії можуть не лише значно пришвидшити обробку та передавання інформації, але й скоротити обсяги паперової роботи, зменшивши ризики втрати даних. Використання таких систем дозволяє створювати та відстежувати маршрути документів, встановлювати контрольні точки та строки виконання, що забезпечує прозорість та оперативність у взаємодії з зовнішніми партнерами.

Окрім зовнішнього та внутрішнього, ЕДО також класифікують за типами документів [7]:

- **Кадровий ЕДО** спеціалізується на обробці документів, пов'язаних із кадровою діяльністю, таких як трудові договори, особисті справи співробітників, накази про прийняття та звільнення, відпустки, лікарняні та інші довідки. Ця система дозволяє ефективно управляти документацією протягом усього життєвого циклу співробітника в організації, полегшує ведення звітності й облік кадрових змін, знижуючи ризики помилок та підвищуючи безпеку даних.
- **Управлінський документообіг** включає обробку внутрішніх розпоряджень, наказів, протоколів засідань, звітів і планів. Основна мета – забезпечення злагодженої роботи управлінських процесів, контроль за виконанням задач, а також створення умов для швидкої реакції на зміни в операційній діяльності. ЕДО допомагає автоматизувати процеси затвердження й візування таких документів, що знижує час ухвалення рішень.
- **Складський документообіг** зосереджений на документах, пов’язаних з обліком товарів і матеріальних цінностей на складах. Документи, які входять до складського документообігу, включають накладні, акти приймання та передачі, інвентаризаційні документи та звіти про залишки. Завдяки автоматизації обліку й контролю над рухом товарів і матеріалів, компанія може оперативно реагувати на потреби складу, вести точний облік запасів і оптимізувати закупівлі.

- **Бухгалтерський документообіг** орієнтований на бухгалтерські документи, призначений для обробки та збереження фінансових документів, таких як рахунки, платіжні доручення, звіти про доходи та витрати, бухгалтерські книги тощо. Це значно полегшує роботу бухгалтерів, дозволяючи їм ефективно вести звітність, забезпечувати вчасне закриття місяця й кварталу, спрощуючи аудит і податковий контроль. Бухгалтерський ЕДО також підвищує прозорість і достовірність фінансової інформації.
- **Архівний документообіг** спрямований на збереження документів, які вже не використовуються в повсякденній роботі, але підлягають довготривалому зберіганню через юридичні або корпоративні вимоги. Архівні документи можуть включати кадрові справи, звіти минулих періодів, історичні договори та інші важливі записи. ЕДО допомагає централізувати й автоматизувати процеси зберігання архівних документів, забезпечуючи легкий доступ до даних при мінімальних витратах на збереження.

1.3. Переваги ЕДО

Електронний документообіг значно перевершує традиційний, оскільки останній має суттєвий недолік: практично неможливо централізовано відслідковувати рух документів в організації в режимі реального часу. Електронний формат натомість забезпечує низку вагомих переваг, таких як додавання мультимедійних даних до документів, використання готових шаблонів, висока швидкість передачі інформації багатьом адресатам, економія паперу, компактне архівування, швидкий пошук та доступ до інформації, а також захист документів від несанкціонованого доступу і контроль прав доступу співробітників. Запровадження електронного документообігу значно зменшує кількість служб, які займаються обробкою документів. Завдяки електронному документообігу витрати на перебудову документообігу у разі змін зовнішніх умов, таких як нові вимоги до форми звітності, стають набагато меншими.

Кожен документ рухається у своєму власному потоці, його розробка та маршрутизація здійснюються різними користувачами. Спільне середовище лише відображає

зв’язки та дозволяє отримувати інформацію не тільки про технічні характеристики продукту, а й про маркетингові, фінансові та адміністративні документи, що з ним пов’язані.

Дослідження, яке було проведене Матвієнком О. та Цивіним М., вивчало наскільки зменшується час виконання окремих етапів роботи з документами при переході від "паперового" процесу до електронного. Вони проаналізували залежність між витраченим часом на обробку документів та їх документообігом, що відображено у вигляді діаграми на рис. 1.2 [8].

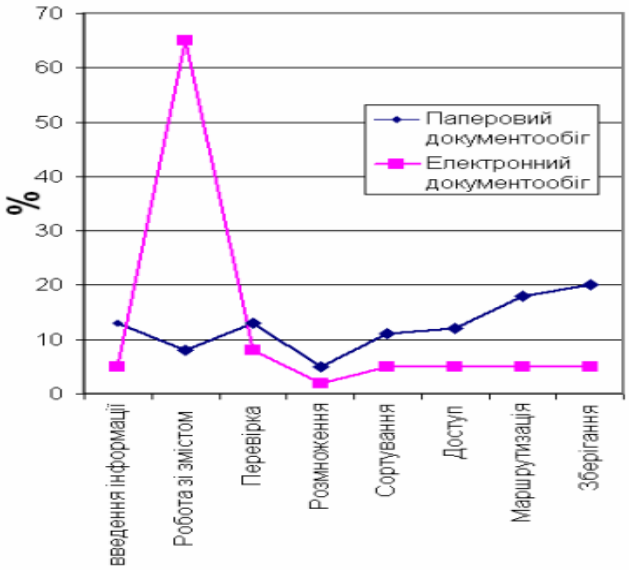


Рис. 1.2 — Переваги електронного документообігу

Проте, поряд із позитивними аспектами електронного документообігу, виділяються і певні його недоліки:

- ускладненість швидкої оцінки значних обсягів інформації та скорочення часу на прийняття рішень;
- потреба в колективному (колегіальному) прийнятті оперативних рішень;
- посилення негативного впливу людського фактору на управлінську якість через ризики, пов'язані зі стресовими ситуаціями, перевтомою та недостатньою швидкістю реагування на зміни зовнішнього середовища.

Однак, попри деякі негативні тенденції, в електронному документообігу виділяються переваги не лише для окремих підприємств, а й для держави загалом, як показано в Таблиці 1.2. [9][10].

Таблиця 1.2

Переваги ЕДО для держави

Мета	Вплив в Україні	Вплив на міжнародному рівні
Політична	Підвищення прозорості різних структур влади, зменшення корупції, розширення політичних зв'язків.	Подолання політичних непорозумінь та глобалізація міжнародних відносин
Економічна	Диверсифікація діяльності підприємств, очікування прибутку від створення нових компаній у цифровому середовищі.	Економічне зростання завдяки розвитку нових послуг та продуктів на основі інформаційних технологій.
Соціальна	Розширення зв'язків, інтеграція культур, популяризація кращих соціальних стандартів.	Перехід до громадянського суспільства, через участь громадян у громадських організаціях та спільнотах.
Правова	Розвиток нормативно-правової бази відповідно до міжнародних стандартів, інтеграція з міжнародним законодавством.	Розширення сфер діяльності завдяки адаптації правових систем до світових стандартів.
Культурна	Збагачення національної культури через міжкультурний обмін.	Взаємне культурне збагачення, обмін традиціями, звичаями, релігією.
Наукова	Скорочення часу на інтеграцію знань для спільних досліджень, випробувань і винаходів.	Міжнародний обмін науковим досвідом, проведення віртуальних семінарів та симпозіумів.
Екологічна	Зменшення витрат на паперові ресурси (за 2,5 роки збережено понад 30т. паперу, що еквівалентно понад 1 тис. дерев).	Захист довкілля, активне використання вторинних ресурсів.

Таким чином, для забезпечення ефективної роботи підприємств та зростання їх конкурентоспроможності в умовах використання інформаційно-комунікаційних технологій, впровадження систем електронного документообігу надає нові можливості в різних сферах: політичній, економічній, соціальній, правовій, культурній, науковій та екологічній.

1.4. Висновки до першого розділу

У першому розділі розглянуто основні аспекти електронного документообігу та його складові. Визначено сутність електронного документа, його особливості, реквізити та типи носіїв. Проаналізовано процес переведення паперових документів у цифровий формат, а також наведено класифікацію форматів файлів для зберігання електронних документів з урахуванням їх характеристик та призначення.

Розділ включає поняття ЕДО, його основні види (внутрішній і зовнішній) та типи (кадровий, управлінський, бухгалтерський, складський, архівний). Деталізовано переваги використання ЕДО, зокрема економію ресурсів, підвищення ефективності роботи, зменшення кількості помилок та швидкість доступу до інформації. Також окреслено певні недоліки, такі як технічні складнощі та вплив людського фактора.

Зазначено, що впровадження ЕДО позитивно впливає на діяльність підприємств, сприяє підвищенню прозорості, покращенню комунікацій і забезпечує довгострокове збереження інформації. Окремо підкреслено екологічну користь від зменшення використання паперу.

Таким чином, впровадження ЕДО є важливим кроком для підвищення ефективності управління інформацією в різних сферах діяльності, що дозволяє вирішувати завдання сучасного суспільства в умовах цифровізації.

РОЗДІЛ 2. ПРОБЛЕМАТИКА СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1. Система електронного документообігу

Система електронного документообігу — це програмне забезпечення, яке дозволяє автоматизувати процес створення, зберігання, обробки, передачі та пошуку документів в електронному форматі. СЕДО інтегрує управління документообігом, забезпечуючи контроль і спрощення процесів обробки документів у рамках організації.

За сучасними мірками, системи електронного документообігу, з'явившись порівняно недавно, вже стали невід'ємною частиною інформаційної структури підприємств. Спочатку їх основним завданням була звичайна автоматизація процесу обігу документів, тобто підтримка роботи діловодів, без заміни паперових потоків документів на підприємстві.

Однак ситуація змінилася, коли розробники СЕДО почали не тільки копіювати існуючі процеси роботи з паперовими документами, але й враховувати завдання, які стоять перед цими процесами та системою документообігу в цілому. Усвідомлення того, що документообіг підприємства має забезпечувати підтримку системи управління, прийшло до СЕДО не відразу.

Якщо подивитися на етапи розвитку систем електронного документообігу в хронологічному порядку, то першим можна назвати період, що почався у 1980-х роках і тривав до кінця XX століття. Цей етап характеризувався розрізненими рішеннями, оскільки підприємства, хоча й усвідомлювали необхідність автоматизації документообігу, ще не мали уніфікованих інструментів для вирішення таких завдань. Окрім того, функціональні можливості ранніх систем ЕДО були обмеженими. Саме тому, функціонал перших систем був обмежений такими можливостями:

- введенням даних у систему та пошуком реєстраційно-контрольних карток;
- веденням журналів обліку вхідних та вихідних документів;
- складанням звітів щодо документообігу для керівництва компанії.

З кінця XX століття підхід до автоматизації документообігу зазнав суттєвих змін, разом із впровадженням концепції управління якістю, з'явився процесний підхід до управління. Інформаційні системи швидко відреагували на ці нововведення, що призвело до появи поняття WorkFlow — робочих потоків, які представляли собою окремі бізнес-процеси, пов'язані з документами. Сучасні СЕДО відповіли на це розробкою процесно-орієнтованих механізмів, що стали новим методологічним етапом, дозволяючи системам ще швидше й ефективніше пристосовуватися до потреб динамічних компаній.

Впровадження WorkFlow дало можливість фахівцям компаній, що використовують системи електронного документообігу, самостійно коригувати автоматизовані процеси для їх оптимального відповідності внутрішнім бізнес-процесам. Це стало значним проривом у розвитку технологій [11].

Всі ці процеси, які почалися з кінця XX, початку XXI століть, сприяли позитивному розвитку ринку інформаційних систем і технологій. Український ринок поповнився новими іноземними інформаційні системи, які були представлені великими міжнародними компаніями, такими як Microsoft і Documentum.

Саме тому, СЕДО сьогодні є необхідною частиною IT-інфраструктури сучасних організацій. Завдяки їм комерційні компанії та промислові підприємства підвищують ефективність роботи, а державні установи використовують ці технології для внутрішнього управління, міжвідомчої взаємодії та роботи з населенням. Сучасні розробники СЕДО орієнтуються на підтримку не лише листування та організаційно-розпорядчих документів, а й інших внутрішніх документів, таких як договори, нормативна, довідкова та проєктна документація, документи з кадрових питань тощо. Також системи електронного документообігу використовуються для вирішення практичних завдань, які потребують обробки електронних документів, зокрема: управління взаємодією з клієнтами, опрацювання звернень громадян, автоматизація роботи сервісних служб, організація документообігу в проєктах тощо. У загальному розумінні, СЕДО – це будь-яка інформаційна система, призначена для забезпечення ефективної роботи з електронними документами.

Технології електронного документообігу використовуються організаціями різного масштабу та галузевої специфіки. Основним користувачем СЕДО традиційно залишається державний сектор.

Основні вимоги до системи електронного документообігу [12]:

- Для забезпечення інформаційного обміну в системі необхідно використовувати корпоративну обчислювальну мережу, яка інтегрує локальні та віддалені системи користувачів. СЕДО повинна мати можливість взаємодії з електронною поштою та автоматизованими системами управління підприємствами. Система має функціонувати в цілодобовому режимі, бути оснащеною засобами моніторингу, діагностики та відображення поточного стану і використання ресурсів.
- СЕД повинна дозволяти змінювати свої параметри, характеристики та адресатів передачі документів відповідно до оновлених правил документообігу підприємства, зокрема норм, регламентів, форматів та порядків.
- Система має будуватися на основі відкритих технологій, що забезпечують можливість її подальшого оновлення без суттєвих змін. Вона повинна підтримувати використання масштабованих апаратних платформ, зокрема просту заміну серверів та пристроїв зберігання інформації на більш продуктивні або місткі.
- СЕД повинна забезпечувати точне розпізнавання документів українською та англійською мовами, а також підтримувати повнотекстову індексацію документів.

2.1.1. Характеристики СЕДО

Система електронного документообігу є комплексом програмного забезпечення, який забезпечує контрольоване створення та управління документами в організації відповідно до встановлених бізнес-процесами правил обробки.

Основні призначення СЕД [12]:

- Підвищення рівня обізнаності керівників і фахівців шляхом збільшення обсягу збереженої інформації, централізованого оброблення даних, зменшення часу на пошук

документів, підготовку звітів і доповідей, а також за рахунок підвищення повноти і точності звітності.

- Зниження витрат на документальне забезпечення управління підприємством завдяки переходу з паперових носіїв на електронні, зменшенню витрат на копіювання та передачу паперових документів.
- Скорочення витрат і часу на пошук документів у архіві через можливість точної електронної адресації, що забезпечує швидкий доступ до необхідних даних, мінімізує ризик втрати документів, дозволяє легко відстежувати місце їх зберігання та надає можливість здійснювати пошук за різними критеріями.
- Інтеграція інформаційних процесів в межах співпраці з іншими підприємствами – забезпечення узгодженого та безпечного обміну даними між організаціями, що дозволяє швидше і ефективніше взаємодіяти в рамках спільних проектів, забезпечує підтримку стандартизованих протоколів передачі даних та автоматичну синхронізацію документів.
- Створення нової інформаційної бази для подальшого вдосконалення процесів документального забезпечення управління та технологій роботи з документами.

СЕДО повинна відповідати існуючій інформаційно-організаційній структурі підприємства або групи підприємств та надавати можливість адаптації відповідно до змін у структурі. Системи електронного документообігу мають широкий спектр функціональних можливостей, що допомагають ефективно управляти документацією, автоматизувати бізнес-процеси та забезпечити безперервний обмін інформацією в організації. Далі будуть розглянуті найважливіші характеристики, що визначають ефективність СЕДО [13].

1. Програмна платформа, на якій побудована система електронного документообігу, є ключовою характеристикою, що визначає гнучкість, надійність і можливості інтеграції СЕДО з іншими корпоративними системами. Вибір платформи залежить від технологічних потреб організації, розміру компанії та специфіки бізнес-процесів. Важливою є можливість масштабування платформи та адаптації під потреби конкретного замовника.

2. СЕДО повинна підтримувати роботу з різними типами документів: текстовими файлами, електронними таблицями, зображеннями, PDF-файлами та ін. Система має забезпечувати обробку як внутрішніх документів (розпорядження, накази), так і зовнішніх (угоди, листування з клієнтами). Таким чином, гнучкість у підтримці різних форматів документів дозволяє організації ефективно управляти інформацією.

3. СЕДО має підтримувати велику кількість користувачів з можливістю гнучкого налаштування рівнів доступу. Важливою характеристикою є можливість створювати різні рівні ієрархії користувачів та обмежувати доступ до документів або дій у системі залежно від ролі співробітника. Це дозволяє захищати конфіденційну інформацію і гарантувати, що доступ до документів мають лише ті співробітники, які це потребують.

4. Також СЕДО повинна мати засоби для визначення маршрутних схем проходження документів, які будуть дозволяти автоматизувати процеси передачі документів між різними підрозділами або співробітниками на основі визначених правил і логіки. Вони дають змогу налаштовувати маршрути для кожного типу документа, створювати послідовні або паралельні етапи обробки, а також контролювати виконання на кожному етапі. Використання цих засобів значно покращує ефективність обробки документів та знижує кількість помилок, пов'язаних з людським фактором.

5. Одна з найважливіших характеристик СЕДО — це забезпечення безпеки інформації. Система повинна мати вбудовані механізми шифрування даних, багаторівневе розмежування доступу і надійні засоби автентифікації користувачів. Важливою функцією є ведення журналів дій користувачів, що дозволяє відстежувати, хто, коли і які зміни вносив у документи. Це допомагає гарантувати безпеку корпоративної інформації і контролювати доступ до конфіденційних даних.

6. Можливості контролю за проходженням документів – ці функції забезпечують моніторинг і відстеження всіх етапів обробки документа. Система дозволяє бачити, хто відповідає за виконання завдання на кожному етапі, і контролювати статус його виконання в реальному часі. Це дозволяє швидко виявляти затримки чи порушення в процесі та оперативно реагувати на них, що забезпечує своєчасне завершення кожного етапу та уникнення затримок.

7. Для забезпечення високого рівня безпеки документів важливо, щоб СЕДО підтримувала сучасні методи криптографічного захисту даних. Це дозволяє захищати документи від несанкціонованого доступу або втрати даних у процесі обміну або зберігання.

8. Також, СЕДО повинна містити певні засоби, для повідомлення про порушення у регламенті проходження документів, для того щоб автоматично сповіщати відповідальних осіб про будь-які порушення у регламенті, наприклад, затримки або несанкціоновані дії з документами. Повідомлення можуть надходити через електронну пошту, внутрішні повідомлення в системі або мобільні додатки, залежно від налаштувань організації. Це забезпечує миттєву реакцію та швидке усунення проблем.

9. Однією з важливих функцій СЕДО є можливість ведення кількох версій одного й того ж документа. Це дозволяє зберігати історію змін, здійснених в документі, і при необхідності повертатися до попередніх версій для відстеження процесу редагування або вирішення конфліктних ситуацій.

10. СЕДО забезпечує можливість колективної роботи над документами, що важливо для організацій, де процеси вимагають участі кількох співробітників одночасно. Система надає інструменти для паралельного редагування, коментування і обговорення документів, що підвищує продуктивність роботи команди, а також зменшує час, який витрачається на узгодження, та внесення коректив.

Об'єктом автоматизації є такі процеси:

- створення документів;
- підготовка, облік, систематизація, архівне зберігання, пошук і отримання організаційно-розпорядчих, звітно-статистичних, облікових, планових, інформаційно-довідкових та інших управлінських документів;
- робота з документами, яка включає передачу, облік і контроль виконання тощо.

У сучасних умовах впровадження інформаційних технологій відбувається трансформація основної парадигми управлінського документообігу. Раніше його сприймали як одну з ключових функцій діловодства, спрямовану на організацію роботи з документами всередині установи. Натомість зараз управлінський документообіг розглядається

як контрольована документальна комунікація, яка реалізується з використанням сучасних інформаційних технологій як у внутрішніх процесах організації, так і у взаємодії із зовнішніми суб'єктами. Учасниками електронного документообігу стають всі підрозділи та посадові особи організації, які залучені до документованих управлінських процесів.

На рис. 2.1 схематично представлені функції системи електронного документообігу в організації та підприємствах.

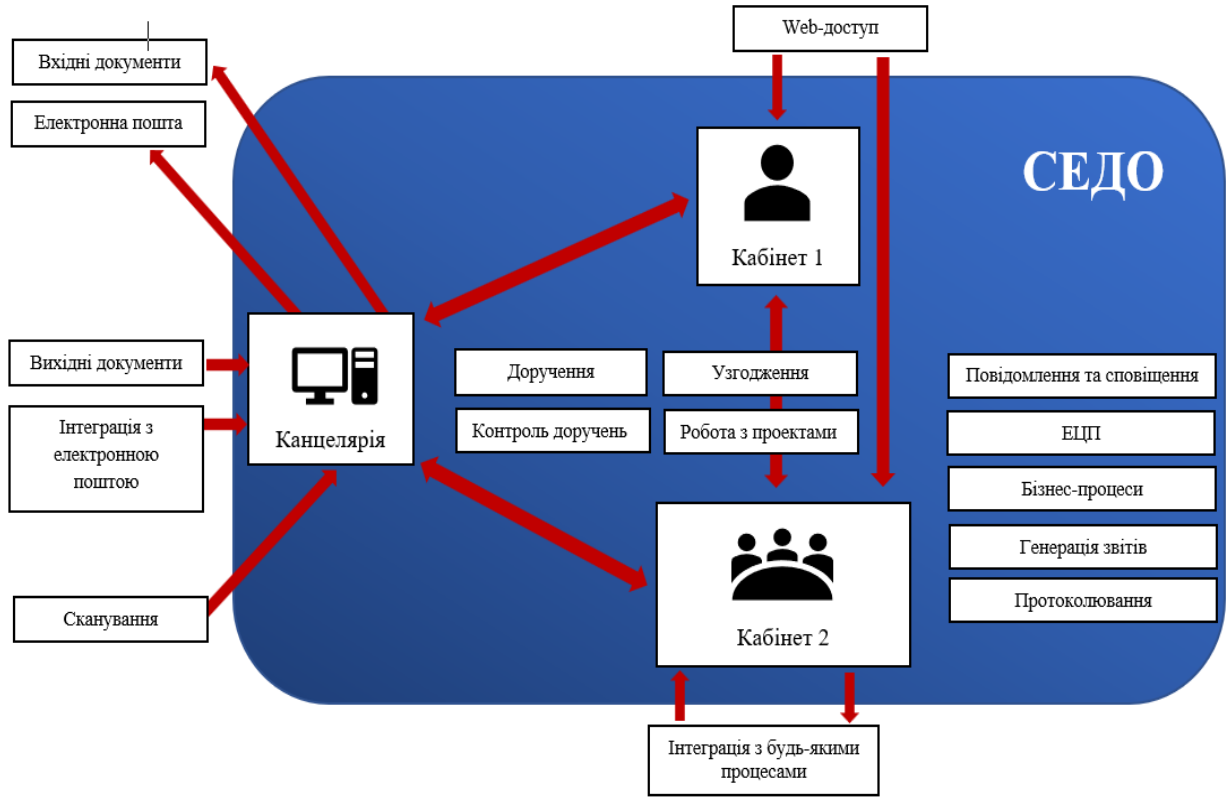


Рис. 2.1 — СЕДО в організації

Загалом, в умовах цифровізації суспільства, впровадження інструментів діджиталізації в різні сфери підприємницької діяльності є невідворотним. Обліковий процес, який слугує інформаційною базою для своєчасної підготовки управлінських рішень та є інструментом оперативного реагування на зміни навколишнього середовища, виступає активним учасником цих процесів.

Для обліку та контролю доцільно використовувати визначення, наведені в нормативних документах. Відповідно до ст. 9 Закону України «Про електронні документи

та електронний документообіг», електронний документообіг варто розглядати як «сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та, за потреби, з підтвердженням факту одержання таких документів» [2].

В аспекті організації документообігу поняття «процедура» практично повністю відповідає поняттю «процес», маючи на увазі процес, пов'язаний з документами. Підтримуючі процеси документообігу призначені для забезпечення функцій підтримки документообігу, подібно до того, як сам документообіг забезпечує підтримку окремих управлінських процесів та організаційної взаємодії [14].

У Таблиці 2.1 наведено порівняння основних принципів документообігу на підприємстві при використанні традиційного підходу до управління документами та електронного документообігу.

Таблиця 2.1

Порівняння принципів традиційного та паперового документообігу

Продовження таблиці 2.1

Принципи традиційного паперового документообігу	Принципи електронного документообігу
Поняття документообігу зводиться до руху документів в межах конкретної організації	Поняття електронного документообігу включає як внутрішній, так і зовнішній документообіг
Поділ технічних і змістовних операцій при роботі з документами, їх відокремлення в процесі роботи	Стирання меж між технічними та змістовними операціями при створенні документів і їх обробці за допомогою сучасних інформаційних технологій
Більшість формальних і технічних операцій із документами виконується службою діловодства, змістовна частина обробляється в інших підрозділах	Співробітники організації, включаючи фахівців і керівників, стають учасниками електронного документообігу у ділових і управлінських процесах

Вимоги до систем електронного документообігу включають [15]:

- забезпечення ефективного управління через автоматичний контроль виконання завдань та прозорість діяльності організації на всіх рівнях;

- підтримку системи контролю якості, яка відповідає міжнародним стандартам;

Скорочення кількості зворотних переміщень документів в організації	Оптимізація ділових і управлінських процесів завдяки маршрутизації документів з використанням корпоративних інформаційних технологій, що дає можливість спільної роботи над документом
Відмова від реєстрації більшості внутрішніх документів	Реєстрація в СЕДО усіх основних типів документів організації, зокрема внутрішніх, а також облік проектів і процедур електронного погодження
Єдина реєстрація документів в організації	Єдина реєстрація документів у СЕДО, у тому числі для підвідомчих організацій або інших учасників, що діють в рамках корпоративних угод
Централізована реєстрація, прийом і відправка документів	Ведення єдиної бази для реєстрації вхідних, вихідних і внутрішніх документів з можливістю децентралізації їх прийому, реєстрації та відправки
Служба діловодства виконує технічні функції та обслуговує керівництво й інші підрозділи	Документаційна служба забезпечує організацію управління документацією та документообігом в організації, зосереджуючись на завданнях, що потребують централізації

- ефективне накопичення, управління та доступ до інформації та знань;
- забезпечення кадрової гнучкості шляхом більшої формалізації діяльності кожного співробітника та зберігання всієї історії його діяльності;
- протоколювання загальної діяльності підприємства, що включає внутрішні розслідування, аналіз діяльності підрозділів;
- оптимізацію бізнес-процесів і автоматизацію їх виконання та контролю;
- усунення паперових документів із внутрішнього обігу компанії, що дозволяє економити ресурси за рахунок зменшення витрат на управління потоками документів;

2.1.2. Функціональні особливості СЕДО

Функціональні особливості СЕДО є критично важливими для ефективного управління інформацією в організації. Вони забезпечують автоматизацію процесів реєстрації, контролю та маршрутизації документів, що сприяє скороченню часу на їх обробку та підвищенню точності виконання завдань. Крім того, такі системи полегшують колективну роботу з документами, дозволяючи швидкий доступ до інформації для всіх

учасників процесу. В Таблиці 2.2 перелічено всі основні функції сучасних систем електронного документообігу [7].

Таблиця 2.2

Функціональні можливості СЕДО

Функції	Особливості
Реєстрація документів	– Реєстрація та облік документів. – Ведення журналів реєстрації та обліку. – Управління номенклатурою справ.
Контроль виконання	– Управління контрольними завданнями. – Перенесення термінів виконання. – Відстеження статусу виконання завдань. – Зняття завдань з контролю на основі звітів. – Визначення результатів виконання. – Підтримка як централізованих, так і децентралізованих завдань.
Маршрутизація об'єктів документообігу	– Управління реєстраційними картками. – Контрольними картками. – Електронними версіями документів. – Звітами щодо виконання контрольних завдань.
Пошук	– Пошук об'єктів документообігу за атрибутами. – Повнотекстовий пошук документів.
Звітність	– Ведення журналів реєстрації та обліку. – Ведення контрольних карток. – Аналіз виконання завдань. Генерація аналітичних і статистичних довідок.
Адміністрування	– Розмежування доступу і прав користувачів. – Управління технічними процесами.

Системи електронного документообігу в першу чергу використовуються великими та середніми компаніями, які потребують ефективних інструментів для роботи з великим обсягом документів. Для малих підприємств і приватних підприємців фінансові та організаційні переваги можуть не виправдати початкові витрати на придбання та впровадження таких систем. Проте наразі існує низка доступних рішень, що орієнтовані на малий і мікробізнес, які роблять впровадження СЕДО більш доступним для цих категорій.

2.1.3. Система WorkFlow

Системи WorkFlow стали ключовим компонентом сучасних СЕДО відіграючи важливу роль в автоматизації процесів обробки, передавання та контролю документів на підприємстві. Впровадження технології WorkFlow дозволяє суттєво підвищити ефективність управління інформаційними потоками, забезпечуючи підприємствам можливість оптимізувати бізнес-процеси та швидко адаптуватися до змін в організаційній структурі та зовнішніх умовах.

WorkFlow — це технологія управління потоками робіт, яка забезпечує автоматизацію бізнес-процесів через передачу завдань, документів і інформації між учасниками процесу. Основна ідея полягає в тому, щоб стандартизувати та автоматизувати послідовність операцій, завдяки чому зменшується час на виконання задач і підвищується контроль за їхнім виконанням [16].

Системи з розвинутими можливостями WF дозволяють автоматизувати управління робочими потоками. Ось кілька визначень WF:

- Завдання, що виконується одним або кількома членами робочої групи, послідовно або паралельно, з метою досягнення спільного результату.
- Автоматизація бізнес-процесу в повному обсязі або частково, за якої документи, інформація чи завдання передаються між учасниками для виконання узгоджених дій.
- Координація людей, інформаційних потоків, об’єктів та подій для забезпечення виконання послідовних операцій і досягнення визначених цілей.

Усі ці визначення об'єднують бізнес-процеси, інформацію і персонал. Технологія WF включає:

- Автоматизація передачі документів: Система автоматично передає документи між співробітниками відповідно до заданого маршруту, що суттєво знижує ймовірність помилок і затримок, пов’язаних із людським фактором.

- Контроль виконання завдань: Кожен етап роботи з документом супроводжується контролем виконання. Система автоматично відстежує статус завдань, повідомляє про затримки чи порушення регламенту, а також надає можливість керівникам отримувати звіти про стан виконання процесів.
- Управління завданнями: Система WF дозволяє чітко розподілити відповідальність між учасниками процесу. Всі завдання та відповідні до них операції автоматично призначаються виконавцям, що дозволяє керівникам зосередитися на стратегічних завданнях.
- Моделювання бізнес-процесів: WF дає можливість створювати та моделювати нові процеси в рамках організаційних змін або розширення функціональних завдань. Це важливо для гнучкого реагування на зміни ринку та потреб підприємства.

Основні поняття технології WF [17]:

- об'єкт — елемент, який використовується в бізнес-процесі (наприклад, документ або креслення);
- подія — дія, яка здійснюється над об'єктом (наприклад, підписання документа);
- операція — конкретна дія в межах бізнес-процесу (наприклад, перевірка документа або внесення змін);
- виконавець — посадова особа, відповідальна за виконання операції.

Кожна система класу WF вирішує три основні завдання:

- опис бізнес-процесу;
- управління його виконанням;
- моніторинг процесу.

Управління виконанням потоку робіт включає:

- перевірку умов переходу між операціями;
- передавання документів між виконавцями;
- інформування користувачів про необхідні дії.

2.2. Хмарні технології в СЕДО

Впровадження автоматизованих систем управління дозволяє підвищити ефективність і прибутковість роботи підприємства. Сучасні керівники розуміють важливість впровадження нових інформаційних технологій та активно інвестують у розвиток IT-відділів. Крім того, необхідність взаємодії з контролюючими та державними органами на різних рівнях також стимулює впровадження електронних систем документообігу, оскільки ці структури вже давно переходять на електронні системи в рамках цільових програм.

Компанії, що займаються впровадженням СЕД, підключають до систем як окремих співробітників, так і філії разом із дочірніми підрозділами, розташованими в різних регіонах країни. Перспективним рішенням у цьому контексті є використання хмарних технологій.

Хмарні технології представляють собою інфраструктуру та сервіси, які дозволяють обробляти і керувати даними через Інтернет за допомогою віддалених серверів. Іншими словами, вся інформація зберігається у "хмарі", а не на пристроях кінцевих користувачів.

Сучасні хмарні технології забезпечують легкий та швидкий доступ до комп'ютерних ресурсів, таких як обчислювальні потужності чи сховища даних, без потреби мати фізичні сервери на місці. Вони пропонують справді гнучкі та масштабовані рішення як для звичайних користувачів, так і для бізнесу [18].

Щодо СЕД, це означає, що для використання системи не потрібно закуповувати дороге обладнання, здійснювати складні установки або відправляти співробітників на навчання. Достатньо зареєструватися на сайті, щоб отримати доступ до всіх функцій. Користувач платить лише за фактично використані ресурси та може зайти в систему з будь-якого пристрою, будь то комп’ютер, планшет чи смартфон, у будь-який час і в будь-якому місці.

Хмарний документообіг — це система управління електронними документами, яка функціонує через хмарні сервіси. Такий підхід дозволяє користувачам зберігати, обробляти та обмінюватися документами в Інтернеті без необхідності мати фізичне

сховище або потужне обладнання на місці. Також він дозволяє уникнути покупки програмного забезпечення, надаючи можливість тимчасового використання лише за потреби, з оплатою виключно за фактичний час роботи з ресурсом. Таким чином, будь-який співробітник компанії з доступом до Інтернету може зі свого комп'ютера, ноутбука чи планшета працювати з електронними документами: створювати, редагувати, погоджувати та затверджувати їх у будь-який час, незалежно від свого місця перебування.

Аналіз моделей хмарних послуг з точки зору безпеки. Існуючі моделі хмарних сервісів [19]:

- Cloud Software as a Service. Користувачу надається доступ до програмних рішень провайдера, які працюють на хмарній інфраструктурі та доступні з будь-якого пристрою через веб-інтерфейс або спеціальні додатки. Основна його перевага — можливість працювати з програмами без необхідності керування інфраструктурою. Недоліком є відсутність контролю над хмарною структурою, хоча користувач може мати доступ до певних параметрів кофігурації.

- Cloud Platform as a Service. Користувач може розгортати власні додатки, використовуючи інструменти, що підтримуються провайдером, на хмарній інфраструктурі. Ця модель забезпечує більший контроль над процесом обробки даних, але вимагає від користувача відповідальності за розробку й обслуговування додатків, що може спричинити додаткові витрати.

- Cloud Infrastructure as a Service. Користувачу надаються обчислювальні ресурси для розгортання і управління власними програмами, операційними системами та іншими компонентами.

Хоча користувач не має доступу до управління всією хмарною інфраструктурою, він контролює операційні системи, зберігання даних і деякі мережеві елементи. IaaS забезпечує найбільший рівень безпеки завдяки широкому контролю над ресурсами, але потребує більших фінансових вкладень на впровадження.

Аналіз моделей розгортання хмар з точки зору безпеки [20]:

- Private cloud**.** Призначена для використання однією організацією, така хмара управляється самою організацією або третьою стороною. Інфраструктура може бути розміщена локально на території організації (on-premise) або у зовнішнього провайдера (off-premise).
- Community cloud**.** Створена для кількох організацій із загальними цілями та вимогами до безпеки, спільна хмара підтримує спільноту користувачів з однаковими інтересами або регуляторними вимогами. Керувати такою хмарою можуть як самі організації, так і зовнішній постачальник, при цьому вона може існувати як на базі клієнта, так і поза його територією.
- Public cloud. Ця хмара призначена для широкого кола споживачів і знаходиться під управлінням організації, що надає хмарні послуги. Споживачі можуть бути з різних галузей або працювати в одній індустрії, що може включати специфічні для галузі застосування. Публічна хмара найкраще виявляє всі переваги хмарних технологій, але часто вважається менш безпечною.
- Hybrid cloud. Це комбінація двох і більше типів хмар (приватних, спільних або публічних), що об’єднані для забезпечення сумісності даних та програм. Вони залишаються окремими сутностями, але завдяки технологіям перенесення даних і балансування навантаження можуть працювати разом.

Очевидними перевагами хмарного документообігу є значна економія коштів на придбання, встановлення та обслуговування програмного забезпечення, а також на створення і підтримку IT-інфраструктури. Гнучкість і масштабованість таких рішень забезпечують можливість підключення до системи необмеженої кількості користувачів у будь-який момент часу і з будь-якої географічної точки, що особливо важливо в умовах підвищеної мобільності сучасного бізнесу. Для компаній зі складною структурою, наприклад, із численними філіями або дочірніми підприємствами, хмарний документообіг дозволяє уніфікувати процеси завдяки використанню єдиної версії програмного забезпечення.

Попри численні переваги, існують і певні недоліки. Найбільша загроза пов’язана з передачею конфіденційної інформації третім особам, а також із можливими технічними збоями, наприклад, через форс-мажорні обставини, що можуть тимчасово зупинити роботу сервісу.

Хмарні технології стрімко набирають популярності. За оцінками аналітиків, використання моделі Software as a Service для управління документами дозволяє скоротити витрати на інфраструктуру та її обслуговування на понад 50% у порівнянні з традиційними підходами. У найближчі роки попит на хмарні рішення зростатиме, особливо серед малого та середнього бізнесу.

Хмарні сервіси вигідні всім учасникам. Масове використання дозволяє провайдерам встановлювати доступні ціни на дорогі ресурси, забезпечуючи їхню високу завантаженість і швидку окупність. Користувачі ж отримують доступ до якісних технологій за помірну ціну. Крім того, відповідальність за безпеку та збереження даних покладається на провайдера.

Перехід на хмарний документообіг має такі переваги:

- Відсутність потреби у власній інфраструктурі — немає необхідності купувати серверне обладнання, встановлювати ПЗ та інвестувати в IT-інфраструктуру.
- Масштабованість — за зростання обсягів даних можна швидко орендувати додаткові ресурси в хмарі.
- Доступність — співробітники мають цілодобовий доступ до документів, а резервне копіювання та технічна підтримка гарантують швидке відновлення інформації у разі потреби.

Сучасні хмарні дата-центри забезпечують рівень безпеки, який часто перевищує захист локальних систем. Проте існують певні ризики ризики:

- Можливість витоку конфіденційної інформації через недосконаліть механізмів захисту або людський фактор;
- Загрози втрати даних унаслідок технічних збоїв чи кібератак;
- Залежність від стабільності інтернет-з’єднання та надійності провайдера.

Важливим є також питання відповідності законодавчим нормам та регулюванням, особливо при роботі з персональними даними.

Одним із популярних безкоштовних сервісів для управління документами є Google Docs — онлайн-офісний пакет від компанії Google. Він включає текстовий і табличний процесори, інструмент для створення презентацій, а також хмарний сервіс для зберігання файлів із функціями спільного доступу. Сервіс доступний з будь-якого пристрою — комп'ютера, ноутбука, планшета чи смартфона, і навіть підтримує офлайн-режим.

Google Docs тісно інтегрований із Google Диском, де зберігаються всі створені, завантажені та відредаговані файли. Для зручності можна встановити програму синхронізації на пристрої, що спрощує процес завантаження та обміну документами.

Основні переваги Google Docs:

1) Миттєва публікація даних в інтернеті — з можливістю приховати їх або зробити публічними.

2) Інструменти для створення вебформ з подальшою інтеграцією на сайти та збором статистики.

3) Спільне редагування документів кількома користувачами одночасно за посиланням чи через запрошення.

4) Коментування виділених фрагментів тексту.

5) Автоматичне збереження всіх змін.

6) Синхронізація з локальними файлами через Google Drive.

7) Колективна робота над одним документом у реальному часі.

8) Швидке передавання великих файлів через інтернет.

9) Створення трьох типів файлів: текстові документи (аналог Word), електронні таблиці (аналог Excel), презентації (аналог PowerPoint).

10) Доступ із будь-якої точки світу за наявності інтернету.

Google Docs забезпечує гнучкий і зручний спосіб спільної роботи, що робить його особливо популярним серед команд і віддалених працівників.

2.3 Класифікація СЕДО

Використання систем електронного документообігу значно підвищує продуктивність праці персоналу, оптимізує організаційно-розпорядчу діяльність і сприяє покращенню бізнес-процесів. Основою такого документообігу є електронний документ, який створюється за допомогою комп'ютерних технологій та зберігається у вигляді файлу певного формату на електронних носіях.

В даний час існує широкий вибір рішень і продуктів від різних розробників, впровадження яких сприяє спрощенню доступу до даних. Вони дозволяють створити централізоване та впорядковане зберігання документів в електронному архіві, скоротити час пошуку й доступу до інформації, підвищити рівень безпеки, а також забезпечити цілісність і збереженість даних. Окрім цього, такі системи значно оптимізують процес узгодження документів, зменшуючи витрати часу на їх опрацювання.

Найбільшим попитом в СЕДО є наступні функції:

1) Зберігання та пошук документів.

2) Підтримка діловодства.

3) Маршрутизація та контроль виконання: створення маршрутів для документів, автоматичний контроль термінів, повідомлення про нові документи.

4) Створення звітів: поточна зайнятість, статус виконання завдань, прострочені доручення.

5) Забезпечення інформаційної безпеки: автентифікація, підтримка електронного підпису, шифрування, аудит роботи в системі.

Деякі СЕДО можуть інтегруватися з іншими системами, розширюючи можливості управління даними.

З точки зору апаратного та програмного забезпечення, СЕДО включає в собі сервери, робочі станції, програмні модулі, мережеве обладнання та додаткові пристрої [13].

Сервери обробляють інформацію та виконують операції з документами. Вони можуть бути як фізичними, так і віртуальними, залежно від постачальника.

Робочі станції забезпечують взаємодію користувачів із системою, виконуючи функції управління документами.

Програмне забезпечення виконує ключові операції з управління документацією та є фундаментом системи електронного документообігу. Воно зазвичай складається з трьох основних компонентів: функціонального модуля, адміністративного модуля та користувацького інтерфейсу. Функціональний модуль відповідає за управління та обробку інформації. Адміністративний модуль забезпечує налаштування системи відповідно до потреб організації. Користувацький інтерфейс представляє дані в зручному та зрозумілому вигляді для кінцевих користувачів.

Додаткове обладнання може включати пристрої для введення та шифрування даних.

Мережеве обладнання необхідне для спільної роботи користувачів і взаємодії компонентів СЕД.

Такі системи дозволяють компаніям ефективно управляти своїми документами, забезпечуючи високу якість і безпеку бізнес-процесів.

На практиці обмін електронними документами здійснюється двома основними способами:

- **Прямий обмін**. Якщо у сторін є офіційно зареєстрований електронний підпис, документи можна надсилати через звичайну електронну пошту. У разі відсутності кваліфікованого підпису перед початком співпраці необхідно укласти попередню угоду, в якій детально описуються всі умови та порядок обміну інформацією.
- **Обмін через оператора**. Для передачі особливо важливих документів використовуються послуги спеціалізованих операторів. Вони забезпечують високий рівень технічного захисту і юридичну підтримку для збереження конфіденційності. У цьому випадку наявність попередньо зареєстрованого електронного підпису є обов’язковою умовою.

Обидва способи мають свої переваги й недоліки. Прямий обмін є швидким і зручним, проте може бути менш безпечним, особливо у разі недостатнього рівня технічного захисту. Обмін через посередника забезпечує високу надійність і відповідність вимогам законодавства, але може бути дорожчим і складнішим в інтеграції.

З погляду функціональності, система електронного документообігу складається з модулів, які виконують такі завдання: введення даних, індексація, обробка документів, управління доступом, маршрутизація, системна інтеграція та зберігання [11].

- **Модуль введення даних**. Він дозволяє вводити початкову інформацію в систему з різних джерел: сканованих паперових документів, електронної пошти, онлайн-форм тощо. Цей модуль забезпечує первинну обробку отриманих даних.
- **Модуль індексації**. Відповідає за реєстрацію та систематизацію даних. Завдяки цьому модулю СЕДО дозволяє структурувати документи та організувати швидкий пошук відповідно до потреб користувачів.
- **Модуль обробки документів**. Після введення дані проходять обробку та розподіл за заданими правилами. Це забезпечує подальшу роботу з документами, включаючи їх збереження у системі.
- **Модуль управління доступом**. Дає можливість розподіляти доступ до документів між користувачами. Кожен користувач отримує доступ лише до тих документів, які необхідні для його роботи.
- **Модуль маршрутизації**. Організовує процеси руху документів у системі. Цей модуль встановлює правила передачі та обробки документів на основі попередньо визначених бізнес-процесів.
- **Модуль системної інтеграції**. Забезпечує взаємодію СЕДО з іншими інформаційними системами, такими як CRM, ERP або OLAP. Це дозволяє обмінюватися даними між платформами даного типу.
- **Модуль зберігання документів**. Реалізує функції архівування, резервного копіювання, відновлення та зберігання документів у базі даних, що забезпечує довготривале збереження інформації та її доступність.

Кожен документ в СЕДО має свій набір характеристик, таких як назва, автор, дата створення та інші. Ці атрибути можуть змінюватися залежно від типу документа, проте залишаються сталими для документів одного типу. Усі атрибути зберігаються в реляційній базі даних. Для кожного типу документів у СЕДО створюється шаблон картки, який у зручному графічному форматі відображає назви відповідних атрибутів. Під час

введення документа в систему вибирається відповідний шаблон, після чого користувач заповнює картку, вносячи значення атрибутів. На рис. 2.2 зображено функціональну архітектуру типової СЕДО.

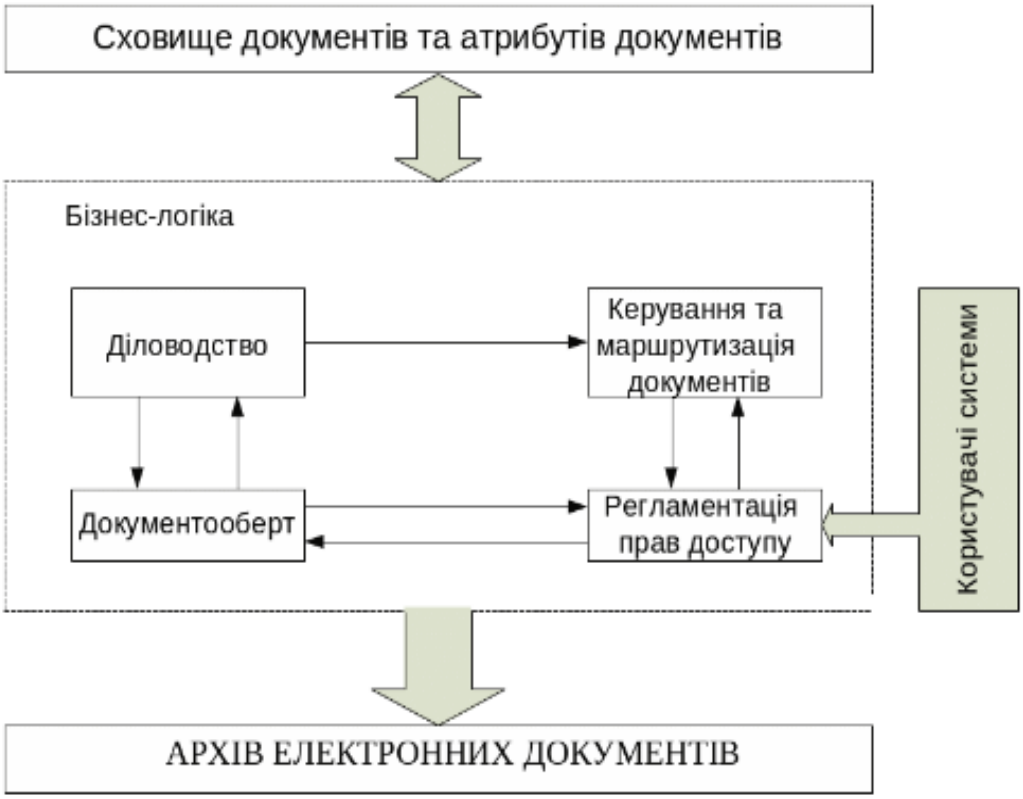


Рис. 2.2 — Функціональна архітектура СЕДО

2.3.1. Види систем електронного документообігу

Системи електронного документообігу відрізняються за використовуваними технологіями, рівнем інтеграції та сферою застосування.

За типом технологій можна виділити чотири основні категорії:

- **Клієнт-серверні системи.** Основні модулі розміщуються на сервері, а користувачі взаємодіють із системою через клієнтський інтерфейс. Переваги таких систем – висока швидкість роботи та надійність.
- **Системи на основі баз даних.** Вони інтегруються з базами типу SQL чи Oracle, де зберігається вся інформація. Обробка даних виконується через окремі модулі. Головна перевага – здатність зберігати великі обсяги даних.

- **Системи на основі веб-технологій.** Функціонують через віддалений доступ до сервера, що дозволяє відмовитися від клієнтських додатків. Доступ до документів здійснюється через веб-браузери.
- **Системи на основі хмарних технологій.** Вони схожі на веб-системи, але сервери розміщуються у провайдера хмарних послуг. Це забезпечує гнучкість і масштабованість.

За рівнем інтеграції СЕДО поділяють на:

- **Універсальні системи документообігу** (Electronic Document Management Systems**)** Це автономні рішення, призначені для повної автоматизації управління документацією. Зазвичай вони працюють за клієнт-серверною архітектурою.
- **Системи управління груповою роботою.** Орієнтовані на спільне опрацювання документів користувачами. Їх функціонал обмежений порівняно з EDMS.
- **Інтегровані модулі в управлінських системах.** Є частиною ERP-систем, мають обмежений функціонал і працюють лише в межах базової ERP-інфраструктури.

Ще одним критерієм класифікації систем електронного документообігу є сфера їх застосування. Існують СЕДО, спеціально розроблені для роботи з певними типами документації або для використання в окремих галузях. Наприклад, це можуть бути PDM-системи для управління проєктною документацією, платформи для підтримки розробки програмного забезпечення, системи типу HelpDesk, а також рішення для обробки медичної документації тощо.

Будь-яка класифікація є умовною, оскільки вона може базуватися на різних критеріях і принципах. Системи електронного документообігу можна розрізняти за функціональністю, масштабами підприємств, архітектурою тощо.

Залежно від функцій і завдань, які вирішують ці системи, традиційно виділяють такі їх види [21]:

1. Системи діловодства. Ці рішення застосовуються в організаціях із чітко регламентованими процесами документообігу та вертикальною структурою управління, незалежно від їх розміру чи сфери діяльності. Вони допомагають виконувати такі завдання:

Організувати обробку вхідної та вихідної кореспонденції.

- Оптимізувати внутрішній документообіг компанії.
- Ефективно працювати зі зверненнями клієнтів.
- Створити внутрішній електронний архів документів.

Фактично ці системи є цифровими наступниками традиційного паперового діловодства.

2. Електронні архіви. Призначені для структурованого зберігання документів з акцентом на безпеку, обмеження доступу, швидкий і зручний пошук. Їх впровадження доцільне для впорядкування різноманітної електронної інформації, будь то текстові файли, графічні зображення чи мультимедійні дані. Основні функції:

- Оцифрування паперових документів.
- Управління веб-контентом.
- Швидке введення даних і пошук.

Завдяки цим архівам зменшується час доступу до інформації, знижуються ризики втрати або пошкодження документів, підвищується рівень інформаційної безпеки.

3. Workflow-системи. Вони автоматизують не окремі функції, а повноцінні бізнес-процеси. Назва «Workflow» перекладається як «потік робіт». Ці системи чітко визначають, хто, коли і як повинен виконати ту чи іншу задачу.

- Користувачу не потрібно думати, як створити або відправити документ — усі дії регламентовані.
- Система контролює строки виконання завдань, нагадує про них і повідомляє керівника про затримки чи помилки.
- Workflow-системи ефективні для компаній із формалізованими процесами та великими обсягами документів.

Головний недолік — складність і тривалість впровадження. Крім того, вони зберігають лише ті документи, які беруть участь у бізнес-процесах, і не можуть повноцінно замінити електронні архіви.

4. ECM-системи. Ці платформи забезпечують збір, управління, зберігання інформації (контенту) та доступ до неї. На перший погляд, вони виконують ті ж функції, що й інші системи, але мають ключові відмінності:

- Працюють як зі структурованою, так і з неструктурованою інформацією.
- Забезпечують більшу гнучкість у роботі з контентом.

ECM-системи поєднують функції електронного документообігу, управління файлами й записами, знаннями, Workflow, а також управління веб-контентом. У деяких рішеннях доступні навіть CRM-функції та управління завданнями й дорученнями.

Загалом, одними з найпопулярніших СЕДО в Україні є наступні ситеми [22]:

1) Сервіс «Paperless» є зручним рішенням для компаній та підприємців, які здійснюють обмін документами в електронному форматі. Сервіс працює з кваліфікованим електронним підписом, який підтримується усіма акредитованими центрами сертифікації ключів України, включаючи ключі, видані державними структурами, такими як Державна фіскальна служба та Міністерство юстиції. Для використання сервісу не потрібно встановлювати додаткове програмне забезпечення: достатньо зареєструватися та встановити браузерний додаток.

Документи у «Paperless» зберігаються в трьох копіях на незалежних серверах, що забезпечує надійний захист даних від втрати чи пошкодження. Для додаткової безпеки користувачі мають можливість завантажувати копії документів на локальні пристрої. У найближчих оновленнях заплановано інтеграцію з популярними хмарними сервісами, такими як Dropbox та Google Drive, що дозволить автоматично синхронізувати документи між платформами.

2) Сервіс «Document.Online» на відміну від «Paperless», «Document.Online» є умовно безкоштовним сервісом. Користувачам надається базовий тариф з обмеженням на кількість документів, що обробляються щомісяця. Сервіс підтримує завантаження, створення та використання шаблонів, а також обмін документами з можливістю надсилання їх кільком отримувачам одночасно. «Document.Online» сумісний з усіма акредитованими центрами сертифікації ключів України та може працювати на будь-якому пристрої з доступом до Інтернету, незалежно від операційної системи.

Документи зберігаються на хмарних серверах Microsoft Azure, що забезпечує високу надійність та доступність даних на рівні 99,98%. Це означає, що можливі лише короткочасні перебої у доступі до інформації (не більше п’яти хвилин на місяць). Завдяки автоматичному резервуванню та багаторівневому дублюванню даних, навіть у випадку виходу з ладу одного із серверів або фізичного пошкодження обладнання, інформація буде відновлена протягом години.

3) «ІІТ Користувач ЦСК-1» створений для роботи з електронним підписом і надає частковий функціонал для електронного документообігу. Її основна особливість полягає у спеціалізації на роботі з криптографічним захистом інформації та кваліфікованими електронними підписами.

Функціонал програми включає:

- накладання електронного підпису або печатки на файли різних форматів, включно з текстовими документами, аудіо- та відеофайлами, а також захист інформації шляхом шифрування;
- створення ключів для кваліфікованого електронного підпису, їх резервне копіювання та безпечне знищення;
- перевірку автентичності та статусу сертифікатів користувачів, а також доступ до списків відкликаних сертифікатів;
- формування запитів на блокування чи скасування сертифікатів користувачів;
- роботу із сертифікатами кваліфікованого надавача електронних довірчих послуг та пошук необхідних сертифікатів у файлових сховищах.

Інтерфейс програми є інтуїтивно зрозумілим, що спрощує її використання навіть для непідготовлених користувачів. Завдяки своїй функціональності та орієнтації на криптографічний захист, «ІІТ Користувач ЦСК-1» забезпечує надійну роботу з електронними підписами та підвищує загальну безпеку обробки даних в системах електронного документообігу.

2.3.2. Класифікація функціоналу та компонентів СЕДО

Систематизації підлягають не лише цілісні системи електронного документообігу, але й окремі функції та компоненти цих систем. Наприклад, виділяють 17 основних функціональних компонентів СЕДО:

- введення документів;
- реєстрація за визначеними формами;
- розпізнавання тексту;
- масове завантаження даних;
- індексація;
- лінгвістичний аналіз;
- пошук;
- експорт/імпорт даних;
- веб-сервер для доступу до архіву документів;
- обмін повідомленнями;
- реплікація;
- робота в мережах;
- маршрутизація виконання завдань;
- захист від несанкціонованого доступу;
- виведення документів;
- інструменти для розробки додатків і API;
- засоби управління знаннями.

Фахівці вважають таку класифікацію ефективною, оскільки вона дозволяє не тільки описувати існуючі СЕД, але й формулювати вимоги до нових систем, обираючи необхідні функціональні компоненти з цього переліку.

Системи електронного документообігу класифікують за масштабом підприємств на три основні категорії: корпоративні СЕДО, СЕДО для середнього бізнесу та СЕДО для персонального використання.

Корпоративні СЕДО призначені для великих компаній, ці системи відрізняються високим рівнем адаптації та інтеграції в управлінську інфраструктуру підприємства. Вони забезпечують широкий спектр функцій, вимагають значних технічних ресурсів,

мають високу продуктивність та високу вартість. Впровадження таких систем часто супроводжується залученням розробників для налаштування під конкретні бізнес-процеси. Завдяки цим системам підприємства можуть ефективно автоматизувати документообіг і перейти до безпаперових технологій. Однак впровадження потребує суттєвих фінансових витрат і займає багато часу.

СЕДО для середніх підприємств орієнтовані на підприємства середнього масштабу. Вони забезпечують помірні витрати на впровадження, широкий функціонал при збереженні високих вимог до технічного оснащення та рівня кваліфікації персоналу. Вони є оптимальним варіантом для бізнесів, які не можуть дозволити собі повномасштабні корпоративні рішення, але все ще потребують потужних інструментів автоматизації.

СЕДО для організації персонального використання є найпопулярнішим варіантом для малих підприємств і приватних користувачів. Їх перевагами є:

- простота налаштування;
- зручний інтерфейс;
- невисока вартість
- мінімальні технічні вимоги.

Ці системи впроваджуються швидко й часто включають кілька інтегрованих модулів, таких як діловодство, електронний архів і контроль завдань [23].

Разом із перевагами впровадження систем електронного документообігу існують і певні недоліки. Серед них: необхідність навчання персоналу, правильне внесення інформації в електронну базу, а також один із найбільш вагомих – значні початкові витрати на впровадження системи. Однак ці інвестиції швидко окупаються завдяки перевагам, які надає СЕД.

Сучасні компанії, зокрема в Україні, зазвичай обирають СЕД, орієнтуючись на загальну стратегію розвитку, конкуренцію на ринку, бажану структуру системи та очікувану економічну вигоду. Важливу роль також відіграють можливості віддаленої роботи, швидкість впровадження, вартість встановлення та обслуговування, а також рі-

вень інформаційної безпеки. Зокрема, система повинна забезпечувати контроль доступу до документів відповідно до політики безпеки організації. Зручність і простота використання теж є важливими факторами: автоматизоване заповнення типових форм, інтеграція з іншими системами та інтуїтивно зрозумілий інтерфейс значно спрощують роботу.

2.4. Основні загрози для СЕДО

Автоматизація процесів документообігу в організаціях має очевидні переваги, і попит на системи електронного документообігу стабільно зростає. Однак важливо пам’ятати про необхідність забезпечення їхньої безпеки, адже конфіденційна інформація завжди є привабливою ціллю для зловмисників.

Захист СЕДО повинен охоплювати не лише документи, але й усю систему в цілому. Це включає забезпечення її безперебійної роботи, швидке відновлення після збоїв чи пошкоджень і навіть після повного знищення даних. Комплексний підхід до захисту СЕДО передбачає багаторівневу безпеку: від фізичного захисту носіїв інформації до організаційних заходів, що мінімізують ризики несанкціонованого доступу. Ключові аспекти захисту СЕД:

- **Апаратна частина**. Це робочі станції, сервери, мережеве обладнання та інші елементи інфраструктури. Серед загроз для апаратних компонентів – поломки, фізичний доступ зловмисників, відключення електроенергії тощо.
- **Програмне забезпечення та бази даних**. Уразливості в цих компонентах можуть стати точками входу для зовнішніх атак. Зловмисники можуть скопіювати чи пошкодити файли, використовуючи вразливості операційної системи або помилки обладнання.
- **Документи та дані**. Усі документи, що обробляються в СЕД, також потребують захисту. Необхідно запобігати їхньому несанкціонованому доступу, змінам чи видаленню.

СЕДО є складною організаційно-технічною системою, яка автоматизує створення, обробку та розповсюдження електронних документів у межах організації. Вона

забезпечує управління доступом і контроль над документопотоками, підвищуючи ефективність роботи та захищаючи чутливу інформацію.

Основними загрозами для систем електронного документообігу є:

- **Загроза цілісності**: пошкодження, знищення або спотворення інформації. Це може статися як ненавмисно (внаслідок помилок чи збоїв), так і навмисно через зловмисні дії.
- **Загроза конфіденційності**: будь-яке порушення конфіденційності, включаючи крадіжку, перехоплення даних або зміну маршрутів передачі інформації.
- **Загроза доступності**: ситуація, коли користувачі з належними правами доступу не можуть отримати необхідну інформацію в прийнятний термін.
- **Загроза працездатності системи**: порушення або зупинка роботи системи внаслідок зловмисних атак, помилок користувачів чи збоїв у роботі обладнання або програмного забезпечення.
- **Неможливість доведення авторства**: якщо в документообігу не використовується електронний підпис, неможливо довести, що документ створив конкретний користувач. Це унеможливлює надання документообігу юридичної сили.

Основними джерелами загроз для СЕДО є:

- **Легальні користувачі системи**: вони можуть ненавмисно чи навмисно порушувати безпеку — від фізичного пошкодження обладнання до навмисного викрадення інформації з корисливих мотивів.
- **Адміністративний IT-персонал**: маючи розширені повноваження та доступ до даних, ця група є особливо небезпечною. Незалежно від мотиву (корисливий умисел чи помилка), результат один — втрата або розголошення інформації. Згідно з дослідженнями, до 80% втрат відбуваються внаслідок внутрішніх атак.
- **Зовнішні зловмисники**: залежно від сфери діяльності організації, це можуть бути конкуренти, партнери, клієнти тощо.

Захист електронного документообігу є актуальною для різних сфер: це захист документообігу промислових підприємств, забезпечення конфіденційності інформації в

медичних установах, а також захист електронних документів, що забезпечують функціонування платіжних систем у банківській сфері.

Особливо гостро питання захисту СЕДО постає для організацій із територіально-розподіленою структурою. Такі організації можуть мати кілька локальних мереж, розташованих у різних регіонах, і змушені використовувати для передачі даних неконтрольовані глобальні мережі загального користування. Найбільш надійним способом забезпечення конфіденційності в таких умовах є шифрування.

Захист СЕДО необхідно здійснювати з позиції класичної моделі безпеки інформаційних систем. Для забезпечення безпеки СЕДО використовуються такі заходи:

- Аутентифікація користувачів і розмежування доступу.
- Підтвердження авторства електронного документа.
- Контроль цілісності документів.
- Забезпечення конфіденційності документів.
- Надання документам юридичної значимості.

Для ефективного захисту СЕДО необхідно впроваджувати:

- Контроль цілісності програмного забезпечення.
- Реєстрацію подій у системі.
- Криптографічний захист.
- Антивірусний захист.
- Аудит інформаційної безпеки.

Ці заходи є базовими для спеціалістів із захисту інформації та сприяють надійній роботі СЕД.

Кожна система електронного документообігу повинна забезпечувати захист від ключових загроз. До основних заходів безпеки належать:

- **Збереження документів**: захист від втрати, пошкодження або несанкціонованого видалення.
- **Безпечний доступ**: обмеження доступу лише для авторизованих користувачів.
- **Підтвердження автентичності**: гарантія того, що документ є справжнім і не був змінений.

- **Протоколювання дій користувачів**: запис усіх операцій для моніторингу та аналізу.

Захищений доступ до інформації в СЕДО реалізується через **аутентифікацію** та **розмежування прав доступу**. Аутентифікація передбачає процеси підтвердження особи користувача та перевірку його прав на виконання певних дій або доступ до конкретних даних.

Аутентифікація включає весь комплекс заходів, що здійснюються як під час входу користувача в систему, так і протягом його подальшої роботи. Найпоширеніший метод — парольний. Основною проблемою цього способу є людський фактор, який значно знижує надійність.

Для підвищення захисту використовуються багатоетапні методи аутентифікації, які об’єднують кілька кроків, наприклад, комбінацію пароля з USB-ключем або пароля з біометричним параметром. Такий підхід значно ускладнює несанкціонований доступ, оскільки навіть при компрометації одного способу залишається ще один бар’єр для входу. Користувач проходить кожен етап по черзі, що дозволяє системі максимально надійно перевірити особу.

Важливим параметром аутентифікації є кількість факторів. Вона може бути однофакторною, двофакторною тощо. Наприклад, користувач може вводити пароль і підтверджувати особу за допомогою відбитка пальця.

Також, розмежування прав доступу — обов’язкова вимога в будь-якій системі. Чим детальніше та гнучкіше налаштовані права доступу, тим краще. Це може бути окрема підсистема, розроблена спеціально для СЕД, або функціонал системи управління базами даних.

2.4.1. Криптографічні методи захисту в СЕДО

Шифрування є одним із найефективніших методів захисту інформації в системах електронного документообігу. Воно забезпечує конфіденційність даних, тобто гарантує, що доступ до документів матимуть лише авторизовані користувачі. Шифрування

базується на математичних алгоритмах, які перетворюють вихідну інформацію у вигляд, зрозумілий лише за наявності відповідного ключа.

Шифрування може бути реалізовано у двох основних формах:

1) Симетричне шифрування, яке використовує один і той самий ключ для шифрування та дешифрування даних. До популярних алгоритмів належать Advanced Encryption Standard, Data Encryption Standard та Triple DES.

Основна формула 2.1 симетричного алгоритму шифрування виглядає так:

$$C = E(K, P) \tag{2.1}$$

де C – зашифрований текст, P – відкритий текст, K – ключ шифрування, E – алгоритм шифрування.

В той же час, дешифрування здійснюється за зворотною формулою 2.2:

$$P = D(K, C) \tag{2.2}$$

де D – алгоритм дешифрування.

Перевагою симетричного шифрування є висока швидкість обробки даних, що робить його ефективним для великих обсягів інформації, однак існує необхідність безпечного передавання ключа між користувачами.

2) Асиметричне шифрування використовує пару ключів: відкритий і закритий ключі. Документ шифрується за допомогою відкритого ключа, а дешифрується лише за допомогою закритого ключа, що належить отримувачу. Найпоширеніші алгоритми — Rivest-Shamir-Adleman та Elliptic Curve Cryptography.

Оскільки асиметричний метод шифрування використовує відкритий і закритий ключі, то формула шифрування виглядає так:

$$C = P^e \, mod N \tag{2.3}$$

де C – зашифрований текст, P – відкритий текст, e – відкритий експонент, $n = p \cdot q$ – модуль, отриманий множенням двох великих простих чисел p і q.

В той же час, процес дешифрування обчислюється за формулою 2.4:

$$P = C^d \, mod N \tag{2.4}$$

де d – закритий експонент, яка обчислюється як обернена до e за модулем $(p-1)(q-1)$.

Перевагою такого методу шифрування є відсутність потреби у передачі закритого ключа, що підвищує безпеку, а недоліком — порівняно повільна робота, особливо при обробці великих обсягів даних [24].

У системах електронного документообігу шифрування застосовується на таких рівнях:

- **Файлове шифрування** — кожен документ у СЕДО шифрується окремо перед його збереженням у системі. Це забезпечує захист навіть у разі несанкціонованого доступу до бази даних.
- **Шифрування на рівні транспорту (Transport Layer Encryption)** — під час передачі документа через мережу (наприклад, між користувачами чи серверами) застосовуються протоколи SSL/TLS для захисту від перехоплення даних.
- **Шифрування на рівні зберігання (Storage Encryption)** — шифрується вся база даних або окремі її частини, що містять конфіденційну інформацію.

Окрім цього, ефективне використання шифрування залежить від правильного управління ключами. Це включає:

- **Генерацію ключів** — ключі мають генеруватися за допомогою надійних криптографічних алгоритмів.
- **Зберігання ключів** — для зберігання ключів застосовуються спеціалізовані апаратні модулі безпеки.
- **Регулярну заміну ключів** — що знижує ризик компрометації.
- **Відкликання ключів** — у разі виявлення загрози старий ключ повинен бути відкликаний, а дані – повторно зашифровані.

Також, в сучасних СЕДО широко використовуються такі криптографічні протоколи [25]:

1. PGP (Pretty Good Privacy) є хорошим криптографічним протоколом для захисту конфіденційності та автентичності даних. Він комбінує асиметричне та симетричне шифрування: відкритий ключ використовується для шифрування даних, а закритий — для їх дешифрування. PGP також дозволяє користувачам підписувати документи цифровим

підписом, що гарантує їх цілісність і автентичність. Цей протокол широко застосовується для захисту електронних листів, файлів та документів в рамках систем електронного документообігу.

2. SSL/TLS (Secure Sockets Layer / Transport Layer Security) — протоколи використовуються для забезпечення безпечного зв’язку між клієнтами і серверами в Інтернеті. Вони використовують асиметричне шифрування для ініціалізації з’єднання та симетричне шифрування для швидшої передачі даних після встановлення з’єднання. SSL/TLS також забезпечує аутентифікацію та перевірку цілісності даних, що передаються, запобігаючи їх змінам або перехопленню.

3. IPsec (Internet Protocol Security) — це набір протоколів для захисту даних на мережевому рівні, забезпечуючи їх шифрування та автентифікацію. Він застосовується для створення захищених каналів між мережевими пристроями, такими як маршрутизатори, сервіси VPN або інші точки доступу. IPsec шифрує пакети даних, що передаються через мережу, і використовує механізми для верифікації їх походження та цілісності. Це дозволяє захистити інформацію від перехоплення та змін, забезпечуючи безпеку корпоративних мереж і з'єднань між віддаленими офісами.

2.4.2. Забезпечення автентичності документів

На сьогодні основним способом забезпечення автентичності електронних документів є електронний цифровий підпис**.**

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 накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. ЕЦП дає змогу підписувати електронні документи, користуватися державними та комерційними електронними послугами, а також здійснювати реєстрацію на офіційних порталах. Документи, підписані за допомогою ЕЦП, є юридично рівноцінними паперовим, підписаним власноруч [26].

Електронний підпис забезпечує юридичну силу та доказовість електронного документа. Згідно зі статтею 6 Закону України "Про електронні документи та електронний документообіг", електронний підпис є обов’язковим елементом електронного документа, який дозволяє ідентифікувати автора або підписанта. У цій статті також зазначено, що процес створення електронного документа завершується накладанням електронного підпису. Таким чином, саме з цього моменту електронний документ набуває юридичної чинності.

Закон України "Про електронний цифровий підпис" зосереджує увагу на правовому регулюванні відносин, пов’язаних із застосуванням одного з видів електронного підпису — електронного цифрового підпису. Цей нормативний акт (Відомості Верховної Ради України, 2003, № 36, ст. 276) визначає правовий статус електронного цифрового підпису та встановлює порядок його використання.

Окрім цього, він дозволяє:

- Перевірити цілісність документа, тобто визначити, чи були внесені зміни після підписання;
- Підтвердити авторство, встановити належність підпису власнику відповідного сертифіката;

Електронний підпис може використовуватися як фізичними, так і юридичними особами для підписання будь-яких файлів, захищаючи їх від підробки та несанкціонованого доступу.

Також ЕЦП має декілька складових:

- Електронний підпис — це електронні дані, що приєднуються або логічно пов’язані з іншими електронними даними і слугують для підтвердження особи підписувача.
- Відкритий ключ — це параметр криптографічного алгоритму, який використовується для перевірки електронного цифрового підпису та є доступним для всіх учасників відносин у сфері застосування електронного цифрового підпису.
- Особистий ключ — це параметр криптографічного алгоритму, призначеного для створення електронного цифрового підпису, доступний виключно підписувачу.

Технологія використання електронного цифрового підпису базується на криптографічних методах. З криптографії запозичено поняття "ключ" — це набір двійкових даних фіксованої довжини. У практиці криптографії застосовують пари ключів, які пов’язані між собою: один використовується для шифрування, а інший — для дешифрування. Ці ключі є параметрами криптографічних алгоритмів. Як вже і було вказано, в контексті ЕЦП застосовується аналогічний принцип — пара ключів: особистий ключ, що використовується для створення підпису, і відкритий ключ, який забезпечує перевірку підпису.

Генерація ключів здійснюється за допомогою спеціальних засобів ЕЦП на основі алгоритмів, що працюють із випадковими числами високої розрядності. Надійність таких засобів передбачає, що кожна пара ключів створюється лише один раз, а їх захищеність гарантована навіть після перенесення даних на зовнішні носії. Дані, збережені в засобах генерації, після перенесення на інший носій видаляються і стають недоступними. Крім того, технології ЕЦП повинні гарантувати, що ключі не можуть бути відтворені чи отримані шляхом сторонніх маніпуляцій, а сам підпис є надійно захищеним від підробки.

Термін "особистий ключ", що вказує на персональне використання із закритим доступом для сторонніх осіб, в англійській мові має відповідник "private key". Значення особистого ключа підкреслюється в законодавстві. Згідно зі статтею 11 Закону України "Про електронну ідентифікацію та електронні довірчі послуги ", підписувач зобов’язаний зберігати свій ключ у таємниці. [27].

Вимоги до зберігання відкритих ключів у законодавстві відсутні. Відкриті ключі можуть зберігатися у вигляді запису на папері або на електронних носіях — таких як диски, флеш-накопичувачі чи апаратні пристрої. На ринку широко представлені апаратні носії для ключової інформації, які не лише зберігають відкриті ключі, але й виконують криптографічні операції. Такі носії, як правило, мають вигляд USB-пристроїв і забезпечують захист особистих ключів від несанкціонованого доступу з боку програмного забезпечення. У внутрішній пам’яті таких пристроїв можуть зберігатися як особисті, так і відкриті ключі, що гарантує їхню безпеку.

2.4.3 Перевірка правильності ключів ЕЦП

Криптографічна стійкість ЕЦП до різноманітних загроз та атак може бути гарантована лише за умови збереження цілісності, автентичності та доступності пари ключів (q, Q). Це забезпечується постійним контролем коректності як відкритого, так і приватного ключів.

Перевірка правильності відкритого ключа заключається в наступному:

ВК цифрового підпису Q, як правило, представлений у вигляді сертифіката відкритого ключа і має відповідати таким вимогам:

1) **Приналежність основному полю:** Координати точки еліптичної кривої, що визначають ключ, повинні належати основному полю, тобто бути двійковими рядками фіксованої довжини m;

2) **Відсутність нульового значення:** відкритий ключ має задовольняти умову $Q \neq 0$ (він також має задовольняти умові $Q \neq P$, тобто d = 1);

3) **Відповідність рівнянню кривої:** Точка $Q = (x_Q, y_Q)$ повинна задовольняти рівняння використовуваної еліптичної кривої.

4) **Виконання умови порядку:** Порядок точки n має задовольняти умову $nQ = 0$.

Виконання вищезазначених умов підтверджує коректність відкритого ключа. Однак, на практиці така перевірка може бути опущена, якщо реалізація алгоритму цифрового підпису передбачає використання безпечних механізмів зберігання та обробки відкритого ключа, які виключають можливість його заміни, модифікації чи знищення.

В той же час, перевірка правильності особистого полягає наступному:

Коректність приватного ключа d перевіряється виключно його власником.

1) **Обчислення точки:** Визначається точка $Q' = -dP$, де P — базова точка еліптичної кривої, а d — ОК.

2) **Порівняння результату:** Якщо $Q' = Q$, де Q — відкритий ключ, то приватний ключ коректний і відповідає відкритому ключу.

Ця перевірка також може бути опущена, якщо в алгоритмі ЕЦП передбачено використання безпечних засобів зберігання приватного ключа, які виключають ризик його модифікації, заміни або видалення.

Таким чином, забезпечення коректності пари ключів є критичним етапом для гарантування надійності ЕЦП в реальних умовах використання [24].

2.4.4 Надійність ЕЦП

Також в приклад можна взяти рекомендації Національного банку України, в яких було наголошено на необхідності зменшення ризиків під час використання інформаційних технологій у банківських системах. Зокрема, рекомендовано використовувати апаратні носії для збереження ключів у системах криптографічного захисту інформації [28].

Надійність електронного цифрового підпису у захисті від підробки чи несанкціонованого відтворення ґрунтується на використанні криптографічних методів. Наприклад, алгоритм, затверджений ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис на основі еліптичних кривих”, забезпечує високий рівень стійкості. При довжині ключа 264 біти, час, необхідний для теоретичного зламування такого підпису із застосуванням сучасних методів криптоаналізу на комп’ютері з процесором частотою 3 ГГц, оцінюється експертами у близько тисячу років. Саме ця тривалість є основою для гарантії стійкості ЕЦП [29].

Для оцінки часу зламування ЕЦП при заданій довжині ключа можна використати формулу 2.5, яка враховує кількість можливих комбінацій ключів і швидкість обчислень:

$$T = \frac{2^n}{S \cdot P} \tag{2.5}$$

де T — час, необхідний для зламування (у секундах);

n — довжина ключа (у бітах);

S — кількість операцій, які процесор може виконати за секунду (наприклад, 3×10^9 операцій для процесора з частотою 3 ГГц);

P — ймовірність успіху зламування за одну спробу (зазвичай P=1P = 1P=1, якщо розглядається повний перебір усіх можливих ключів).

Для ключа довжиною $n = 264$ біт і процесора з частотою 3 ГГц $= 3 \times 10^9$ операцій/с, підставляємо значення в формулу 2.6:

$$T = \frac{2^{264}}{3 \cdot 10^9} \tag{2.6}$$

Щоб отримати час у роках доповнюємо значення в формулу 2.7:

$$T_{\text{роки}} = \frac{T}{3 \cdot 10^9 \cdot 60 \cdot 60 \cdot 24 \cdot 365} \tag{2.7}$$

Підставимо значення в формулу 2.8, щоб отримати числову оцінку:

$$T_{\text{роки}} = \frac{2^{264}}{3 \cdot 10^9 \cdot 60 \cdot 60 \cdot 24 \cdot 365} \tag{2.8}$$

Таким чином, ця формула демонструє експоненційну залежність часу зламування від довжини ключа.

Додатковим бар’єром для потенційних зловмисників є обмежений термін використання особистого ключа. Підписувач регулярно оновлює свій особистий ключ разом із відкритим. У разі підозри щодо компрометації ключа, тобто ризику його доступності стороннім особам, підписувач має можливість достроково замінити особистий ключ. Це суттєво ускладнює спроби зламування, оскільки ключ, який може бути використаний для підробки, швидко втрачає актуальність.

Згідно із Законом України «Про електронні довірчі послуги» [30], ЕЦП може існувати в трьох форматах, кожен з яких відповідає певному рівню довіри до власника, як зображено на рис. 2.3.

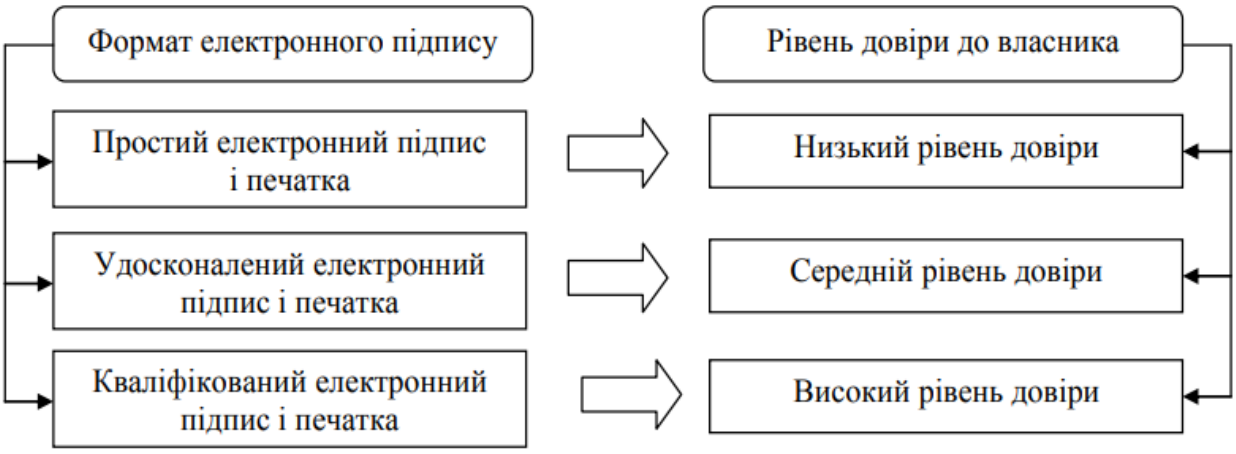


Рис. 2.3 — Рівень довіри власників до різних форматів ЕЦП

Існують два типи електронних підписів: прості та удосконалені. У свою чергу удосконалені підписи мають два види: кваліфікований та некваліфікований.

Простий електронний підпис являє собою поєднання логіна та пароля, яке підтверджує, що електронне повідомлення було відправлене певною особою.

Удосконалений некваліфікований підпис ідентифікує відправника та гарантує, що документ не змінювався після підписання.

Для визнання документа підписаним ПЕП необхідно дотримання таких умов:

- підпис включений до самого документа.
- ключ простого електронного підпису використовується відповідно до правил, визначених оператором інформаційної системи, а документ містить інформацію про особу, яка його створила або відправила.

Посилені некваліфіковані та кваліфіковані електронні підписи створюються шляхом криптографічної обробки даних із використанням ключа електронного підпису. Вони мають такі основні властивості:

- дозволяють ідентифікувати особу, яка підписала електронний документ;
- забезпечують виявлення будь-яких змін у документі після його підписання;
- формуються за допомогою спеціальних засобів електронного підпису.

Кваліфікований електронний підпис, окрім зазначених характеристик, має відповідати додатковим вимогам:

- ключ перевірки підпису повинен бути включений до кваліфікованого сертифіката;
- як для створення, так і для перевірки підпису мають використовуватися засоби, які пройшли сертифікацію та відповідають законодавчим вимогам щодо електронних підписів.

Протоколювання дій користувачів є важливим елементом захисту електронного документообігу. Його правильна реалізація в системі дозволяє відстежувати всі неправомірні дії, встановлювати винних, а в окремих випадках навіть запобігати спробам нанесення шкоди або порушень. Така функція повинна бути обов'язково інтегрована в саму систему електронного документообігу. Окрім цього, можна скористатися продуктами сторонніх розробників або партнерів, які забезпечують інтеграцію своїх рішень із СЕДО. Також не варто забувати про вбудовані в операційні системи інструменти протоколювання та сторонні програми для цього завдання.

Підхід до захисту електронного документообігу має бути комплексним. Захист СЕДО не обмежується лише охороною документів та розмежуванням доступу до них. Важливо забезпечити захист апаратного забезпечення системи, включаючи персональні комп'ютери, принтери та інші пристрої; захист мережевого середовища, у якому функціонує система, каналів передачі даних і мережевого обладнання.

2.5. Висновки до другого розділу

Другий розділ висвітлює проблематику систем електронного документообігу та аналіз їх еволюції. Визначено основні етапи розвитку СЕДО — від початкової автоматизації документообігу до сучасних універсальних систем, що забезпечують інтеграцію з іншими інформаційними технологіями та бізнес-процесами. Також підкреслено важливість захисту інформації, особливо в умовах використання хмарних технологій, які набирають популярності завдяки їхній економічній ефективності, доступності та гнучкості.

У розділі розглянуто основні методи захисту систем електронного документообігу, що охоплюють апаратні та програмні заходи безпеки. До апаратних засобів належать фізичний захист серверів і мережевого обладнання, резервне копіювання даних і використання сучасної техніки для підвищення надійності системи. Програмний захист включає регулярне оновлення ПЗ, антивірусні програми, шифрування даних, електронний підпис і багаторівневий контроль доступу.

Основними загрозами для СЕДО є порушення цілісності, конфіденційності та доступності інформації, збої у працездатності системи, а також неможливість доведення авторства документів без використання електронного підпису. Комплексний підхід до захисту, що включає апаратні та програмні заходи, дозволяє мінімізувати ризики, забезпечити стабільну роботу системи та безпеку даних.

РОЗДІЛ 3. ВДОСКОНАЛЕННЯ БЕЗПЕКИ НА ПРИКЛАДІ СЕДО PAPERLESS

3.1. Характеристика СЕДО Paperless

Система Paperless — це сучасний продукт програмного забезпечення, призначений для автоматизації процесів електронного документообігу. Мета використання будь-якого інструменту СЕДО полягає в тому, щоб зменшити використання паперу, скоротити час обробки документів і створити середовище для безпечного, прозорого та ефективного управління інформацією. Paperless пропонує власну платформу, яка дозволяє невеликим організаціям оптимізувати свої операції, підвищити продуктивність і захистити свої дані. Інтерфейс СЕДО Paperless показано на рис. 3.1.

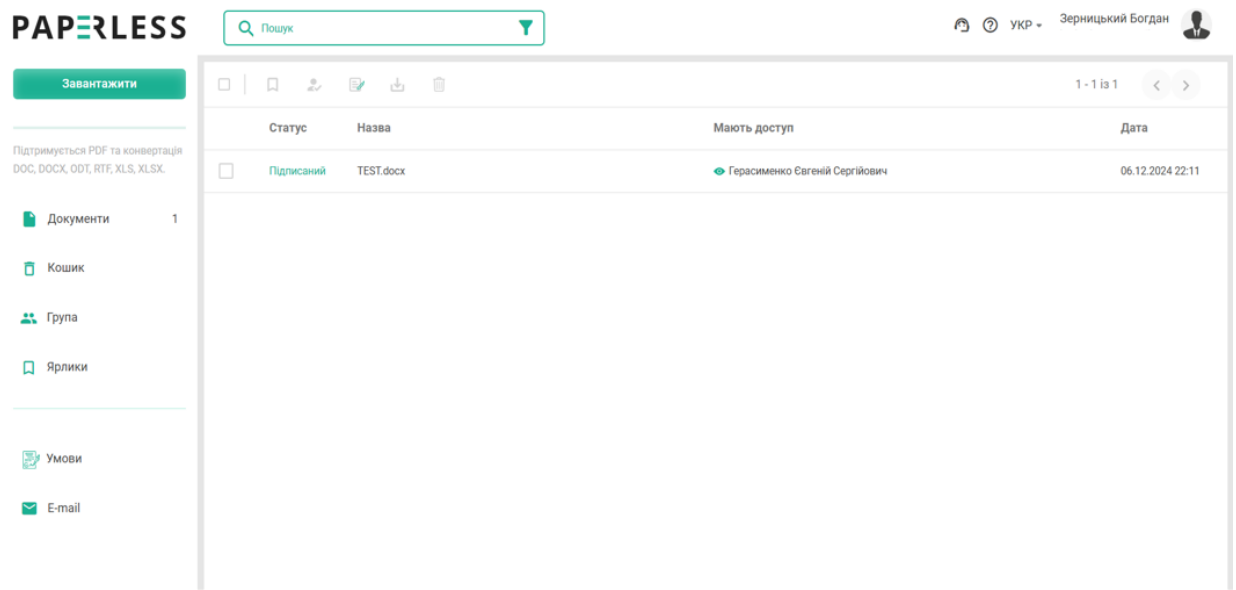


Рис. 3.1 — Інтерфейс СЕДО Paperless

Здатність охоплювати всі етапи життєвого циклу документів, починаючи від імпорту та архівування, а також забезпечувати зручний пошук, є однією з основних переваг Paperless. У системі є можливість автоматичного індексування документів, що значно спрощує роботу. Користувачі можуть швидко отримати необхідні дані без необхідності витрачати час на ручне сортування даних завдяки цьому. Інтеграція механізму електронного підпису є ще однією важливою функцією, яка дозволяє підтверджувати правомірність і автентичність документів без паперових копій.

Paperless побудована на сучасній клієнт-серверній архітектурі, що забезпечує її гнучкість і масштабованість. Веб-інтерфейс дозволяє користувачам працювати з документами без необхідності встановлення додаткового програмного забезпечення, що зручно для великих організацій із численними віддаленими офісами. База даних, яка використовується для зберігання документів і метаданих, побудована з урахуванням вимог високої доступності та надійності. Це забезпечує стабільну роботу системи навіть за умов значного навантаження.

Таким чином, Paperless є універсальним рішенням, яке забезпечує зручність, ефективність і безпеку обробки документів. Її впровадження дозволяє не лише автоматизувати рутинні процеси, але й забезпечити стратегічний контроль за інформаційними потоками організації. Ця система не просто відповідає вимогам сучасного бізнесу, а й закладає фундамент для подальшого розвитку цифрових технологій управління документами.

3.1.1. Призначення та основні функціональні можливості

Призначення системи Paperless тісно пов'язане з її головною метою – створенням умов для повноцінного електронного документообігу та усуненням недоліків паперової бюрократії. Це включає зниження витрат на папір, прискорення обробки документів і підвищення ефективності бізнес-процесів. Paperless дозволяє забезпечити швидкий доступ до необхідної інформації, мінімізуючи ризики втрати чи пошкодження документів, що є типовими для традиційного паперового документообігу.

Основними функціональними можливостями Paperless є імпорт документів із різних джерел, їх подальша індексація та класифікація. Завдяки цим функціям документи можуть бути швидко організовані у відповідні категорії, що спрощує їх подальше використання. Крім того, система підтримує погодження документів, дозволяючи узгоджувати різні версії між учасниками процесу. Інтеграція функції електронного підписання забезпечує юридичну силу цифрових документів, підвищуючи їхню легітимність і цілісність.

Пошук документів здійснюється за допомогою гнучких інструментів фільтрації та ключових слів, що значно економить час користувачів. Особливу увагу приділено функції спільної роботи, яка дозволяє кільком учасникам одночасно працювати над документами, обмінюватися коментарями та відстежувати зміни.

Таким чином, Paperless виступає не просто інструментом для автоматизації документообігу, а й надійною платформою для управління всіма аспектами документів у цифровій формі, що відповідає сучасним вимогам ефективності, прозорості та безпеки.

3.1.2. Архітектура та технічні особливості

Система Paperless побудована на клієнт-серверній моделі, яка забезпечує ефективну організацію роботи та легку масштабованість. Веб-інтерфейс системи дозволяє користувачам отримувати доступ до функціоналу з будь-якого пристрою, що підтримує браузер, без необхідності встановлення додаткового програмного забезпечення. Це значно спрощує впровадження системи, особливо для організацій із віддаленими офісами чи мобільними працівниками. Центральний компонент архітектури – база даних – використовується для зберігання як документів, так і їхніх метаданих. Завдяки сучасним технологіям бази даних забезпечують високу швидкість доступу до інформації, надійність і можливість резервного копіювання.

Paperless також включає базові заходи безпеки, передбачені розробниками, що є важливим аспектом для захисту конфіденційної інформації. До них належать рольова модель доступу, яка дозволяє чітко розмежовувати права користувачів відповідно до їхніх обов'язків. Журналювання дій користувачів забезпечує можливість відстеження всіх операцій у системі, що сприяє прозорості та контролю за безпекою. Для збереження цілісності даних Paperless використовує механізми шифрування, які захищають інформацію як під час її передачі, так і під час зберігання.

3.2. Аналіз переваг та недоліків СЕДО Paperless з точки зору безпеки

СЕДО Paperless пропонує низку переваг у забезпеченні інформаційної безпеки, які роблять її надійним рішенням для управління документами в організаціях. Однією

з ключових особливостей є рольова модель доступу, яка дозволяє чітко розмежувати права користувачів залежно від їхніх функціональних обов'язків. Це забезпечує контроль за доступом до документів і значно знижує ризик несанкціонованого доступу до конфіденційної інформації. Крім того, система веде аудит дій користувачів, що дозволяє відстежувати всі зміни та дії в рамках документообігу, забезпечуючи прозорість і можливість аналізу активності.

Ще однією важливою перевагою Paperless є використання електронних цифрових підписів, які додають юридичної сили цифровим документам і забезпечують цілісність даних. Завдяки цьому організації можуть бути впевнені, що зміни в документах виконуються лише уповноваженими особами, а самі документи залишаються незмінними після підписання.

Paperless також забезпечує надійний захист від втрати даних завдяки механізмам резервного копіювання. Система регулярно створює резервні копії документів і метаданих, що дозволяє відновити інформацію навіть у разі технічних збоїв або атак. Це знижує ризик втрати критично важливих даних і підвищує загальний рівень надійності системи.

Таким чином, Paperless надає інструментарій для забезпечення інформаційної безпеки, поєднуючи контроль доступу, захист даних і прозорість документообігу. Ці переваги роблять систему незамінним рішенням для організацій, які прагнуть забезпечити високий рівень безпеки своїх інформаційних ресурсів.

3.2.1. Недоліки та потенційні вразливості

Однак, попри численні переваги, система Paperless має деякі недоліки та потенційні вразливості, які можуть впливати на загальний рівень інформаційної безпеки. Однією з ключових проблем є обмежені стандартні налаштування безпеки, які можуть не відповідати специфічним вимогам організацій, однак в той же час для невеликих організацій це може бути не критичною проблемою. Однак система має один дуже великий недолік, який стосується, зокрема, недостатньої гнучкості автентифікації до СЕДО, що обмежує можливості адаптації системи до сучасного стану речей.

Ще одним критичним аспектом є ризики, пов'язані з веб-вразливостями, такими як SQL-ін’єкції або атаки типу XSS. У разі неправильного налаштування або несвоєчасного оновлення системи ці вразливості можуть бути використані зловмисниками для отримання несанкціонованого доступу до даних.

Також, недостатній рівень моніторингу є ще однією проблемою, яка перешкоджає виявленню потенційних загроз в системі. У разі виникнення атак або інших інцидентів безпеки, відсутність детального моніторингу та звітності подій, може ускладнити аналіз ситуації та вжиття оперативних заходів для її вирішення. Це може створити серйозні ризики для організацій, що покладаються на систему Paperless.

Останнім, але не менш важливим чинником є людський фактор. Відсутність належного навчання користувачів може призводити до помилок у роботі з системою, таких як використання слабких паролів або нехтування правилами безпеки. Людський фактор залишається одним із найслабших місць у забезпеченні інформаційної безпеки, і його необхідно враховувати при впровадженні системи.

Таким чином, недоліки та потенційні вразливості Paperless вимагають ретельного аналізу та розробки додаткових заходів безпеки, які дозволять мінімізувати ризики та забезпечити максимальний рівень захисту інформації в організації.

3.3. Рекомендації щодо вдосконалення захисту Paperless

Забезпечення надійного захисту інформації є важливим завданням для будь-якої організації, яка використовує систему Paperless. Враховуючи виявлені недоліки та потенційні вразливості, розробка рекомендацій для їх усунення стає необхідним кроком для підвищення загального рівня безпеки в системі та в організаціях в цілому. Основна увага приділяється посиленню автентифікації, вдосконаленню криптографічних механізмів, покращенню моніторингу, а також врахуванню людського фактору. Реалізація запропонованих заходів дозволить знизити ризики, пов'язані з несанкціонованим доступом, вразливостями системи та помилками користувачів. У наступних підрозділах будуть представлені конкретні рекомендації, спрямовані на вирішення цих проблем.

3.3.1. Захист від несанкціонованого доступу

Автентифікація та авторизація є ключовими аспектами захисту будь-якої системи, зокрема Paperless, і вимагають постійного вдосконалення для забезпечення належного рівня безпеки. Основна перевага двофакторної автентифікації полягає в тому, що навіть у разі компрометації паролю, зловмисники не зможуть отримати доступ до системи без додаткового підтвердження, наприклад, одноразового коду, надісланого на мобільний телефон або генерованого спеціальним додатком. Це значно знижує ризик несанкціонованого доступу до конфіденційної інформації, включаючи електронні документи, ключі ЕЦП та інші критично важливі дані.

Запровадження MFA є обов'язковим елементом сучасної безпеки СЕДО, оскільки воно мінімізує загрозу кібератак та забезпечує високий рівень захисту корпоративних даних від несанкціонованих дій.

На даний час, СЕДО Paperless потребує для входу в акаунт лише Логін та Пароль, однак користувач може підключити двофакторну автентифікацію на основі одноразового паролю, а саме використовуючи окремий додаток-автентифікатор Google Authenticator. Хоча даний спосіб захисту, на даний час, являється ефективним, однак при втраті доступу до облікового запису Google, потенційні зловмисники зможуть отримати доступ, до додатку-автентифікатора і таким чином зламати обліковий запис користувача в СЕДО Paperles. Тому необхідно розширити варіанти двофакторної автентифікації.

Для виконання даного завдання, найкращим чином підійдуть наступні методи:

1) MFA на основі SMS – для цього необхідно інтегрувати в систему перевірку, на основі того, що користувач повинен приєднати свій номер телефону до системи. Таким чином, під час входу до системи користувач логін, пароль та одноразовий код, який надсилається на зареєстрований номер у вигляді SMS. Хоча цей спосіб теж має слабкі місця, наприклад, зловмисники можуть отримати доступ до коду, якщо вкрадуть SIM-карту користувача або якщо SMS потрапить на пристрій, заражений шкідливим програмним забезпеченням, однак даний метод є більш ефективним, оскільки отримати доступ до телефону важче, ніж до облікового запису.

2) MFA на основі ключа безпеки – це один із найбільш надійних способів багатофакторної автентифікації. Ключ безпеки є фізичним пристроєм, який підключається до комп'ютера через USB-порт. Під час автентифікації користувач вводить логін і пароль, після чого підключає ключ безпеки. Пристрій генерує одноразовий код, який потрібно ввести для підтвердження особи. Цей метод вирізняється високою надійністю, оскільки ключ майже неможливо підробити, а без нього зловмисник не зможе отримати доступ до системи.

Окрім цього, серед найефективніших способів автентифікації виділяється використання біометричних даних, які базуються на унікальних фізичних характеристиках користувача, таких як відбитки пальців, структура райдужної оболонки або риси обличчя. Такий підхід забезпечує високий рівень захисту, адже біометричні параметри майже неможливо підробити. Однак впровадження такого методу потребує спеціалізованого обладнання для зчитування біометричних показників, що суттєво підвищити витрати на реалізацію та підтримку СЕДО.

Для посилення безпеки також використовуються багаторівневі методи автентифікації, які поєднують кілька етапів, наприклад, пароль у комбінації з біометричним параметром або USB-ключем. Завдяки цьому навіть компрометація одного з етапів не забезпечить зловмиснику доступу до системи. Хоча багатофакторний підхід ускладнює процес авторизації, він значно підвищує рівень захисту, створюючи додаткові бар'єри для несанкціонованого входу. Саме тому поєднання таких варіантів захисту для захисту СЕДО Paperless може стати найкращим варіантом захисту від несанкціонованого доступу.

Особливості біометричної автентифікації:

- **Відбитки пальців.** Перевірка за відбитками пальців базується на аналізі унікального рельєфу поверхні шкіри. Сучасні сканери додатково аналізують такі параметри, як температура та вологість шкіри, що робить підробку відбитків надзвичайно складною. Для обходу цього методу зловмиснику потрібно не лише створити точну 3D-копію відбитка, але й імітувати фізичні показники, що потребує значних технічних ресурсів. Просте зчитування залишків відбитків із поверхонь зазвичай не дає можливості створити копію високої точності.

- **Розпізнавання обличчя**. Цей метод передбачає аналіз геометрії обличчя: відстані між очима, форми носа, контурів підборіддя та інших унікальних характеристик. Системи сучасного розпізнавання здатні перевіряти динамічні зміни, як-от мікрорухи обличчя, що виключає можливість використання статичних зображень або масок. Створення 3D-копії обличчя є складним, дорогим процесом, який потребує точних вихідних даних.
- **Сканування райдужної оболонки та сітківки ока**. Автентифікація за допомогою райдужної оболонки або сітківки базується на аналізі детальної структури ока, яка є унікальною для кожної людини. Для зчитування таких даних використовується інфрачервоне освітлення, що дозволяє фіксувати найдрібніші деталі. Відтворення точних копій вимагає високоякісного обладнання та доступу до оригінальних даних, що робить цей метод одним із найнадійніших.

Також, ефективне управління обліковими записами користувачів є одним із ключових аспектів захисту СЕДО Paperless. Регулярна зміна паролів відіграє важливу роль у мінімізації ризиків, пов’язаних із компрометацією облікових даних. Рекомендації щодо встановлення паролів включають дотримання політик складності, які вимагають використання мінімальної кількості символів, комбінації великих і малих літер, цифр і спеціальних символів. Такий підхід суттєво знижує вірогідність успішної атаки методом перебору.

Додатково, заборона повторного використання старих паролів запобігає створенню шаблонів, які можуть бути передбачуваними для потенційних зловмисників. Також, створення певного алгоритму в системі, який буде контролювати унікальність кожного нового пароля, підвищує загальний рівень захисту. Це особливо важливо в контексті атак, коли зловмисники сподіваються на повторне використання користувачем попередніх паролів.

Усі ці заходи спрямовані на створення умов, у яких доступ до облікових записів стає значно складнішим для зловмисників. Політика складних паролів і регулярних змін не лише захищає систему від несанкціонованого доступу, а й робить її більш стійкою до сучасних атак, таких як атаки методом брутфорсу. Таким чином, управління

обліковими записами користувачів, забезпечує «фундаментальну лінію оборони» в захисті СЕДО Paperless.

Однією з проблем в системі СЕДО Paperless користувач має необмежену кількість спроб для входу у власний обліковий запис, навіть якщо буде використано багато невдалих спроб входу, то система буде писати, що користувач ввів «Неправильний логін або пароль», як показано на рис. 3.2. Це відкриває великі можливості для потенційних зловмисників, щоб здійснювати атаки типу брутфорс.

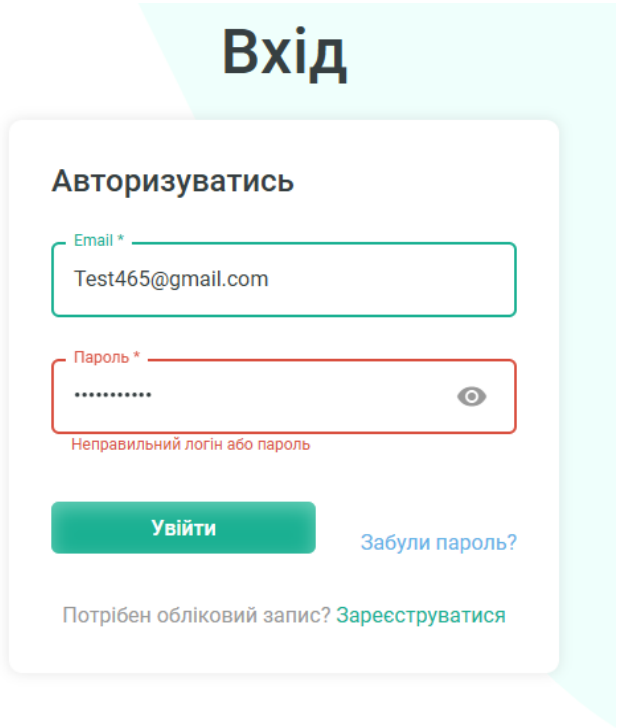


Рис. 3.2 — Невдала спроба входу в обліковий запис

Тому моніторинг аутентифікації користувачів є важливим елементом для оперативного виявлення підозрілих дій. Рішення даної проблеми є те, що система повинна фіксувати невдалі спроби входу та повідомляти користувачів про підозрілу активність. Одним із варіантів запровадження безпеки є блокування облікових записів після певної кількості невдалих спроб входу дозволяє запобігти атакам методом перебору. Також блокування може бути як частковим, тобто розблокування облікового запису відбудеться через певний час, так і до того моменту, доки користувач сам не розблокує власний обліковий запис, це можна зробити таким чином, щоб система відправляла спеціальні посилання на електронну адресу користувача і при переході по ним, обліковий

запис розблоковувався за проханням користувача. Таким чином, можна мінімізувати ризики, при атаці типу брутфорс.

Останній, але не менш важливий аспект безпеки в системах електронного документообігу – це управління тривалістю сесій користувачів. Цей механізм спрямований на зниження ризику несанкціонованого доступу, особливо у випадках, коли користувач залишає робоче місце або пристрій без нагляду.

Обмеження часу активності сесії має передбачати автоматичне завершення сеансу користувача після певного періоду бездіяльності. Наприклад, якщо система фіксує відсутність будь-якої активності з боку користувача протягом 10-15 хвилин, обліковий запис автоматично виходить із системи. Це дозволяє уникнути ситуацій, коли сторонні особи можуть скористатися активною сесією, отримавши доступ до конфіденційних даних або функцій системи.

Крім часу бездіяльності, в СЕДО Paperless можна додати можливість максимальної тривалості активного сеансу, після якої користувач буде змушений повторно пройти автентифікацію, навіть якщо він продовжує працювати. Наприклад, така політика може бути реалізована для сеансів, що тривають більше 7-8 годин, аби запобігти тривалому збереженню сеансових даних, які можуть бути використані зловмисниками.

Окрім цього, важливим компонентом безпеки є чітка рольова модель доступу, яка забезпечує розмежування прав користувачів відповідно до принципу мінімально необхідного доступу. Це означає, що кожен користувач отримує лише ті права, які необхідні для виконання його службових обов’язків. Регулярний аудит ролей і привілеїв допоможе виявляти та усувати надмірні права, що потенційно можуть бути використані зловмисниками.

3.3.2. Модернізація криптографічних механізмів захисту

Удосконалення криптографічних механізмів захисту дозволяє значно підвищити стійкість системи до зовнішніх загроз і забезпечити відповідність сучасним стандартам безпеки.

Перш за все, необхідно використовувати сучасні криптографічні алгоритми, які визнані надійними міжнародними стандартами. Наприклад, алгоритм AES-256 є одним із найпоширеніших і найстійкіших методів для шифрування даних. Використання таких алгоритмів забезпечує захист даних навіть у разі отримання зловмисником фізичного доступу до серверів або носіїв інформації.

Крім застосування сучасних алгоритмів, важливо дотримуватися принципу регулярної заміни криптографічних ключів. Ключі, які використовуються для шифрування, мають обмежений термін придатності, після якого вони підлягають заміні. Це знижує ризик їхнього компрометації. Управління ключами повинно здійснюватися відповідно до чітко визначених політик безпеки, що включають їх зберігання, генерацію, розповсюдження та утилізацію.

Окрім цього, особливу увагу слід приділити механізмам електронного підпису, які є ключовими для підтвердження автентичності та цілісності документів. Перевірка надійності існуючих механізмів електронного підпису та їх відповідності сучасним вимогам має бути регулярною. У разі виявлення застарілих або вразливих механізмів слід переходити на використання кваліфікованих електронних підписів, які відповідають чинному законодавству та стандартам безпеки. Використання таких сертифікатів забезпечує не лише технічний захист, але й юридичну силу підписаних документів.

Модернізація криптографічних механізмів у системі Paperless дозволить не тільки захистити дані від сучасних загроз, але й забезпечити довіру до системи з боку користувачів і партнерів, гарантуючи високий рівень безпеки та відповідність актуальним стандартам.

3.3.3 Додавання дозволених IP-адрес для доступу в СЕДО Paperless

Використання IP-адрес для обмеження доступу, може стати ефективним засобом підвищення безпеки в системі електронного документообігу Paperless. Цей підхід дозволить забезпечити доступ виключно для користувачів із визначеними IP-адресами.

Наприклад, організація може налаштувати систему таким чином, щоб доступ був дозволений лише для співробітників, які працюють в офісі, тоді як усі спроби входу з інших місць будуть заблоковані.

Налаштування списку дозволених IP-адрес у Paperless є ефективним методом захисту від несанкціонованого доступу. Завдяки цьому лише пристрої з попередньо визначених IP-адрес отримають доступ до системи. Це може запобігти спробам злому ззовні та значно знизити ризики компрометації, навіть якщо логін і пароль користувача було викрадено.

Однак цей підхід має певні обмеження. По-перше, IP-адреси можуть бути підроблені, що потребує додаткових заходів захисту. По-друге, користувачі з динамічними IP-адресами можуть стикатися з проблемами доступу через зміну їхніх мережевих параметрів. Це вимагає ретельного адміністрування та регулярного оновлення списку дозволених IP-адрес, щоб уникнути непередбачених ситуацій.

Для підвищення ефективності цього методу рекомендується періодично переглядати та оновлювати список дозволених IP-адрес. Це дозволить видалити доступ для користувачів, які більше не повинні працювати з системою, а також заблокувати підключення з небезпечних або підозрілих мереж.

3.3.4. Покращення моніторингу та аналізу подій безпеки

Забезпечення якісного моніторингу та аналізу подій безпеки є критично важливим для підтримки високого рівня захисту в системі Paperless. Ці аспекти дозволяють своєчасно виявляти потенційні загрози, аналізувати причини інцидентів та оперативно реагувати на них.

Першим кроком до вдосконалення, є впровадження деталізованого запису подій. Усі ключові операції, які здійснюються в системі, мають бути належним чином зафіксовані. Це включає створення, зміну, видалення документів, спроби доступу до них, входи та виходи користувачів, зміну прав доступу та інші дії, які впливають на безпеку. Створення детального журналу подій забезпечить прозорість процесів і створюють основу для аналізу у випадку виникнення непередбачуваних інцидентів.

Для більш глибокого аналізу та автоматизації виявлення загроз слід інтегрувати систему Paperless з SIEM-системами. Такі системи дозволяють обробляти великі обсяги логів у режимі реального часу, виявляти аномалії в поведінці користувачів або системи та автоматично генерувати сповіщення про потенційні інциденти. Завдяки цьому можна оперативно реагувати на загрози, знижуючи ризик витоку даних або несанкціонованого доступу.

Крім того, проведення тестів на проникнення допоможе виявити нові вразливості, які могли залишитися непоміченими під час стандартного моніторингу. Результати таких тестів дозволяють оцінити ефективність застосованих заходів безпеки та визначити напрямки для подальшого вдосконалення.

3.3.5. Посилення захисту від людського фактору

Людський фактор є одним із найслабших місць у системах інформаційної безпеки, в цілому, тому його врахування є критично важливим для ефективного захисту СЕДО Paperless. Загрозу інсайдерських дій як у сфері інформаційної безпеки, так і сфері безпеки СЕДО, багато аналітичних служб визнають однією з найбільш критичних проблем сучасності. Такі дії, що можуть бути як навмисними, так і спричиненими недбалістю або недостатньою кваліфікацією співробітників, стали серйозним викликом для багатьох організацій. В останні десятиліття ця проблема не лише набула значного поширення, але й продовжує загострюватися, стаючи одним із ключових трендів у сфері інформаційної безпеки. На рис. 3.3 зображено відношення кількості навмисних та ненавмисних витоків інформації [31].

Саме тому, підвищення рівня обізнаності співробітників і впровадження організаційних заходів здатні значно знизити ризики, пов'язані з помилками чи недбалим поводженням з інформацією.

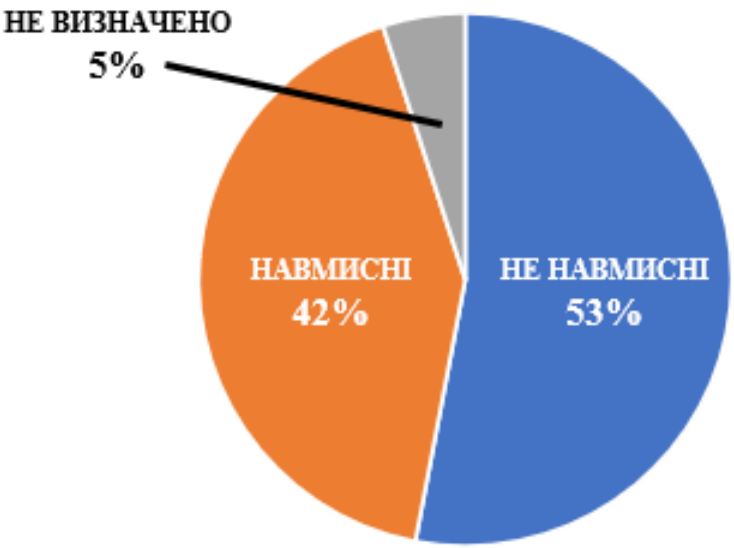


Рис. 3.3 — Відношення кількості навмисних та ненавмисних витоків конфіденційної інформації

Одним із основних заходів, має стати навчання персоналу основам інформаційної безпеки. Проведення регулярних тренінгів дозволяє співробітникам дізнатися про сучасні загрози, такі як фішинг-атаки чи соціальна інженерія, а також про способи їх уникнення.

Окрім цього, організації необхідно розробити внутрішні інструкції для роботи з документами. Вони мають містити чіткі правила щодо зберігання, передачі та доступу до конфіденційної інформації. Контроль за дотриманням цих політик повинен бути систематичним, наприклад, шляхом проведення регулярних перевірок чи аудитів. Чіткі інструкції сприяють формуванню культури безпечної роботи та зменшують імовірність випадкових порушень.

Політика мінімізації доступу є важливим інструментом для зниження ризиків, пов’язаних із зловживанням доступом. Надання користувачам лише тих прав, які необхідні для виконання їхніх функцій, дозволяє зменшити потенційний вплив від компрометації облікового запису. Регулярний аудит прав доступу забезпечує своєчасне виявлення та усунення надмірних привілеїв, які можуть створювати загрози для системи.

Посилення захисту від людського фактора є невід'ємною складовою комплексного підходу до забезпечення інформаційної безпеки. Поєднання освітніх ініціатив, чітких інструкцій і організаційних заходів дозволяє створити середовище, де ризики,

пов’язані з помилками співробітників, зведені до мінімуму. Це сприяє підвищенню загальної захищеності системи Paperless та її надійності.

3.6. Висновки до другого розділу

У розділі розглянуто систему електронного документообігу Paperless, її ключові функції, архітектуру, а також переваги та недоліки з точки зору безпеки. Paperless забезпечує ефективну автоматизацію обробки документів, спрощуючи їхнє управління та обмін завдяки інструментам індексації, електронного підпису та зручного пошуку.

Особливу увагу приділено аналізу рівня інформаційної безпеки системи, включаючи механізми контролю доступу, захисту даних і моніторингу активності користувачів.

Водночас визначено низку потенційних вразливостей, серед яких обмежена гнучкість автентифікації, недостатній рівень моніторингу та вплив людського фактора. Запропоновані рекомендації для вдосконалення захисту Paperless включають впровадження багатофакторної автентифікації, додавання списку дозволених IP-адрес, покращення криптографічних механізмів і посилення заходів проти внутрішніх загроз.

Реалізація запропонованих рішень дозволить підвищити надійність системи, мінімізувати ризики безпеки та забезпечити ефективний захист інформації в організаціях, що використовують СЕДО Paperless.

ВИСНОВОК

У кваліфікаційній роботі досліджено ключові аспекти електронного документообігу, його особливості та проблематику, а також визначено напрями вдосконалення системи захисту інформації на прикладі сучасних рішень. Розгляд електронного документообігу розпочато з визначення його сутності, особливостей та переваг у контексті автоматизації робочих процесів і забезпечення ефективного управління інформацією. Встановлено, що впровадження електронних документів дозволяє не лише зменшити використання паперових ресурсів, а й забезпечити швидкий доступ до інформації, її надійне збереження та централізовану обробку.

Проблематика сучасних систем електронного документообігу пов'язана зі складністю захисту даних від несанкціонованого доступу та вразливостями, що виникають у процесі їх зберігання та передавання. У роботі наголошено на важливості впровадження надійних засобів безпеки, включаючи багаторівневий захист, шифрування інформації та контроль доступу. Водночас підкреслено значну роль хмарних технологій як перспективного напрямку розвитку систем електронного документообігу, що дозволяє оптимізувати управління інформаційними потоками й мінімізувати витрати на апаратне забезпечення.

На прикладі СЕДО Paperless проаналізовано архітектуру, переваги та можливі ризики. Виявлено основні загрози безпеці даних, серед яких вразливість до несанкціонованих змін, витоків та збоїв. Запропоновано практичні рекомендації щодо вдосконалення безпеки, зокрема впровадження багатофакторної автентифікації, використання сучасних криптографічних алгоритмів та посилення контролю активності користувачів.

Таким чином, результати дослідження підтверджують, що впровадження сучасних систем електронного документообігу є важливим інструментом підвищення ефективності управління інформацією в організаціях. Незважаючи на існуючі виклики в сфері безпеки, їх подолання можливе завдяки впровадженню комплексних технічних та організаційних заходів, що забезпечать надійний захист даних та оптимізують документообіг у цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію». Офіц. вид. Київ : Парлам. вид-во, 2002. 24 с.

2. Закон України «Про електронні документи та електронний документообіг», від 22.05.2003 № 851-IV : станом на 1 січ. 2024 р. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/851-15.

3. Що таке електронний документ [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://smarttender.biz/terminy/view/elektronniy-dokument/

4. «Про затвердження Інструкції з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну в Міністерстві культури України»: Наказ М-ва культури України від 29 серпня 2018 року №753 [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://ips.ligazakon.net/document/view/mus30607?an=1&ed=2018_08_29

5. Закон України «Про бухгалтерський облік та фінансову звітність в Україні». Офіц. вид. Київ : Парлам. вид-во, 1999. 16 с.

6. «Перелік форматів даних електронних документів постійного і тривалого (понад 10 років) зберігання» : Наказ М-ва юстиції України від 11.11.2014 № 1886/5. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/z1422-14#Text

7. Матвієнко О. Основи організації електронного документообігу : навчальний посібник – Київ. : Центр учбової літератури, 2008. 116 с.

8. Шебаніна О.В. Впровадження систем електронного документообігу в установі / Клочан В.П., Клочан І.В. : навчальний посібник – Миколаїв: МНАУ, 2021. 69 с.

9. «Про затвердження завдань Національної програми інформатизації на 2022-2024 роки» : Постанова Верхов. Ради України від 08.07.2022 № 2360-IX. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/2360-20#Text

10. «Про визначення окремих завдань (проектів) Національної програми інформатизації, їх державних замовників та передачу деяких бюджетних призначень, передбачених Міністерству цифрової трансформації на 2021 рік : «Розпорядж. Каб. Міністрів України від 28.04.2021 № 375-р : станом на 17 листоп. 2021 р. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/375-2021-р#Text

11. Azad A. A brief history of electronic document and records management systems and related standards – US: Auerbach Publications, 2007. – P. 260

12. Карпенко М. Ю. Системи електронного документообігу : конспект лекцій для студентів усіх форм навчання першого (бакалаврського) рівня вищої освіти спеціальності 122 – Комп’ютерні науки / М. Ю. Карпенко; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2021. – 68 с.

13. William B. Introduction to Electronic Document Management Systems – US: Academic Press, 2015. – P. 268

14. Асеєв Г.Г. Електронний документообіг – К.: Кондор, 2007. – 500 с.

15. ТУ 30.0-33240054- 001:2005: «Система електронного документообігу органу виконавчої влади» в редакції зі змінами, внесеними Наказом Держзв'зку від 10.04.2006 №52. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://ips.ligazakon.net/document/FIN14540

16. Hee K. V Workflow Management: Models, Methods, and Systems – US: MIT Press, 2004. – P. 384

17. Chang J. F. Business Process Management Systems: Strategy and Implementation – US:. Taylor & Francis Group, 2006. – P. 303

18. Що таке хмарні технології: визначення, важливість та застосування [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://wezom.com.ua/ua/blog/scho-take-hmarni-tehnologiyi-viznachennya-vazhlivist-ta-zastosuvannya

19. Хмарна піраміда: IaaS, PaaS та SaaS [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://gigacloud.ua/blog/navchannja/hmarna-piramida-iaas-paas-i-saas

20. What’s the Difference between Public, Private, Hybrid, and Community Clouds [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.aba-cusnext.com/blog/whats-difference-between-public-private-hybrid-and-community-clouds/

21. Електронний документообіг: види систем та їхні функції [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://dealssign.com/blog/elektronnij-dokumentoobig-vidi-sistem-ta-yixni-funkciyi/

22. Найпопулярніші сервіси електронного документообігу [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://yur-gazeta.com/publications/practice/inshe/naypopulyarnishi-servisi-elektronnogo-dokumentoobigu.html

23. Електронний документообіг: системи, види, особливості впровадження та як він працює в Україні [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://inbase.com.ua/elektronnyj-dokumentoobig-systemy-vydy-osoblyvosti-vprovadzhennya-ta-yak-vin-praczyuye-v-ukrayini/

24. Горбенко Ю.І. Інфраструктури відкритих ключів. Електроний цифровий підпис. Теорія та практика / Горбенко І.Д. – Х.: Форт, 2010. – 608 с.

25. Mammeri Z. Z. Cryptography: Algorithms, Protocols, and Standards for Computer Security – US: Wiley & Sons, 2023. – P. 624

26. Електронний цифровий підпис [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://dealssign.com/blog/elektronnij-cifrovij-pidpis/

27. Закон України «Про електронну ідентифікацію та електронні довірчі послуги», від 05.10.2017 № 2155-VIII : станом на 18 груд. 2024 р. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

28. Про використання апаратних носіїв ключової інформації систем криптографічного захисту інформації : Лист Нац. банку України від 10.12.2010 № 24-112/2550-22346 [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/v2550500-10#Text

29. ДСТУ 4145-2002 Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння [Текст] : Інформаційні технології. – К. : Держспоживстандарт, 2003. – 31 с.

30. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII : станом на 18 груд. 2024 р. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

31. Електронний документообіг та захист інформації: навч. посіб./ О.Б. Кукарін / За заг. ред. д.держ.упр., професора Н.В. Грицяк – К.: НАДУ, 2015. – 84 с

ДОДАТОК А

Перелік форматів даних електронних документів постійного і тривалого зберігання

№ з/п	Призначення форматів даних електронних документів	Формати даних електронних документів (розширення)	Обґрунтування	Примітка
1	2	3	4	5
1	Для створення текстових електронних документів	PDF/A-1 (*.pdf)	1. Відкрита специфікація. 2. Стандарт ISO для довгострокового зберігання електронних документів. 3. Масово використовується для обміну інформацією. 4. Наявність поширених програмно-технічних засобів на різних платформах спроможних відтворювати дані цього формату. 5. Самодостатній у відтворенні електронних документів	Формат специфікації PDF 1.4 (ISO 19005-1:2005)
2	Для створення фотоелектронних документів	TIFF (*.tif)	1. Відкрита специфікація. 2. Стандарт ISO. 3. Масово використовується для обміну інформацією. 4. Наявність поширених програмно-технічних засобів на різних платформах 5. Самодостатній у відтворенні електронних документів	Застосовується у варіанті без стиснення, формат специфікації TIFF 6.0 (ISO 12639:2004)
3	Для створення аудіоданих аудіовізуальних електронних документів	FLAC (*.flac)	1. Відкрита специфікація. 2. Стандарт Xiph.Org Foundation. 3. Масово використовується для обміну інформацією. 4. Наявність поширених програмно-технічних засобів на різних платформах спроможних відтворювати дані цього формату. 5. Самодостатній у відтворенні електронних документів	Формат специфікації FLAC Format Specification, 2008

Продовження ДОДАТКА А

1	2	3	4	5
4	Для інкапсуляції даних аудіовізуальних електронних документів	Matroska (*.mkv)	1. Відкрита специфікація. 2. Стандарт WebM. 3. Масово використовується для обміну інформацією. 4. Наявність поширених програмно-технічних засобів на різних платформах (операційних системах і технічних засобах), спроможних відтворювати дані цього формату. 5. Самодостатній у відтворенні електронних документів	Формат специфікації The standard of multimedia container formats Matroska (04/11/2011)
5	Для створення відеоданих аудіовізуальних електронних документів	Реалізація MPEG-4 AVC/H.264 у FFmpeg	1. Відкрита специфікація. 2. Стандарти International Telecommunication Union - Radiocommunications sector (ITU-R) та Moving Picture Experts Group (MPEG). 3. Відкритий код та рекомендації на сайті розробника. 4. Масово використовується для зберігання відеоданих без втрати якості. 5. Відповідає вимогам довгострокового зберігання аудіовізуальних електронних документів: малий вплив (відсутній) на якість зображення навіть за багаторазового застосування; забезпечення простого та швидкого доступу до будь-якого кадру (кожен кадр стискається незалежно від інших). 6. Наявність поширених програмно-технічних засобів на різних платформах, спроможних відтворювати дані цього формату. 7. Самодостатній у відтворенні електронних документів	Застосовується стиснення без втрат, формат специфікацій ISO/IEC 14496-10:2010, ISO/IEC 13818-1:2007/Cor.3:2011, формат рекомендації ITU-T H.264

ДОДАТОК Б

Презентаційний матеріал до магістерської кваліфікаційної роботи

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

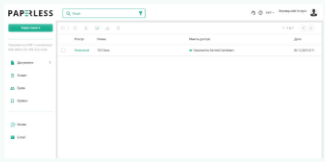
ЗЕРНИЦЬКИЙ БОГДАН МИКОЛАЙОВИЧ

Кваліфікаційна робота
здобувача освітнього ступеня «МАГІСТР»

Тема:

ТЕХНОЛОГІЯ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Спеціальність: 125 – Кібербезпека та захист інформації
Керівник: канд. техн. наук, доц. Андрій КОТЕНКО



Київ – 2025

АКТУАЛЬНІСТЬ РОБОТИ

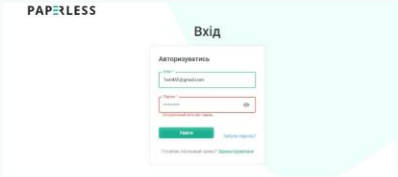
2

- зростання обсягів електронних документів і цифровізація бізнес-процесів
- СЕДО обробляють конфіденційні, фінансові та персональні дані
- кібератаки, фішинг і брутфорс створюють ризики витоку документів
- віддалена робота підвищує вимоги до автентифікації та контролю доступу

Об'єкт дослідження:
методи захисту, можливі для реалізації захисту систем електронного документообігу.

Предмет дослідження:
технології захисту, які забезпечують безпеку в системах електронного документообігу.

Мета кваліфікаційної роботи:
підвищити надійність захисту систем електронного документообігу.



ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

3

1. РОЗДІЛ 1. Проаналізовано електронний документ, електронний документообіг, формати файлів і переваги ЕДО.

2. РОЗДІЛ 2. Досліджено проблематику СЕДО, хмарні технології, WorkFlow, класифікацію систем та основні загрози.

3. РОЗДІЛ 3. Розглянуто СЕДО Paperless і сформовано рекомендації щодо підвищення безпеки доступу, криптографії та моніторингу.

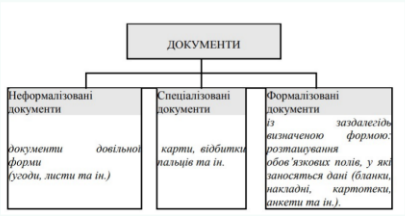
4. ВИСНОВКИ. Обґрунтовано комплекс організаційних і технічних заходів для захисту систем електронного документообігу.

ПЕРШИЙ РЕЗУЛЬТАТ

4

ЕЛЕКТРОННИЙ ДОКУМЕНТ ТА ЙОГО СТРУКТУРА

• електронний документ містить електронні дані та обов'язкові реквізити
• його автентичність і цілісність підтверджуються електронним підписом
• структура включає зміст, реквізити та носій електронного документа



Результат: систематизовано властивості електронного документа як базового об'єкта захисту в СЕДО.

ПЕРШИЙ РЕЗУЛЬТАТ

5

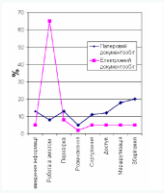
ПЕРЕВЕДЕННЯ ДОКУМЕНТІВ В ЕЛЕКТРОННУ ФОРМУ

Сканування
створення цифрового образу документа та контроль якості зображення

Розпізнавання
перетворення зображення на редагований текст і відновлення форматування

Зберігання
текст, образ або комбінований варіант з можливістю пошуку та архівування

Захист
контроль доступу, цифровий підпис, резервне копіювання та перевірка цілісності

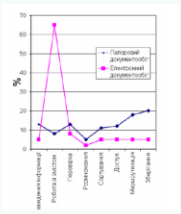


ПЕРШИЙ РЕЗУЛЬТАТ

6

ПЕРЕВАГИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

• скорочення часу обробки, погодження та передавання документів
• централізований пошук, архівування та маршрутизація
• контроль прав доступу до конфіденційних документів
• зниження витрат на паперові ресурси та прискорення управлінських процесів

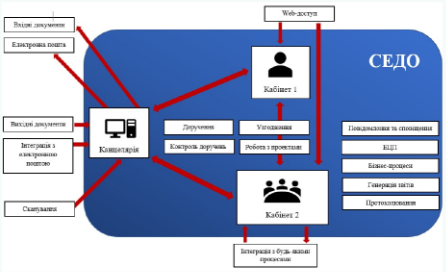


Висновок: ЕДО формує технологічну основу для прозорого, контрольованого та захищеного документообігу.

ДРУГИЙ РЕЗУЛЬТАТ

7

СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ



- **СЕДО автоматизує створення, обробку, маршрутизацію, зберігання та пошук документів**
- **ключовими є кабінети користувачів, канцелярія, повідомлення, ЕЦП та протоколювання**
- **захист залежить від розмежування прав, автентифікації та журналювання дій**

Результат: визначено функціональні компоненти СЕДО та їх зв'язок із забезпеченням інформаційної безпеки.

ДРУГИЙ РЕЗУЛЬТАТ

8

АРХІТЕКТУРА ТА КОМПОНЕНТИ СЕДО

Сховище документів
централізоване зберігання файлів, реквізитів і метаданих

Бізнес-логіка
діловодство, маршрутизація, документообіг і регламентація прав доступу

Архів
довгострокове збереження електронних документів і контроль доступу

9

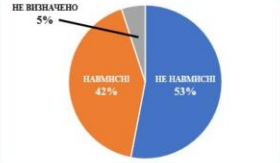
ДРУГИЙ РЕЗУЛЬТАТ

ОСНОВНІ ЗАГРОЗИ ДЛЯ СЕДО

Зовнішні загрози
- **фішинг**
- **брутфорс**
- **шкідливе ПЗ**
- **атаки на веб-доступ**

Внутрішні загрози
- **помилки персоналу**
- **слабкі паролі**
- **порушення регламентів**
- **інсайдерські дії**

Технічні загрози
- **втрата даних**
- **відсутність резервування**
- **помилки доступу**
- **недостатній аудит**



Захист СЕДО повинен охоплювати користувачів, документи, канали доступу, журнали подій і криптографічну інфраструктуру.

10

ДРУГИЙ РЕЗУЛЬТАТ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ТА ЕЛЕКТРОННИЙ ПІДПИС

- ЕЦП підтверджує авторство, цілісність і юридичну значущість електронного документа
- криптографічні алгоритми захищають документ від несанкціонованої модифікації
- перевірка ключів і сертифікатів є обов'язковою умовою довіри до СЕДО

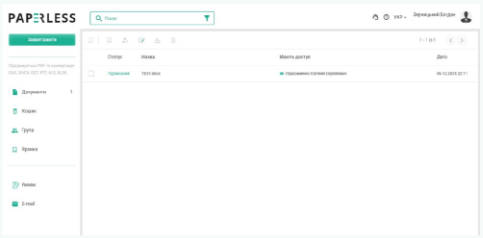
Рівні довіри: простий, удосконалений і кваліфікований електронний підпис.

Висновок: криптографічний механізм є базою довіри до електронного документа та електронного документообігу.

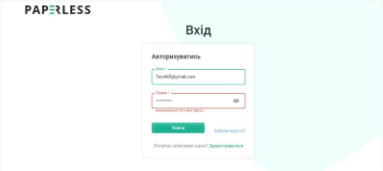
11

ТРЕТІЙ РЕЗУЛЬТАТ

ХАРАКТЕРИСТИКА СЕДО PAPERLESS



- Paperless забезпечує завантаження, підписання, пошук і зберігання документів
- система підтримує групи, умови, e-mail, кошик і роботу з підписаними документами
- веб-доступ потребує посиленого контролю автентифікації та політик безпеки



12

ТРЕТІЙ РЕЗУЛЬТАТ

ПЕРЕВАГИ ТА НЕДОЛІКИ PAPERLESS З ПОГЛЯДУ БЕЗПЕКИ

Переваги
- зручний веб-доступ
- централізоване зберігання
- підтримка підписаних документів
- протоколювання дій

Недоліки
- ризик слабких паролів
- залежність від веб-доступу
- потреба в MFA
- необхідність моніторингу подій

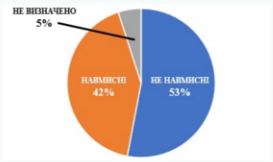
Ключовий висновок: підвищення захисту Paperless повинно поєднувати автентифікацію, криптографію, IP-фільтрацію, резервування та аудит.

13

ТРЕТІЙ РЕЗУЛЬТАТ

РЕКОМЕНДАЦІЇ ЩОДО ВДОСКОНАЛЕННЯ ЗАХИСТУ PAPERLESS

• впровадити багатофакторну автентифікацію для всіх критичних облікових записів
• обмежити доступ дозволеними IP-адресами та VPN-каналами
• посилити криптографічний захист і контроль сертифікатів ЕЦП
• налаштувати журналювання, SIEM-моніторинг і сповіщення про підозрілі події
• проводити навчання користувачів щодо фішингу, паролів і правил роботи з документами



Результат: сформовано комплекс заходів для зменшення ризику витоку документів і несанкціонованого доступу.

14

ВИСНОВКИ

• проаналізовано електронні документи, ЕДО та особливості їх захисту
• визначено функціональні компоненти СЕДО та основні загрози для електронного документообігу
• розглянуто криптографічні методи захисту, ЕЦП та механізми автентифікації
• на прикладі Paperless запропоновано заходи щодо MFA, IP-фільтрації, моніторингу та зниження впливу людського фактора

ДЯКУЮ ЗА УВАГУ!