ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ
ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ
ДІЯЛЬНОСТІ

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: «Методи та технології забезпечення інформаційної безпеки в системах електронного документообігу»

на здобуття освітнього ступеня	бакалавра
зі спеціальності	029 Інформаційна, бібліотечна та архівна справа
освітньо-професійної програми	Інформаційна аналітика та зв'язки з громадськістю

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

_____ Дар'я ШЕВЧУК
(підпис)

Виконала: здобувачка вищої освіти
гр. АЗД-41
Дар'я ШЕВЧУК

Керівник: Алла БУРМАКА
доктор філософії (PhD)

Рецензент: Оксана ПЛУЖНИК
Доктор філософії (PhD), доцент

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра документознавства та інформаційної діяльності
Ступінь вищої освіти бакалавр
Спеціальність 029 Інформаційна, бібліотечна та архівна справа
Освітньо-професійна програма Інформаційна аналітика та зв'язки з громадськістю

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____
_____ Тетяна СИДОРЕНКО
«____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шевчук Дар'ї Сергіївни

1. Тема кваліфікаційної роботи: «Методи та технології забезпечення інформаційної безпеки в системах електронного документообігу»
керівник кваліфікаційної роботи Алла Бурмака
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 р. № 56
2. Строк подання кваліфікаційної роботи «16» травня 2025 р.
3. Вихідні дані до кваліфікаційної роботи
Мета дослідження: дослідити та обґрунтувати ефективні методи забезпечення інформаційної безпеки в системах електронного документообігу.
Об'єктом дослідження є процеси обміну, зберігання та обробки електронних документів.
Предметом дослідження є практичні методи, технології та засоби захисту інформації, що застосовуються у системах електронного документообігу.
4. Перелік питань, які потрібно розробити.
1. Теоретичні засади забезпечення інформаційної безпеки в системах електронного документообігу.
2. Аналіз методів і технологій захисту інформації на прикладі системи АСКОД.
3. Практичні рекомендації щодо підвищення рівня інформаційної безпеки в СЕД.
5. Перелік ілюстративного матеріалу: презентація, 4 рисунки, 1 таблиця
6. Дата видачі завдання «26» вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1	Визначення тематики, вибір наукового керівника, уточнення теми	18.09.2024	
2	Розроблення та складання плану кваліфікаційної бакалаврської роботи	26.09.2024	
3	Підготовка 1 розділу	07.01.2025	
4	Підготовка 2 розділу	22.04.2025	
5	Підготовка 3 розділу	01.05.2025	
6	Висновки	09.05.2025	
7	Підготовка остаточного варіанта роботи	12.05.2025	
8	Написання відгуку науковим керівником	14.05.2025	
9	Оформлення й представлення роботи на кафедру та перевірка на плагіат	16.05.2025	
10	Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія	20.05.2025	
11	Попередній захист роботи	11.06.2025	
12	Основний захист кваліфікаційної бакалаврської роботи	26.06.2025	

Здобувачка вищої освіти _____ Дар’я ШЕВЧУК
(*підпис*)

Керівник
кваліфікаційної роботи _____ Алла БУРМАКА
(*підпис*)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 61 стор., 4 рис., 1 табл., 36 джерел.

Мета роботи – дослідити та обґрунтувати ефективні методи забезпечення інформаційної безпеки в системах електронного документообігу

Об'єкт дослідження – процеси обміну, зберігання та обробки електронних документів.

Предмет дослідження – практичні методи, технології та засоби захисту інформації, що застосовуються для забезпечення конфіденційності, цілісності та доступності даних у системах електронного документообігу.

Короткий зміст роботи: у кваліфікаційній роботі проаналізовано архітектуру СЕД, загрози цілісності даних, роль КЕП та функціонал системи АСКОД. Висвітлено вразливості системи й запропоновано рекомендації щодо підвищення рівня захисту – автентифікація, шифрування, аудит, резервне копіювання та навчання персоналу.

КЛЮЧОВІ СЛОВА: електронний документообіг, інформаційна безпека, система АСКОД, КЕП, криптографічний захист, контроль доступу, загрози, захист даних, Workflow, електронний архів.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСКОД	Автоматизована система контролю і організації діловодства
ПЗ	Програмне забезпечення
ЕД	Електронний документ
ЕДО	Електронний документообіг
КЕП	Кваліфікований електронний підпис
СЕД	Система електронного документообігу

ВСТУП

Актуальність дослідження. У сучасному світі спостерігається активна трансформація суспільства в напрямку цифровізації управлінських процесів, що супроводжується переходом від традиційного паперового документообігу до електронного. У зв'язку з цим актуалізується проблема забезпечення інформаційної безпеки, адже основною складовою будь-якої системи електронного документообігу є саме документ. Зростає потреба не лише у захисті самих документів, але й у забезпеченні стабільного функціонування таких систем, їх швидкого відновлення після збоїв, ушкоджень або кібератак. Захист повинен мати комплексний характер і охоплювати всі рівні – від фізичного захисту носіїв інформації до впровадження організаційних заходів.

Одним із головних викликів сьогодення є ефективне збереження інформації та захист документів від несанкціонованого доступу. Це формує потребу у побудові комплексної системи безпеки для електронного документообігу. Такий захист має включати: безпеку апаратної складової, захист системного програмного забезпечення, файлових структур та баз даних, а також інформації та документів, що циркулюють і зберігаються всередині системи.

Попри значну увагу до теми, питання повного забезпечення інформаційної безпеки в системах електронного документообігу все ще залишається відкритим. Багато організацій не мають у своєму розпорядженні достатніх засобів для ефективного захисту таких систем, що зумовлює порушення в роботі, втрату важливих документів і витік конфіденційних даних унаслідок дій кіберзлочинців.

Значний внесок у вивчення проблем інформаційної безпеки та кіберзахисту зробили такі науковці, як В. М. Нагаєв [18-19], І. Л. Бородкіна [6], І. І. Килимник [12], Ю. Є. Мегель [15-16] та інші. Важливими також є дослідження правових аспектів інформаційної безпеки, зокрема авторів Л. Л. Левченко [14], Л. В. Піддубна [27], В. В. Шемчук [33]. Питання захисту

інформації саме в системах електронного документообігу розглядають у своїх працях Піддубна Л. та Павліченко В. Проведений аналіз літератури засвідчує актуальність обраної теми в умовах сучасних реалій, водночас вказуючи на те, що багато аспектів цієї проблематики ще потребують подальшого вивчення.

Метою кваліфікаційної роботи є дослідження, аналіз та обґрунтування ефективних методів і технологій забезпечення інформаційної безпеки в системах електронного документообігу з метою розробки рекомендацій щодо підвищення рівня захисту інформації в умовах сучасних кіберзагроз.

У процесі виконання кваліфікаційної роботи було поставлено такі основні завдання дослідження:

– виявити основні загрози інформаційній безпеці, що виникають у процесі функціонування систем електронного документообігу;

– узагальнити існуючі підходи, методи та технології забезпечення інформаційної безпеки в системах електронного документообігу;

– дослідити нормативно-правове забезпечення інформаційної безпеки у сфері електронного документообігу в Україні;

– розробити рекомендації щодо вдосконалення комплексного захисту системи електронного документообігу.

Об’єктом дослідження є процеси обміну, зберігання та обробки електронних документів у системах електронного документообігу, а також пов’язані з ними інформаційні відносини в організаціях, що породжують потребу у забезпеченні інформаційної безпеки.

Предметом дослідження у роботі є практичні методи, технології та засоби захисту інформації, що застосовуються для забезпечення конфіденційності, цілісності та доступності даних у системах електронного документообігу.

Дослідження здійснювалося на принципах науковості, об’єктивності із послуговуванням методами: загальнонауковими (логіки, аналізу, синтезу, індукції, дедукції) та спеціальними – структурно-функціонального аналізу, контент-аналізу, наративного, узагальнення. Для підвищення ефективності

роботи було залучено технології штучного інтелекту, зокрема допомагали у пошуку релевантних джерел, систематизації даних та формуванні окремих текстових блоків. Важливо зазначити, що використання штучного інтелекту відбувалося з дотриманням академічних норм, а кінцевий результат, включаючи аналіз та висновки, повністю належить автору дослідження.

Наукова новизна проведеного дослідження полягає в уточненні та подальшому розвитку підходів до забезпечення інформаційної безпеки в системах електронного документообігу.

У межах дослідження удосконалено систему класифікації загроз для електронного документообігу з позиції потенційного впливу на цілісність, конфіденційність і доступність документів. Також дістав подальший розвиток підхід до оцінювання вразливостей систем електронного документообігу, що враховує не лише технічні, а й організаційні чинники.

Особистий внесок автора полягає в аналізі практичних кейсів порушення інформаційної безпеки, розробці узагальненої моделі захисту електронного документообігу та формуванні комплексу рекомендацій щодо посилення захисту на апаратному, програмному та організаційному рівнях.

Отримані результати дослідження можуть бути використані в IT-відділах підприємств та установ, що впроваджують або вже використовують системи електронного документообігу, для підвищення рівня інформаційної безпеки. Запропоновані заходи можуть стати основою для розробки внутрішніх політик безпеки, удосконалення інструкцій для персоналу, а також для вибору або проєктування технічних і програмних засобів захисту відповідно до реальних умов функціонування організацій.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, загального висновку та переліку посилань. Загальний обсяг роботи склав – 61 сторінка, включаючи 36 використаних посилань, 1 таблицю та 4 рисунки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1.1. Інформаційна безпека як складова загальної системи безпеки інформаційних технологій

Починаючи з кінця XX століття, спостерігається стрімке розширення сфер використання комп'ютерних мереж, а також зростання кількості користувачів як у локальних мережах, так і в глобальному середовищі Інтернету. Це спричиняє зниження рівня захищеності інформації, що зберігається на клієнтських та серверних частинах мережевої інфраструктури організацій та установ.

Одним із ключових напрямів використання комп'ютерних мереж останніми роками стало впровадження в органи державної влади й управління систем електронного документообігу. Такі системи безпосередньо впливають на надійність і безпеку діяльності, оскільки інформація, яка зберігається й опрацьовується в цих системах, має стратегічне значення для функціонування державних структур. Водночас ефективність їх роботи значною мірою залежить від рівня інформаційної безпеки [6, с. 110].

Розвиток цифрових технологій, підвищення вартості інформаційних активів і необхідність їх захисту обумовлюють актуальність теми. Захист даних у системах електронного документообігу на сьогодні постає як одна з ключових проблем у сфері інформаційної безпеки.

Забезпечення безпеки інформаційних технологій є одним із найважливіших завдань сучасного суспільства, що зумовлено стрімким розвитком інформаційних систем, поширенням кіберзагроз та зростаючою залежністю різних сфер діяльності від функціонування цифрових даних. Загальна система безпеки інформаційних технологій є багатогранним і комплексним явищем, що охоплює сукупність організаційних, технічних, правових та програмних заходів, спрямованих на захист інформаційних

ресурсів від несанкціонованого доступу, використання, розголошення, спотворення, модифікації, знищення або відмови в обслуговуванні. У цьому контексті інформаційна безпека виступає як фундаментальна та невід'ємна складова, що забезпечує реалізацію основних принципів захисту інформації на всіх рівнях її життєвого циклу [26].

Законодавчою основою, що регулює захист інформації в українських комунікаційних мережах, є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [1], прийнятий у січні 2006 року. До цього закону, підходи до захисту інформації в системі визначалися як діяльність, що забезпечувала запобігання несанкціонованому доступу до неї. Термін «об'єкт захисту в інформаційній системі», згідно з інтерпретацією О. Нішанбаєва та Ф. Рахімова, позначає структурний компонент системи, який містить або може містити інформацію, що підлягає захисту.

Такий об'єкт повинен відповідати наступним критеріям:

– бути частиною організаційного компонента системи;

– здійснювати обробку інформації, що включає обробку людиною або автоматизовану обробку;

– мати локалізацію (обмеження) з точки зору просторового розташування в системі.

Таким чином, в комп'ютерній системі об'єктом захисту є будь-яка документована інформація, неправомірне володіння, використання або розголошення якої може завдати шкоди її власнику, користувачу або іншим особам. Передусім, це стосується такої інформації, що є власністю держави, конфіденційної документованої інформації, інформації з обмеженим доступом, даних, що вимагають захисту згідно із законом, а також персональних даних, що зберігаються в інформаційних системах.

Відповідно до положень Закону, захист інформаційних систем вимагає створення інтегрованої системи безпеки, що включає використання засобів, які пройшли сертифікацію відповідності або отримали позитивний висновок державної експертизи у сфері технічного та/або криптографічного захисту

інформації. Цей нормативний акт розмежовує два ключові напрями забезпечення безпеки інформації: технічний та криптографічний.

Технічний захист інформації охоплює сукупність інженерно-технічних заходів, а також програмних і апаратних засобів, спрямованих на запобігання несанкціонованому витоку, знищенню, блокуванню, порушенню цілісності та режиму доступу до інформації [7].

Криптографічний захист інформації – це метод захисту, що реалізується шляхом перетворення інформації за допомогою спеціальних (ключових) даних. Його основна мета полягає у приховуванні або відновленні змісту інформації, а також у підтвердженні її автентичності, цілісності та авторства.

У процесі розробки та вдосконалення систем захисту інформації, Ж. Солдером та М. Шредером були сформульовані та узагальнені певні універсальні вимоги, які слугують основою для їх побудови.

Захист інформації в системах електронного документообігу, що є однією з форм колективних інформаційних систем, слід розглядати як комплексний набір методів та інструментів. Їхнє призначення полягає у забезпеченні цілісності, конфіденційності, достовірності, автентичності та доступності (можливості використання) інформації в умовах потенційних загроз як природного, так і штучного походження [32, с. 72].

Постійне використання ефективних засобів та методик захисту даних сприяє досягненню необхідного рівня надійності інформації, яка зберігається та обробляється в системі електронного документообігу. При цьому надійність інформації в контексті електронного документообігу є інтегральним показником, що відображає якість інформації з таких позицій:

– фізична цілісність, що означає відсутність спотворень чи знищення будь-яких складових інформації;

– довіра до інформації (автентичність), яка гарантує відсутність несанкціонованих змін чи підміни елементів інформації, зберігаючи її первісну цілісність;

– захищеність інформації (конфіденційність), що забезпечує недопущення несанкціонованого доступу до інформації особами або процесами, які не мають відповідних дозволів;

– запобігання неправомірному копіюванню, тобто иключає можливість несанкціонованого розмноження інформаційних ресурсів.

Ефективний захист інформації в системі електронного документообігу можливий лише за умови гарантування її надійності на всіх рівнях та елементах системи, що потенційно можуть бути піддані впливу дестабілізуючих факторів.

Комплексність завдань із забезпечення інформаційної безпеки в системах електронного документообігу обумовлена низкою важливих чинників. У сучасних умовах функціонування електронних систем документообігу висуваються надзвичайно високі вимоги до забезпечення цілісності програмного забезпечення. Йдеться як про системне, так і прикладне програмне забезпечення, яке повинне працювати без збоїв і гарантувати надійне збереження та обробку даних. Окрім того, особливої уваги потребує цілісність електронних документів — довідкових, статистичних, звітних матеріалів, інструкцій тощо, які зберігаються та циркулюють у межах електронної системи. Враховуючи активне впровадження безпаперових технологій, постає потреба в офіційному підтвердженні юридичної значущості таких електронних документів, що дає їм силу нарівні з паперовими аналогами.

Особливістю сучасних інформаційних систем є їхній розподілений характер, що передбачає використання ресурсів різними категоріями користувачів. У зв’язку з цим виникає потреба у чіткому розмежуванні прав доступу до інформації та забезпеченні надійного контролю за її використанням з точки зору інформаційної безпеки. Крім того, у багатьох випадках зміст електронних документів повинен залишатися конфіденційним, що вимагає реалізації механізмів його приховування. В окремих ситуаціях потрібно забезпечити навіть повну неможливість несанкціонованого

копіювання чи розповсюдження інформації, що ще більше підкреслює актуальність заходів інформаційного захисту в таких системах.

Таким чином, усі механізми, призначені для захисту інформації, так чи інакше регулюють, забороняють або обмежують користувачам можливість доступу до певної інформації. У свою чергу, інформаційна безпека розглядається як стан захищеності інформації, що забезпечує її конфіденційність, цілісність та доступність, а також стійкість до загроз різного походження. Конфіденційність інформації означає її захист від несанкціонованого ознайомлення, розголошення або отримання доступу сторонніми особами. Це передбачає обмеження доступу до даних лише для авторизованих користувачів та процесів [19, с. 31].

Цілісність інформації гарантує її повноту, достовірність та незмінність протягом усього життєвого циклу, виключаючи несанкціоновану модифікацію або знищення. Це охоплює як захист від навмисних спотворень, так і від випадкових помилок. Доступність інформації передбачає можливість отримання доступу до неї авторизованими користувачами в необхідний час і за необхідних обставин, а також безперебійне функціонування інформаційних систем.

Інформаційна безпека не є самодостатньою одиницею, а органічно інтегрується в загальну систему безпеки, яка, своєю чергою, включає:

– захист фізичних об'єктів, де зберігається та обробляється інформація (сервери, мережеве обладнання, носії інформації) від крадіжок, пожеж, стихійних лих та інших фізичних загроз;

– розробку та впровадження політик, процедур та регламентів, що регулюють доступ до інформації, її обробку, зберігання та передачу. Це включає розподіл обов'язків, управління персоналом, навчання співробітників, аудит та моніторинг;

– застосування спеціалізованих програмних та апаратних засобів для захисту інформаційних систем. До них належать міжмережеві екрани, антивірусне програмне забезпечення, системи виявлення та запобігання

вторгненням (IDS/IPS), криптографічні засоби, системи управління ідентифікацією та доступом (IAM) тощо;

– дотримання законодавчих та нормативних актів, що регулюють захист інформації, включаючи закони про захист персональних даних, комерційної таємниці, авторського права, а також норми кіберзлочинності.

Взаємодія цих компонентів забезпечує багатошаровий захист, де інформаційна безпека відіграє центральну роль, оскільки вона визначає принципи та методи захисту саме інформації, що є найціннішим активом у цифровому середовищі. Без ефективної інформаційної безпеки, навіть при наявності міцної фізичної та організаційної захищеності, дані залишаються вразливими до логічних атак, несанкціонованих маніпуляцій та кібершпигунства [18].

Таким чином, інформаційна безпека є досить важливим елементом загальної системи безпеки інформаційних технологій, що забезпечує безперервність бізнес-процесів, довіру до інформації та сталий розвиток у цифрову епоху. Захист інформації сьогодні є невід'ємною частиною стратегічного управління будь-якої організації та держави в цілому.

1.2. Електронний документ як ключовий об’єкт захисту в інформаційних системах

Основою інформаційно-аналітичного забезпечення функціонування будь-якої організації є насамперед обробка документів, які потребують створення, фіксації та систематизації в певному форматі. Документи знаходять своє застосування в широкому спектрі галузей знань, сферах людської діяльності та суспільного життя. Вони є предметом дослідження різноманітних наукових дисциплін, що робить термін "документ" багатогранним, і його тлумачення залежить від конкретного контексту та мети використання [16, с. 32].

Згідно зі статтею 1 Закону України «Про інформацію» [3], документ визначається як матеріальний носій, що містить інформацію. Його ключові функції полягають у забезпеченні її збереження та передачі крізь час і простір. В інших джерелах поняття «документ» розглядається як структурована інформаційна одиниця, призначена для сприйняття людиною. Вона оформлюється та фіксується на матеріальному носії відповідно до встановлених правил, з дотриманням визначеної форми представлення та наявністю обов'язкових атрибутів:

– функціональність, що передбачає визначений вплив документа (включно з подальшими діями) на його одержувачів після ознайомлення зі змістом, що відповідає існуючим суспільним відносинам;

– санкціонованість, яка вказує на визначену фізичну та/або юридичну особу, відповідальну за існування документа в певний момент часу;

– реєстрованість, що забезпечує унікальну ідентифікацію документа серед інших документів.

Стаття 5 Закону України «Про електронні документи та електронний документообіг» [2] визначає електронний документ (ЕД) як документ, інформація в якому представлена у вигляді електронних даних. Він містить обов'язкові реквізити, склад та порядок розташування яких встановлюється законодавством. ЕД може бути створений, переданий, збережений та трансформований за допомогою електронних засобів у візуальний формат, що відображає його зміст, або ж перетворений на паперову форму, придатну для сприйняття людиною. Дані, що становлять обов'язкові реквізити ЕД, є критично важливими, оскільки без них документ не може бути врахований для обліку та не матиме юридичної сили.

Як і будь-який інший тип документації, електронний документ має власну структуру, яка поділяється на внутрішню та зовнішню. Внутрішня структура охоплює основний зміст документа – текстову чи інформаційну частину, тоді як зовнішня описує технічне середовище, у якому функціонує електронний документ. Таким середовищем можуть бути носії інформації

(наприклад, жорсткий диск, флеш-пам’ять), формат електронного файлу або інші параметри представлення даних.

Суттєвою особливістю є те, що електронний документ містить не лише основну інформацію, а й метадані, тобто відомості, що характеризують або описують ці дані. Метадані виконують роль «інформації про інформацію» і забезпечують глибше розуміння основного змісту документа. У сучасних інформаційних архівах значна частка роботи зосереджена саме на формуванні метаданих, адже вони є ключовим інструментом для ефективного пошуку, аналізу та інтерпретації збережених матеріалів.

Метадані також відіграють важливу роль у підтриманні достовірності та цілісності електронного документа. Вони гарантують, що зміст не було змінено, і дозволяють ідентифікувати автора, перевірити справжність та дату створення документа. Такі ознаки є надзвичайно важливими для дослідників, користувачів і правових структур. Свідчення цілісності та справжності можуть мати різний характер – юридичний, організаційний, діловий або процедурний.

Таким чином, метадані становлять невід’ємну частину електронного документа і слугують основою для його зберігання, відтворення та легітимного використання в різних сферах діяльності.

Електронний документ, безумовно, має специфічні особливості, що виокремлюють його серед інших форм документації. До ключових характеристик, які визначають його унікальність, можна віднести наступні аспекти:

– електронний документ є залежним від програмного та технічного забезпечення, тобто його функціональність та доступність напряму пов’язані з конкретними технологічними рішеннями;

– він здатен відображати різноманітні типи інформації – від традиційного тексту до графіки, електронних таблиць, структур баз даних і навіть мультимедійних елементів;

– можливість фрагментації вмісту, коли документ фізично зберігається не як єдиний файл, а розділений на частини (наприклад, у вигляді записів у базі даних);

– електронний документ може містити зовнішні гіперпосилання або зв'язки з іншими ресурсами, які не контролюються автором. Це можуть бути файли з Інтернету чи елементи з корпоративних баз даних, які мають обмежений період доступності [26].

Ще однією важливою ознакою є зберігання електронних документів на матеріальних носіях (магнітні диски, флеш-пам'ять, оптичні носії тощо), які з плином часу можуть втрачати працездатність унаслідок технічних пошкоджень, впливу зовнішніх чинників або змін у програмному забезпеченні.

Що стосується класифікації електронних документів, існує кілька підходів до їхнього поділу. Один з міжнародно визнаних стандартів – ISBD (International Standard Bibliographic Description), тобто Міжнародний стандартний бібліографічний опис. Це набір уніфікованих правил, розроблених Міжнародною федерацією бібліотечних асоціацій та установ (IFLA), який призначений для систематичного оформлення бібліографічних записів та каталогів. Цей підхід дозволяє описувати будь-який тип інформаційного ресурсу незалежно від його носія чи форми представлення [35].

Електронний документ набуває статусу оригіналу лише за умови, що його електронна версія містить усі передбачені законодавством реквізити, зокрема – кваліфікований електронний підпис (КЕП) автора. Водночас варто зауважити, що роздрукований на папері примірник такого документа не визнається оригіналом. Це означає, що документ зберігає статус оригінального лише тоді, коли він існує у цифровому форматі.

Відповідно до положень статті 7 Закону України «Про електронні документи та електронний документообіг» [2], оригінал електронного документа повинен містити можливості для підтвердження його автентичності

та цілісності згідно з вимогами чинного законодавства. У передбачених законом випадках такий документ може бути пред'явлений у вигляді візуального подання, зокрема у формі роздрукованої копії.

Окрему увагу слід приділити питанню збереження цілісності електронних документів, які передаються на архівне зберігання. У контексті архівної справи цілісність електронного документа виконує роль доказу того, що його зміст відповідає оригінальному варіанту, без змін чи втрат; зафіксований час створення або передачі відповідає фактичному часу дії та авторство документа підтверджується особою, яка вказана як його створювач або відправник. Тому забезпечення цілісності архівного електронного документа є необхідною умовою його юридичної достовірності та належного збереження в архівних установах.

Крім того, під автентичністю електронного документа розуміється підтвердження того, що поданий документ є цілісним, містить усі необхідні складові та не був змінений сторонніми особами без належних повноважень.

У ході таких технічних процесів, як перенесення, конвертація або адаптація документа до нових версій програмного забезпечення чи технічних платформ, існує ризик порушення його первинної структури. Це, своєю чергою, може призвести до втрати цілісності документа та поставити під сумнів його достовірність у майбутньому [33, с. 290].

Обов'язковим елементом електронного документа є електронний підпис. Його основне призначення – засвідчення особи автора або підписувача документа для інших учасників системи електронного документообігу, а також підтвердження цілісності самого документа. Завершальною дією при створенні електронного документа є накладення кваліфікованого електронного підпису (КЕП). Варто підкреслити, що саме КЕП визнається юридично рівноцінним до власноручного підпису або печатки. Інші різновиди електронного підпису не мають такої правової сили.

У випадку надсилання документа кільком адресатам або його збереження на кількох носіях, кожна версія, яка відповідає цим критеріям,

визнається оригіналом. Якщо ж документ існує одночасно у цифровому та паперовому форматах і має ідентичний зміст і реквізити, обидва примірники визнаються оригіналами з рівною юридичною силою. Електронна копія повинна бути засвідчена відповідно до вимог чинного законодавства. У разі створення паперової копії електронного документа, вона має містити його точне візуальне відображення та бути засвідченою згідно з установленим порядком.

Статус електронного документа визначається за спеціальним реквізитом, що може позначати:

– версію, тобто варіант документа на етапі підготовки, який містить часткові зміни;

– оригінал – перший офіційний примірник документа, чинність якого зафіксована під час реєстрації;

– дублікат, що має ту саму юридичну силу, що й оригінал;

– копію, тобто повне відтворення змісту та реквізитів оригіналу;

– витяг – частковий варіант документа, що містить обмежений обсяг структурної та змістової інформації.

У сучасних умовах практично кожна установа або підприємство активно використовує електронні документи. Вони можуть містити як відкриту, загальнодоступну інформацію, так і конфіденційні відомості. Часто технологічна, комерційна та виробнича інформація має високу цінність, і її втрата або витік можуть завдати суттєвих фінансових збитків.

З розвитком систем електронного документообігу питання інформаційної безпеки стає дедалі актуальнішим. Для захисту цифрових документів від несанкціонованого доступу, модифікацій або втрати необхідно впроваджувати комплекс організаційних і технічних рішень.

Загрози інформаційній безпеці можуть виникати як через навмисні дії зловмисників, так і через людські помилки чи природні катастрофи.

Ці ризики класифікуються на три основні групи:

1. Порушення конфіденційності.

2. Порушення цілісності.

3. Порушення доступності інформації.

Для запобігання таким загрозам застосовуються спеціалізовані методи та інструменти: програмні засоби, технічні рішення, правові регламенти, організаційні механізми та фізичні заходи безпеки. Найпоширенішим способом збереження конфіденційності є шифрування, яке перетворює відкриту інформацію у захищену форму з використанням криптографічних алгоритмів. Крім захисту від несанкціонованого доступу, шифрування також дозволяє забезпечити достовірність джерела даних і цілісність інформації [12, с. 54].

Ефективність алгоритму шифрування залежить від його криптостійкості. Ідеальним вважається варіант, коли зусилля, час і ресурси, необхідні для злому шифру, не виправдовують цінність отриманої інформації або коли дані втрачають актуальність до моменту розшифрування.

Одним із найпростіших способів захисту цифрових документів є використання вбудованих функцій безпеки в Microsoft Office. Наприклад, можна встановити пароль на відкриття документа, що дозволить отримати доступ лише після введення коду. Також можна обмежити редагування, дозволяючи лише перегляд без змін, або використати цифровий підпис, який автоматично видаляється, якщо в документ вносяться правки.

Проте ці функції мають певні обмеження – наприклад, цифрові підписи Microsoft Office несумісні між різними версіями (Word 2010 не читається у Word 2007 і навпаки), що знижує універсальність їх застосування. Крім того, в деяких країнах через експортні обмеження постачаються версії Office із зменшеною довжиною ключів шифрування, що знижує їхню надійність [23, с. 231].

Архіватори, такі як WinRAR, також надають можливість зашифрувати архівований файл. У версії WinRAR 5 використовується AES-256 шифрування, яке робить підбір пароля надзвичайно складним і

ресурсомістким. У попередніх версіях застосовувалося шифрування AES-128, що є менш захищеним.

Для більш надійного захисту електронної інформації існують сторонні криптографічні програми. Однак експерти звертають увагу на ризики, пов’язані з програмами із закритим вихідним кодом – у них потенційно можуть бути «закладки» або вразливості, залишені розробниками. Одним із популярних рішень із відкритим кодом є TrueCrypt – безкоштовна програма, яка використовує стійкі алгоритми шифрування та дозволяє створювати захищені файлові контейнери.

Принцип роботи TrueCrypt полягає у створенні віртуального шифрованого диска, який функціонує як звичайний логічний диск у системі. Всі операції з файлами відбуваються автоматично і непомітно для користувача, що забезпечує як зручність, так і безпеку. Контейнер може бути замаскований під будь-який тип файлу, наприклад, відео або зображення. Крім того, програма підтримує створення прихованих томів у незайнятому просторі, що значно ускладнює виявлення самого контейнера. Завдяки цьому навіть при наявності доступу до комп’ютера сторонні особи не зможуть довести, що конкретний файл є шифрованим сховищем [23, с. 231].

1.3. Огляд та аналіз функціональних характеристик систем електронного документообігу

Електронний документообіг (ЕДО) – це система організації роботи з документами, яка передбачає їх створення, обмін, підписання та зберігання в цифровій формі, без використання паперових носіїв. Такий підхід забезпечує ефективне управління документопотоками, значно прискорює процеси погодження та затвердження, а також зменшує витрати на папір і архівне зберігання.

Серед ключової переваги ЕДО є оперативність і автоматизація. Документи можуть миттєво надсилатися на підпис чи узгодження,

відстежуватися в реальному часі, а також автоматично проходити задані маршрути погодження. Крім того, цифровий документообіг суттєво підвищує рівень інформаційної безпеки та робить систему управління документами зручною й прозорою. Для реалізації ЕДО використовують спеціалізоване програмне забезпечення, яке дозволяє організовувати захищене середовище для обробки документів. Такі рішення забезпечують не лише збереження та передачу даних, але й їх автентифікацію, контроль доступу та аудит дій користувачів.

Система електронного документообігу – це програмна платформа або хмарний сервіс, який допомагає організаціям керувати повним циклом роботи з електронними документами. Вона включає інструменти для їх створення, пересилання, підписання за допомогою електронного цифрового підпису (КЕП), збереження та моніторингу статусу на кожному етапі.

Такі системи також оснащені функціоналом для автоматизації рутинних задач: встановлення маршрутів проходження документів, нагадування про терміни виконання, надсилання сповіщень, механізми погодження та затвердження. Усе це дозволяє значно підвищити продуктивність і зменшити людський фактор в управлінні документацією.

У сучасному інформаційному суспільстві, що характеризується постійним зростанням обсягів даних та необхідністю їх ефективного управління, системи електронного документообігу набувають ключового значення для забезпечення безперебійної діяльності організацій усіх форм власності та державних установ. СЕД є складними програмно-апаратними комплексами, що дозволяють автоматизувати процеси створення, обробки, зберігання, пошуку та передачі документів у цифровому форматі, забезпечуючи при цьому їхню юридичну значущість та безпеку.

Захист інформації в системах електронного документообігу, що є одним з різновидів інформаційних систем колективного використання, слід розуміти як інтегрований комплекс методів та засобів, які гарантують цілісність, конфіденційність, достовірність, автентичність та доступність (тобто

можливість використання) інформації, незалежно від природних чи штучних загроз. Постійне застосування таких засобів та методів забезпечує необхідну надійність даних, що зберігаються та обробляються в СЕД.

Складність завдань із забезпечення інформаційної безпеки в СЕД зумовлена низкою важливих чинників, зокрема необхідності забезпечення бездоганної цілісності як системного, так і прикладного програмного забезпечення; потребі у високій цілісності електронних документів (довідкових, статистичних, звітних, інструкцій тощо), що зберігаються в системі; юридичній значущості електронних документів: розподілене використання ресурсів; розподіленому характері використання ресурсів СЕД обумовлює необхідність забезпечення інформаційної безпеки на рівні чіткого розмежування доступу до даних та в тому, що значна частина електронних документів потребує гарантій безпеки на рівні приховування їхнього змісту, а в окремих випадках – і повного недопущення несанкціонованого розмноження [5].

Функціональні можливості сучасних систем електронного документообігу (СЕД), без сумніву, є одним із визначальних факторів при їх виборі та успішному впровадженні. По-перше, слід зазначити, що основний функціонал таких систем охоплює управління документами. Це включає можливість створення нових документів, їх реєстрацію з автоматичним присвоєнням унікального ідентифікатора, заповнення реквізитів та фіксацію автора. Електронний документ, у свою чергу, може бути не лише створений і збережений у цифровій формі, але й трансформований у паперовий вигляд. Водночас, важливо підкреслити, що документ має містити обов’язкові реквізити, без яких він не набуде юридичної сили.

По-друге, сучасні СЕД забезпечують надійне централізоване зберігання документів, підтримку резервного копіювання та ведення версійності. Це дозволяє зберігати історію змін, відновлювати попередні варіанти документів і дотримуватись нормативних вимог щодо архівування. Крім того, системи зазвичай оснащені потужними інструментами пошуку – контекстного,

атрибутивного та повнотекстового, що значно полегшує доступ до необхідної інформації. Не менш важливою є можливість індексації документів за різноманітними критеріями, їх класифікації за типами, проєктами чи категоріями.

По-третє, варто відзначити управління потоками робіт, яке передбачає автоматизовану або напівавтоматизовану маршрутизацію документів між співробітниками та підрозділами відповідно до встановлених бізнес-процесів. До таких процесів належать узгодження, візування, підписання, виконання чи ознайомлення. При цьому здійснюється постійний моніторинг статусу документів, контроль термінів виконання завдань та надсилання нагадувань у разі прострочення. Також підтримується можливість реалізації як послідовних, так і паралельних маршрутів обробки документів.

По-четверте, надзвичайно важливим аспектом є забезпечення юридичної значущості та безпеки документів. Тут йдеться про інтеграцію з системами кваліфікованого електронного підпису (КЕП), що дозволяє ідентифікувати підписувача та перевірити цілісність документа. Крім того, реалізується гнучка система управління доступом до документів на основі ролей, груп або індивідуальних налаштувань користувачів. Ведення детальних журналів усіх дій забезпечує прозорість та можливість проведення аудитів або розслідувань у разі виникнення інцидентів. До цього додаються й технічні та криптографічні засоби захисту, що запобігають витоку, втраті або порушенню інформації.

По-п’яте, не можна оминути увагою інтеграційні можливості СЕД. Зокрема, важливою є здатність взаємодіяти з іншими корпоративними системами, такими як ERP, CRM чи бухгалтерське програмне забезпечення, що створює єдиний інформаційний простір підприємства. Більш того, дотримання міжнародних та національних стандартів, як-от ДСТУ ISO/IEC 27001:2015, гарантує відповідність вимогам інформаційної безпеки.

І, нарешті, сучасні СЕД пропонують низку додаткових функцій, які підвищують їх зручність та функціональність. Наприклад, доступ до системи

через мобільні додатки дозволяє користувачам працювати з документами в будь-який час і з будь-якого місця. Також важливими є функції створення звітів щодо руху документів, ефективності процесів та завантаженості персоналу. Не менш корисною є підтримка багатомовного інтерфейсу, що робить систему зручною для використання в багатонаціональних організаціях. Саме тому функціональні можливості СЕД охоплюють широкий спектр завдань і суттєво впливають на якість організації електронного документообігу, безпеку інформації та загальну ефективність управлінських процесів [29].

Системи електронного документообігу можна класифікувати за різними критеріями, тому класифікацію було подано у табл. 1.1.

Таблиця 1.1

Класифікація систем електронного документообігу

Критерій класифікації	Типи СЕД	Опис
За масштабом використання	– Корпоративні – Локальні	Корпоративні для великих організацій із розгалуженою структурою. Локальні для невеликих підприємств або окремих підрозділів.
За типом реалізації	– Клієнт-серверні – Веб-орієнтовані	Клієнт-серверні потребують встановлення на сервер і робочі місця. Веб-системи – працюють через браузер.
За функціональним призначенням	– Універсальні – Спеціалізовані	Універсальні – підтримують широкий спектр завдань та типів документів. Спеціалізовані для окремих галузей або видів документообігу.
За способом впровадження	– Хмарні – Локальні	Хмарні працюють через інтернет без встановлення на локальні сервери. Локальні – потребують власної IT-інфраструктури.
За рівнем автоматизації	– З ручним управлінням – З частковою автоматизацією – З повною автоматизацією	Від простих систем з базовими функціями до повноцінних рішень, що автоматизують всі етапи життєвого циклу документа.

Здійснена класифікація систем електронного документообігу дозволяє зробити висновок, що вибір СЕД має ґрунтуватися на цілому ряді факторів, серед яких – масштаб діяльності організації, технічні можливості, потреба в

автоматизації, галузева специфіка та рівень інтеграції з іншими інформаційними системами.

Розподіл систем за критеріями дає змогу чітко структурувати ринок програмного забезпечення в цій сфері та допомагає організаціям обирати оптимальні рішення відповідно до власних завдань. Наприклад, великі корпорації з розгалуженою структурою надають перевагу корпоративним, універсальним СЕД з повною автоматизацією, тоді як малі підприємства можуть ефективно використовувати локальні або хмарні рішення з базовим функціоналом [27, с. 62].

Таким чином, класифікаційний підхід дозволяє не лише зрозуміти функціональні особливості різних типів СЕД, а й забезпечити обґрунтованість при прийнятті управлінських рішень щодо їх впровадження.

Системи електронного документообігу також класифікують на зовнішні та внутрішні.

Системи для зовнішнього електронного документообігу – це IT-рішення для обміну ЕД з контрагентами, партнерами, клієнтами та підрядниками і підписання цих документів за допомогою КЕП.

Системи для внутрішнього електронного документообігу – це програми для обміну електронними документами всередині компанії. До таких документів належать накази, заяви, інструкції, службові записки, статути, протоколи, положення підрозділів тощо. Всі їх можна створювати та редагувати у системі, автоматично узгоджувати, швидко шукати та зручно зберігати у захищеному архіві [22, с. 92].

Зазвичай, зовнішні та внутрішні системи можна інтегрувати, щоб увесь документообіг компанії вівся в одному інформаційному середовищі. Також системи автоматизації електронного документообігу можна класифікувати за такими типами:

1. Діловодство – класична система зовнішнього документообігу для обміну документами між контрагентами.

2. Workflow – це система, що дозволяє налаштувати, автоматизувати й координувати виконання бізнес-процесів компанії, пов’язаних із документами.

3. Архівне зберігання для зберігання ЕД у захищених архівах з різним рівнем доступу і з можливістю швидкого гнучкого пошуку за різними атрибутами.

4. ECM (Enterprise Content Management) – комплексна система управління контентом, яка зазвичай має функції всіх перерахованих систем [29].

Загалом, система електронного документообігу повинна забезпечувати комплексний підхід до обробки, зберігання та обміну документами в цифровому середовищі. Насамперед, вона має створювати можливості для віддаленої взаємодії між користувачами. Зокрема, завдяки використанню кваліфікованих електронних підписів, включаючи й хмарні ключі, користувачі можуть погоджувати документи з будь-якого місця, де є доступ до Інтернету. Це особливо актуально в умовах віддаленої роботи або географічної розосередженості працівників, оскільки дозволяє здійснювати повноцінний документообіг цілодобово та безперервно.

Крім того, важливою складовою є електронне зберігання документів. Така система дозволяє не лише уникнути громіздких паперових архівів, але й гарантує зручний та швидкий доступ до інформації. Вся документація зберігається на захищених серверах, що мінімізує ризики втрати чи пошкодження важливих даних. До того ж, завдяки розширеним можливостям пошуку, користувачі можуть за лічені секунди знайти потрібний документ за вказаними параметрами.

Варто також звернути увагу на функцію електронного обміну документами, яка значно пришвидшує внутрішню та зовнішню комунікацію. Відтепер немає потреби в очікуванні доставки паперових примірників або витратах на кур'єрські послуги. Система дозволяє миттєво передавати документи між працівниками, відділами чи партнерами, що сприяє

оперативному прийняттю рішень і загальній динаміці бізнес-процесів. Не менш суттєвим є й аспект автоматизації. Рутинні операції, такі як пересилання, підписання або архівація документів, можуть виконуватись автоматично згідно з налаштованими маршрутами та регламентами. Завдяки цьому скорочується кількість ручної роботи, зменшується ризик помилок та підвищується точність виконання завдань. До того ж, автоматизовані процеси полегшують контроль за виконанням процедур і пришвидшують документообіг у цілому.

Ще одним визначальним елементом є система безпеки та контролю. СЕД дає змогу детально налаштовувати права доступу до кожного документа або його окремих частин, враховуючи посаду користувача, належність до певної групи чи індивідуальні повноваження. Окрім цього, фіксуються всі дії користувачів у журналах, що дозволяє проводити аудит та розслідування у випадку виявлення інцидентів. Такий рівень контролю гарантує збереження конфіденційності даних і відповідає високим стандартам інформаційної безпеки. Таким чином, система електронного документообігу – це не просто засіб зручного зберігання файлів, а потужний інструмент управління інформаційними потоками, який забезпечує надійність, швидкість, прозорість і захищеність усіх процесів, пов’язаних з документообігом у сучасній організації [30, с. 175].

Отже, у даному розділі дипломної роботи окреслено ключові теоретичні засади інформаційної безпеки систем електронного документообігу, розкриваючи як загальні підходи до захисту інформації в цифровому середовищі, так і специфіку електронного документа як об'єкта захисту. В умовах цифрової трансформації та зростання кіберзагроз інформаційна безпека набуває стратегічного значення для організацій усіх рівнів, а електронний документообіг – стає критично важливою складовою управлінської та ділової діяльності.

Було детально розглянуто комплекс заходів, що забезпечують конфіденційність, цілісність та доступність інформації, а також правові та

нормативні основи, на яких базується захист вітчизняних інформаційних систем. Особливу увагу приділено засобам технічного й криптографічного захисту, ролі метаданих, а також КЕП в забезпеченні автентичності та юридичної значущості електронних документів. Проаналізовано функціональні характеристики систем електронного документообігу, їхні класифікації, переваги впровадження та критерії вибору оптимального рішення. Системи ЕДО розглядаються як інструмент підвищення ефективності, прозорості та безпеки документообігу в організаціях, здатний адаптуватися до умов сучасного інформаційного суспільства.

Таким чином, вивчення теоретичних основ інформаційної безпеки у контексті електронного документообігу дозволяє зробити висновок про необхідність цілісного, багаторівневого підходу до захисту інформаційних активів та інтеграції безпекових механізмів у всі етапи життєвого циклу електронного документа.

РОЗДІЛ 2. АНАЛІЗ МЕТОДІВ І ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ «АСКОД»

2.1. Загальна характеристика та архітектура типових систем електронного документообігу

В умовах стрімкого розвитку інформаційних технологій та глобалізації бізнес-процесів, ефективне управління документами стає ключовим фактором успішного функціонування будь-якої організації. Традиційний паперовий документообіг, попри свою усталеність, має низку суттєвих недоліків: повільність обробки, високі витрати на зберігання, труднощі з пошуком та копіюванням, а також ризик втрати або пошкодження документів. Відповіддю на ці виклики стало запровадження систем електронного документообігу.

Сучасні системи електронного документообігу є ключовими компонентами цифрової трансформації управлінських процесів як у державному, так і в приватному секторах. Вони забезпечують автоматизовану обробку документів у цифровому форматі, включаючи їх створення, збереження, пересилання, підписання та архівування без потреби у використанні паперових носіїв [30, с. 174].

Система електронного документообігу (СЕД) – це програмно-технічний комплекс, призначений для автоматизації процесів управління документами на всіх етапах їхнього життєвого циклу, починаючи від створення або надходження та закінчуючи архівуванням або знищенням.

Залежно від масштабу, функціональності та призначення, СЕД можна класифікувати за різними критеріями.

1. За масштабом впровадження:

– локальні СЕД, що призначені для використання в межах одного підрозділу або невеликої організації;

– корпоративні СЕД, які охоплюють усі структурні підрозділи великої компанії, забезпечуючи централізоване управління документами;

– галузеві СЕД, тобто розроблені для специфічних потреб певної галузі (наприклад, банківської, медичної, освітньої);

– міжвідомчі СЕД, що забезпечують обмін документами між різними організаціями та державними установами.

2. За функціональним призначенням:

– системи діловодства, які зосереджені на реєстрації, обліку та контролі виконання документів;

– системи управління контентом підприємства (ECM - Enterprise Content Management), це комплексні рішення, що охоплюють не тільки документообіг, а й управління веб-контентом, мультимедійними даними, знаннями тощо;

– системи автоматизації бізнес-процесів (BPM - Business Process Management), що акцентують увагу на моделюванні, виконанні та моніторингу бізнес-процесів, інтегруючи документообіг у ширший контекст управління підприємством;

– системи архівування та зберігання документів, які у свою чергу, сфокусовані на довгостроковому зберіганні та забезпеченні цілісності електронних документів.

3. За архітектурою:

– монолітні СЕД, які представляють собою єдиний програмний комплекс, що містить усі необхідні модулі;

– модульні СЕД, побудовані за принципом окремих модулів, які можуть бути інтегровані відповідно до потреб організації;

– хмарні СЕД (SaaS - Software as a Service), доступ до функціоналу системи надається через інтернет, що зменшує витрати на інфраструктуру та обслуговування;

– on-premise СЕД, що встановлюються та експлуатуються на власних серверах організації [20, с. 168].

Типова архітектура сучасної СЕД є багаторівневою та модульною, що забезпечує гнучкість, масштабованість та можливість інтеграції з іншими інформаційними системами, тому основні компоненти архітектури схематично відображені на рис. 2.1.

Рис. 2.1. – Архітектура типових СЕД

Архітектура типових систем електронного документообігу визначає логічну та фізичну організацію компонентів, які забезпечують функціонування всієї системи з обробки цифрових документів. Вона побудована за модульним принципом, що забезпечує масштабованість, гнучкість, безпеку та можливість інтеграції з іншими інформаційними системами. Така архітектура дозволяє адаптувати СЕД під потреби організацій різного масштабу та типу діяльності [8].

Центральним елементом архітектури є інтерфейс користувача, що забезпечує взаємодію між системою та кінцевим користувачем. Він може бути реалізований як веб-інтерфейс (браузерна версія) або як окрема десктопна програма. Інтерфейс надає доступ до основного функціоналу: створення, перегляду, погодження, підписання та відправлення документів. Його

зручність та інтуїтивність є критично важливими для ефективного використання системи.

Серверна частина відповідає за реалізацію бізнес-логіки системи, обробку запитів, маршрутизацію документів та керування взаємодією між модулями. Вона може бути реалізована як у вигляді локального серверного рішення, так і на базі хмарної інфраструктури.

База даних містить всю службову інформацію: документи, метадані (назва, автор, дата створення, статус, маршрут погодження тощо), а також історію змін. Підтримка резервного копіювання, версіонування та довготривалого зберігання є обов'язковою.

Модуль електронного підпису забезпечує створення, перевірку та зберігання кваліфікованих електронних підписів (КЕП), що гарантує юридичну значущість електронного документа згідно з чинним законодавством України.

Модуль безпеки реалізує автентифікацію, контроль доступу, аудит, шифрування та інші механізми захисту, відповідно до стандарту ISO/IEC 27001:2015 [9].

Інтеграційні модулі дають змогу СЕД взаємодіяти з іншими інформаційними системами (ERP, CRM, 1С, бухгалтерські сервіси, СЕВ ОВВ тощо). Це дозволяє створити єдиний інформаційний простір в межах організації або відомства.

Один із найбільш показових прикладів архітектури СЕД в Україні – система АСКОД (Автоматизована система контролю документообігу), що широко використовується в органах виконавчої влади, місцевого самоврядування, державних підприємствах та установах.

АСКОД має модульну архітектуру, що включає:

- модуль реєстрації та обліку документів;
- модуль контролю виконання;
- модуль погодження та візування;
- модуль обігу звернень громадян;

– архівний модуль;

– інструменти інтеграції з СЕВ ОВВ (Системою електронної взаємодії органів виконавчої влади).

Ключовою особливістю АСКОД є гнучка маршрутизація документів, підтримка шаблонів, управління версіями документів, електронне підписання за допомогою КЕП, а також можливість аудиту дій усіх користувачів.

У системі реалізовані інструменти контролю термінів виконання, ведення журналів обліку, формування звітів, а також багаторівнева система прав доступу до даних. Завдяки високому ступеню кастомізації, АСКОД може адаптуватися до специфіки кожного окремого органу чи підприємства.

Система елеткронного документообігу АСКОД підтримує веб-інтерфейс, а також мобільні додатки, що дає змогу працювати з документами дистанційно. Збереження документів відбувається у централізованій базі даних, яка захищена відповідно до вимог КСЗІ та проходить періодичну сертифікацію [25].

Архітектура систем електронного документообігу визначає ефективність, гнучкість і безпеку документообігу в цифровому середовищі. Типова СЕД базується на модульному підході, що дозволяє адаптувати систему до конкретних потреб організації та забезпечити її інтеграцію з іншими ІТ-системами.

Приклад системи АСКОД демонструє вдалу реалізацію сучасних вимог до архітектури: від зручного інтерфейсу до захищеної обробки даних. Таким чином, правильно спроєктована архітектура СЕД є запорукою сталого функціонування інформаційної системи документообігу, її надійності, масштабованості та відповідності нормативно-правовим вимогам.

2.2. Забезпечення конфіденційності та цілісності інформації в системі електронного документообігу «АСКОД»

Відповідно до статті 9 Закону України «Про електронні документи та електронний документообіг» [2], процес електронного документообігу можна охарактеризувати як упорядковану сукупність операцій, що охоплюють створення, обробку, передачу, надсилання, приймання, зберігання, застосування та подальше знищення електронних документів. Усі ці дії супроводжуються контролем цілісності даних, а за потреби – фіксацією факту їх отримання адресатом.

Для впровадження електронних систем зберігання й обробки інформації використовується сукупність організаційних, технологічних, програмних та інформаційних компонентів. Такі системи виконують широкий спектр завдань: від оцифрування паперових документів до реалізації механізмів безпечного доступу, розподілу прав користувачів, маршрутизації документопотоків, погодження, контролю виконання та інших процесів.

Одним із прикладів таких рішень є система електронного документообігу АСКОД, яка спрямована на автоматизацію основних напрямів діловодної діяльності, включно з управлінськими, господарськими та службовими процесами. Завдяки АСКОД забезпечується спільна робота з документами в електронному середовищі, з повною відмовою від паперових носіїв. Важливою перевагою цієї системи є підтримка юридично значущого документообігу за допомогою КЕП, що гарантує автентичність, цілісність та захист інформації.

Сучасна версія системи електронного документообігу АСКОД побудована на основі платформи баз даних Oracle, яка належить до об’єктно-реляційних систем управління даними. Компанія Oracle є визнаним лідером у сфері розробки потужних систем управління базами даних для великих інформаційних систем. АСКОД успішно функціонує впродовж багатьох років у структурах державного управління, органах місцевого самоврядування,

банківських і фінансових установах, на підприємствах промисловості, енергетики та житлово-комунального господарства [25].

Окрім основних функцій обробки документації, АСКОД надає можливість створення переліків відкритої інформації для подальшого оприлюднення, зокрема – формування електронних копій документів, які можуть бути опубліковані на офіційних вебресурсах. Однією з ключових переваг системи є наявність спеціалізованого модуля АРМ Керівника, що дозволяє керівному складу організації здійснювати підписання документів за допомогою електронного цифрового підпису, розгляд вхідної кореспонденції, винесення рішень, накладення резолюцій, формування доручень та контроль за їх виконанням у цифровому середовищі.

Система електронного документообігу АСКОД підтримує широкий спектр функціональних можливостей, спрямованих на комплексну автоматизацію діловодства та внутрішнього документообігу. До основних функцій системи належить:

– автоматизоване виконання типових процедур обліку, обробки, маршрутизації та виконання як електронних документів різних форматів, так і паперових носіїв;

– підтримка повного циклу обробки вхідної, вихідної та внутрішньої документації, включаючи організаційно-розпорядчі, нормативні та інші види документів;

– обробка звернень громадян та запитів на надання публічної інформації;

– супровід процесів подання та розгляду заяв на надання адміністративних послуг;

– облік договорів, моніторинг їх виконання, контроль термінів та відповідальних осіб [21, с. 83].

Крім того, АСКОД інтегрується з системою електронної взаємодії органів виконавчої влади (СЕВ ОВВ), що дозволяє здійснювати безпечний обмін документами між державними установами. Система також забезпечує

формування переліків публічної інформації для подальшого оприлюднення на офіційних веб-сайтах, включаючи електронні копії документів.

Особливе місце в архітектурі системи займає АРМ Керівника – окремий функціональний модуль, розроблений для керівного складу установ. Цей модуль дозволяє:

– накладати кваліфікований електронний підпис (КЕП) на документи;
– переглядати та опрацьовувати службову документацію;
– формулювати доручення, резолюції, коментарі;
– здійснювати моніторинг виконання доручень.

АРМ Керівника адаптований для роботи як на стаціонарних комп’ютерах, так і на мобільних пристроях, що працюють на операційних системах Windows, iOS та Android. Це забезпечує мобільність керівника та доступ до документації незалежно від місцезнаходження. Система АСКОД реалізує сучасну технологію Workflow, яка дозволяє налаштовувати маршрути проходження документів, визначати бізнес-процеси, контролювати виконання завдань і надсилати автоматичні повідомлення через вбудовані канали зв’язку: електронну пошту, SMS або системні сповіщення. За потреби, система може автоматично виконувати запрограмовані дії при досягненні певного етапу обробки документа або зміни його статусу.

Завдяки гнучкій архітектурі, АСКОД ефективно функціонує в організаціях із територіально розподіленою структурою, забезпечуючи централізовану модель документообігу та повноцінну підтримку віддаленої роботи через WEB-інтерфейс [4].

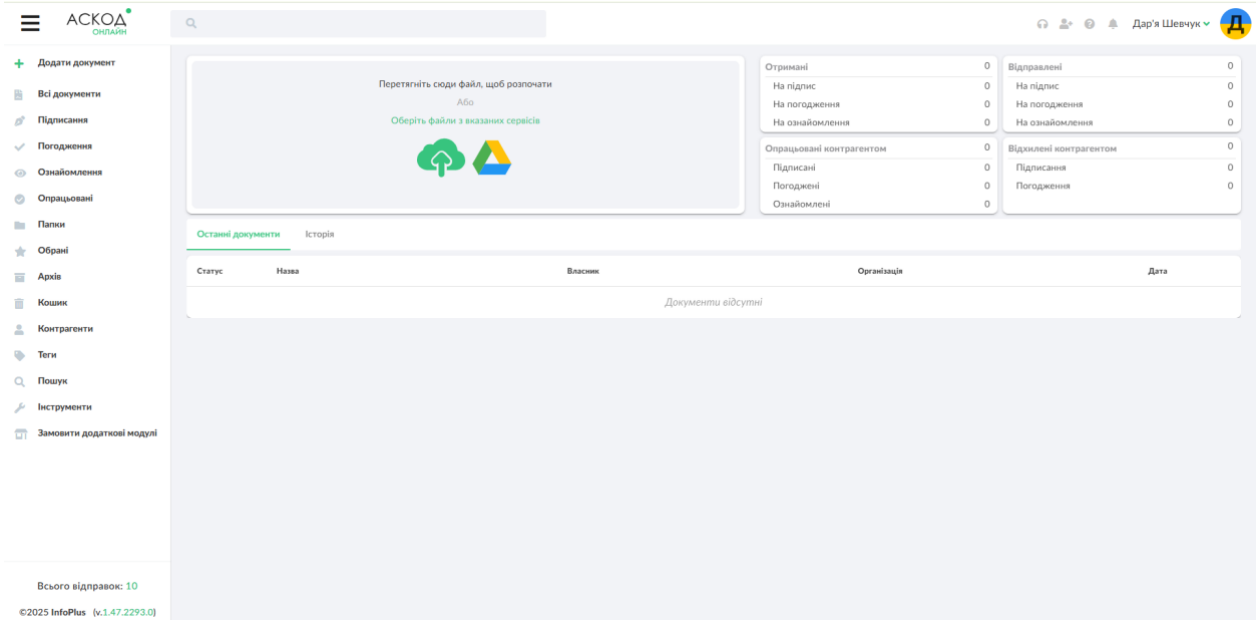

Рис. 2.2. – Інтерфейс системи АСКОД

Використання WEB-інтерфейсу системи АСКОД забезпечує повноцінний доступ територіально віддаленим працівникам та мобільним користувачам до централізованої бази даних, що дозволяє виконувати всі необхідні дії у межах електронного документообігу. Залежно від рівня наданих прав і повноважень, користувачі мають змогу здійснювати як обробку загальної документації, так і вести локальний документообіг у своїх підрозділах.

Доступ до системи можливий через найпоширеніші веб-браузери, зокрема, Google Chrome, Internet Explorer, Safari та Opera, що значно спрощує її використання на різних пристроях без потреби встановлення додаткових програмних засобів.

Мобільні працівники, а також представники віддалених структурних одиниць організації можуть працювати в системі або через браузерний WEB-доступ, або за допомогою планшетів, що підтримують роботу з веб-інтерфейсами. Такий підхід дозволяє реалізувати гнучку модель роботи в системі незалежно від географічного розташування користувача.

WEB-додаток виконує функції повної автоматизації документообігу для територіально віддалених локацій. Його застосування не потребує встановлення спеціалізованого програмного забезпечення на користувацькі

пристрої, достатньо лише стабільного з'єднання з центральним сервером системи через мережу Інтернет або інші засоби телекомунікації. Завдяки WEB-доступу система АСКОД демонструє високу адаптивність до сучасних умов цифрової мобільності, забезпечуючи безперервність документообігу та доступність для користувачів з будь-якої точки мережі [24].

На рис. 2.3. схематично відображено автоматизацію адміністративних послуг за допомогою АСКОД.

Рис. 2.3. – Автоматизація адміністративних послуг за допомогою системи електронного документообігу АСКОД

Вищенаведена схема відображає етапи обробки адміністративних послуг у цифровому середовищі системи АСКОД із залученням електронної приймальні, централізованої бази даних та структурних підрозділів установи.

У межах цифровізації управлінських процесів в органах влади та муніципальних установах особливе значення має автоматизація надання адміністративних послуг. Система електронного документообігу АСКОД відіграє ключову роль у цьому процесі, забезпечуючи повний цикл обробки документів – від їх надходження до прийняття рішення та передачі результату заявнику.

Схема функціонування АСКОД при наданні адміністративних послуг охоплює кілька послідовних етапів, які реалізуються з використанням електронних технологій та автоматизованих модулів. Початковим етапом є подання документів заявником. Це може здійснюватися як особисто, так і через електронну форму. Вхідний комплект документів потрапляє до електронної приймальні, де відбувається його попередня обробка: сканування оригіналів, створення електронних копій та реєстрація у системі. Після внесення до бази даних документи набувають статусу електронного документа та отримують унікальні реквізити.

Наступним етапом є маршрутизація документів – система направляє їх для погодження у відповідні структурні підрозділи або дозвільні установи. Після проходження погодження документи потрапляють на розгляд до керівництва установи, де вони підлягають затвердженню, накладенню резолюції або формулюванню доручення. Усі дії супроводжуються використанням кваліфікованого електронного підпису (КЕП), що надає юридичну силу електронним рішенням. У підсумку формується відповідь або адміністративне рішення, яке зберігається в електронному архіві та надається заявнику.

Система АСКОД підтримує WEB-інтерфейс, що дозволяє працювати з нею через браузери без встановлення додаткового програмного забезпечення. Це забезпечує можливість повноцінної роботи як для стаціонарних, так і для мобільних користувачів, включаючи посадовців у віддалених підрозділах [31].

Однією з ключових вимог до електронного документообігу є захист інформації, як під час обробки, так і при зберіганні даних. У системі АСКОД реалізовано цілісний комплекс заходів для забезпечення конфіденційності та цілісності інформації. Конфіденційність досягається шляхом розмежування прав доступу до документів відповідно до посадових обов’язків користувачів, використанням персональної автентифікації, шифруванням каналів передачі даних, а також обмеженням доступу до окремих функціональних модулів системи.

Цілісність даних гарантується використанням кваліфікованого електронного підпису, який фіксує зміст документа на момент підписання і забезпечує виявлення будь-яких змін у подальшому. Також у системі впроваджено журнали аудиту (audit trail) – це механізм реєстрації всіх дій користувачів щодо документа: від створення до архівування. Система контролює версії документів, дозволяє порівнювати зміни та відновлювати попередні редакції у разі потреби. Регулярне резервне копіювання даних та централізоване зберігання забезпечують додатковий рівень безпеки, особливо у випадках збоїв або аварійних ситуацій.

Отже, система АСКОД не лише забезпечує ефективну автоматизацію надання адміністративних послуг, але й гарантує високий рівень інформаційної безпеки, що відповідає сучасним стандартам та вимогам законодавства України.

2.3. Аналіз застовування механізмів забезпечення безпеки електронних документів у середовищі АСКОД

Система електронного документообігу АСКОД передбачає гнучке та масштабоване розгортання, що дозволяє забезпечити її ефективне функціонування як у центральному офісі підприємства або установи, так і у віддалених підрозділах. На головному вузлі, тобто в центральному офісі, встановлюється серверне програмне забезпечення та розміщується база даних, що працює на платформі ORACLE. Усі компоненти системи взаємодіють через IP-мережу, що забезпечує централізований контроль та єдиний доступ до електронної інформації [10].

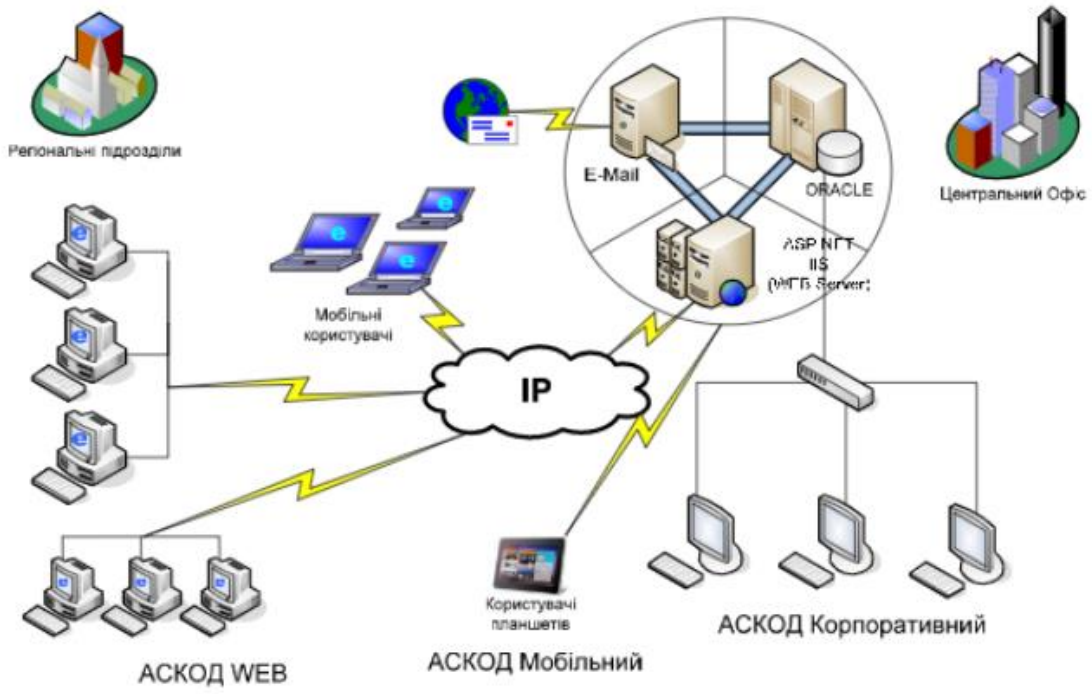

Рис. 2.4. – Розгортання системи електронного документообігу АСКОД

Архітектура системи включає окремі модулі для корпоративного користування (АСКОД Корпоративний), мобільного доступу (АСКОД Мобільний), а також WEB-доступу (АСКОД WEB). Через інтернет-з'єднання або внутрішні телекомунікаційні мережі користувачі мають можливість працювати із системою незалежно від місця розташування. Зокрема, мобільні користувачі та користувачі планшетів можуть здійснювати доступ до системи без потреби встановлення додаткового клієнтського програмного забезпечення, достатньо лише наявності веб-браузера та стабільного підключення до мережі.

Система АСКОД підтримує інтеграцію з іншими програмними продуктами завдяки вбудованому програмному інтерфейсу (API), що дозволяє обмінюватися даними у форматах XML, MS Office та інших. Така гнучкість сприяє її адаптації до різних інформаційних середовищ та забезпечує сумісність з іншими інформаційними системами організації (наприклад, ERP або CRM) [25].

WEB-додаток системи АСКОД є ключовим елементом організації документообігу у територіально віддалених підрозділах. Його головною перевагою є відсутність потреби у встановленні прогамного забезпечення на кожен комп'ютер, оскільки система функціонує у браузерному середовищі, надаючи доступ до повного функціоналу: перегляду, погодження, підписання та контролю виконання документів. Завдяки цьому забезпечується оперативна обробка інформації, незалежно від фізичного місцезнаходження користувача. У контексті роботи з електронними документами особливе значення має питання інформаційної безпеки, і система АСКОД впроваджує цілий спектр заходів для її забезпечення.

Основним підходом до забезпечення безпеки в АСКОД є розмежування доступу. Це реалізується через систему ролей та прав, де кожному користувачу або групі користувачів призначаються чітко визначені дозволи на виконання операцій з документами та системними ресурсами. Наприклад, одні користувачі можуть лише переглядати документи, інші – редагувати, а треті – підписувати та відправляти. Система дозволяє гнучко налаштовувати ці права на рівні окремих документів, тек, або навіть типів документів, що мінімізує ризики внутрішніх загроз та витоку інформації. Кожен користувач системи має індивідуальні права доступу, які визначаються його посадовими обов'язками. Вхід до системи здійснюється через логін і пароль, із можливістю підключення двофакторної автентифікації [11].

Усі ключові дії з документами, включаючи погодження та затвердження, супроводжуються накладенням КЕП, що гарантує юридичну силу документа, автентичність автора та захист від несанкціонованих змін. АСКОД підтримує інтеграцію з акредитованими центрами сертифікації ключів, що дозволяє користувачам підписувати документи за допомогою КЕП, що не тільки підтверджує особу підписанта, а й гарантує незмінність документа після його підписання, оскільки будь-яка зміна призведе до недійсності підпису. Це є фундаментальним для забезпечення довіри до електронних документів,

особливо при їх обміні із зовнішніми контрагентами або державними органами.

Для захисту даних під час їх передачі та зберігання в АСКОД застосовуються криптографічні методи. Зокрема, можуть використовуватися протоколи шифрування (наприклад, SSL/TLS) для захисту каналів зв'язку між клієнтським робочим місцем та сервером АСКОД. Це запобігає перехопленню та прослуховуванню інформації зловмисниками. Крім того, в окремих реалізаціях АСКОД або при інтеграції з додатковими засобами захисту інформації, можливе шифрування самих файлів документів на сервері зберігання, що забезпечує конфіденційність навіть у випадку несанкціонованого доступу до серверної інфраструктури. Аудит та журналювання є невід'ємною частиною механізмів безпеки АСКОД. Система веде детальні журнали всіх операцій з документами: хто, коли і які дії виконував. Це включає створення, перегляд, редагування, підписання, відправлення, видалення документів, а також зміни прав доступу. Журнали аудиту є важливим інструментом для моніторингу активності користувачів, виявлення підозрілих дій, проведення розслідувань інцидентів безпеки та забезпечення відповідності регуляторним вимогам [4].

Важливим аспектом є також управління життєвим циклом ключів КЕП та сертифікатів. АСКОД, як правило, передбачає механізми для інтеграції з корпоративною інфраструктурою відкритих ключів, що дозволяє централізовано управляти видачею, оновленням, призупиненням та анулюванням сертифікатів КЕП. Це забезпечує надійність та актуальність криптографічних засобів захисту.

Незважаючи на наявність потужних вбудованих механізмів, ефективність їх застосування в середовищі АСКОД багато в чому залежить від правильності налаштування та дотримання політик безпеки. Необхідно регулярно проводити аудит прав доступу, оновлювати програмне забезпечення, навчати користувачів правилам безпечної роботи з електронними документами та використовувати надійні паролі. Крім того, для

посилення захисту можуть бути інтегровані додаткові засоби захисту інформації, такі як системи виявлення вторгнень, антивірусне програмне забезпечення та міжмережеві екрани.

Таким чином, система АСКОД не лише забезпечує ефективну інтеграцію і мобільність при роботі з електронними документами, але й гарантує надійний рівень захисту даних, відповідно до вимог законодавства України та міжнародних стандартів інформаційної безпеки, зокрема ДСТУ ISO/IEC 27001:2015.

РОЗДІЛ 3. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ПОСИЛЕННЯ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ В СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ АСКОД

3.1. Забезпечення цілісності електронних документів в системі електронного документообігу АСКОД на основі технології кваліфікованого електронного підпису

З розвитком цифрових технологій та активним впровадженням електронного документообігу постала нагальна потреба у забезпеченні високого рівня достовірності, захисту та правової сили електронних документів. У цьому контексті одним із ключових аспектів є цілісність документа, тобто гарантія, що його зміст не було змінено або викривлено з моменту створення або підписання, а також що він відповідає своєму первісному вигляду. В контексті системи електронного документообігу АСКОД, забезпечення цілісності електронних документів є фундаментальним для довіри до інформації, її юридичної значущості та відповідності регуляторним вимогам. Серед усіх доступних механізмів, технологія кваліфікованого електронного підпису (КЕП) є наріжним каменем у побудові надійної системи захисту цілісності [13].

Цілісність у системі АСКОД забезпечується за рахунок криптографічного зв’язування електронного підпису з вмістом документа. При накладенні КЕП формується унікальний хеш-функціонал (контрольна сума), що створюється на основі вмісту електронного документа. Цей хеш потім шифрується особистим закритим ключем підписувача, утворюючи електронний підпис. Під час перевірки документа АСКОД автоматично обчислює новий хеш з отриманого документа і порівнює його з тим, що зашифрований у підписі. Якщо вони не співпадають документ вважається зміненим, а підпис – недійсним. Такий механізм гарантує, що будь-яке стороннє втручання або спроба фальсифікації буде виявлена системою.

В архітектурі системи АСКОД процес інтеграції з кваліфікованим електронним підписом (КЕП) реалізується через низку послідовних кроків, які гарантують збереження цілісності та автентичності електронних документів. Насамперед, перед самим підписанням система формує унікальний хеш – своєрідний цифровий відбиток документа. Цей хеш являє собою компактну, але цілковито однозначну за змістом послідовність символів, що генерується на основі всього вмісту документа. Важливо підкреслити, що навіть найдрібніша зміна в документі призведе до повного перетворення хешу, що унеможливлює підміну даних без виявлення.

Далі, сформований хеш передається на пристрій або програмне забезпечення, яке відповідає за створення КЕП, зазвичай це токен, смарт-карта або хмарне середовище. Там хеш шифрується особистим (приватним) ключем підписанта. У результаті цього криптографічного перетворення утворюється електронний підпис, який не лише підтверджує авторство, а й захищає дані від змін. Після цього отриманий підпис прикріплюється до документа. Це може бути реалізовано по-різному: або як окремий файл підпису, що зберігається поряд із самим документом, або як вбудована частина документа — усе залежить від обраного формату (наприклад, XML, PDF, P7S) та налаштувань, які діють у межах системи АСКОД.

Насамкінець, при кожному відкритті підписаного документа, його передачі чи перевірці, відбувається процес верифікації. Суть цієї перевірки полягає в тому, що система знову генерує хеш з фактичного вмісту документа і порівнює його з розшифрованим хешем, який витягується з електронного підпису за допомогою відкритого ключа підписанта. Цей відкритий ключ, своєю чергою, міститься в кваліфікованому сертифікаті, виданому відповідним акредитованим центром сертифікації. Якщо обидва хеші повністю збігаються, це означає, що документ не був змінений, тобто зберіг свою цілісність. У разі ж невідповідності хешів система негайно сигналізує про можливе порушення цілісності й маркує документ як недійсний або такий, що зазнав змін.

Завдяки такій архітектурі, інтеграція АСКОД із КЕП забезпечує надійний механізм контролю за справжністю та незмінністю електронних документів у межах електронного документообігу. Застосування КЕП у середовищі АСКОД має і юридичне значення, оскільки підписаний документ прирівнюється до підписаного власноруч, відповідно до Закону України «Про електронні довірчі послуги». АСКОД інтегрований з державними центрами сертифікації ключів та дозволяє користувачам використовувати особисті КЕП, видані акредитованими надавачами електронних довірчих послуг. Це означає, що кожна дія в системі, зокрема підпис, затвердження, погодження, має підтвердженого автора з унікальними повноваженнями, які неможливо підмінити або анулювати без відповідного ключа [28].

Для підвищення прозорості та контролю, АСКОД також реалізує журналювання дій користувачів (audit trail), де фіксується вся історія взаємодії з кожним документом: хто і коли його створив, підписав, передав на погодження, редагував тощо. Такий підхід підсилює гарантії збереження цілісності не лише на рівні окремого файлу, а й у межах повного життєвого циклу документа. Особливу роль відіграє внутрішня перевірка КЕП, яку система здійснює автоматично при кожній взаємодії з документом. У разі виявлення спроби змінити підписаний документ або підробити електронний підпис, система АСКОД блокує можливість його подальшого обігу, інформуючи відповідальних осіб про порушення.

Крім того, для роботи з електронними підписами система використовує сучасні криптографічні алгоритми, сертифіковані в Україні (наприклад, DSTU 4145-2002), а також підтримує середовище захищених ключових носіїв, таких як токени та смарт-карти, що виключає можливість крадіжки ключа з комп’ютера користувача [25].

Проте, забезпечення цілісності КЕП в АСКОД потребує не лише технічної реалізації, а й суворого дотримання організаційних та процедурних аспектів. Це включає забезпечення безпечного зберігання особистих ключів користувачами на токенах, навчання персоналу правилам роботи з КЕП, а

також регулярний моніторинг стану сертифікатів. Лише комплексний підхід, що поєднує надійні технологічні рішення АСКОД з високою культурою інформаційної безпеки, дозволяє повною мірою реалізувати потенціал КЕП для гарантування цілісності електронних документів.

Саме тому, використання КЕП у системі АСКОД не лише забезпечує цілісність електронних документів, але й надає їм офіційний статус, юридичну силу та захищеність від фальсифікації. Поєднання криптографічних механізмів, контрольних журналів та сертифікованих засобів захисту робить АСКОД надійним інструментом ведення сучасного електронного документообігу в умовах зростаючих вимог до інформаційної безпеки .

3.2. Практичні рекомендації щодо вдосконалення захисту документів в системі електронного документообігу АСКОД

У зв’язку з активною цифровізацією документообігу в державних та комерційних установах, забезпечення інформаційної безпеки в системах електронного документообігу, таких як АСКОД, набуває критичного значення. Попри наявність вбудованих механізмів захисту, система АСКОД, як і будь-яка інша інформаційна система, піддається впливу різноманітних вразливостей та джерел загроз, що можуть компрометувати конфіденційність, цілісність та доступність електронних документів. Глибокий аналіз цих факторів є передумовою для розробки дієвих рекомендацій щодо вдосконалення захисту. Оскільки АСКОД є однією з найпоширеніших систем в Україні, вона стає потенційною мішенню для кіберзагроз, особливо у контексті обміну службовими, конфіденційними та нормативними документами [28].

У ході аналізу функціонування системи АСКОД були виявлені низка потенційних вразливостей та загроз, які можуть порушити цілісність, конфіденційність або доступність електронних документів.

Серед основних вразливих місць у системі АСКОД можна виділити кілька критичних напрямів. По-перше, це поведінкові фактори: недбале ставлення користувачів до безпеки – використання слабких паролів, небажання змінювати облікові дані або недотримання правил користування електронним підписом. По-друге, відсутність багаторівневої автентифікації підвищує ризик несанкціонованого доступу до системи ззовні, особливо в разі атак на веб-інтерфейс або через фішингові посилання. До цього додаються технічні загрози, пов’язані з уразливістю зовнішніх компонентів (наприклад, серверів IIS або баз даних ORACLE), недостатнім контролем оновлень або експлуатацією застарілих протоколів. Окремо слід відзначити загрозу перехоплення переданих даних при роботі в публічних мережах або через незашифровані канали, а також відсутність належного журналювання дій, що ускладнює своєчасне виявлення та аналіз інцидентів.

З метою мінімізації цих ризиків доцільним є впровадження комплексу практичних заходів із вдосконалення захисту документів у середовищі системи АСКОД. Насамперед, це реалізація двофакторної автентифікації, яка дозволить значно знизити ймовірність доступу сторонніх осіб до облікових записів. Усі канали передачі даних повинні бути захищені за допомогою SSL/TLS протоколів, щоб унеможливити перехоплення інформації під час передачі між клієнтом та сервером. Важливо налаштувати контроль доступу на основі ролей, із чітким розмежуванням прав для кожного користувача відповідно до його службових функцій. Додатково рекомендується впровадити інтеграцію з DLP-системами, які дозволяють відстежувати та блокувати спроби несанкціонованого копіювання чи передавання електронних документів за межі системи.

Окрему увагу варто приділити регулярному оновленню програмного забезпечення, як самої АСКОД, так і її серверного оточення. Встановлення оновлень і патчів закриває відомі вразливості та зменшує ризик зламу. Не менш важливим є налаштування повноцінного журналювання дій користувачів: система має фіксувати кожну спробу доступу, редагування,

погодження або підпису документа, що дозволяє своєчасно реагувати на підозрілу активність. Також критично важливим є налагоджене резервне копіювання баз даних і налаштування процесів відновлення у разі втрати або пошкодження даних. Із погляду безпеки електронного документообігу, особливу увагу слід звернути на методи захищеного обміну інформацією. Використання кваліфікованого електронного підпису (КЕП) повинно бути обов'язковим не лише на етапі затвердження фінальної версії документа, а й під час внутрішнього погодження та передачі між підрозділами. Це гарантує не лише цілісність документа, але й автентичність автора.

На основі проведеного аналізу, пропонується комплекс практичних рекомендацій, спрямованих на суттєве вдосконалення захисту документів в системі АСКОД. Ці рекомендації охоплюють як технічні, так і організаційні аспекти.

Для посилення контролю доступу необхідно провести повний аудит прав доступу всіх користувачів в АСКОД, запровадити принцип мінімальних привілеїв та періодично переглядати права доступу. Для підвищення безпеки облікових записів рекомендується застосування багатофакторної автентифікації, особливо для адміністраторів та користувачів, що працюють з критично важливими документами. Посилення криптографічного захисту вимагає забезпечення використання актуальних та стійких криптографічних алгоритмів (наприклад, AES-256, SHA-256) для всіх операцій, регулярного оновлення ПЗ АСКОД та впровадження централізованої системи управління ключами шифрування.

Для своєчасного виявлення загроз необхідно вдосконалити систему журналювання та моніторингу, налаштувавши максимальне журналювання подій та інтегрувавши АСКОД із системою управління подіями безпеки та інформацією для автоматичного аналізу аномалій. Для запобігання витокам конфіденційної інформації рекомендовано впровадження системи захисту від витоків даних (DLP), що інтегруватиметься з АСКОД. Важливим аспектом є регулярне тестування на проникнення та аудит безпеки сторонніми фахівцями

для виявлення та усунення вразливостей. Необхідно розробити та впровадити чіткі політики інформаційної безпеки, що охоплюватимуть правила роботи з електронними документами, використання ЕЦП та дії у випадку інцидентів.

Ключовим є навчання та підвищення обізнаності користувачів шляхом регулярних тренінгів та семінарів з питань інформаційної безпеки та розпізнавання загроз. Також слід розробити та регулярно тестувати план відновлення після збоїв та катастроф, який забезпечить безперервність бізнес-процесів та збереження даних. Нарешті, необхідно запровадити управління постачальниками та сторонніми сервісами, оцінюючи ризики безпеки при роботі з підрядниками, які мають доступ до системи АСКОД. Також для зменшення ризиків у середовищах з відкритим доступом або з підвищеним навантаженням, доцільно встановлювати захищені шлюзи (gateway) між внутрішнім ядром системи АСКОД та зовнішніми каналами зв’язку – такими як електронна пошта або зовнішні API. Такі шлюзи дозволяють здійснювати фільтрацію запитів, аналізувати вміст даних та блокувати небезпечну активність до її проникнення в систему.

Упровадження всіх зазначених заходів має бути підкріплене системною роботою з персоналом. Регулярне навчання з інформаційної безпеки, роз’яснення принципів використання КЕП, практики кібергігієни та вміння розпізнавати фішингові атаки формує культуру безпечної поведінки в електронному середовищі.

Отже, система АСКОД, будучи ефективним інструментом цифрового управління документами, повинна супроводжуватись надійним захистом від загроз, що виникають у цифровому середовищі. Впровадження сучасних засобів автентифікації, шифрування, контролю доступу, навчання персоналу та забезпечення прозорості операцій значно знижує ризики витоку або спотворення інформації. Комплексне підсилення інформаційної безпеки дозволить не лише захистити документи, але й зберегти довіру до електронного документообігу в організації загалом.

ВИСНОВКИ

У даній роботі на тему «Методи та технології забезпечення інформаційної безпеки в системах електронного документообігу» присвячена актуальній та надзвичайно важливій проблемі сучасного інформаційного суспільства – захисту інформаційних ресурсів в умовах активної цифровізації та зростання кіберзагроз. У роботі було комплексно досліджено теоретичні основи інформаційної безпеки, проаналізовано існуючі методи та технології захисту в системах електронного документообігу, а також розроблені практичні рекомендації щодо підвищення рівня безпеки.

У першому розділі кваліфікаційної роботи «Теоретичні основи інформаційної безпеки систем електронного документообігу» ґрунтовно досліджено ключові аспекти інформаційної безпеки в контексті сучасних інформаційно-комунікаційних технологій та, зокрема, систем електронного документообігу.

Встановлено, що інформаційна безпека є невід'ємною складовою загальної системи безпеки інформаційних технологій, що забезпечує конфіденційність, цілісність та доступність інформації. Визначено основні законодавчі засади регулювання захисту інформації в Україні, зокрема Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який розмежовує технічний та криптографічний захист інформації. Наголошено на важливості комплексного підходу до захисту інформації в системах електронного документообігу, що включає організаційні, технічні, правові та програмні заходи.

Окрему увагу приділено електронному документу як ключовому об'єкту захисту. Проаналізовано його визначення, структуру, особливості (залежність від ПЗ, здатність відображати різні типи інформації, можливість фрагментації, наявність зовнішніх гіперпосилань) та значення метаданих для підтримання достовірності та цілісності. Підкреслено юридичну силу електронного документа лише за наявності кваліфікованого електронного підпису (КЕП) та

необхідність збереження його цілісності при архівному зберіганні. Класифіковано основні загрози інформаційній безпеці (порушення конфіденційності, цілісності, доступності) та розглянуто методи їх запобігання, такі як шифрування (зокрема, використання AES-256 в архіваторах) та спеціалізовані криптографічні програми (TrueCrypt).

Надано огляд функціональних характеристик систем електронного документообігу (ЕДО), визначивши їх як програмні платформи для управління повним циклом роботи з електронними документами. Висвітлено ключові переваги ЕДО, такі як оперативність, автоматизація, підвищення рівня інформаційної безпеки, а також роль КЕП у цих системах.

Таким чином, у першому розділі надано теоретичну базу для подальшого дослідження, систематизуючи знання про інформаційну безпеку, електронні документи та системи електронного документообігу, що є основою для аналізу методів та технологій їх захисту.

У другому розділі проаналізовано методи і технології захисту інформації в системі електронного документообігу АСКОД, детально розглянуто основні загрози, що постають перед СЕД, та проаналізовано різноманітні підходи до їх мінімізації.

Було виявлено, що основними загрозами є несанкціонований доступ, модифікація даних, відмова в обслуговуванні, а також загрози, пов'язані з програмним забезпеченням та людським фактором. Особливу увагу приділено впливу кібератак та вірусного програмного забезпечення. Розглянуто комплексні методи захисту, що включають криптографічні засоби (шифрування, електронний підпис), розмежування доступу, резервне копіювання, міжмережеві екрани, системи виявлення вторгнень та антивірусне програмне забезпечення.

Окремо висвітлено роль кваліфікованого електронного підпису як ключового інструменту для забезпечення автентичності, цілісності та конфіденційності електронних документів, підкреслено його юридичну значущість та нормативно-правове регулювання в Україні.

Проведено аналіз архітектурних рішень та надано характеристику сучасної СЕД АСКОД, з акцентом на її вбудовані механізми безпеки. Визначено, що ефективний захист СЕД вимагає не тільки технічних рішень, а й належної організації процесів та підвищення обізнаності персоналу щодо правил інформаційної безпеки. Запропоновано розглядати інформаційну безпеку не як окрему функцію, а як інтегровану частину життєвого циклу електронного документа та функціонування всієї системи документообігу.

У третьому розділі роботи було розроблено практичні рекомендації, спрямовані на підвищення рівня захисту інформації в системах електронного документообігу. На основі аналізу нормативно-правової бази, зокрема Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про електронні довірчі послуги», а також міжнародних стандартів (ISO/IEC 27001), було сформовано комплексний підхід до вдосконалення інформаційної безпеки.

Детально описано рекомендації щодо використання передових методів автентифікації та контролю доступу (двофакторна автентифікація, біометричні системи), впровадження сучасних криптографічних засобів для шифрування даних під час зберігання та передачі, а також забезпечення цілісності електронних документів за допомогою електронного підпису. Розглянуто важливість створення комплексних систем резервного копіювання та планів відновлення після збоїв, що є критично важливим для забезпечення безперервності бізнес-процесів.

Особлива увага приділена організаційним заходам, таким як розробка політик безпеки, регулярне навчання персоналу, проведення аудитів безпеки та тестування на проникнення. Підкреслена необхідність управління ризиками, пов’язаними з постачальниками та сторонніми сервісами. Запропоновано встановлення захищених шлюзів для фільтрації зовнішніх запитів, що підвищить стійкість системи до атак.

Всі запропоновані заходи, що стосуються як технічних, так і організаційних аспектів, спрямовані на створення багаторівневої системи

захисту, що мінімізує ризики витоку, спотворення або втрати конфіденційних даних в СЕД.

Кваліфікаційна бакалаврська робота комплексно охоплює теоретичні основи, практичні аспекти та рекомендації щодо забезпечення інформаційної безпеки в системах електронного документообігу. Підтверджено, що інформаційна безпека є критично важливою умовою ефективного функціонування СЕД, особливо в контексті правової значущості електронних документів. Практичний аналіз системи АСКОД виявив сильні сторони та потенційні вразливості, що дозволило сформувати реалістичні пропозиції щодо її удосконалення. Результати дослідження можуть бути застосовані в установах для впровадження політик безпеки та підвищення рівня захисту інформації в цифровому середовищі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://surl.li/njwybu (дата звернення: 05.01.2025)

2. Закон України «Про електронні документи та електроннийдокументообіг». URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 05.01.2025)

3. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 05.01.2025)

4. Автоматизована система контролю і організації діловодства «АСКОД». Веб-сайт. URL: http://www.scritub.com/limba/ucraineana/72294.php (дата звернення: 16.04.2025)

5. Боровікова Н. Способи захисту конфіденційної інформації. URL: https://surli.cc/tyfxcc (дата звернення: 05.01.2025)

6. Бородкіна І. Л. Методи й технології захисту інформації в системах електронного документообігу. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки.* 2018. Т. 29, № 68. С. 110–114. URL: http://nbuv.gov.ua/UJRN/sntuts_2018_29(68)_4(1)__21 (дата звернення: 05.01.2025)

7. Гребенніков В. В. Нормативно-правове забезпечення інформаційної безпеки. ДВНЗ «Ужгор. нац. ун-т», 2013. 18 с.

8. Інформація про основні вимоги до систем електронногодокументообігу. Веб-сайт. URL: https://studfile.net/preview/10849102/page:47/ (дата звернення: 15.04.2025)

9. Інформація про стандарти інформаційної безпеки. Веб-сайт. URL: https://surli.cc/qiycxj (дата звернення: 14.04.2025)

10. Інформація про систему керування базами даних Oracle Database. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Oracle_Database (дата звернення: 17.04.2025)

11. Захист систем електронного документообігу: юридичні й технічні моменти. Веб-сайт. URL: https://surli.cc/rtnwka (дата звернення: 16.04.2025)

12. Килимник І. І. Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. *Науковий вісник Ужгородського національного університету*. 2023. № 76. С. 53–57.

13. Копняк К. В., Костунець Т. А. Автоматизація документообігу як складова підвищення ефективності діяльності підприємства. *Економіка, фінанси, менеджмент.* 2017. №11. С. 57-68. URL: https://surli.cc/xetpqf (дата звернення: 25.04.2025)

14. Левченко Л. Л. Вирішення стратегічних завдань у галузі забезпечення збереженості електронних документів: міжнародний проект InterPARES. *Студії з архівної справи та документознавства*. 2012. Т. 20. С. 287–294. URL: http://nbuv.gov.ua/UJRN/sasd_2012_20_45 (дата звернення: 05.01.2025)

15. Мегель Ю. Є., Путятін В. П. Основи електронного документообігу (частина 1). Харків: ХНТУСГ ім. П. Василенка, 2020. С. 48

16. Мегель Ю. Є., Путятін В. П. Основи пошуку науково-економічної інформації в Інтернет. Харків: ХНТУСГ ім. П. Василенка, 2018. С. 32

17. Мохова Ю. Л., Шапошник Т. М. Правові засади електронного документообігу в органах державної влади. Держава та регіони. 2018. № 4 (64). URL: http://www.pa.stateandregions.zp.ua/archive/4_2018/23.pdf. (дата звернення: 04.01.2025)

18. Нагаєв В. М., Гіржева О. М., Чалий І. В., Міненко С. І. Digital трансформації публічних комунікацій, кібербезпеки та цифрового лідерства в системі електронного урядування. *Публічне адміністрування та національна безпека: електронне наукове видання.* 2024. № 4(45). С. 78-88. URL: https://doi.org/10.25313/2617-572X-2024-4-9837 (дата звернення: 05.01.2025)

19. Нагаєв В. М., Чалий І. В., Олійник Т. І., Міненко С. І. Електронне урядування як невід'ємний атрибут публічних комунікацій громадянського

суспільства. Актуальні проблеми інноваційної економіки та права. 2024. № 2. С. 30–34.

20. Назарова І. Я. Можливості та функції електронного документообігу. *Економічний простір.* 2020. №159. С. 166-170. URL: http://nbuv.gov.ua/UJRN/ecpros_2020_159_36 (дата звернення: 15.04.2025)

21. Овсієнко А.С. Сучасні напрями використання електронних ресурсів державними органами влади. *Економіка. Менеджмент. Бізнес.* № 1-2 (39), 2022. ДУІКТ. С. 80-85. URL: https://surli.cc/ekagzc (дата звернення 16.04.2025)

22. Овсієнко А.С., Дубовчук М.В. Впровадження електронного документообігу в системі управління підприємством. *Економіка. Менеджмент. Бізнес*. № 1(44), 2024. ДУІКТ. С. 87-93. URL: https://surli.cc/hssrcc (дата звернення: 04.01.2025)

23. Ольховський В. О., Карцева В. В. Програмні засоби захисту електронних документів. 2016. С. 231. URL: https://core.ac.uk/reader/300238125 (дата звернення: 05.01.2025)

24. Опис системи електронного документообігу «АСКОД» Веб-сайт. URL: http://www.docflow.ua/products/10324/ (дата звернення: 16.04.2025)

25. Офіційний сайт автоматизованої системи керування офіційними документами «АСКОД». Веб-сайт. URL: https://askod.online/ (дата звернення: 13.04.2025)

26. Офіційний вебпортал Державної архівної служби України. Електронний документ. URL: https://old.archives.gov.ua/Electronic/E_D.php (дата звернення: 05.01.2025)

27. Піддубна Л. В., Павліченко В. М. Інформаційна безпека в системах електронного документообігу. *Науковий вісник ПУЕТ. Серія «Економічні науки».* 2019. № 4. С. 59-66.

28. Система електронного документообігу «АСКОД». Веб-сайт. URL: https://surli.cc/hjybar (дата звернення: 26.04.2025)

29. Системи електронного документообігу: функції, види, критерії вибору, етапи впровадження. URL: https://surl.li/nxrhrw (дата звернення: 05.01.2025)

30. Ситник І. П., Мельниченко А. І. Системи електронного документообігу в електронному бізнесі. *Науковий вісник Ужгородського національного університету. Серія «Міжнародні економічні відносини та світове господарство»*. 2015. №4. С. 174-178.

31. Стислий опис системи електронного документообігу «АСКОД». Центр комп'ютерних технологій «ІнфоПлюс». Веб-сайт. URL: https://surli.cc/ojhllp (дата звернення: 16.04.2025)

32. Хошаба О. М. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. Частина 13: Захист інформації в системах електронного урядування. 2017. 72 с. URL: https://surli.cc/mrgwzw (дата звернення: 04.01.2025)

33. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління*. 2020. № 1. С. 285–296. URL: https://surli.cc/sdycet (дата звернення: 05.01.2025)

34. Як підвищити рівень кіберзахисту систем електронного документообігу. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://surli.cc/szcwfh (дата звернення: 20.04.2025)

35. ISBD Міжнародний стандартний бібліографічний опис Консолідоване видання. Міжнар. федерація бібл. асоц. та установ, 2023. Т. 44. URL: https://unimarc.org.ua/wiki/ISBD (дата звернення: 04.01.2025)

36. Isaikina O., Dybkova L, Yaremenko S, Mashkova I, Sydorenko T., Ovsiienko A. Information resources and features of communicative interaction in the modern information space of Ukraine. *AD ALTA: Journal of Interdisciplinary Research*, 2022. Vol. 12, Issue 1, Spec. Issue XXVII. P. 47-53. URL: https://surli.cc/jbaogx (дата звернення: 05.01.2025)