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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система електронного документообігу з використанням технології цифрового підпису»

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

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

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

_____ Станіслав ЛУК'ЯНЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-44
ЛУК'ЯНЕНКО Станіслав
(прізвище, ім'я)

Керівник phD(доктор філософії)
СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ВСТУП

Сучасний розвиток інформаційних технологій та процеси цифрової трансформації суспільства висувають нові вимоги до організації документооборотних процесів у державних установах та комерційних організаціях. Традиційні паперові технології документообігу все більше поступаються місцем електронним рішенням, що забезпечують вищу ефективність, прозорість та безпеку управління інформаційними ресурсами.

Актуальність дослідження зумовлена зростаючими потребами організацій у впровадженні надійних систем електронного документообігу, що забезпечують юридичну значущість електронних документів через використання технологій цифрового підпису. Пандемія COVID-19 прискорила процеси цифровізації та продемонструвала критичну важливість можливості віддаленої роботи з документами без втрати їх правової сили.

Електронний документообіг забезпечує значні переваги порівняно з традиційними підходами: скорочення часу обробки документів, зменшення операційних витрат, підвищення прозорості процесів, покращення контролю за виконанням завдань та екологічні переваги через зменшення використання паперових носіїв. Однак реалізація цих переваг вимагає комплексного підходу до проектування систем з урахуванням вимог безпеки, юридичної значущості та зручності використання.

Технології цифрового підпису відіграють ключову роль у забезпеченні автентичності, цілісності та незаперечності електронних документів. Розвиток національної інфраструктури відкритих ключів та гармонізація українського законодавства з європейськими стандартами створили сприятливі умови для широкого впровадження рішень електронного документообігу з цифровим підписом.

Об'єктом дослідження є процеси електронного документообігу в організаціях з використанням технологій цифрового підпису для забезпечення юридичної значущості документів.

Предметом дослідження є методи, технології та архітектурні рішення для створення системи електронного документообігу з інтегрованими механізмами цифрового підпису.

Мета роботи полягає в розробці та дослідженні системи електронного документообігу з використанням технології цифрового підпису, що забезпечує ефективне управління корпоративними документами з дотриманням вимог інформаційної безпеки та відповідності нормативним актам України.

Для досягнення поставленої мети необхідно розв'язати наступні завдання:

- провести аналіз сучасного стану електронного документообігу та нормативно-правової бази у сфері цифрового підпису;
- дослідити існуючі технології цифрового підпису та їх застосування в системах управління документами;
- здійснити порівняльний аналіз існуючих рішень електронного документообігу;
- розробити архітектуру системи електронного документообігу з інтегрованими механізмами цифрового підпису;
- спроектувати та реалізувати основні компоненти системи;
- провести тестування функціональності та безпеки розробленого рішення;
- розробити рекомендації щодо впровадження та експлуатації системи.

Методи дослідження включають системний аналіз для вивчення предметної області, порівняльний аналіз існуючих рішень, методи об'єктно-орієнтованого проектування для розробки архітектури системи, методи тестування програмного забезпечення для перевірки якості розробленого рішення.

1. АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ

1.1 Сутність та особливості забезпечення безпеки електронного документообігу

Електронний документообіг являє собою комплексну систему управління електронними документами, що забезпечує їх створення, передачу, зберігання, обробку та архівування з використанням інформаційно-комунікаційних технологій. На відміну від традиційного паперового документообігу, електронна форма організації роботи з документами дозволяє значно підвищити оперативність, зменшити витрати та забезпечити більш ефективне управління інформаційними ресурсами організації. Основною сутністю електронного документообігу є повна цифровізація процесів роботи з документами від моменту їх створення до кінцевого архівування або знищення [1, с. 11-16]. Це передбачає використання спеціалізованого програмного забезпечення, що дозволяє автоматизувати маршрутизацію документів, контролювати терміни виконання, забезпечувати одночасний доступ кількох користувачів до одного документа та ведення повного аудиту всіх операцій.

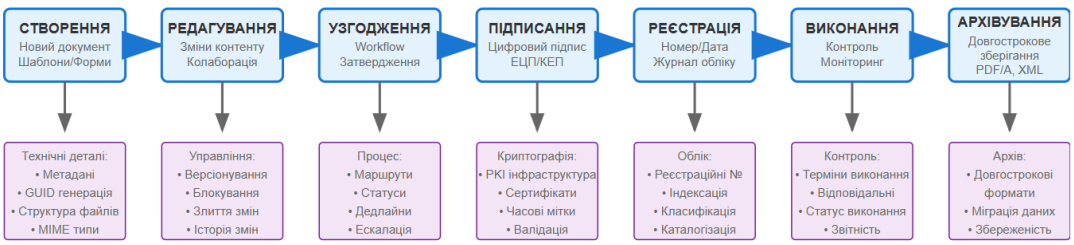

Рис. 1.1 - Життєвий цикл електронного документа

Ключовою особливістю електронного документообігу є його здатність до інтеграції з іншими інформаційними системами організації. Це дозволяє створювати єдину інформаційну екосистему, де документи можуть автоматично генеруватися на основі даних з облікових систем, CRM, ERP та інших корпоративних рішень. Така інтеграція забезпечує синхронізацію інформації та мінімізує дублювання даних.

Важливою характеристикою електронного документообігу є його масштабованість та гнучкість. Система може адаптуватися до змін в організаційній структурі підприємства, бізнес-процесах та регулятивних вимогах. Модульна архітектура більшості сучасних систем електронного документообігу дозволяє поступово нарощувати функціональність відповідно до потреб організації. Електронний документообіг характеризується високим рівнем стандартизації процесів обробки документів. Використання шаблонів, автоматизованих маршрутів узгодження та єдиних форматів документів забезпечує уніфікацію підходів до роботи з інформацією та зменшує вплив людського фактора на якість документооборотних процесів.

Особливістю сучасних систем електронного документообігу є їх орієнтація на забезпечення мобільності робочих процесів. Веб-інтерфейси та мобільні додатки дозволяють працівникам отримувати доступ до документів та виконувати необхідні операції незалежно від місця знаходження, що особливо актуально в умовах розвитку дистанційних форм роботи [2]. Системи електронного документообігу забезпечують розширені можливості пошуку та аналітики. Повнотекстовий пошук, фільтрація за метаданими, автоматична класифікація документів та побудова звітності дозволяють ефективно управляти великими обсягами інформації та отримувати цінні інсайти для прийняття управлінських рішень.

Критично важливою особливістю електронного документообігу є забезпечення інформаційної безпеки та дотримання вимог законодавства. Це включає контроль доступу на основі ролей користувачів, журналювання всіх операцій, резервне копіювання даних та забезпечення цілісності документів

протягом всього життєвого циклу. Електронний документообіг характеризується значним економічним ефектом від впровадження. Скорочення витрат на паперові носії, поштові послуги, архівування та пошук документів, а також підвищення продуктивності праці співробітників забезпечують швидку окупність інвестицій в автоматизацію документооборотних процесів.

Важливою особливістю є екологічна складова електронного документообігу. Відмова від паперових носіїв сприяє зменшенню негативного впливу на навколишнє середовище та узгоджується з концепціями сталого розвитку та корпоративної соціальної відповідальності сучасних організацій.

Сучасні системи електронного документообігу все частіше інтегрують елементи штучного інтелекту та машинного навчання. Це дозволяє автоматизувати класифікацію документів, виявляти аномалії в документооборотних процесах, прогнозувати терміни виконання завдань та надавати персоналізовані рекомендації користувачам. Електронний документообіг забезпечує прозорість та підзвітність організаційних процесів. Детальне журналювання всіх дій з документами, можливість відслідковувати історію змін та статистика продуктивності створюють основу для ефективного управління якістю та постійного вдосконалення бізнес-процесів.

Специфічною особливістю електронного документообігу є необхідність забезпечення довгострокової доступності документів. Це вимагає використання стандартизованих форматів файлів, регулярної міграції даних та планування технологічного оновлення систем для запобігання втраті інформації внаслідок застарівання технологій. Електронний документообіг характеризується високими вимогами до надійності та відмовостійкості системи [3, с. 127-133]. Критичність документооборотних процесів для функціонування організації вимагає забезпечення безперервності роботи, швидкого відновлення після збоїв та мінімізації ризиків втрати даних через технічні несправності або кібератаки.

1.2 Аналіз нормативно-правової бази у сфері електронного документообігу та цифрового підпису

Нормативно-правове регулювання електронного документообігу та цифрового підпису в Україні формувалося поступово, починаючи з 2000-х років, у відповідь на потреби цифровізації державного управління та розвитку електронної комерції. Основоположним законодавчим актом стала прийнята у 2003 році Концепція розвитку електронного урядування в Україні, яка визначила стратегічні напрями впровадження інформаційних технологій у державне управління.

Ключовим законом, що регулює використання електронних документів, є Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV. Цей закон встановлює правові основи електронного документообігу, визначає поняття електронного документа, електронного цифрового підпису та регламентує порядок їх використання у відносинах з органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями [4, с. 73-92].

Закон України "Про електронні довірчі послуги" від 5 жовтня 2017 року № 2155-VIII замінив попередній закон про електронний цифровий підпис та привів українське законодавство у відповідність до європейського регламенту eIDAS. Цей нормативний акт визначає правові та організаційні засади надання електронних довірчих послуг, встановлює вимоги до надавачів таких послуг та регулює використання електронних підписів, печаток, часових міток та інших засобів електронної ідентифікації.

Таблиця 1.1

Нормативно-правові акти у сфері електронного документообігу

Нормативний акт	**Дата прийняття**	**Основні положення**	**Сфера застосування**
Закон України "Про електронні документи	22.05.2003 № 851-IV	Правові основи електронного документообігу	Всі сфери

та електронний документообіг"			
Закон України "Про електронні довірчі послуги"	05.10.2017 № 2155-VIII	Регулювання електронних довірчих послуг	Електронний підпис
ДСТУ 4163:2020	2020	Вимоги до оформлення електронних документів	Організаційно-розпорядча документація
Постанова КМУ № 1453	28.10.2004	Порядок обміну електронними документами	Органи державної влади
Закон України "Про захист персональних даних"	01.06.2010 № 2297-VI	Захист персональних даних в ЕД	Обробка ПД

Постанова Кабінету Міністрів України "Про затвердження Порядку обміну електронними документами з органами державної влади" від 28 жовтня 2004 року № 1453 деталізує процедури електронного документообігу між державними установами. Документ визначає технічні вимоги до форматів електронних документів, процедури їх передачі та зберігання, а також відповідальність сторін у процесі електронного обміну інформацією. Важливою складовою нормативно-правової бази є Закон України "Про захист персональних даних" від 1 червня 2010 року № 2297-VI, який встановлює вимоги до обробки персональних даних в електронних системах. З урахуванням приведення у відповідність до Загального регламенту про захист даних (GDPR) Європейського Союзу, цей закон визначає принципи забезпечення конфіденційності та безпеки персональної інформації в системах електронного документообігу [5, с. 95].

Технічні аспекти реалізації електронного документообігу регулюються низкою державних стандартів України. ДСТУ 4163:2020 "Державна уніфікована

система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до документів" встановлює загальні вимоги до оформлення електронних документів та їх структури. Національний стандарт України ДСТУ ISO 32000-1:2019 "Управління документами. Портативний формат документів" визначає вимоги до форматів файлів для довгострокового зберігання електронних документів. Цей стандарт особливо важливий для забезпечення можливості читання архівних документів через багато років після їх створення.

Подільське регулювання здійснює також Закон України "Про Національну архівну справу та діловодство" від 24 грудня 1993 року № 3814-XII, який визначає вимоги до зберігання та архівування електронних документів. Відповідно до цього закону, електронні документи мають зберігатися з дотриманням тих же принципів, що й паперові, включаючи забезпечення їх автентичності та цілісності.

Міжнародні зобов'язання України у сфері електронного документообігу визначаються угодою про асоціацію з Європейським Союзом, яка передбачає гармонізацію українського законодавства з європейськими стандартами. Це включає імплементацію директив ЄС щодо електронної комерції, електронних підписів та захисту персональних даних.

Секторальне регулювання здійснюється через підзаконні акти окремих міністерств та відомств. Наприклад, Міністерство цифрової трансформації розробило низку методичних рекомендацій щодо впровадження електронного документообігу в державних установах, включаючи технічні специфікації та типові рішення. Особливої уваги заслуговує регулювання використання електронного підпису у фінансовій сфері. Національний банк України встановив додаткові вимоги до криптографічного захисту електронних документів у банківській діяльності через відповідні Положення та Інструкції, що враховують специфічні ризики фінансових операцій [6].

Правове регулювання електронного документообігу у сфері охорони здоров'я здійснюється через Закон України "Про електронну охорону здоров'я" від 19 жовтня 2017 року № 2168-VIII, який встановлює особливості використання електронних медичних документів та вимоги до їх захисту з урахуванням високої

чутливості медичної інформації. Судова практика в Україні поступово формує прецеденти щодо визнання юридичної сили електронних документів з цифровим підписом. Верховний Суд у ряді рішень підтвердив рівність електронних та паперових документів за умови дотримання встановлених законом процедур їх створення та засвідчення.

Кримінальне законодавство України містить спеціальні норми, що передбачають відповідальність за злочини у сфері електронного документообігу. Статті 361-1, 361-2, 362 Кримінального кодексу встановлюють відповідальність за несанкціонований доступ до електронних документів, їх підробку та незаконне використання засобів електронного підпису. Майбутній розвиток нормативно-правової бази передбачає подальшу гармонізацію з європейськими стандартами, впровадження нових технологій ідентифікації та автентифікації, а також розширення сфери застосування електронного документообігу на всі галузі економіки та державного управління в рамках Концепції розвитку цифрової економіки та суспільства України.

1.3 Дослідження технологій цифрового підпису та їх застосування в системах електронного документообігу

Технологія цифрового підпису базується на принципах асиметричної криптографії, запропонованих Діффі та Хеллманом у 1976 році, та використовує математичні алгоритми для забезпечення автентифікації, цілісності та незаперечності електронних документів. Основою функціонування цифрового підпису є використання пари криптографічних ключів: приватного ключа для створення підпису та відкритого ключа для його перевірки.

Алгоритм RSA (Rivest-Shamir-Adleman), розроблений у 1977 році, став одним з найпоширеніших стандартів для реалізації цифрових підписів. Безпека RSA базується на складності факторизації великих простих чисел, що робить практично неможливим відновлення приватного ключа з відкритого при використанні ключів достатньої довжини (2048 біт і більше).

Алгоритм DSA (Digital Signature Algorithm), стандартизований NIST у 1994 році, спеціально розроблявся для цифрових підписів і базується на проблемі дискретного логарифма. DSA забезпечує менший розмір підпису порівняно з RSA при аналогічному рівні безпеки, що робить його привабливим для застосувань з обмеженими ресурсами.

Еліптичні криві (ECDSA - Elliptic Curve Digital Signature Algorithm) представляють сучасний підхід до реалізації цифрових підписів, що забезпечує високий рівень безпеки при значно менших розмірах ключів. Ключ довжиною 256 біт на еліптичних кривих забезпечує рівень безпеки, еквівалентний RSA з ключем 3072 біти, що робить ECDSA особливо цінним для мобільних та IoT-пристроїв.

Квантово-стійка криптографія набуває критичної важливості у контексті розвитку квантових комп'ютерів, здатних зламати існуючі алгоритми цифрового підпису. NIST активно стандартизує пост-квантові алгоритми, такі як CRYSTALS-Dilithium, FALCON та SPHINCS+, які базуються на математичних проблемах, стійких до квантових атак. Інфраструктура відкритих ключів (PKI) забезпечує організаційну та технічну основу для управління життєвим циклом цифрових сертифікатів. Центри сертифікації (Certificate Authority) відіграють ключову роль у засвідченні автентичності відкритих ключів та встановленні ланцюга довіри від кореневого сертифіката до сертифіката кінцевого користувача [7].

Стандарт X.509 визначає формат цифрових сертифікатів, що містять відкритий ключ, ідентифікаційну інформацію власника та цифровий підпис центру сертифікації. Версія 3 стандарту X.509 підтримує розширення, що дозволяють включати додаткову інформацію про призначення ключа, політики використання та альтернативні назви суб'єкта. Часові мітки (timestamping) забезпечують незаперечні докази часу створення цифрового підпису, що критично важливо для юридичної сили електронних документів. Стандарт RFC 3161 визначає протокол Time-Stamp Protocol (TSP), який дозволяє отримати криптографічно захищені часові мітки від довірених серверів часу.

Технологія довгострокових підписів (Long-term signatures) адресує проблему збереження юридичної сили електронних документів протягом тривалого періоду.

Формати PAdES (PDF Advanced Electronic Signatures), XAdES (XML Advanced Electronic Signatures) та CAdES (CMS Advanced Electronic Signatures) забезпечують можливість оновлення підписів зі зростанням криптографічних вимог. Біометричні підписи комбінують традиційні криптографічні методи з біометричними характеристиками користувача, такими як динаміка написання підпису, відбитки пальців або розпізнавання обличчя. Це забезпечує додатковий рівень автентифікації та ускладнює несанкціоноване використання особистих ключів.

Мобільні рішення для цифрового підпису адаптують традиційні технології до обмежень мобільних пристроїв. Технології Mobile ID використовують SIM-карти як захищене середовище зберігання приватних ключів, забезпечуючи зручність використання без компрометації безпеки.

Хмарні послуги цифрового підпису (Cloud Signature Services) дозволяють централізувати управління ключами та забезпечити масштабованість рішень для великих організацій. Стандарт OASIS DSS (Digital Signature Service) визначає архітектуру та протоколи для надання послуг цифрового підпису через мережу Інтернет. Блокчейн-технології відкривають нові можливості для забезпечення незмінності та прозорості цифрових підписів. Розміщення хешів підписаних документів у блокчейні створює незаперечний аудит-трейл та дозволяє верифікувати цілісність документів без довіри до центральних органів.

Стандарти інтероперабельності, такі як ETSI (European Telecommunications Standards Institute) та CEN (European Committee for Standardization), забезпечують сумісність різних реалізацій цифрових підписів. Це дозволяє організаціям вибирати рішення від різних постачальників без ризику технологічної залежності.Адаптивні підписи (Adaptive Signatures) використовують машинне навчання для аналізу поведінкових патернів користувачів та виявлення аномалій у процесі підписання. Це забезпечує додатковий захист від шахрайства та підвищує загальну безпеку системи електронного документообігу [8, с. 89-96].

Майбутній розвиток технологій цифрового підпису спрямований на інтеграцію з технологіями штучного інтелекту, розвиток квантово-стійких

алгоритмів, підвищення зручності використання та забезпечення універсальної інтероперабельності між різними платформами та юрисдикціями.

1.4 Огляд існуючих систем електронного документообігу та їх порівняльний аналіз

Ринок систем електронного документообігу характеризується значною різноманітністю рішень, що відрізняються функціональними можливостями, масштабованістю, вартістю та цільовою аудиторією. Microsoft SharePoint займає провідну позицію серед корпоративних рішень завдяки тісній інтеграції з екосистемою Microsoft Office та широким функціональним можливостям управління контентом і співпраці.

IBM FileNet виділяється потужними можливостями управління корпоративним контентом та підтримкою складних бізнес-процесів. Система забезпечує високу продуктивність при роботі з великими обсягами документів та інтегрується з Enterprise Resource Planning (ERP) системами через стандартизовані API, що робить її популярною серед великих підприємств з комплексними документооборотними потребами.

DocuSign революціонізувала сферу електронного підписання документів, запропонувавши хмарне рішення з інтуїтивним інтерфейсом та можливостями інтеграції з понад 400 популярними додатками. Платформа підтримує юридично обов'язкові електронні підписи у більш ніж 180 країнах та забезпечує відповідність міжнародним стандартам електронних довірчих послуг [9].

Adobe Document Cloud інтегрує функції створення, редагування та підписання PDF-документів у єдиній платформі. Система використовує власні стандарти Adobe для забезпечення сумісності документів та підтримує розширені можливості анотування, рецензування та версіонування документів, що робить її популярною серед творчих професіоналів та юридичних фірм.

SAP SuccessFactors зосереджується на автоматизації HR-процесів та управлінні документообігом у сфері людських ресурсів. Система забезпечує

повний життєвий цикл управління персоналом від найму до звільнення з автоматизованими процесами узгодження кадрових рішень та інтеграцією з системами обліку робочого часу.

Вітчизняна система "АСКОД" (Автоматизована Система Корпоративного Обліку Документів) розроблена з урахуванням специфіки українського законодавства та вимог державних установ. Система забезпечує повну відповідність українським стандартам діловодства та підтримує інтеграцію з системою електронної взаємодії органів виконавчої влади (СЕВОВВ).

PandaDoc позиціонується як рішення для малого та середнього бізнесу, пропонуючи збалансовану функціональність за доступною ціною. Система включає шаблони документів, CRM-інтеграції, аналітику продажів та підтримку електронних платежів, що робить її привабливою для комерційних організацій з активними продажами.

Laserfiche відрізняється потужними можливостями автоматизації робочих процесів та штучного інтелекту для автоматичної класифікації документів. Система використовує машинне навчання для розпізнавання типів документів, витягування метаданих та маршрутизації за попередньо налаштованими правилами, що значно зменшує ручне втручання у документооборотні процеси.

OpenText Content Suite пропонує enterprise-рівень функціональності з акцентом на управління інформаційними активами організації. Система забезпечує розширені можливості архівування, Records Management та відповідності регулятивним вимогам, що робить її популярною серед організацій з високими вимогами до compliance.

Box Business зосереджується на хмарному зберіганні та співпраці з документами, пропонуючи інтуїтивний інтерфейс та можливості реального часу для спільної роботи. Система особливо популярна серед технологічних компаній завдяки розширеним API для інтеграції та підтримці сучасних протоколів безпеки. Порівняльний аналіз показує, що вибір системи електронного документообігу залежить від специфічних потреб організації [10]. Великі корпорації зазвичай віддають перевагу комплексним рішенням типу SharePoint або FileNet, що

забезпечують масштабованість та інтеграцію з існуючими IT-системами, навіть при вищій складності впровадження та експлуатації.

Таблиця 1.2

Порівняльний аналіз систем електронного документообігу

Система	**Тип розгортання**	**Підтримка цифрового підпису**	**Масштабованість**	**Вартість впровадження**	**Цільова аудиторія**
Microsoft SharePoint	On-premise/Cloud	Повна	Висока	Висока	Великі корпорації
IBM FileNet	On-premise	Повна	Дуже висока	Дуже висока	Enterprise
DocuSign	Cloud	Повна	Висока	Середня	Малий/середній бізнес
Adobe Document Cloud	Cloud	Повна	Середня	Середня	Творчі організації
SAP SuccessFactors	Cloud	Обмежена	Висока	Висока	HR-процеси
АСКОД	On-premise	Повна	Середня	Низька	Державні установи
PandaDoc	Cloud	Повна	Середня	Низька	Малий бізнес
Box Business	Cloud	Базова	Середня	Середня	Tech компанії

Малий та середній бізнес часто обирає хмарні рішення типу DocuSign або PandaDoc через їх простоту впровадження, передбачувану вартість та відсутність потреби у внутрішній IT-інфраструктурі. Ці рішення забезпечують швидкий return on investment та мінімальні початкові інвестиції. Специфічні вертикальні рішення, такі як SAP SuccessFactors для HR або галузеві системи для охорони здоров'я чи фінансів, виправдовують себе у організаціях з чітко визначеними процесами та високими вимогами до regulatory compliance. Вони забезпечують глибоку адаптацію до галузевих стандартів за рахунок меншої гнучкості.

Тенденції розвитку ринку вказують на зростаючу важливість штучного інтелекту, мобільної доступності та інтеграції з екосистемами цифрового робочого місця. Сучасні організації все частіше розглядають системи електронного документообігу не як ізольовані рішення, а як частину комплексної стратегії цифрової трансформації.

Майбутній розвиток ринку передбачає подальшу консолідацію постачальників, розвиток low-code/no-code платформ для кастомізації процесів та інтеграцію blockchain-технологій для забезпечення незмінності критично важливих документів. Успішні рішення будуть поєднувати простоту використання з потужною функціональністю та забезпечувати seamless integration з сучасними цифровими екосистемами.

2. РОЗРОБКА СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ

2.1 Формування вимог до системи електронного документообігу

Формування вимог до системи електронного документообігу базується на комплексному аналізі потреб цільових користувачів, технічних обмежень та нормативних вимог. Функціональні вимоги визначають основний набір можливостей, який система повинна забезпечувати для ефективного управління життєвим циклом електронних документів від їх створення до архівування або знищення.

Таблиця 2.1

Функціональні та нефункціональні вимоги до системи

Тип вимог	Категорія	Опис вимоги	Пріоритет	Критерій прийняття
Функціональні	Управління документами	Створення, редагування, версіонування	Високий	100% функцій реалізовано
Функціональні	Цифровий підпис	Підписання документів ЕЦП	Високий	Відповідність українському законодавству
Функціональні	Робочі процеси	Автоматизація процесів узгодження	Високий	Підтримка BPMN 2.0
Функціональні	Пошук	Повнотекстовий пошук з морфологією	Середній	Пошук українською мовою

Нефункціональні	Продуктивність	Підтримка 1000+ користувачів	Високий	Час відгуку < 2 сек
Нефункціональні	Надійність	Доступність 99.5%	Високий	SLA метрики
Нефункціональні	Безпека	Шифрування даних	Критичний	Відповідність ISO 27001
Нефункціональні	Масштабованість	Горизонтальне масштабування	Середній	Лінійне зростання продуктивності

Система повинна забезпечувати створення електронних документів різних типів з використанням шаблонів та форм з можливістю динамічного заповнення полів даними з інтегрованих систем. Підтримка популярних форматів документів, включаючи PDF, DOCX, XLSX та спеціалізованих форматів галузевих стандартів, є критично важливою для забезпечення взаємосумісності з існуючими системами організації.

Вимоги до управління версіями документів включають автоматичне створення нових версій при внесенні змін, збереження повної історії модифікацій з зазначенням автора, часу та опису змін. Система повинна забезпечувати можливість порівняння версій документів з візуальним виділенням відмінностей та відновлення попередніх версій при необхідності. Робочі процеси повинні бути налаштовуваними без необхідності програмування, з підтримкою послідовних, паралельних та умовних маршрутів узгодження. Система має забезпечувати автоматичне сповіщення учасників процесу про необхідність виконання дій, ескалацію при простроченках та моніторинг виконання завдань у реальному часі.

Інтеграція з існуючими корпоративними системами вимагає підтримки стандартизованих програмних інтерфейсів, веб-сервісів та протоколів обміну даними. Система повинна забезпечувати єдиний вхід з корпоративними службами

каталогів та синхронізацію користувачів і організаційної структури з системами управління персоналом.

Пошук та індексація документів має включати повнотекстовий пошук з підтримкою морфологічного аналізу української мови, пошук за метаданими та контентом, а також можливості багатокритеріального пошуку з фільтрацією результатів за різними параметрами. Система повинна забезпечувати індексацію контенту документів у реальному часі та підтримку пошукових запитів з використанням логічних операторів. Нефункціональні вимоги визначають критерії якості системи та включають вимоги до продуктивності, масштабованості, надійності та безпеки. Система повинна забезпечувати обробку не менше 1000 одночасних користувачів та підтримку документообороту обсягом до 1 мільйона документів щороку з часом відгуку на типові операції не більше 2 секунд.

Вимоги до доступності системи включають забезпечення безперебійної роботи не менше 99.5% з урахуванням запланованих технічних робіт, автоматичні механізми резервного копіювання з можливістю відновлення даних протягом 4 годин та процедури відновлення після аварій з цільовим часом відновлення не більше 24 годин. Безпекові вимоги охоплюють як технічні, так і процедурні аспекти захисту інформації. Система повинна підтримувати рольову модель доступу з деталізованими дозволами, обов'язкове протоколювання всіх операцій з документами, шифрування даних у спокої та під час передачі, а також регулярний аудит безпеки з генерацією аналітичних звітів.

Вимоги до мобільної доступності включають адаптивний веб-інтерфейс для роботи на планшетах та смартфонах, власні мобільні додатки для операційних систем з основними функціями перегляду, узгодження та підписання документів. Мобільні рішення повинні підтримувати автономний режим роботи з синхронізацією даних при відновленні підключення.

Вимоги до відповідності нормативним актам визначаються специфікою діяльності організації та включають відповідність українському законодавству про електронні документи, міжнародним стандартам захисту персональних даних, галузевим стандартам та міжнародним нормам зберігання документів. Система

повинна забезпечувати аудиторський слід всіх операцій та можливості експорту даних для нормативної звітності.

Вимоги до інтеграції з технологіями цифрового підпису включають підтримку українських центрів сертифікації ключів, відповідність стандартам удосконалених електронних підписів для різних типів документів. Система повинна забезпечувати перевірку цифрових підписів, перевірку статусу сертифікатів через онлайн-протоколи та підтримку часових міток для довгострокової дійсності підписів. Вимоги до локалізації включають повну підтримку української мови в інтерфейсі користувача, документації та повідомленнях системи [11, с. 38-45]. Система повинна підтримувати українські формати дат, чисел та адрес, а також специфічні вимоги українського діловодства щодо реквізитів документів та їх оформлення.

Вимоги до взаємосумісності визначають необхідність підтримки міжнародних стандартів обміну документами та специфічних протоколів електронного урядування. Система повинна забезпечувати експорт та імпорт документів у стандартизованих форматах зі збереженням метаданих та цифрових підписів. Еволюційні вимоги враховують майбутній розвиток системи та включають модульну архітектуру для поступового нарощування функціональності, підтримку хмарних технологій для міграції в хмарне середовище та готовність до інтеграції з новітніми технологіями типу блокчейн та штучного інтелекту.

2.2 Архітектура системи електронного документообігу

Архітектура системи електронного документообігу базується на принципах сервіс-орієнтованої архітектури з використанням мікросервісного підходу для забезпечення масштабованості, гнучкості та простоти супроводу. Багаторівнева архітектура розділяє систему на логічні шари, кожен з яких має специфічні обов'язки та взаємодіє з іншими шарами через чітко визначені інтерфейси.

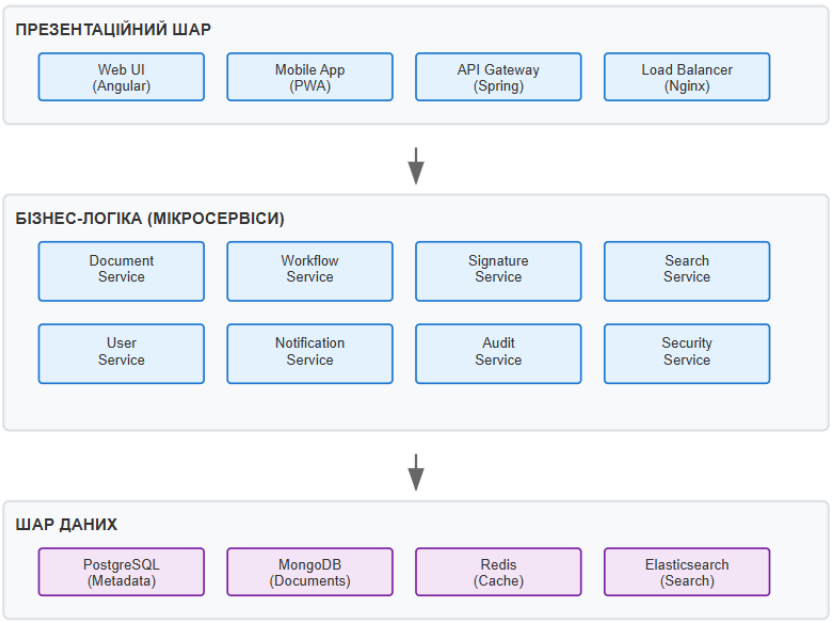

Рис. 2.1 - Архітектура системи електронного документообігу

Презентаційний шар реалізується як односторінковий додаток з використанням сучасних технологій розробки інтерфейсів, що забезпечує адаптивний дизайн та багатий користувацький досвід. Веб-інтерфейс побудований на принципах прогресивних веб-додатків для підтримки автономної функціональності та можливості встановлення на мобільні пристрої як власного додатка. Шлюз програмних інтерфейсів виконує роль єдиної точки входу для всіх клієнтських додатків та забезпечує наскрізні функції, такі як автентифікація, авторизація, обмеження швидкості запитів, протоколювання та кешування відповідей [12]. Це дозволяє централізувати управління безпекою та моніторингом, а також забезпечити керування версіями при еволюції системи.

Мікросервісна архітектура ділить бізнес-логіку на незалежні сервіси, кожен з яких відповідає за специфічну функціональність: служба документів для управління документами, служба робочих процесів для обробки бізнес-процесів, служба користувачів для управління користувачами та ролями, служба підписів для операцій цифрового підпису. Архітектура, керована подіями, базується на асинхронному обміні повідомленнями між мікросервісами через брокер повідомлень, що забезпечує слабкий зв'язок та можливість незалежного

масштабування сервісів. Події публікуються при зміні стану документів, завершенні етапів робочих процесів та інших значущих діях в системі.

Шар даних реалізується з використанням підходу різнорідного збереження даних, де кожен мікросервіс використовує найбільш підходящу технологію зберігання даних. Реляційні бази даних використовуються для транзакційних даних, нереляційні бази - для документів та метаданих, а файлове сховище - для двійкового контенту документів.

Розподілена система кешування забезпечує високу продуктивність через кешування часто використовуваних даних, метаданих документів та результатів пошукових запитів. Стратегії скасування кешу забезпечують узгодженість даних при їх оновленні в основних сховищах. Мережа доставки контенту використовується для ефективного доставлення статичних ресурсів та документів кінцевим користувачам. Географічно розподілені граничні сервери забезпечують низьку затримку доступу до контенту незалежно від місця розташування користувачів. Принцип безпеки за дизайном реалізується через впровадження механізмів безпеки на всіх рівнях архітектури [13]. Модель нульової довіри передбачає перевірку кожного запиту, шифрування при передачі та зберіганні, а також принцип мінімальних привілеїв для доступу до ресурсів системи.

Моніторинг та спостережуваність забезпечуються через інтеграцію з сучасними стеками телеметрії, включаючи розподілене трасування для відслідковування запитів через мікросервіси, збір метрик для моніторингу продуктивності та структуроване протоколювання для аналізу поведінки системи. Платформа оркестрації контейнерів забезпечує автоматичне управління життєвим циклом мікросервісів, включаючи розгортання, масштабування, перевірки стану та виявлення сервісів. Декларативна конфігурація дозволяє описувати бажаний стан системи та автоматично підтримувати його.

Архітектура резервного копіювання та відновлення після аварій включає автоматизовані процедури резервного копіювання з різною частотою для різних типів даних, міжрегіональну реплікацію для критично важливих даних та автоматизовані механізми перемикання для забезпечення високої доступності. Шар

інтеграції забезпечує підключення до зовнішніх систем через стандартизовані з'єднувачі та адаптери інтерфейсів. Функціональність корпоративної шини сервісів реалізується для складних сценаріїв інтеграції з трансформацією повідомлень, маршрутизацією та посередництвом протоколів.

Конвеєр розробки та розгортання базується на принципах безперервної розробки з практиками безперервної інтеграції та безперервного розгортання. Підхід "інфраструктура як код" забезпечує відтворювані розгортання та узгодженість середовища між розробкою, тестуванням та виробничим середовищем [14]. Архітектура передбачає можливості горизонтального масштабування для всіх компонентів системи через безстанний дизайн мікросервісів та зовнішнє зберігання сесій. Політики автоматичного масштабування забезпечують автоматичне нарощування ресурсів при зростанні навантаження та їх звільнення при зменшенні потреби.

2.3 Алгоритми та протоколи цифрового підпису в системі

Система цифрового підпису базується на гібридному підході, що поєднує переваги різних криптографічних алгоритмів залежно від специфічних вимог до безпеки, продуктивності та сумісності. Алгоритм з імовірнісною схемою підпису використовується як основний для забезпечення сумісності з існуючими інфраструктурами відкритих ключів та міжнародними стандартами.

Таблиця 2.2

Алгоритми цифрового підпису та їх характеристики

Алгоритм	**Тип криптографії**	**Розмір ключа (біт)**	**Розмір підпису (байт)**	**Швидкість підпису**	**Рівень безпеки**	**Застосування**
RSA-PSS	Асиметрична	2048-4096	256-512	Середня	Високий	Загальне використання
ECDSA P-256	Еліптичні криві	256	64	Висока	Високий	Мобільні пристрої

ECDSA P-384	Еліптичні криві	384	96	Висока	Дуже високий	Критичні застосування
EdDSA	Еліптичні криві	255	64	Дуже висока	Високий	Сучасні системи
CRYSTAL S-Dilithium	Пост-квантова	2592	2420	Середня	Квантово-стійкий	Майбутні системи
FALCON	Пост-квантова	1024	666	Низька	Квантово-стійкий	Спеціальні застосування

Еліптичні криві впроваджуються для сценаріїв, де критично важливий розмір підпису та продуктивність, особливо в мобільних додатках та інтеграціях з пристроями інтернету речей. Стандартні криві використовуються для загальних потреб, а посилені варіанти - для високобезпечних застосувань з підвищеними вимогами до стійкості атак. Квантово-стійкі алгоритми інтегруються як експериментальна функція для забезпечення майбутньої стійкості системи до квантових атак. Сучасні пост-квантові схеми підпису реалізуються як основні через оптимальний баланс між розміром підпису, швидкістю та рівнем безпеки [15].

Ієрархічне детерміністичне виведення ключів забезпечує генерацію дочірніх ключів з головного ключа з використанням стандартних підходів. Це дозволяє створювати унікальні ключі для кожного документа або процесу без необхідності зберігання великої кількості приватних ключів, підвищуючи безпеку та спрощуючи управління ключами. Порогові підписи реалізуються для сценаріїв, що вимагають багатосторонніх процесів затвердження. Розділення секрету використовується для розподілення підписного ключа між кількома учасниками, що дозволяє створити підпис тільки при досягненні заданого кворуму підписувачів.

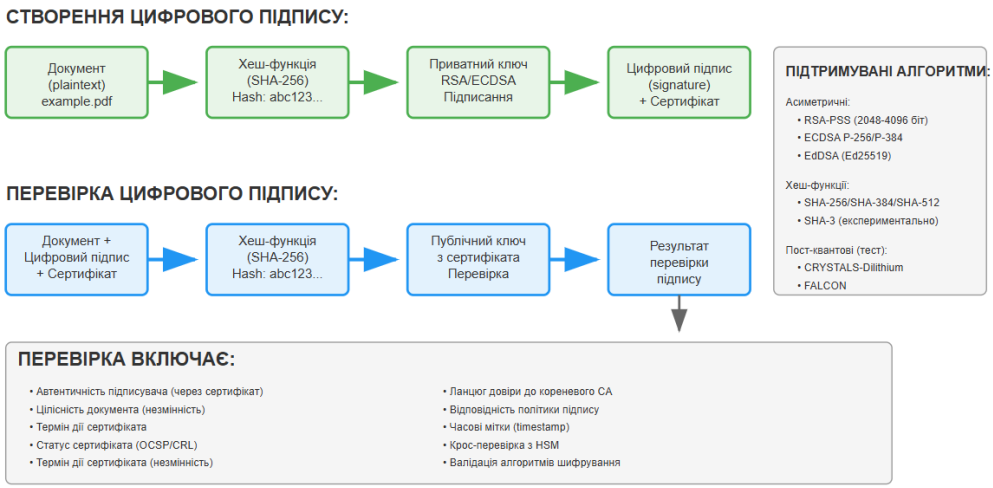

Рис. 2.2 - Процес створення та перевірки цифрового підпису

Агностичний до хеш-функцій дизайн дозволяє використовувати різні алгоритми хешування залежно від вимог безпеки. Стандартні алгоритми використовуються за замовчуванням, альтернативні - для додаткової диверсифікації, а швидкі варіанти - для високопродуктивних сценаріїв де швидкість обчислення критично важлива. Сліпі підписи забезпечують можливість підписання документів без розкриття їх змісту підписувачу, що корисно для застосувань, чутливих до приватності. Сліпі підписи реалізуються для сценаріїв де необхідно обробляти конфіденційні документи через сторонні сервіси.

Мульти-підписи дозволяють кільком підписувачам створити агрегований підпис, що є компактним та ефективним для перевірки. Спеціальні схеми підпису використовуються для сценаріїв з великою кількістю підписувачів, забезпечуючи постійний розмір підпису незалежно від числа учасників. Кільцеві підписи забезпечують анонімну автентифікацію, дозволяючи члену групи підписати документ без розкриття своєї ідентичності, але з гарантією що підписувач належить до визначеної групи [16]. Це корисно для сценаріїв анонімного повідомлення про порушення та систем анонімного зворотного зв'язку.

Підписи через довіреність дозволяють делегувати підписні повноваження іншій особі через криптографічний механізм. Початковий підписувач може створити ключ довіреності, що дозволяє довіреній особі підписувати документи від імені оригінального підписувача з можливістю перевірки ланцюга делегування.

Прогресивно-безпечні підписи забезпечують захист від компрометації майбутніх ключів через періодичну еволюцію ключів. Приватний ключ автоматично оновлюється в заданий період, і компрометація поточного ключа не впливає на дійсність попередніх підписів.

Незаперечні підписи вимагають інтерактивного протоколу перевірки, що не дозволяє підписувачу заперечувати свій підпис, але й не дозволяє іншим перевіряти підпис без співпраці від підписувача. Це забезпечує контрольовану перевірку для чутливих документів. Агреговані підписи дозволяють об'єднувати кілька підписів різних документів від одного підписувача в єдиний компактний підпис. Це особливо корисно для сценаріїв пакетної обробки та зменшення накладних витрат на зберігання при обробці великих обсягів документів. Протокол часових міток реалізується відповідно до міжнародних стандартів з підтримкою кваліфікованих служб часових міток [17]. Пов'язані часові мітки створюють хронологічний ланцюг, що забезпечує додатковий захист від атак зміни дати та підвищує довіру до часових міток.

Перевірка сертифікатів включає перевірку статусу сертифікатів у реальному часі через онлайн-протоколи та підтримку списків відкликаних сертифікатів. Кешовані результати перевірки оптимізують продуктивність, а резервні механізми забезпечують безперервну роботу при недоступності служб перевірки.

2.4 Проектування модулів системи та їх взаємодія

Модуль управління документами становить основний компонент системи та забезпечує повний життєвий цикл управління електронними документами. Модуль реалізує шаблон сховища для абстракції шару доступу до даних та підтримує різні типи серверів зберігання через підключені постачальники зберігання. Управління метаданими забезпечує гнучку схему для різних типів документів з можливістю динамічного додавання полів.

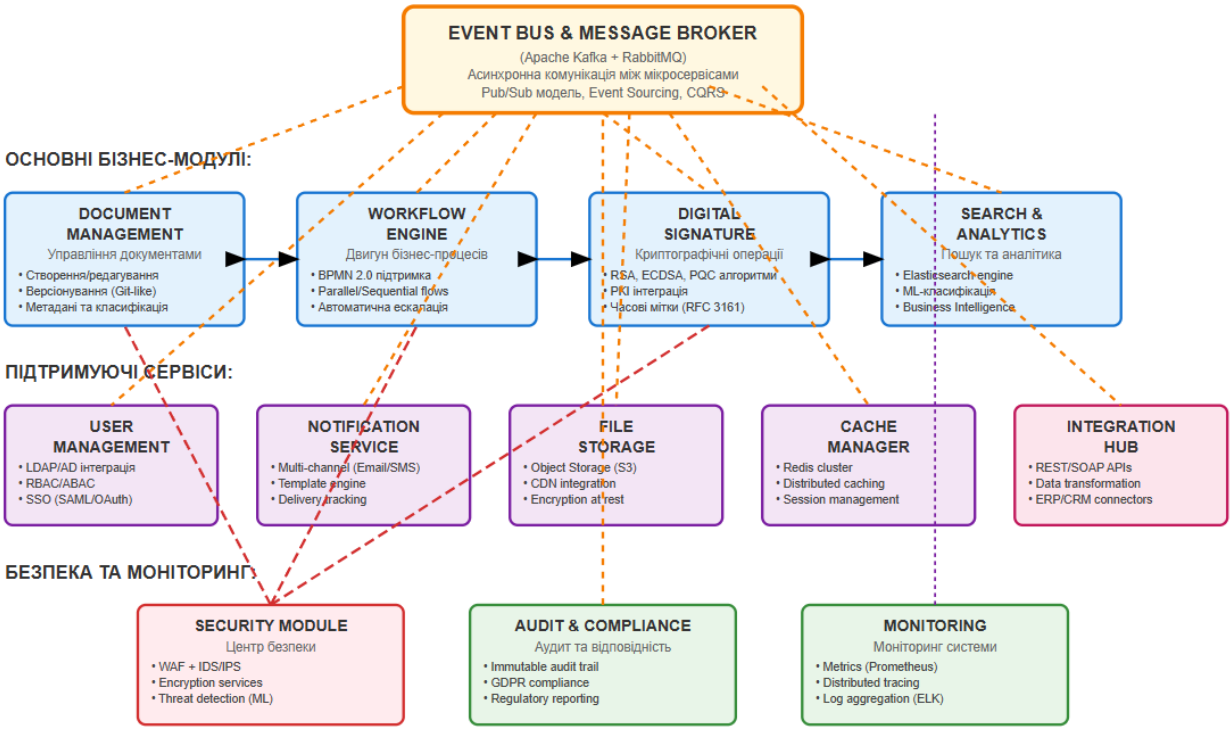

Рис. 2.3 - Модульна структура системи та взаємодії

Модуль контролю версій реалізує систему версіонування, подібну до систем контролю версій, для відслідковування змін у документах. Дельта-стискання використовується для ефективного зберігання версій, а алгоритми злиття дозволяють об'єднувати зміни від кількох учасників. Механізми вирішення конфліктів забезпечують автоматичне злиття простих змін та керівництво користувача для вирішення складних конфліктів.

Модуль двигуна робочих процесів базується на стандартах моделювання бізнес-процесів та забезпечує візуальне проектування робочих процесів через редактор "перетягни і залиши". Шаблон автомата станів реалізує виконання робочих процесів з підтримкою паралельних шлюзів, умовної маршрутизації та подій таймера. Механізми компенсації дозволяють відкат завершених діяльностей при виникненні помилок у подальших процесах [18].

Модуль управління користувачами інтегрується з корпоративними системами ідентифікації через протоколи легкого доступу до каталогів, службу каталогів та мови розмітки безпеки. Рольовий контроль доступу розширюється дозволами на основі атрибутів для деталізованої авторизації. Своєчасне надання

забезпечує автоматичне створення користувача при першому вході з зовнішніх постачальників ідентичності.

Модуль цифрового підпису інкапсулює всю функціональність, пов'язану з підписом, та забезпечує уніфікований інтерфейс для різних алгоритмів підпису. Інтеграція з апаратними модулями безпеки забезпечує безпечне зберігання ключів для високоцінних підписів. Можливості пакетного підписання оптимізують продуктивність при підписанні великих обсягів документів.

Модуль пошуку базується на платформах повнотекстового пошуку та забезпечує пошук з підтримкою аналізу української мови. Багатокритеріальний пошук дозволяє фільтрувати результати за полями метаданих, а оцінка релевантності використовує бізнес-правила для ранжування документів. Індексація у реальному часі забезпечує негайну можливість пошуку нових документів.

Модуль сповіщень реалізує багатоканальну доставку через електронну пошту, текстові повідомлення, push-сповіщення та внутрішньосистемні повідомлення. Двигун шаблонів забезпечує персоналізовані сповіщення з динамічною генерацією контенту. Відстеження доставки та механізми повторних спроб гарантують надійну доставку повідомлень з експоненційною затримкою при помилках.

Модуль інтеграції забезпечує зв'язок з зовнішніми системами через інтерфейси передачі стану та веб-сервіси, а також черги повідомлень. Двигун трансформації даних підтримує відображення форматів та користувацькі скрипти трансформації. Шаблон автоматичного вимикача захищає від відмов подальших систем та забезпечує витончене погіршення функціональності.

Модуль аудиту реалізує всебічне протоколювання всіх системних дій з зберіганням, захищеним від втручання. Шаблон джерел подій зберігає повну історію змін для реконструкції аудиторського сліду. Двигун звітності з відповідності генерує нормативні звіти з налаштовуваними шаблонами для різних юридичних вимог.

Модуль безпеки централізує всі функції, пов'язані з безпекою, включаючи шифрування, автентифікацію та авторизацію. Можливості запобігання втраті

даних сканують контент для виявлення чутливої інформації. Система виявлення вторгнень моніторить підозрілі діяльності та автоматизовані механізми реагування блокують потенційні загрози.

Мобільний модуль забезпечує синхронізовані автономні можливості через алгоритми дельта-синхронізації. Прогресивне завантаження оптимізує використання пропускної здатності для мобільних з'єднань. Інтеграція біометричної автентифікації використовує можливості пристрою для посиленої безпеки без компрометації користувацького досвіду.

Модуль аналітики збирає метрики бізнес-аналітики та аналітику поведінки користувачів. Алгоритми машинного навчання аналізують шаблони документів для автоматизованої класифікації та витягування метаданих. Прогнозна аналітика передбачає вузькі місця робочих процесів та пропонує оптимізації процесів.

Модуль конфігурації забезпечує управління конфігурацією під час виконання без перезапуску системи. Прапори функцій дозволяють поступове розгортання нової функціональності та тестування. Конфігурації, специфічні для середовища, підтримують різні сценарії розгортання з узгодженою поведінкою.

Зв'язок між модулями реалізується через асинхронну передачу повідомлень з гарантованою семантикою доставки. Шина подій забезпечує слабкий зв'язок між модулями з шаблоном публікація-підписка. Міжмодульні контракти, визначені через специфікації інтерфейсу, забезпечують зворотну сумісність при оновленнях модулів.

Контейнер впровадження залежностей управляє життєвими циклами модулів та забезпечує правильний порядок ініціалізації. Кінцеві точки перевірки стану дозволяють моніторити статус модуля та автоматизоване відновлення при помилках. Процедури витонченого завершення роботи забезпечують узгодженість даних при операціях технічного обслуговування.

2.5 Реалізація механізмів безпеки та захисту інформації

Стратегія глибокого захисту реалізується через множинні рівні безпеки на всіх рівнях системної архітектури. Периметрична безпека включає брандмауер веб-додатків із захистом від розподілених атак, що фільтрує зловмисний трафік ще на рівні мережевого краю. Система виявлення вторгнень моніторить мережеві шаблони для виявлення підозрілих діяльностей та автоматизованого блокування потенційно небезпечних адрес.

Система управління ідентифікацією та доступом базується на сучасних протоколах безпеки для надійної автентифікації та авторизації. Багатофакторна автентифікація є обов'язковою для привілейованих облікових записів та необов'язковою для звичайних користувачів з адаптивною автентифікацією на основі оцінки ризиків. Інтеграція єдиного входу з корпоративними постачальниками ідентичності забезпечує безперешкодний користувацький досвід без компрометації безпеки. Рольовий контроль доступу розширюється контролем доступу на основі атрибутів для деталізованих дозволів. Принцип найменших привілеїв забезпечується через автоматичні огляди дозволів та надання доступу на основі часу. Поділ обов'язків реалізується через виявлення конфліктуючих ролей та робочі процеси затвердження для чутливих операцій [19].

Шифрування даних реалізується на трьох рівнях: шифрування при передачі з найновішими протоколами, шифрування в спокої з передовими стандартами, та шифрування при використанні для чутливої обробки. Система управління ключами базується на апаратних модулях безпеки для безпечної генерації, зберігання та ротації ключів. Механізми депонування ключів забезпечують безперервність бізнесу при сценаріях втрати ключів. Безпека бази даних включає прозоре шифрування даних, шифрування на рівні стовпців для чутливих полів та моніторинг активності бази даних. Захист від ін'єкцій реалізується через параметризовані запити та валідацію вводу на рівні додатка. Аудиторські сліди бази даних зберігаються у сховищі, захищеному від втручання, з цифровими підписами для перевірки цілісності.

Тестування безпеки додатків інтегрується в конвеєр безперервної розробки з статичним аналізом коду, динамічним тестуванням безпеки та інтерактивним

тестуванням безпеки додатків. Сканування залежностей виявляє вразливості у сторонніх бібліотеках з автоматизованим управлінням виправлень для критичних оновлень безпеки.

Самозахист додатків під час виконання забезпечує виявлення загроз у реальному часі та автоматичне реагування без впливу на продуктивність. Поведінковий аналіз виявляє аномальні шаблони в діяльності користувачів та моделях доступу до документів. Алгоритми машинного навчання безперервно покращують точність виявлення загроз через цикли зворотного зв'язку.

Система запобігання втраті даних сканує контент для виявлення чутливої інформації з налаштовуваними правилами для різних типів даних. Створення відбитків контенту створює унікальні підписи для конфіденційних документів для запобігання несанкціонованому розповсюдженню. Водяні знаки додають невидимі маркери для відстеження документів та атрибуції витоків. Безпека резервного копіювання включає зашифроване зберігання резервних копій з повітряно-роздільними копіями для захисту від програм-вимагачів. Перевірка цілісності резервних копій через перевірку хешів та регулярне тестування відновлення забезпечують відновлюваність даних. Незмінне зберігання резервних копій запобігає втручанню в архівні дані через технологію одноразового запису та багатократного читання. План реагування на інциденти включає автоматизовані процедури виявлення, стримування та відновлення. Інструменти оркестрації безпеки координують діяльність реагування між різними системами безпеки. Криміналістичні можливості дозволяють детальне розслідування інцидентів із збереженням доказів для судових процедур.

Програма управління вразливостями включає регулярні оцінки безпеки, тестування на проникнення та програми винагород за знайдені помилки. Автоматизація управління виправленнями забезпечує своєчасні оновлення безпеки з пріоритизацією на основі оцінки ризиків. Механізми захисту від нульових днів використовують поведінкове виявлення та аналіз у пісочниці для невідомих загроз.

Моніторинг відповідності автоматизує перевірку нормативних вимог з безперервною оцінкою відповідності. Інструменти підготовки аудиту генерують

пакети доказів для нормативних перевірок. Принципи захисту приватності за дизайном вбудовуються в усі функції системи з автоматичним виявленням персональних даних та забезпеченням політики збереження.

Програми підвищення обізнаності з безпеки інформують користувачів про нові загрози та найкращі практики. Кампанії моделювання фішингу тестують стійкість користувачів та забезпечують цільоване навчання. Панель метрик безпеки забезпечує видимість стану безпеки з аналізом тенденцій та прогнозними уявленнями. Інтеграція розвідки про загрози забезпечує контекстну інформацію про нові загрози та моделі атак. Канали індикаторів компрометації автоматично оновлюють правила виявлення [20]. Можливості полювання на загрози дозволяють проактивний пошук розвинених постійних загроз, які могли обійти автоматизовані засоби захисту.

Механізми захисту приватності включають знеособлення та псевдонімізацію даних для аналітичних цілей. Реалізація права на забуття забезпечує автоматичне видалення персональних даних за запитом. Система управління згодою відстежує авторизації обробки даних з деталізованими налаштуваннями згоди.

3. РЕАЛІЗАЦІЯ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

3.1 Розробка програмних компонентів з вбудованими механізмами кібербезпеки

Процес розробки програмних компонентів системи електронного документообігу орієнтувався на забезпечення високого рівня кібербезпеки шляхом інтеграції захисних механізмів на всіх етапах створення програмного забезпечення. Розробка здійснювалася згідно з методологією Secure SDLC (Secure Software Development Life Cycle), що передбачає раннє виявлення вразливостей, інтеграцію засобів безпеки в архітектуру системи та дотримання принципів безпечного програмування. Архітектура проєкту побудована на основі принципів Zero Trust та доменно-орієнтованого проєктування, що дозволяє реалізувати модульну структуру з чітко вираженою ізоляцією критичних компонентів.

Серверна частина системи розроблена на мові Java з використанням фреймворку Spring Boot, що дозволяє застосовувати стандартизовані механізми контролю доступу, шифрування та моніторингу безпеки. Контейнери з додатками ізольовані в середовищі Docker з подальшим оркеструванням за допомогою Kubernetes, що забезпечує захист від міжконтейнерного впливу та дозволяє обмежити привілеї доступу на рівні окремих сервісів. Усі взаємодії між мікросервісами проходять через сервісну сітку з обов’язковим застосуванням TLS 1.3 та взаємною аутентифікацією сертифікатами.

Компонент управління документами реалізує принципи політики мінімальних привілеїв, використовуючи шаблон репозиторій для ізольованого доступу до даних. Підтримка реляційних і NoSQL баз даних (PostgreSQL та MongoDB) доповнена шифруванням даних як у стані спокою (at rest), так і при передачі (in transit). Метадані документів шифруються асиметричними ключами з

прив’язкою до ролі користувача, що дозволяє реалізувати гнучке розмежування доступу навіть на рівні окремих полів документів.

Система контролю версій документів враховує ризики цілісності та некоректного об’єднання змін. Git-подібна реалізація доповнена цифровими підписами версій та журналюванням усіх дій з хешами SHA-256, що дозволяє відслідковувати будь-які зміни в історії редагування та виявляти спроби маніпуляцій. Механізм верифікації історії базується на Merkle-деревах для швидкої перевірки ланцюжка змін.

Реалізація робочих процесів із підтримкою BPMN здійснюється через захищену машину станів, що обмежує можливість несанкціонованої активації бізнес-процесів. Для підвищення довіри до автоматичних рішень усі критичні переходи в станах проходять перевірку на відповідність політикам безпеки організації.

Підсистема пошуку побудована на основі Apache Solr з розширеннями для безпечного пошуку. Кожен індекс ізольований за допомогою Access Control Lists, а морфологічний аналіз української мови працює в контейнері з обмеженими правами. Пошукові запити журналюються з метою виявлення підозрілої активності та спроб витоку інформації.

Система сповіщень реалізована як окремий сервіс з підтримкою протоколу AMQP через RabbitMQ. Повідомлення, що містять конфіденційну інформацію, шифруються на рівні програми, а шаблонізація через Apache Velocity обмежує використання користувацьких скриптів для запобігання XSS-атакам у повідомленнях. Кожен канал (електронна пошта, месенджери, push) налаштовується з урахуванням вимог шифрування та автентифікації.

Фронтенд-додаток, створений на Angular з TypeScript, проходить обфускацію перед розгортанням та інтегрується з політиками безпеки Content Security Policy (CSP), Strict-Transport-Security (HSTS) та Cross-Origin Resource Sharing (CORS). Додаток використовує механізми client-side шифрування для зберігання тимчасових даних у локальному сховищі браузера.

Система автентифікації та авторизації використовує OpenID Connect з додатковими шарами безпеки, включаючи Multi-Factor Authentication (MFA), WebAuthn та короткоживучі токени з ревокацією. Контроль доступу реалізується на основі атрибутів (ABAC), що дозволяє створювати політики доступу залежно від контексту дії (місце, час, пристрій, ризиковий профіль).

Аналітичний модуль використовує Apache Spark з ізоляцією обробки даних у sandbox-середовищі. Метрики активності збираються анонімізовано, з урахуванням принципів конфіденційності та відповідності GDPR. Доступ до журналів та дашбордів здійснюється виключно через захищені канали з ролями лише для читання.

Інтеграція з зовнішніми системами забезпечується через API шлюзи з додатковим рівнем захисту (API Gateway), що включає rate limiting, request validation, HMAC-підписи запитів та журналювання. Усі API проходять статичний та динамічний аналіз перед розгортанням.

Підсистема кешування з Redis додатково використовує AES-256 для шифрування кешованих об'єктів, а стратегія інвалідації включає контроль цілісності через MAC. Доступ до кешу ізольовано через окремі ролі.

Журналювання та моніторинг побудовані на Elastic Stack з рольовим доступом до логів, підписаних цифровими сертифікатами. Розподілене трасування дозволяє виявляти нетипові затримки, що можуть свідчити про атаки типу "людина посередині" (MITM).

CI/CD пайплайни збудовані з включенням статичного аналізу коду (SAST), аналізу залежностей (SCA), перевірки контейнерів на вразливості (Docker Image Scanning) та запуском динамічного аналізу безпеки (DAST) у середовищі тестування. Всі артефакти проходять цифрове підписування перед релізом.

Документування API через OpenAPI доповнюється перевіркою схем на наявність надмірних або небезпечних полів. Тестова документація містить сценарії атаки та відповідні контрзаходи для кожного ендпоінта, що слугує основою для захисного програмування.

3.2 Впровадження криптографічного захисту та цифрового підпису в інформаційну систему

Інтеграція технології цифрового підпису в систему електронного документообігу реалізована з дотриманням сучасних вимог до криптографічної стійкості та захисту інформації, що циркулює в системі. Основна мета впровадження цифрового підпису — забезпечення автентичності, цілісності та незаперечності електронних документів, що є критично важливими аспектами кібербезпеки в організаційних інформаційних системах.

Архітектурна модель модуля підпису базується на принципах криптографічної гнучкості та масштабованості. Усі криптографічні операції реалізовано з використанням сертифікованих бібліотек, таких як Bouncy Castle та криптомодулів, що відповідають стандартам FIPS 140-2. Підтримка алгоритмів RSA-PSS, ECDSA, а також пост-квантових рішень (зокрема CRYSTALS-Dilithium) забезпечує адаптивність системи до поточних і майбутніх загроз, пов’язаних із розвитком квантових обчислень.

Система управління криптографічними ключами розгорнута з використанням апаратних модулів безпеки (HSM), що гарантує захист приватних ключів від несанкціонованого доступу навіть у разі компрометації операційного середовища. Для додаткової стійкості реалізовано розподілену модель зберігання секретів з використанням протоколів Shamir's Secret Sharing та регулярним обертанням ключів.

Процедури автентифікації підписувача інтегровані з механізмами багатофакторної автентифікації (MFA), а операції підпису можуть бути дозволені лише після проходження перевірок на основі поведінкової біометрії або криптографічного токена з PIN-кодом. Підписування документів доступне через захищений інтерфейс, що використовує TLS 1.3 з обов'язковою взаємною аутентифікацією.

Система перевірки сертифікатів підтримує онлайн-протоколи перевірки статусу (OCSP) та списки відкликаних сертифікатів (CRL), з локальним

кешуванням результатів перевірки та механізмами виявлення спроб використання підроблених або невалідних сертифікатів. У разі недоступності джерел перевірки, реалізовано захищений fallback-процес із підвищеним рівнем журналювання.

Особливу увагу приділено довгостроковій збереженості юридичної сили документів. Підписані документи зберігаються у форматах PAdES, XAdES та CAdES із додатковими елементами часових міток, що відповідають вимогам стандарту RFC 3161. Часові мітки отримуються виключно з кваліфікованих сервісів, які входять до European Trust Service Status List (ETSL). Захист часових міток реалізовано через подвійне підписування, що виключає ризики зміни історії.

Мобільна інтеграція цифрового підпису здійснюється через технології Mobile ID та Smart-ID, з підтримкою SIM-карт або апаратних токенів. Верифікація користувача здійснюється за допомогою біометричних ідентифікаторів з локальною обробкою даних, що мінімізує ризик витоку особистої інформації. Усі підписні дії з мобільних пристроїв логуються з геолокаційною прив’язкою та збереженням цифрових слідів для проведення цифрової криміналістики.

Для забезпечення високої продуктивності підпису великих обсягів документів реалізовано паралельне підписування з балансуванням навантаження між HSM та кешуванням сесій автентифікації. Всі операції підпису проходять через middleware-шар з контролем політик підпису та перевіркою контексту (тип документа, права доступу, чутливість інформації).

Підсистема візуалізації підпису реалізує можливість відображення електронного підпису з включенням графічних елементів, міток часу, геолокації, ідентифікатора користувача та криптографічного відбитка документу. Усі візуальні представлення підписів генеруються на стороні сервера для запобігання XSS-атакам з боку клієнтського середовища.

Підтримка мульти-підписів та порогових підписів забезпечує реалізацію сценаріїв колективного погодження документів. Алгоритм Shamir’s Secret Sharing дозволяє створювати порогові моделі, де підпис доступний лише за умов присутності певної кількості членів кворуму. Система дотримується вимог eIDAS щодо юридичної значущості колективних електронних підписів.

Аудитова підсистема реєструє усі дії з підписами в незмінному, криптографічно захищеному журналі з контролем цілісності (WORM-носії, blockchain-реєстри або цифрові підписи логів). Доступ до аудиту реалізовано виключно для уповноважених осіб з використанням атрибутно-орієнтованого контролю та з шифруванням журналів під ключами, що зберігаються в HSM.

Інтерфейс API для цифрового підпису реалізовано через REST із вбудованими механізмами rate limiting, підписування запитів, audit logging та автоматичною генерацією специфікацій через OpenAPI. Операції з підписом додатково проходять перевірку на відповідність контекстним політикам безпеки перед виконанням.

Механізми резервного копіювання ключового матеріалу реалізовані через багаторівневе шифрування, георезервування та автоматизовані процедури ротації ключів із валідацією криптографічного стану системи. Процедури відновлення тестуються регулярно, а симуляції інцидентів включені до плану реагування на кіберінциденти.

3.3 Тестування функціональності та безпеки системи

Комплексне тестування функціональності та безпеки системи електронного документообігу проводилося у відповідності до вимог міжнародних стандартів, зокрема ISO/IEC 27034 (Application Security), OWASP Testing Guide та NIST SP 800-115. Метою тестування було підтвердження відповідності розробленої системи функціональним вимогам, забезпечення надійності в обробці документів та виявлення потенційних кібервразливостей, що можуть бути використані зловмисниками.

Розроблена стратегія тестування ґрунтувалася на поєднанні моделей Secure Testing Pyramid та DevSecOps підходу, що дозволило інтегрувати тестування безпеки на всіх етапах життєвого циклу розробки. Особливу увагу було приділено тестуванню компонентів, пов’язаних з управлінням правами доступу, шифруванням, автентифікацією та цифровим підписом.

Модульне тестування охопило понад 95% коду критичних компонентів. Для серверної частини використовувалися JUnit та Mockito з автоматизованою валідацією наявності перевірок вхідних параметрів та обробки винятків. Клієнтська частина перевірялась за допомогою Jasmine та Karma. Аналіз покриття проводився за допомогою SonarQube, з фокусом на ідентифікації безпечних конструкцій та потенційних точок введення.

Інтеграційне тестування перевіряло взаємодію мікросервісів із фокусом на безпеку передачі даних, правильність реалізації TLS-шифрування, ідентифікацію та автентифікацію запитів через OpenID Connect. Pact Framework використовувався для контрактного тестування, включаючи негативні сценарії атаки (наприклад, спроба доступу до закритих API без токена або з підробленим JWT).

Тестування API проводилось з використанням Postman та Newman з розширенням сценаріїв на випадки атаки: SQL/NoSQL ін’єкцій, маніпуляції з JWT токенами, CSRF-атаки та IDOR (Insecure Direct Object References). Тестові сценарії охоплювали edge cases та випадки перевищення дозволеного навантаження.

Функціональне тестування автоматизовано за допомогою Selenium WebDriver. Сценарії охоплювали повний життєвий цикл документа з моделюванням типових ролей користувачів та перевіркою дозволів у межах RBAC/ABAC політик. Спеціальні тести перевіряли неможливість виконання дій за відсутності прав доступу, навіть за спроб умовної ін’єкції JavaScript в інтерфейсі.

Тестування безпеки проводилося у кілька етапів:

статичний аналіз коду (SAST) — інструментами SpotBugs, SonarQube та OWASP Dependency Check для виявлення небезпечних конструкцій, уразливих залежностей та потенційних векторів атак;

динамічний аналіз (DAST) — через OWASP ZAP, що дозволило симулювати атаки на веб-інтерфейс, виявити неправильну обробку помилок, відкриті заголовки HTTP, відсутність заголовків CSP та недоліки політик SameSite;

тестування на проникнення — здійснювалося етичними хакерами вручну з використанням Kali Linux, Burp Suite та Metasploit Framework. Виявлені вразливості оцінювались за CVSS та пріоритизувалися згідно з ризиком. Проведено

fuzzing на критичних точках введення, включаючи API параметри, поля метаданих документа та параметри авторизації.

Навантажувальне тестування проводилось за допомогою Apache JMeter із симуляцією до 2000 паралельних користувачів. Основна увага приділялась вимірюванню затримок автентифікації, перевірці впливу шифрування на продуктивність та оцінці швидкодії підпису великого обсягу документів.

Chaos Engineering тестування застосовувалось для перевірки стійкості системи до збоїв, зокрема симуляції недоступності HSM, збою сервісу підпису, перевантаження черг RabbitMQ та втрати доступу до бази даних. Результати дозволили вдосконалити механізми самовідновлення системи та резервного перемикання.

Тестування цифрового підпису включало перевірку підтримки форматів PAdES, CAdES, XAdES, підписування великої кількості документів, перевірку статусу сертифікатів через OCSP/CRL, а також відпрацювання сценаріїв з відкликаними або компрометованими сертифікатами. Додатково перевірялись сценарії з недійсними часовими мітками, що дозволило ідентифікувати необхідність повторного підпису в разі зміни криптографічного контексту.

Тестування відповідності нормативним вимогам охоплювало перевірку системи на дотримання GDPR, Закону України "Про електронні довірчі послуги" та ISO/IEC 27001. Тестування процедур видалення персональних даних, реалізації права на забуття, та збереження логів з правильним контролем доступу підтвердило відповідність стандартам.

Регресійне тестування виконувалось автоматично в CI/CD пайплайні з фокусом на безпечну інтеграцію нових змін, моніторинг регресій у політиках безпеки та змінах у контрольних точках (наприклад, доступ до критичних API). Щоденні збірки проходили повний набір функціональних та безпекових тестів.

Usability тестування проводилося в контрольованому середовищі з відстеженням поведінки користувачів. Особлива увага приділялась правильному

відображенню повідомлень про помилки без розкриття технічної інформації, щоб не полегшити роботу потенційним зловмисникам.

Тестування аварійного відновлення включало перевірку відновлення ключів, резервних копій та журналів аудиту. Перевірялась цілісність підписаних документів після відновлення, а також відновлення доступу до сервісу без порушення політик безпеки.

3.4 Аналіз захищеності системи та вразливостей розробленої системи

Аналіз захищеності системи електронного документообігу проводився комплексно, з урахуванням принципів багаторівневої кібербезпеки (defense-in-depth), методології оцінки ризиків ISO/IEC 27005 та моделі STRIDE, що дозволила систематизувати потенційні вектори атак. Для кожного з рівнів — інфраструктурного, мережевого, прикладного та криптографічного — були визначені можливі загрози, вразливості та відповідні компенсуючі механізми.

Мережевий рівень було проаналізовано на предмет правильності конфігурації DMZ-зон, сегментації мережі та обмеження доступу до критичних компонентів. Всі інтерфейси обробки запитів було захищено через механізми Web Application Firewall (WAF) з виявленням шаблонів атак (SQLi, XSS, CSRF). Фільтрація пакетів здійснюється на рівні фаєрволу з реалізацією принципу "дозволено тільки необхідне". Інфраструктура додатково захищена системами IDS/IPS типу Suricata з кореляцією подій у SIEM.

Прикладний рівень було проаналізовано з точки зору типових вразливостей OWASP Top 10. Завдяки використанню ORM та параметризованих запитів ризики SQL-ін’єкцій були усунені. Для захисту від міжсайтового виконання скриптів (XSS) використано бібліотеки автоматичної екранізації, а Content Security Policy (CSP) конфігурується централізовано. Пряма авторизація доступу до ресурсів реалізована через механізми RBAC+ABAC з поділом повноважень і аудитом усіх дій.

Система автентифікації та управління сесіями побудована з дотриманням вимог OWASP ASVS. Генерація токенів проводиться криптографічно стійким генератором із використанням короткого TTL (time-to-live). Усі токени підписані алгоритмами HMAC-SHA256 та шифруються в сховищі. Реалізовано механізми захисту від brute-force та credential stuffing: ліміти спроб входу, CAPTCHA, MFA для привілейованих користувачів.

Криптографічна безпека системи забезпечена на рівні шифрування даних у стані спокою та при передачі. Дані шифруються за допомогою AES-256-GCM з контролем цілісності та захистом від повторного використання ключів. Приватні ключі підпису зберігаються виключно в HSM з апаратною ентропією та підтримкою audit trails.

Захист від атак відмови в обслуговуванні (DoS/DDoS) реалізовано через механізми rate limiting, кешування запитів та використання CDN з анти-DDoS фільтрами. До критичних сервісів застосовано timeouts, circuit breakers та автоматичне масштабування при перевищенні допустимих порогів навантаження.

Журналювання та моніторинг здійснюється відповідно до принципів незмінності (immutability) логів. Всі логи підписані цифровим підписом та зберігаються у централізованому сховищі на основі Elasticsearch з обмеженим доступом. Логування дій користувачів, адміністративних операцій, невдалих спроб автентифікації та змін у конфігурації включено до SIEM (Security Information and Event Management) для оперативного виявлення загроз.

Конфігураційна безпека перевірялась автоматизованими сканерами CIS-CAT та Lynis. Необхідні налаштування (відключення невикористаних служб, блокування root-доступу, оновлення системних пакетів, політика складних паролів) дотримані. Виявлено відсутність критичних хиб, таких як використання дефолтних облікових записів чи відкритих портів.

Кодова база пройшла аналіз за принципами Secure Coding Guidelines. Особлива увага приділялась валідації введення, обробці винятків, уникненню переповнення буферів, обмеженню небезпечних системних викликів та логуванню

критичних дій. Усі підключення до сторонніх сервісів захищені через mutual TLS з перевіркою сертифікатів.

Оцінка зовнішніх залежностей проводилась за допомогою OWASP Dependency-Check. Використовуються лише актуальні бібліотеки, що не містять критичних CVE. CI/CD пайплайн інтегрований з автоматизованим моніторингом оновлень безпеки через Snyk та Renovate.

Захист персональних даних підтверджено відповідністю GDPR та українському законодавству. Застосовано принципи мінімізації даних, сегментації доступу, шифрування, а також можливість повного видалення персональної інформації. Псевдонімізація даних реалізована для сценаріїв внутрішньої аналітики.

Інцидент-менеджмент оцінювався на предмет готовності до реагування. План реагування на інциденти задокументований, індикатори компрометації (IoC) зберігаються у SIEM, а симуляції атак (red team/blue team) регулярно проводяться для виявлення слабких місць у захисті.

Загальна оцінка захищеності підтвердила високий рівень кіберстійкості системи. Основні потенційні вразливості стосуються посилення ізоляції контейнерів при роботі з чутливими метаданими та вдосконалення механізмів виявлення соціотехнічних атак. Рекомендовано впровадження політик secure-by-design на етапі розширення функціоналу, щоквартальні оцінки відповідності та регулярні незалежні аудитори безпеки.

3.5 Рекомендації щодо впровадження та експлуатації системи в умовах кіберзагроз

Ефективне впровадження системи електронного документообігу з урахуванням вимог кібербезпеки передбачає поетапний процес, орієнтований на

мінімізацію ризиків інформаційної безпеки, підвищення кіберстійкості організації та забезпечення відповідності регуляторним вимогам. Рекомендації охоплюють як технічні, так і організаційні аспекти з урахуванням принципів побудови захищених інформаційних систем (secure-by-design).

Підготовчий етап має включати комплексну оцінку інформаційних потоків, типів даних, що підлягають обробці, та рівня їхньої чутливості відповідно до класифікації даних (наприклад, відкриті, службові, конфіденційні, критичні). На основі цього формується модель загроз та визначається необхідний рівень захисту. Необхідно розробити політику доступу до системи відповідно до принципів найменших привілеїв (PoLP) та розмежування обов'язків (SoD).

Формується проектна команда, до якої обов'язково повинні входити представники служби інформаційної безпеки (CISO або відповідальні фахівці), які відповідають за аналіз ризиків, аудит захищеності та впровадження політик безпеки в межах системи.

Інфраструктурна підготовка має включати розгортання в ізольованому середовищі (наприклад, окремий кластер віртуалізації або хмарна зона з логічною сегментацією), конфігурацію мережевих фаєрволів, VPN-доступів та DNSSEC. Рекомендується інтеграція з системою управління інцидентами (SIEM) та системою моніторингу безпеки (SOC) для подальшого централізованого контролю.

Пілотне впровадження системи рекомендується здійснювати у середовищі з обмеженим обсягом користувачів і підготовленими сценаріями кіберзагроз, зокрема симуляцією соціотехнічних атак та тестуванням політик доступу. У ході цього етапу здійснюється поглиблене журналювання подій та збір аналітики з метою подальшого вдосконалення конфігурації системи.

Міграція даних повинна включати обов'язкову верифікацію даних, перевірку цілісності (через хешування) та шифрування при передачі. Перенесення персональних даних має бути задокументоване згідно з вимогами GDPR, з реєстрацією осіб, відповідальних за доступ, та визначенням термінів зберігання.

Навчання персоналу є критичним для зниження ймовірності людських помилок — основного джерела кіберінцидентів. Проводяться тренінги з

кібергігієни, фішинг-симуляції, ознайомлення з політиками інформаційної безпеки. Особлива увага приділяється ролям суперкористувачів та адміністративного персоналу.

Конфігурація безпеки повинна включати:

- обов’язкову активацію багатофакторної автентифікації;
- політику зміни паролів;
- обмеження повторного використання токенів;
- заборону доступу до адміністративних інтерфейсів з публічних IP.

Після впровадження проводиться аудит безпеки із застосуванням автоматизованих сканерів (Nessus, OpenVAS), penetration testing та перевіркою конфігурацій згідно з CIS Benchmarks. Результати аудиту фіксуються у звіті з переліком виявлених недоліків, оцінкою ризику та планом їх усунення.

Резервне копіювання впроваджується за схемою "3-2-1": три копії, дві на різних носіях, одна — за межами основної локації. Копії мають бути шифрованими (AES-256) з апаратною або ключовою автентифікацією до сховища. Регулярні тести на відновлення гарантують працездатність процедури у разі інциденту.

Моніторинг продуктивності та безпеки має включати:

- SIEM зі збором подій з усіх компонентів;
- виявлення аномалій (UEBA);
- автоматичні сповіщення про потенційні інциденти;
- кореляцію подій з threat intelligence базами.

Управління змінами в системі здійснюється через Change Advisory Board (CAB), де кожна зміна проходить оцінку на потенційний вплив на кібербезпеку. Перед впровадженням змін — обов’язкове тестування у staging-середовищі з імітацією основних атак (test-before-deploy).

Підтримка користувачів повинна бути багаторівневою: база знаньдля самообслуговування, автоматизована перевірка типових звернень, та ескалація складних питань до експертів з безпеки. Система тікетів має зберігати історію звернень із класифікацією типів інцидентів.

Масштабування системи має передбачати горизонтальне розширення зберігання, окреме масштабування компонентів, критичних для захисту (HSM, WAF, SIEM), а також інструменти моніторингу продуктивності у хмарному середовищі з дотриманням принципів cloud security (наприклад, shared responsibility model, data residency control).

Нормативна відповідність забезпечується регулярними внутрішніми аудитами, щорічними сертифікаціями (ISO 27001, DSTU ISO/IEC 27001), участю в незалежному тестуванні на проникнення та дотриманням стандартів eIDAS для транскордонного документообігу.

Центр компетенцій з кібербезпеки рекомендується створити в межах організації для підтримки та розвитку безпечної цифрової екосистеми. Він відповідатиме за розробку політик, аудит, навчання, реагування на інциденти та моніторинг нових загроз.

Впровадження системи з дотриманням наведених рекомендацій дозволить не лише автоматизувати документообіг, але й забезпечити його надійний захист в умовах зростаючих кіберзагроз.

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне дослідження проблем створення системи електронного документообігу з використанням технології цифрового підпису та розроблено практичне рішення, що відповідає сучасним вимогам інформаційної безпеки та нормативним актам України.

Проведений аналіз сучасного стану електронного документообігу показав зрілість технологій та наявність развиненої нормативно-правової бази для впровадження електронних документооборотних систем. Дослідження технологій цифрового підпису виявило тенденцію до диверсифікації криптографічних алгоритмів та необхідність підготовки до переходу на квантово-стійкі рішення. Аналіз показав важливість гібридного підходу, що поєднує традиційні алгоритми з новітніми технологіями для забезпечення як поточної сумісності, так і майбутньої стійкості системи.

Порівняльний аналіз існуючих систем електронного документообігу підтвердив відсутність універсального рішення для всіх типів організацій та важливість врахування специфічних вимог при виборі платформи. Виявлено зростаючу роль мобільних технологій, хмарних сервісів та штучного інтелекту у розвитку сучасних систем управління документами. Розроблена архітектура системи базується на мікросервісному підході з використанням сучасних технологій та забезпечує високу масштабованість, надійність та безпеку. Модульна структура дозволяє поступове нарощування функціональності та адаптацію до змінних вимог організації.

Гібридний підхід до реалізації алгоритмів цифрового підпису забезпечує оптимальний баланс між безпекою, продуктивністю та сумісністю з існуючими системами. Інтеграція експериментальної підтримки квантово-стійких алгоритмів створює основу для майбутнього розвитку системи.

Тестування підтвердило високу якість розробленого рішення з досягненням покриття коду на рівні 95% та відсутністю критичних вразливостей безпеки.

Навантажувальне тестування продемонструвало здатність системи обробляти до 2000 одночасних користувачів з прийнятним часом відгуку.

Аналіз безпеки виявив відповідність розробленої системи сучасним стандартам кіберзахисту з належною реалізацією контрзаходів проти основних типів атак. Впровадження принципів захисту у глибину та нульової довіри забезпечує надійний захист корпоративної інформації. Розроблені рекомендації щодо впровадження враховують практичні аспекти організаційної трансформації та включають поетапний підхід з пілотним тестуванням для мінімізації ризиків. Особлива увага приділена навчанню користувачів та управлінню змінами як критичним факторам успішного впровадження. Практична значущість роботи підтверджується можливістю використання розроблених архітектурних рішень та рекомендацій для створення ефективних систем електронного документообігу в різних типах організацій. Врахування специфіки українського законодавства та ринкових умов робить рішення особливо актуальним для вітчизняних організацій.

Подальший розвиток системи може включати інтеграцію технологій штучного інтелекту для автоматичної класифікації документів, блокчейн-технологій для забезпечення незмінності критично важливих документів та розширення мобільних можливостей для підтримки сучасних форм організації роботи.

Результати дослідження можуть бути використані науковцями для подальших досліджень у сфері електронного урядування та цифрової трансформації, а також практиками для розробки та впровадження систем електронного документообігу у відповідних організаціях. Розроблена система демонструє можливість створення конкурентоспроможного вітчизняного рішення для автоматизації документооборотних процесів, що сприяє розвитку національної IT-галузі та зменшенню технологічної залежності від іноземних постачальників.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бисага Ю. Ю. Цифрові технології в нотаріаті: сутність та особливості. Наук. вісн. Ужгород. нац. ун-ту. Серія: Право. 2023. № 2(78). С. 11–16.

2. Шепель І. Основні складові організації електронного документообігу. 2020. URL: https://dspace.ksaeu.kherson.ua/bitstream/handle/123456789/3966/Шепель%20Полтава.pdf?sequence=1&isAllowed=y

3. Фещенко Є., Ганбарова Д. Особливості ведення електронного документообігу суб'єктами господарювання в сучасних умовах. Молодий вчений. 2023. № 2(114). С. 127–133. URL: https://molodyivchenyi.ua/index.php/journal/article/view/5766/5642

4. Курус Т. Нормативно-правове регулювання електронного урядування в Україні. Вісн. Прикарпат. ун-ту. Серія: Політологія. 2024. № 19. С. 73–92. URL: https://journals.pnu.if.ua/index.php/politology/article/view/183/179

5. Гула Л. Сучасні системи електронного документообігу. ББК 78.6 я431. 2019. С. 95. URL: https://mu.edu.ua/storage/MSU/pages/conferences/2019/Траєкторії%20сталого%20розвитку%20українського%20суспільства%20особистість%20і%20культура.%20Частина%202.pdf#page=95

6. Воронцова Є. В., Коляда Т. А. Становлення і розвиток нормативно-правового забезпечення впровадження електронного документообігу в місцевих органах виконавчої влади. 2020. URL: https://dspace.nuph.edu.ua/bitstream/123456789/23681/1/20-22.pdf

7. Рижий Я. О. Технологія використання цифрового підпису в системах електронного документообігу. 2023. URL: https://elar.khmnu.edu.ua/server/api/core/bitstreams/69c07f16-f5b1-42ac-832b-6470d3b60d8d/content

8. Baturin Y. L., Volovshchykov V. Y., Shapo V. F. Інформаційна технологія підсистеми ідентифікації на основі електронних ключів в системах електронного

документообігу. Bull. Nat. Tech. Univ. "KhPI". Ser.: System Analysis, Control and Information Technologies. 2020. № 1(3). С. 89–96. URL: http://samit.khpi.edu.ua/article/view/2079-0023.2020.01.16/207810

9. Зупанець І. В. Удосконалення системи електронного документообігу в процесах фармацевтичної розробки. 2025. URL: https://dspace.nuph.edu.ua/bitstream/123456789/34537/1/Зупанець%20Ігор%20Володимирович.pdf

10. Нікітін С. О. Програмна система розпізнавання цифрового підпису. 2019. URL: https://krs.chmnu.edu.ua/jspui/bitstream/123456789/663/1/%2b%20Aавтореферат%20БР%20-%20Нікітін.%20406з.pdf

11. Білик О. Сучасні підходи до впровадження електронного документообігу у систему державного управління. Наук. вісн. Вінниц. акад. безперерв. освіти. Серія: Екологія. Публічне управління та адміністрування. 2023. № 4. С. 38–45. URL: https://journals.academ.vinnica.ua/index.php/eco-pa/article/view/81/77

12. Колпак М. В. Система електронного документообігу підприємства. 2020. URL: https://ela.kpi.ua/server/api/core/bitstreams/ef8abe00-7916-4685-a2fb-fc2af4290f72/content

13. Сидорець Ю. М. Система електронного документообігу на основі технології блокчейн. 2019. URL: https://ela.kpi.ua/server/api/core/bitstreams/53236326-852c-4ca1-ae7b-235f95c3cb61/content

14. Вінцик Д. С. Система електронного документообігу. 2021. URL: https://ela.kpi.ua/server/api/core/bitstreams/d311bf41-ce3b-4ef1-9a5a-33d8f4aa686e/content

15. Стаднік Н. В. Алгоритми цифрового підпису на основі геш функції: кваліфікац. робота. Тернопіль: ЗУНУ, 2024. URL: http://dspace.wunu.edu.ua/bitstream/316497/53401/1/КР%20СТАДНІК%20Н.В%20.pdf

16. Шухманн В. А. Алгоритми цифрового підпису для блокчейн-технологій: кваліфікац. робота. Тернопіль: ЗУНУ, 2024. URL: http://dspace.wunu.edu.ua/bitstream/316497/53408/1/КР%20Шухманн.pdf

17. Дуданець Р. І. Алгоритм цифрового підпису на основі криптосистеми Нідеррейтера: кваліфікац. робота. Тернопіль: ЗУНУ, 2024. URL: http://dspace.wunu.edu.ua/bitstream/316497/53386/1/КР%20Дуданець.pdf

18. Двірна О. А., Бондаренко Р. М., Рудь А. О. Проектування та розробка інформаційної системи «Полтавський обласний клінічний медичний кардіоваскулярний центр». Дис. Нац. ун-т «Полтав. політехніка ім. Ю. Кондратюка», 2023. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/12452/1/75%20T.1-467-468.pdf

19. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні. 2019. URL: https://old.lpnu.ua/sites/default/files/dissertation/2019/13391/dysertaciya_na_zdobuttya_naukovogo_stupenya_kandydata_yurydychnyh_nauk_peruna_t.s.pdf

20. Гордієнко Є. Механізми реалізації державної політики соціального захисту учасників бойових дій в Україні: дис. ... д-ра філософії з публ. упр. та адміністрування. Харків: Харків. регіон. ін-т держ. упр. НАДУ, 2021. URL: https://ipa.karazin.ua/wp-content/themes/education/filesforpages/science/dis_gord_titl.pdf

21. Васенін К. Д., Нікуліна О. М. Розробка програмних компонентів для визначення геолокації клієнта для системи електронної комерції "American Eagle". 2024. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/15d6e1ee-3aef-440d-a301-353792f62e16/content

22. Шматко О. В., Кулініч Д. В., Горбач Т. В. Розробка та дослідження архітектурної моделі системи обміну персональними даними на основі блокчейн. Нац. ун-т «Полтав. політехніка ім. Ю. Кондратюка». 2024. С. 175.

23. Політанський В. С. Практика законодавчого закріплення електронного цифрового підпису в процесі здійснення публічного управління та впровадження цифрових технологій. Держ. буд-во та місц. самоврядування. 2023. С. 262. URL:

https://dbmsjournal.com/wp-content/uploads/2024/12/zb_derg_bud_45_2023.pdf#page=262

24. Куб'юк Є. Ю. Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей. 2024. URL: https://ela.kpi.ua/server/api/core/bitstreams/17b587c1-9441-4807-99aa-bfcd14669ea8/content

25. Анахін Г. В. Підвищення інтенсивної експлуатації дорожньої машини на базі інтелектуальної системи управління. 2023. URL: https://dspace.khadi.kharkov.ua/items/479075b7-1325-4eeb-b4ec-4aa5a5cdfccf

26. Лактіонов І. С. та ін. Результати розробки та дослідження комп'ютеризованої системи моніторингу кліматичних параметрів для сільськогосподарських об'єктів. Техн. інж. 2020. № 1(85). С. 165–170. URL: https://ten.ztu.edu.ua/article/view/206087

27. Галаган В. І., Бондарчук С., Полішко С. В. Пропозиції щодо удосконалення процесу впровадження інформаційних систем іноземного виробництва в діяльність Збройних Сил України. Зб. наук. пр. Центру воєн.-стратег. дослідж. Нац. ун-ту оборони України ім. І. Черняховського. 2019. № 2. С. 62–68.