ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

КВАЛІФІКАЦІЙНА РОБОТА

Тема: «Гнучке управління з розробки системи надання електронних довірчих послуг»

Ступінь вищої освіти – магістр

Спеціальність – 073 «Менеджмент»

Освітня програма «Agile-технології розробки програмного забезпечення»

ПОЯСНЮВАЛЬНА ЗАПИСКА

Керівник: д.е.н., доц.,професор
кафедри ІММС
Ольга ОРЛОВА-КУРИЛОВА

Виконав: здобувач
групи МЕН/Agile-24м-дист
Андрій ФІЛОНЕНКО

Засвідчую, що кваліфікаційна робота оформлена відповідно до ДСТУ 3008:2015 та не містить запозичень з праць інших авторів без відповідних посилань.
Здобувач: _____
(підпис)

Київ, 2026 р.

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

ЗАТВЕРДЖУЮ:
завідувач кафедри інформаційного менеджменту, математики та статистики
_____ Денис БАЛДИК
«__»____20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Філоненко Андрій Валерійович

Тема роботи	Гнучке управління розробкою системи надання електронних довірчих послуг
Номер та дата наказу про затвердження теми	№ 109-3 від 14 жовтня 2025 року
Коротка постановка завдання	Впровадження гнучкого підходу до управління створенням системи надання електронних довірчих послуг для підвищення ефективності введення системи в експлуатацію за рахунок застосування гнучких методологій
Посилання на джерела інформації (не більше п’яти найменувань, які рекомендує науковий керівник)	1. Manifesto for Agile Software Development // Agile Manifesto – URL: https://agilemanifesto.org/ 2. A Guide to the Project Management Body of Knowledge (PMBOK Guide) // Project Management Institute – URL: https://www.pmi.org/pmbok-guide-standards 3. Закон України "Про електронну ідентифікацію та електронні довірчі послуги" // Верховна Рада України – URL: https://zakon.rada.gov.ua/laws/show/2155-19
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має містити теоретичне та/або практичне дослідження за темою роботи, яку слід розглядати як складне спеціалізоване завдання або практичну проблематику в галузі управління та адміністрування, яка характеризується комплексністю та невизначеністю умов і потребує застосування Agile-технологій.

Дата видачі завдання «27» жовтня 2025 р.

Керівник Ольга ОРЛОВА-КУРИЛОВА

Здобувач Андрій ФІЛОНЕНКО

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання	Примітка
Підготовчий етап			
1	Вибір напряму дослідження та керівника.	01.09.2025 р.	*виконано*
2	Формування теми та призначення керівника.	22.09.2025 р.	*виконано*
3	Затвердження теми кваліфікаційної роботи.	09.10.2025 р.	*виконано*
4	Затвердження завдання на кваліфікаційну роботу.	27.10.2025 р.	*виконано*
Основний етап			
5	Розробка концепції кваліфікаційної роботи.	06.11.2025 р.	*виконано*
6	Підбір та вивчення джерел інформації з напряму дослідження. Огляд існуючих аналогів.	08.11.2025 р.	*виконано*
7	Теоретико-методичний аналіз предметної області та розширена постановка завдання. Підготовка та подання керівнику розділу 1 кваліфікаційної роботи.	13.11.2025 р.	*виконано*
8	Дослідницько-аналітична робота. Підготовка та подання керівнику розділу 2 кваліфікаційної роботи.	20.11.2025 р.	*виконано*
9	Розробка рекомендацій щодо вдосконалення управління із застосуванням Agile-технологій. Підготовка та подання керівнику розділу 3 кваліфікаційної роботи.	27.11.2025 р.	*виконано*
10	Підготовка та подання керівнику першого варіанту всієї кваліфікаційної роботи.	01.12.2025 р.	*виконано*
11	Доопрацювання кваліфікаційної роботи з урахуванням зауважень керівника та представлення керівнику доопрацьованого варіанту кваліфікаційної роботи	03.12.2025 р.	*виконано*
Завершальний етап			
12	Представлення рукопису для перевірки на плагіат.	08.12.2025 р.	*виконано*
13	Підготовка презентації та доповіді на передзахист.	22.12.2025 р.	*виконано*
14	Передзахист кваліфікаційної роботи.	23-24.12.2025 р.	*виконано*
15	Технічна самоекспертиза роботи на відповідність вимогам до оформлення та виправлення недоліків.	12-16.01.2026 р.	*виконано*
16	Експертиза роботи керівником та зовнішнім експертом (рецензентом).	20.01.2026 р.	*виконано*
17	Доопрацювання доповіді та презентації для захисту.	22.01.2026 р.	*виконано*
18	Захист кваліфікаційної роботи.	26-30.01.2026 р.	*виконано*

Керівник Ольга ОРЛОВА-КУРИЛОВА

Здобувач Андрій ФІЛОНЕНКО

АНОТАЦІЯ

Філоненко А. В. Гнучке управління з розробки системи надання електронних довірчих послуг.

Кваліфікаційна робота на здобуття ступеня магістра за спеціальністю 073 «Менеджмент». - Університет економіки та права «КРОК», Київ, 2025.

У кваліфікаційній роботі досліджено особливості застосування Agile-підходу при створенні систем кваліфікованих надавачів електронних довірчих послуг (КНЕДП). Проаналізовано стан ринку довірчих послуг в Україні, виявлено проблеми нормативної зарегульованості та технічної стагнації. Обґрунтовано необхідність інтеграції ролі юридичного аналітика в Agile-команду для забезпечення відповідності вимогам eIDAS та українського законодавства. Розроблено модель гнучкого управління проєктом, побудовано Use Case діаграми, User Persona та Business Model Canvas системи. Розраховано кошторис команди розробки та обґрунтовано економічну ефективність зниження ризиків через ітеративний підхід.

Ключові слова: agile-управління, електронні довірчі послуги, кеп, кнедп, юридичний аналітик, проєктний менеджмент.

ANNOTATION

Filonenko A. V. Agile management for the development of an electronic trust services system.

Master's qualification paper, specialty 073 «Management». - «KROK» University, Kyiv, 2025.

The qualification paper examines the features of applying the Agile approach in creating systems for qualified providers of electronic trust services (QTSP). The state of the trust services market in Ukraine is analyzed, and problems of regulatory rigidity and technical stagnation are identified. The necessity of integrating the role of a Legal Analyst into the Agile team to ensure compliance with eIDAS and Ukrainian legislation requirements is substantiated. An agile project management model is developed, Use Case diagrams, User Persona, and Business Model Canvas of the system are constructed. The development team budget is calculated, and the economic efficiency of risk reduction through an iterative approach is justified.

Keywords: agile management, electronic trust services, qes, qtsp, legal analyst, project management.

ЗМІСТ

ВСТУП

У зв’язку зі стрімким розвитком інформаційних технологій все більше послуг та сервісів стають доступними у форматі онлайн-систем. Сфери життя, що раніше вимагали значних витрат часу, нині вирішуються за лічені секунди. Угоди та контракти, що раніше вимагали особистої присутності, тепер узгоджуються онлайн у різних куточках світу. Це стало можливим завдяки технологіям, що забезпечують безпечні фінансові операції, обмін конфіденційними даними та надійну ідентифікацію особи. Завдяки технологіям електронної довіри підпис документів та укладання договорів можуть здійснюватись через онлайн-системи. Перехід на електронний формат підпису вдосконалює безліч бізнес-процесів та відкриває шлях до повноцінного електронного документообігу. На даний час у законодавстві України ключовим інструментом у цій сфері є Кваліфікований електронний підпис (КЕП).

Варто зазначити, що сьогодні КЕП в Україні є повним юридичним аналогом власноручного підпису. Підписати документ за допомогою КЕП може особа, яка володіє дійсним кваліфікованим сертифікатом відкритого ключа. Надання таких сертифікатів визначається як електронна довірча послуга, яку надають організації зі статусом Кваліфікованих надавачів електронних довірчих послуг (КНЕДП).

Незважаючи на те, що послуга з надання кваліфікованих сертифікатів є затребуваною, в Україні функціонує обмежена кількість КНЕДП (близько 20 активних суб’єктів). Статус надавача мають переважно державні установи та великі фінансові структури. Низька конкуренція на ринку та високий поріг входу призводять до повільного впровадження інновацій у цій сфері.

Причина обмеженої кількості надавачів пов’язана зі складністю розробки, впровадження та підтримки відповідних програмно-технічних комплексів (ПТК). Засоби КЕП повинні проходити експертизу в Державній службі спеціального зв’язку та захисту інформації України (ДССЗЗІ). Діяльність КНЕДП жорстко регулюється Законом України «Про електронну ідентифікацію

та електронні довірчі послуги», а також підзаконними актами, що регламентують процеси ідентифікації, генерації ключів та захисту інформації. Регулярні зміни в законодавстві та необхідність проходження аудитів вимагають постійної адаптації системи.

У сфері надання електронних довірчих послуг законодавство фактично диктує функціонал системи та логіку бізнес-процесів. Відсутність в IT-командах профільних юридичних фахівців та використання жорстких моделей управління (Waterfall) робить розробку таких систем ризикованою та довготривалою. Вирішити цю проблему можуть сучасні Agile-підходи, які дозволяють гнучко реагувати на зміни. Інтеграція ролі юридичного аналітика безпосередньо в Agile-команду відкриває нові можливості для мінімізації ризиків та забезпечення відповідності (compliance) в режимі реального часу.

Метою кваліфікаційної роботи є вдосконалення процесу розробки системи для надання кваліфікованих електронних довірчих послуг шляхом адаптації методології Agile.

Для досягнення мети поставлено такі **завдання**:

1. Дослідити стан використання кваліфікованого електронного підпису та обґрунтувати необхідність створення сучасних систем надання довірчих послуг.
2. Проаналізувати структуру, призначення та вимоги до кваліфікованих надавачів електронних довірчих послуг (КНЕДП).
3. Визначити особливості розробки та впровадження системи надання електронних довірчих послуг у регульованому середовищі.
4. Запропонувати шляхи оптимізації процесу розробки системи КНЕДП з використанням Agile-підходу та інтеграції юридичного контролю.
5. Розробити план реалізації системи та оцінити економічну ефективність запропонованого підходу.

Об’єкт дослідження - процес надання електронних довірчих послуг.

Предметом дослідження є процес управління розробкою програмного забезпечення у сфері електронних довірчих послуг, що регулюється законодавством.

Методи досліджень включають системний аналіз (для вивчення нормативної бази), моделювання бізнес-процесів (Use Case, Business Model Canvas), метод аналогій (порівняння Waterfall та Agile), метод експертних оцінок та економіко-статистичні методи (для розрахунку бюджету).

Наукова новизна полягає у розробці системного підходу до інтеграції юридичного аналітика в Agile-команду як обов'язкового елемента забезпечення відповідності (continuous compliance) у високорегульованих IT-проєктах.

Практична значущість роботи полягає у розробці адаптованої моделі управління проєктом створення КНЕДП, що дозволяє скоротити час виходу на ринок та знизити ризики невідповідності вимогам законодавства.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 74 сторінки. Робота містить 10 таблиць та 6 рисунків. Список використаних джерел налічує 49 найменувань.

РОЗДІЛ 1
СТАН РОЗВИТКУ СФЕРИ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ В УКРАЇНІ

1.1. Визначення особливостей застосування кваліфікованого електронного підпису в актуальних бізнес умовах

Розвиток цифровізації в Україні спричинив стрімке поширення практик електронного документообігу, онлайн-контрактування й віддаленої ідентифікації користувачів, що зробило кваліфікований електронний підпис (КЕП) ключовим інструментом сучасних бізнес-процесів. У правовій площині КЕП визначено як електронний підпис найвищого рівня довіри, прирівняний до власноручного згідно із Законом України «Про електронну ідентифікацію та електронні довірчі послуги» [36], а також гармонізований із вимогами європейського регламенту eIDAS [40]. Це означає, що будь-які ділові відносини, для яких традиційно вимагався підпис фізичного носія документа, тепер можуть здійснюватися в цифровому середовищі з тією ж юридичною силою, якщо використовується коректно сформований і чинний кваліфікований сертифікат. У сучасних умовах бізнесу важливо не лише те, що КЕП є засобом підписання документів, але й те, що він виступає універсальним інструментом ідентифікації, автентифікації та підтвердження намірів сторін у цифровому середовищі.

Практика українських підприємств демонструє, що електронні підписи стали основою внутрішнього і зовнішнього документообігу: контрактування з контрагентами, акти виконаних робіт, податкові документи, листування з органами державної влади, взаємодія з системами публічних закупівель, укладення цивільно-правових договорів із працівниками, автоматизація HR-процесів - усе це зводиться до єдиного стандарту підтвердження юридично значимих дій.

Значного поширення набули кейси використання КЕП у фінансовому секторі, де необхідно забезпечити найвищий рівень захисту операцій і недопущення фактів несанкціонованого доступу. Особливо це проявляється в операціях онлайн-банкінгу, дистанційного відкриття рахунків, ініціювання

платежів, укладення кредитних договорів та ідентифікації клієнтів, коли використання КЕП дозволяє виконувати процедури, які раніше неможливо було проводити без фізичної присутності клієнта.

У бізнес-середовищі все більше компаній відмовляються від паперових носіїв через високі витрати на логістику документів, архівування, фізичну верифікацію підписів керівників та ризики втрати або пошкодження документів. Цифровий підпис демонструє переваги як у швидкості та прозорості бізнес-процесів, так і в забезпеченні інформаційної безпеки.

На відміну від рукописного підпису, КЕП містить шифрований набір даних, який унеможливлює підробку або маніпуляції з документом після його підписання. Крім того, чинні вимоги до кваліфікованих надавачів забезпечують додатковий рівень захисту: обов’язкове проходження аудитів, сертифікація засобів криптографічного захисту, відповідність процедур ідентифікації вимогам закону, ведення надійних журналів подій і використання засобів створення захищених ключів.

Важливим аспектом сучасного застосування КЕП є необхідність дотримання вимог до всіх компонентів процесу підписання: від перевірки чинності сертифіката, формування відмітки часу, роботи довірчих списків до коректного ведення статусів відкликаних або заблокованих ключів. У цифровому середовищі юридична сила документа залежить не лише від факту накладення КЕП, але й від коректної роботи всієї інфраструктури довірчих послуг. Саме тому бізнес-середовище стикається з необхідністю впевненості в безперебійному функціонуванні сервісів, адже будь-які збої, наприклад недоступність OCSP-сервера або помилки в CRL, можуть паралізувати діяльність підприємства.

Оскільки ці сервіси забезпечують працівники кваліфікованих надавачів електронних довірчих послуг (КНЕДП), які несуть юридичну відповідальність за якість наданих послуг, саме функціонування КНЕДП стає фундаментальним інфраструктурним елементом цифрової економіки. Бізнес постійно потребує швидкої та надійної генерації сертифікатів для нових працівників, продовження строків чинності існуючих, перевипуску ключів у випадку втрати, а також

можливості оперативного блокування ключів при зміні повноважень посадових осіб. Це означає, що сучасні компанії напряму залежать від компетентності та технологічної готовності надавачів довірчих послуг, а також від можливості оперативно реагувати на технічні чи правові зміни.

Щоб показати місце КЕП та інших видів електронних підписів у практиці бізнесу, можна узагальнити їхні відмінності у аналітичній таблиці (табл. 1.1).

Таблиця 1.1 - Порівняння видів електронних підписів за рівнями довіри

Критерій	**Простий електронний підпис (ЕП)**	**Удосконалений електронний підпис (УЕП)**	**Кваліфікований електронний підпис (КЕП)**
Рівень юридичної сили	Низький, залежить від договору сторін	Середній, підтверджена ідентифікація	Максимальний, прирівняний до власноручного
Використання у бізнесі	Внутрішні процеси, low-risk дії	Середній рівень ризику, B2B-операції	Контракти, фінансові операції, звітність
Підтвердження особи	Необов’язкове	Обов’язкове	Обов’язкове, із застосуванням КНЕДП
Вимоги до інфраструктури	Мінімальні	Помірні	Строга регуляція, аудит, сертифікація
Можливість використання в судах	Частково	Обмежено	Повна юридична сила

Джерело: складено автором на основі [33]

Застосування КЕП у бізнесі має ще один важливий наслідок - можливість масштабування процесів. Коли компанія переходить на електронний документообіг, вона отримує не лише скорочення часу опрацювання документів, а й можливість автоматизації ланцюгів погоджень, що включають підписання значної кількості однотипних документів.

У багатьох великих підприємствах внутрішня система документообігу фактично не може існувати без КЕП, адже саме він дозволяє реалізувати контроль повноважень, надійний аудит подій та уникнення людського фактору. Це також зменшує кількість суперечок щодо автентичності підписів та спрощує процеси внутрішнього комплаєнсу.

Важливою тенденцією сучасних бізнес-процесів є трансформація моделі взаємодії між компаніями та державними органами. КЕП став базовим

елементом електронної комунікації бізнесу з державою: подання звітності, взаємодія з податковими органами, робота в електронних кабінетах, участь у державних закупівлях, формування первинної бухгалтерської документації, отримання або подання державних послуг через електронні реєстри. В умовах активного розвитку інфраструктури електронного урядування бізнес отримує можливість значно швидше здійснювати дії, які раніше вимагали фізичної присутності, живих підписів та печаток, що підкреслюється й у матеріалах судової та адміністративної практики, де електронний підпис визнається повноцінним інструментом юридичної взаємодії [33].

У практиці компаній дедалі частіше виникає потреба використовувати КЕП не лише для укладення договорів, але й для забезпечення доступу до інформаційних систем. Кваліфікований підпис стає засобом багаторівневої аутентифікації, що дозволяє контролювати повноваження співробітників, розмежовувати доступи та унеможливлювати дії, які можуть здійснювати лише посадові особи. Це стосується доступу до банківських рахунків, погодження фінансових транзакцій, підписання внутрішніх рішень і підтвердження значимих корпоративних операцій, що повністю відповідає вимогам до кваліфікованої електронної ідентифікації, закріпленим у профільному законодавстві України [36].

Паралельно з цим постає питання ризиків, пов’язаних із застосуванням КЕП. Незважаючи на високий рівень захисту, використання електронного підпису потребує суворого дотримання правил з боку підприємств та їхніх працівників. Неправильне зберігання ключів, передавання носіїв третім особам, незахищені робочі станції або відсутність належної політики управління повноваженнями можуть нівелювати безпекові переваги КЕП. У цьому контексті набуває особливого значення інфраструктура надавачів довірчих послуг, які відповідають за генерацію ключів, ведення реєстрів і підтримку сервісів перевірки статусів сертифікатів, що підтверджується вимогами нормативних документів і практикою їх застосування [31].

Використання КЕП у сучасних бізнес-процесах набуває ще більшої актуальності у зв’язку з євроінтеграційними процесами, оскільки законодавство

України поступово гармонізується з вимогами Регламенту eIDAS, що визначає стандарти електронної ідентифікації у країнах ЄС. Це дозволяє українським підприємствам адаптувати свої цифрові процеси до міжнародних вимог, забезпечувати визнання юридично значимих дій за кордоном та брати участь у транскордонних транзакціях, що прямо випливає зі змісту Регламенту №910/2014 [40].

Окремої уваги заслуговує специфіка правової природи кваліфікованого підпису в українській юрисдикції. Закон визнає КЕП повним аналогом власноручного підпису, водночас визначаючи суворі технічні та організаційні вимоги до процедур його створення, зберігання та використання. Юридична сила підпису залежить не лише від волевиявлення особи, але й від коректності всієї інфраструктури, яка забезпечує функціонування ключів, включно з криптографічними алгоритмами, носіями, журналами подій і механізмами перевірки. Такий режим регулювання формує складне техніко-правове середовище, у якому підприємства зобов'язані діяти, а надавачі довірчих послуг - постійно адаптувати свої системи, що прямо випливає з аналізу правових засад функціонування електронного підпису [28].

Саме складність цього середовища пояснює, чому застосування КЕП у бізнесі виходить за межі суто технічного питання. Будь-який процес, пов'язаний із підписанням документів, має відповідати вимогам законодавства щодо ідентифікації, статусу сертифікатів, процедур відкликання, журналювання подій та забезпечення безперервності доступу до сервісів довірчих послуг. Це потребує інтеграції спеціальних компетенцій, що поєднують правові, управлінські та технологічні підходи, на чому акцентують дослідники електронної комерції та цифрової юридичної інфраструктури [34].

Загалом сучасні бізнес-умови формують новий тип цифрової взаємодії між учасниками економічних відносин, де кваліфікований електронний підпис стає базовим компонентом корпоративного управління, комплаєнсу, документообігу та інформаційної безпеки. Його застосування створює передумови для повної цифрової трансформації, але одночасно висуває високі вимоги до технологічної, організаційної та юридичної підтримки з боку кваліфікованих надавачів, від яких

фактично залежить юридична чинність значної частини бізнес-процесів. Ця тенденція узгоджується з науковими підходами до розуміння ролі гнучких цифрових систем у сучасному бізнесі та державному управлінні [21].

1.2. Обґрунтування необхідності створення сучасних систем надання електронних довірчих послуг в Україні

Сучасний стан ринку електронних довірчих послуг (ЕДП) в Україні характеризується вираженою стагнацією та поступовим звуженням конкурентного середовища. Станом на грудень 2025 року, згідно з даними Довірчого списку, що ведеться Центральним засвідчувальним органом (ЦЗО), в Україні діє лише 23 кваліфікованих надавачі електронних довірчих послуг (джерело: czo.gov.ua/ca-registry).

Аналіз структури цих суб'єктів показує, що переважна більшість надавачів (понад 70%) є державними установами (ДП «Дія», Державна податкова служба, МВС, органи правосуддя тощо) або великими державними банками. Приватний сектор представлений обмеженою кількістю гравців, які були зареєстровані ще на етапі становлення ринку. Протягом останніх років спостерігається повна відсутність нових комерційних надавачів, що свідчить про критично високий поріг входу.

Основними деструктивними чинниками для ринкової динаміки є:

1. Жорсткість регулювання. Вимоги щодо побудови КСЗІ та обов'язкової сертифікації СУІБ створюють фінансовий бар'єр у мільйони гривень ще до початку надання послуг.

2. Ризик монополізації. Стрімке домінування екосистеми «Дія», яка пропонує безкоштовні та зручні рішення для широкого загалу, фактично позбавляє приватні КНЕДП економічних стимулів.

3. Складність підтримки відповідності. Необхідність постійної адаптації складних технічних систем до часто змінюваних вимог та європейських регламентів (eIDAS) вимагає значних людських ресурсів.

При цьому, надмірна концентрація ринку та ризики монополізації створюють критичні загрози для національної безпеки в умовах воєнного стану.

За ситуації, коли один надавач (зокрема ДП «Дія») утримує домінуючу частку ринку, виникає проблема єдиної точки відмови. У випадку масштабної кібератаки, технічної аварії або фізичного пошкодження інфраструктури домінуючого надавача внаслідок бойових дій, країна може зіткнутися з раптовою неможливістю мільйонів громадян та тисяч підприємств користуватися довірчими послугами. Це призведе до паралічу електронного документообігу, зупинки надання державних сервісів, неможливості подання податкової звітності та здійснення банківських операцій.

З огляду на це, децентралізація ринку ЕДП та стимулювання появи нових конкурентоспроможних надавачів є питанням стратегічної стійкості (resilience) цифрової економіки України. Необхідно створити умови, за яких приватний сектор зможе ефективно розгортати нові КНЕДП, забезпечуючи резервування та альтернативу державним сервісам.Розширюється коло користувачів - від великих корпорацій до представників малого та середнього бізнесу, а також приватних осіб, які дедалі частіше використовують КЕП для отримання державних послуг, участі в електронних торгах чи подання звітності. Усе це призводить до підвищення вимог до стабільності, продуктивності та масштабованості систем КНЕДП, а їхнє недостатнє технологічне забезпечення створює ризики для всієї цифрової інфраструктури держави [31].

Важливою мотивацією для створення нових систем електронних довірчих послуг є також поступова гармонізація українського законодавства із європейським правовим полем. Регламент №910/2014 (eIDAS) визначає рамкові вимоги щодо електронної ідентифікації та довірчих послуг у ЄС, які стають орієнтиром для України в контексті інтеграційних процесів.

Йдеться про необхідність забезпечення сумісності українських систем із європейськими, що у перспективі дозволить визнання українських електронних підписів у державах-членах ЄС. Для цього потрібне оновлення технологічних платформ та підходів до їх розробки, зокрема використання сучасних моделей управління ІТ-проєктами та ефективної взаємодії технічних і юридичних

спеціалістів, про що свідчить дослідження сучасних підходів до електронної ідентифікації [40].

Не менш важливою є необхідність підвищення довіри користувачів до електронних послуг. Будь-який збій у роботі КНЕДП, недоступність сервісів, складнощі з перевіркою статусів сертифікатів або затримки у генерації ключів можуть мати суттєві наслідки не лише для окремої організації, а й для цілих галузей економіки.

Усе це ставить перед розробниками довірчих систем вимогу формувати такі архітектури, які гарантують високу відмовостійкість, прозорість процесів та відповідність етичним і правовим принципам. У наукових дослідженнях зазначається, що безпека й ефективність електронних транзакцій напряму залежать від того, наскільки коректно побудовані правові та технічні механізми, що підтримують функціонування довірчих послуг, а отже, потребують постійного оновлення та вдосконалення [11].

Потреба створення сучасних систем електронних довірчих послуг зумовлена також низкою управлінських викликів. У реальних умовах КНЕДП не лише генерують сертифікати, а й виконують складні функції з організації клієнтського обслуговування, проведення аудиту відповідності, документування процесів, моніторингу інцидентів безпеки та контролю процедур відкликання ключів. Ці функції взаємодіють між собою в межах складної організаційно-технічної структури, де ефективність системи залежить не лише від технологій, а й від правильного управління, включаючи комунікації, розподіл відповідальності та планування робіт. Саме тому питання управління створенням таких систем стає ключовим - від вибору методології розробки до визначення ролей і компетенцій, необхідних команді, що узгоджується із сучасними підходами до організації проєктної діяльності [22].

Для систематизації основних мотивів, що формують потребу у створенні сучасних КНЕДП, доцільно узагальнити ключові групи чинників у вигляді аналітичної таблиці (табл. 1.2).

Таблиця 1.2 - Основні причини необхідності створення сучасних систем електронних довірчих послуг

Група причин	**Зміст впливу**
Регуляторні	Постійні зміни законодавства, гармонізація з eIDAS, вимоги до аудиту та акредитації
Технологічні	Зростання обсягу користувачів, збільшення навантаження, потреба в масштабованості та стійкості
Ринкові	Низька конкуренція серед КНЕДП, обмежена пропозиція якісних сервісів
Управлінські	Висока складність процесів, необхідність інтеграції юридичного та технічного аналізу
Бізнес-потреби	Оптимізація документообігу, прискорення операцій, підвищення безпеки транзакцій

Джерело: складено автором на основі [36]

Таким чином, необхідність створення сучасних систем електронних довірчих послуг в Україні є комплексною і визначається одночасно регуляторними, технологічними, економічними та управлінськими факторами. Сфера електронних довірчих послуг перестала бути лише допоміжним інструментом документообігу й перетворилася на фундаментальну складову цифрової економіки, від якої залежить стабільність значної частини бізнес-процесів і державних сервісів. Це формує нагальну потребу у впровадженні сучасних підходів до розробки, управління та підтримки таких систем, що відповідають викликам сьогодення.

1.3. Роль підходів управління у процесі створення електронних довірчих послуг

Створення сучасних систем електронних довірчих послуг є складним багатофакторним процесом, у якому поєднуються технологічні, правові та організаційні компоненти. Ефективність таких систем безпосередньо залежить від того, наскільки грамотно обрані та реалізовані підходи до управління їх розробкою. У цій сфері на передній план виходить необхідність інтегрувати технічні стандарти, вимоги законодавства та очікування користувачів у єдину керовану модель. Наукові дослідження засвідчують, що електронні довірчі

послуги не можуть створюватися виключно інженерними засобами, оскільки вони є юридично значимою інфраструктурою, що функціонує в умовах суворого нормативного регулювання [36].

Вибір управлінського підходу значною мірою визначає, яким буде життєвий цикл системи, швидкість її адаптації до законодавчих змін, стійкість до кіберзагроз та здатність інтегрувати нові сервіси. Оскільки КНЕДП виконують суспільно важливі функції - від генерування ключів до ведення реєстрів і забезпечення юридичної достовірності транзакцій, - управління їх створенням потребує поєднання стратегічного бачення та гнучкого реагування на ризики. У цьому контексті можна простежити взаємозв'язок між розвитком електронних довірчих послуг і загальною еволюцією методологій управління, які переходили від класичних до адаптивних моделей, що також підкреслюється у сучасних дослідженнях стратегічного управління [50].

Класичні підходи до управління проєктами, такі як водоспадна модель, історично домінували в розробці критичних IT-систем. Вони передбачали детальне планування, фіксацію обсягу робіт, чітку послідовність етапів і однозначну відповідальність.

Для систем довірчих послуг такий підхід певною мірою залишається актуальним, оскільки забезпечує передбачуваність, формалізованість і контроль якості. Проте він виявляється недостатньо гнучким у ситуаціях, коли законодавчі норми змінюються швидше, ніж завершується типовий цикл розробки. У таких умовах надмірна жорсткість планування може призвести до затримок, перевитрат ресурсів і втрати актуальності технічних рішень до моменту їх впровадження [32].

Сучасні виклики у сфері електронних довірчих послуг зумовлюють потребу в застосуванні адаптивних підходів, які дозволяють швидко реагувати на зміни регуляторного середовища, кіберзагроз, технологічних стандартів і потреб ринку. Agile-методології, зокрема Scrum, Kanban та їх масштабовані модифікації, створюють умови для безперервної адаптації системи, а також регулярного тестування функцій, пов'язаних із безпекою та відповідністю.

У сфері довірчих послуг така гнучкість є критично важливою, адже будь-які недоліки у механізмах перевірки сертифікатів, обробки OCSP-запитів чи захисту ключів від компрометації мають прямі юридичні наслідки. Дослідження сучасних підходів до організації командної взаємодії підтверджують, що гнучкі методи управління дозволяють суттєво скоротити час між виявленням проблеми та її усуненням, що є важливою вимогою у сфері електронної безпеки [39].

Одним із найважливіших аспектів управління в діяльності КНЕДП є синхронізація технічних і юридичних процесів. Жоден модуль такої системи - генерація ключів, випуск сертифікатів, ведення журналів, підтримка CRL або перевірка OCSP - не може бути створений без урахування правових вимог. Тому управління розробкою електронних довірчих послуг повинне включати регулярну юридичну експертизу, перевірку відповідності нормам eIDAS, постановам Кабінету Міністрів, наказам Мінцифри та іншим нормативним актам. Ця потреба створює особливий тип управлінських практик, який поєднує технічне мислення з юридичним аналізом, що знайшло відображення у дослідженнях правової природи механізмів електронної ідентифікації [30].

Не менш важливою складовою управлінського підходу є питання побудови команд та розподілу відповідальності. Створення довірчих послуг потребує залучення криптографів, програмістів, спеціалістів з інформаційної безпеки, юристів, аудиторів, адміністраторів реєстрів і фахівців із ризик-менеджменту. Ефективність роботи такої мультидисциплінарної команди залежить від методології, яка визначає канали взаємодії, цикли перевірок, механізми управління ризиками та процедури документування. У наукових дослідженнях підкреслюється, що саме якість управління змінами, комунікаціями та ризиками формує здатність організації підтримувати стійку роботу критично важливих IT-систем, особливо коли йдеться про сервіси, юридична значимість яких залежить від безперервності їх функціонування [11].

З огляду на складність створення таких систем, доцільно узагальнити ключові управлінські підходи, які застосовуються у практиці розробки електронних довірчих послуг, представимо їх у вигляді таблиці (табл. 1.3).

Таблиця 1.3 - Управлінські підходи у створенні систем електронних довірчих послуг

Підхід	Характерні риси	Значення для КНЕДП
Класичний	Чітка регламентація, послідовні етапи, формальний контроль	Забезпечує передбачуваність і юридичну формалізацію процесів
Процесний	Наголос на повторюваності, стандартах і регламентованих циклах	Оптимальний для побудови реєстрів, аудитів і перевірок сертифікатів
Ресурсний	Орієнтація на унікальні компетенції та ключові можливості організації	Дозволяє формувати стійкі команди та спеціалізовані компетентні центри
Адаптивний (Agile)	Гнучкість, постійні ітерації, можливість реагувати на зміни	Критичний для відповідності законодавству та оперативного усунення ризиків

Джерело: складено автором на основі [50]

Загалом роль управлінських підходів у створенні електронних довірчих послуг є визначальною, оскільки саме вибір методології визначає стійкість, якість, юридичну відповідність та здатність систем адаптуватися до технологічних і нормативних змін. Сфера довірчих послуг функціонує на перетині права, інформаційної безпеки та інженерії, тому управління проєктами у цій галузі потребує глибокого синтезу міждисциплінарних знань. Правильно обрана модель управління дає змогу забезпечити високу якість електронних транзакцій, підвищити довіру користувачів і гарантувати безперервне функціонування критичної цифрової інфраструктури.

Висновки до розділу 1

Проведений у першому розділі аналіз дав змогу комплексно окреслити сучасний стан розвитку кваліфікованого електронного підпису та електронних довірчих послуг в Україні, виявивши їхню важливість для формування цифрової економіки та модернізації бізнес-процесів. Визначення сутності КЕП, його правового статусу та ролі в сучасних комунікаціях показало, що цей інструмент перетворився на ключовий елемент електронної взаємодії між бізнесом, державою та громадянами. Саме КЕП забезпечив перехід від паперових процедур до інтегрованих цифрових процесів, де підтвердження волевиявлення,

автентифікація та юридична чинність документів здійснюються у дистанційному форматі без втрати правової сили.

У межах розділу було встановлено, що КЕП сьогодні виступає не лише технічним рішенням, а й складним юридично-технологічним механізмом, побудованим на основі суворих нормативних вимог, криптографічної інфраструктури та процедур державного контролю. Це зумовлює розширення відповідальності надавачів послуг, які мають забезпечувати не тільки функціональність, але й безпеку, стійкість та відповідність вимогам законодавства. Аналіз законодавчих норм дозволив дійти висновку, що українська система електронних довірчих послуг поступово гармонізується зі стандартами ЄС, проте залишається низка проблем, пов’язаних із оновленням нормативної бази, стандартизацією процедур та узгодженням технічних вимог.

Також було виявлено, що застосування КЕП в актуальних бізнес-умовах виходить далеко за межі підписання договорів чи звітності. Підпис стає компонентом цифрової ідентичності та засобом корпоративного контролю, інтегрується у фінансові, управлінські та організаційні процеси. Ця трансформація демонструє, що кваліфікований електронний підпис набуває значення елемента внутрішньої безпеки підприємства та основи цифрового документообігу.

Отже, перший розділ дозволив сформувати цілісне уявлення про сутність та правову природу електронних довірчих послуг, визначити ключові потреби та проблеми їх подальшого розвитку, а також підкреслити важливість впровадження систем, здатних забезпечити надійність, юридичну визначеність та технологічну стійкість усіх процесів, пов’язаних із використанням КЕП.

РОЗДІЛ 2
АНАЛІЗ МОЖЛИВОСТЕЙ КВАЛІФІКОВАНИХ НАДАВАЧІВ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

2.1. Організаційно-правові вимоги до кваліфікованих надавачів електронних довірчих послуг

Організаційно-правові вимоги до кваліфікованих надавачів електронних довірчих послуг формують нормативний каркас, без якого функціонування систем електронного підпису, печатки, сертифікації та електронної ідентифікації було б юридично неможливим. КНЕДП є суб'єктом, на якого держава покладає обов'язок створювати, підтримувати та забезпечувати цілісність критично важливої інфраструктури довіри, а тому до такого суб'єкта висувається підвищений стандарт відповідності.

Центральним нормативним актом, що визначає ці вимоги, є Закон України «Про електронну ідентифікацію та електронні довірчі послуги», який встановлює юридичну природу довірчих сервісів, порядок акредитації надавачів та перелік їх функцій, що мають бути реалізовані на належному рівні захисту, надійності та технічної сумісності [1].

Юридичний статус надавача електронних довірчих послуг передбачає, що така організація має бути створена у формі суб'єкта господарювання, здатного нести відповідальність за порушення вимог законодавства, включно з майновою, адміністративною та навіть кримінальною відповідальністю у разі компрометації ключів чи сертифікатів. При цьому законодавець вимагає не лише формального дотримання правових норм, але й наявності внутрішньої системи управління ризиками, інформаційною безпекою, а також комплексом організаційних процедур, які гарантують контроль доступу до критичних елементів інфраструктури.

Саме надавач несе відповідальність за генерацію ключів, ведення реєстрів, захист носіїв особистих ключів, підтримку журналів подій та збереження достовірності всієї ланки довіри, що логічно випливає із загальної концепції

правової природи електронного підпису, сформульованої як аналог власноручного підпису за умови дотримання встановлених процедур [32].

Важливим елементом організаційно-правових вимог є забезпечення інституційної стійкості та надійності надавача. З огляду на те, що довірчі послуги не можуть бути тимчасовими або непередбачуваними, закон вимагає від КНЕДП наявності фінансової спроможності, відкритої та прозорої структури власності, документованих внутрішніх політик і чіткої організаційної структури.

Надавач повинен демонструвати здатність забезпечувати безперервне функціонування сервісів, що включає резервування потужностей, відмовостійкі архітектури, дублювання компонентів, а також постійний моніторинг стану системи. Дослідження у сфері електронної ідентифікації підтверджують, що стійкість організації є ключовим фактором довіри до її послуг, оскільки будь-який збій або втрата доступності сервісу може мати прямі юридичні наслідки для громадян та бізнесу [30].

Однією з найбільш складних і водночас критично важливих частин вимог є забезпечення інформаційної безпеки. На рівні нормативних актів визначено, що КНЕДП зобов’язаний впровадити багаторівневу систему захисту, яка включає криптографічні засоби, апаратні модулі безпеки, захищені канали зв’язку, механізми автентифікації та протидії несанкціонованому доступу.

Вимоги до інформаційної безпеки не обмежуються технічними протоколами: вони також охоплюють процедури управління персоналом, регламенти доступу, порядок проведення внутрішніх аудитів та оцінку відповідності міжнародним стандартам. Сучасні дослідження підкреслюють, що інформаційна безпека у сфері довірчих послуг не може розглядатися як окрема функція; вона має бути інтегрована в усі бізнес-процеси організації, формуючи цілісну модель захисту, відповідну критично важливому статусу цих послуг [39].

Особливу увагу законодавець приділяє забезпеченню прозорості й контрольованості діяльності надавачів. КНЕДП зобов’язаний вести повну документацію щодо своїх процесів, включно з технічними інструкціями, політиками сертифікації, журналами генерації ключів, процедурами роботи з

носіями особистих ключів, правилами ідентифікації та автентифікації користувачів.

Усі ці документи становлять основу для проходження регулярних аудитів відповідності, без яких правовий статус надавача не може бути збережений. Саме система зовнішнього контролю забезпечує легітимність інфраструктури довіри, а вимога щодо періодичної атестації відповідає міжнародним підходам, які також передбачають незалежну оцінку систем безпеки перед тим, як вони визнаються здатними забезпечувати юридично значимі транзакції [27].

Окремим і надзвичайно важливим блоком вимог є юридичні гарантії захищеності користувачів, які покладаються на послуги КНЕДП для здійснення електронних операцій. Закон встановлює обов’язок надавача забезпечити коректність інформації у сертифікатах, перевірку правомірності звернення користувача при створенні чи скасуванні ключа, надання достовірної інформації у відкритих реєстрах, а також захист особистих даних.

КНЕДП не має права видавати сертифікат без проходження повної ідентифікації особи, що є однією з ключових юридичних гарантій дійсності підпису. Відсутність належної ідентифікації вважається порушенням юридичних стандартів, що підтверджується низкою досліджень, які акцентують увагу на критичній ролі контролю суб’єктності у процесі електронної взаємодії [12].

З огляду на високі ризики у сфері електронних довірчих послуг, законодавство вимагає впровадження комплексної моделі управління ризиками, яка охоплює технологічні, юридичні та організаційні загрози. Надавач зобов’язаний мати документовані процедури реагування на інциденти, механізми відстеження компрометації ключів, плани відновлення після аварій та алгоритми обмеження шкоди у разі порушення цілісності даних чи доступності сервісів. Ризик-орієнтоване управління є однією з умов акредитації, що логічно узгоджується з сучасними моделями стратегічного управління, у яких адаптивність і швидкість реагування на проблеми є вирішальними факторами успіху [50].

Завершальним, але не менш важливим елементом організаційно-правових вимог є забезпечення технологічної та юридичної сумісності сервісів надавача із

загальноєвропейською інфраструктурою довіри. Україна гармонізує своє законодавство з Регламентом eIDAS, тому КНЕДП мають поступово переходити до моделей, що забезпечують взаємне визнання електронних підписів, печаток і засобів ідентифікації на рівні ЄС. Це означає, що надавач повинен впроваджувати технології, які відповідають європейським технічним стандартам, а також будувати свою внутрішню політику таким чином, щоб усі процеси могли пройти міжнародний аудит. У наукових роботах, присвячених цифровій інтеграції України, підкреслюється, що саме сумісність і відповідність eIDAS відкриває шлях до включення українських надавачів у пан'європейський ринок довірчих сервісів [4].

Організаційно-правові вимоги до кваліфікованих надавачів електронних довірчих послуг охоплюють також питання внутрішнього контролю та корпоративного управління, оскільки ефективність роботи КНЕДП визначається не лише технічними рішеннями, а й тим, яким чином організація структурує свої процеси, розподіляє повноваження та забезпечує незалежний моніторинг критично важливих функцій.

Система внутрішнього контролю включає документовані процедури нагляду за доступом до криптографічних модулів, контроль змін у програмному забезпеченні, а також аудит інцидентів, що стосуються безпеки або можливого порушення регламентованих процедур. У сучасних дослідженнях підкреслюється, що якість корпоративного управління безпосередньо впливає на довіру до цифрових сервісів, оскільки саме внутрішні управлінські практики визначають стійкість системи до зовнішніх загроз і людських помилок [8].

Важливою вимогою для КНЕДП є забезпечення прозорої та контрольованої процедури генерації особистих і кваліфікованих ключів. Ключі можуть створюватися лише у спеціалізованих, сертифікованих засобах криптографічного захисту інформації, які відповідають вимогам державних та міжнародних стандартів.

Порушення процедури генерації або втручання у процес формування пари ключів призводить до абсолютної недійсності підпису, що створює юридичну загрозу як для користувача, так і для надавача. Саме тому регламентація цих

процедур є настільки детальною, і законодавство прямо вимагає, щоб генерація ключів відбувалася в умовах фізичної, мережевої та процедурної безпеки. У роботах, присвячених методології організації захищених систем, наголошується, що контроль за процесом створення ключів є центральним елементом довірчого ланцюга, який забезпечує юридичну силу електронної ідентифікації [17].

Окремого аналізу потребує питання ведення та захисту реєстрів - сертифікатів, статусів, журналів відкликання та блокування ключів. Ці реєстри є юридично значимими інформаційними ресурсами, на основі яких будується можливість перевірити чинність підпису або печатки у конкретний момент часу.

Будь-яка помилка у реєстрі, його недоступність або затримка в оновленні статусів може призвести до того, що транзакції втратять юридичну силу або будуть оскаржені у судовому порядку. Саме тому законодавець встановлює жорсткі вимоги до технічних характеристик цих реєстрів, включаючи їх відмовостійкість, час реакції, точність відображення даних та повноту журналів подій, що підтверджується й науковими роботами, присвяченими функціонуванню відповідних систем у європейській практиці [5].

У сфері організаційних вимог важливою складовою є управління персоналом КНЕДП, адже значна частина загроз походить не від зовнішніх атак, а від людського фактору. Нормативні акти вимагають, щоб до критичних процесів допускалися лише співробітники, які пройшли спеціальну підготовку, мають підтверджену кваліфікацію та підписали угоди про нерозголошення. Крім того, персонал має підлягати регулярному навчанню щодо вимог законодавства, технологій криптографічного захисту та процедур реагування на інциденти.

У дослідженнях з управління ризиками підкреслюється, що саме правильна організація роботи персоналу є одним з найбільш ефективних способів зниження загроз у високорегульованих IT-системах, де людський фактор може стати критичним джерелом вразливостей [13].

Суттєве місце серед організаційно-правових вимог займають зовнішні аудити відповідності, які виконують функцію незалежної оцінки того, наскільки діяльність КНЕДП відповідає нормам закону, технічним регламентам, вимогам до захищеності ключових операцій та правилам роботи з реєстрами. Акредитація

та аудит є не просто формальною процедурою; вони виступають гарантією того, що надавач може функціонувати у складі національної інфраструктури довіри. Наявність документально підтверджених аудитів є також умовою для міжнародного визнання електронних довірчих послуг, особливо у контексті інтеграції України у європейський цифровий ринок, де відповідність стандартам eIDAS має вирішальне значення. У наукових публікаціях, присвячених регулюванню цифрових сервісів у ЄС, підкреслюється, що саме зовнішня оцінка відповідності є ключовим інструментом забезпечення стабільності та прозорості ринку довірчих послуг [22].

У контексті вимог до діяльності КНЕДП надзвичайно важливою є здатність організації підтримувати не лише технологічну, але й юридичну актуальність своїх сервісів. Зміни у законодавстві, оновлення технічних стандартів, ухвалення нових регламентів або рішень регуляторних органів зобов’язують надавача оперативно адаптувати свої процеси, політики та технічні модулі.

Застосування застарілих норм або неврахування нових регуляцій може призвести до невизнання юридичної сили підписів, блокування сертифікатів або навіть втрати статусу кваліфікованого надавача. У дослідженнях з управління змінами в цифровому середовищі наголошується, що нормативна динаміка має бути інтегрованою у процеси розробки, тестування та експлуатації систем, оскільки без цього неможливо забезпечити сталість юридичної інфраструктури [50].

Окремим аспектом організаційно-правових вимог є взаємодія КНЕДП з користувачами, адже саме правильність процедур обслуговування створює підґрунтя для юридичної достовірності підписів у майбутніх правовідносинах. Надавач зобов’язаний забезпечити чіткі правила видачі сертифікатів, ідентифікації осіб, процедури відновлення доступу, механізми скасування ключів та інформування користувачів про зміни у стані їхніх сертифікатів.

Неправильно організована взаємодія з клієнтом може призвести до недійсності всіх транзакцій, виконаних з використанням підпису, або до відповідальності надавача за недотримання стандартів обслуговування. У

сучасних дослідженнях електронного урядування зазначається, що якість сервісної моделі та юридична грамотність процедур взаємодії з користувачами є не менш важливими, ніж технічний рівень системи [26].

Загалом організаційно-правові вимоги до кваліфікованих надавачів електронних довірчих послуг формують комплексну систему регулювання, яка покликана забезпечити надійність, безпеку та юридичну достовірність усіх електронних транзакцій. КНЕДП працюють у сфері, де технічна помилка миттєво перетворюється на юридичний інцидент, а порушення процедури може поставити під сумнів сотні або тисячі документів.

Саме тому законодавство створює багаторівневу модель контролю, що поєднує вимоги до організаційної структури, інформаційної безпеки, управління ризиками, документування процесів, юридичної відповідності та міжнародної сумісності. Такий підхід відповідає світовим практикам і забезпечує здатність української інфраструктури електронної довіри функціонувати стабільно навіть в умовах швидкої цифрової трансформації.

2.2. Аналіз технічних та функціональних можливостей кваліфікованих надавачів електронних довірчих послуг

Аналіз технічних та функціональних можливостей кваліфікованих надавачів електронних довірчих послуг дає змогу оцінити рівень їхньої технологічної готовності до виконання ключових операцій національної інфраструктури довіри та відповідність вимогам законодавства.

КНЕДП забезпечують виконання функцій, які мають безпосередній юридичний ефект: генерування ключів, створення сертифікатів, підтримка механізмів перевірки статусів, захист особистих ключів, ведення журналів подій, аудит процесів та забезпечення доступності сервісів.

У зв’язку з високими регуляторними вимогами та критичністю сервісів для бізнесу та держави, технічні можливості надавачів мають бути не лише якісними, але й адаптивними, масштабованими та стійкими до зовнішніх і внутрішніх загроз. Дослідження у сфері цифрової ідентифікації підкреслюють, що саме

технічна архітектура та якість реалізації протоколів є основою юридичної сили електронних підписів та довірчих транзакцій [12].

Функціональні можливості КНЕДП охоплюють повний цикл життєдіяльності сертифікатів - від моменту заявлення особою наміру отримати ключ до моменту відкликання чи закінчення строку його дії. Центральним елементом є підтримка сертифікаційного центру, який має виконувати операції з генерації криптографічних ключів у захищених апаратних пристроях, створення кваліфікованих сертифікатів, їх підписання кореневими ключами, розміщення у відкритих реєстрах та оновлення статусів. Таким чином забезпечується юридична простежуваність кожного підпису. Сучасні дослідження юридичної природи електронних довірчих послуг підкреслюють, що саме наявність надійної інфраструктури сертифікації є ключовою умовою легітимності всіх транзакцій [1].

Особливо важливою частиною технічних можливостей є підтримка механізмів перевірки статусів ключів та сертифікатів, зокрема OCSP (Online Certificate Status Protocol) та CRL (Certificate Revocation List). Ці механізми забезпечують можливість будь-якому користувачу в режимі реального часу визначити, чи є сертифікат чинним або скасованим. Надійність OCSP-відповідачів, швидкість обробки запитів, відмовостійкість вузлів та повнота CRL-списків визначають можливість визнання електронного підпису дійсним у конкретний момент часу. У міжнародних дослідженнях інфраструктури довіри підтверджено, що саме якість та оперативність реагування механізмів статус-перевірки визначають юридичну стабільність екосистем цифрових підписів [27]. Технічні можливості КНЕДП повинні охоплювати також захищені канали обміну даними, включаючи TLS-шифрування, сегментацію мереж, застосування апаратних модулів безпеки (HSM), що використовуються для генерування та зберігання кореневих ключів центру сертифікації.

Надійність HSM-модулів є критичною, оскільки вони фактично формують ядро довіри: компрометація кореневого ключа означає неможливість довіряти будь-яким сертифікатам надавача. Рекомендації міжнародних експертів у сфері криптографічної безпеки підтверджують, що без застосування сертифікованих

HSM, які відповідають стандартам FIPS 140-2 або вище, неможливо гарантувати цілісність довірчої інфраструктури [39].

У структурі технічних можливостей КНЕДП важливу роль відіграє також система журналів, яка забезпечує фіксацію всіх подій, пов’язаних із ключами, сертифікатами, доступами, змінами конфігурацій та інцидентами інформаційної безпеки. Журнали мають зберігатися у незмінному вигляді протягом визначеного законодавством часу, і саме вони є основним доказовим інструментом у випадку судових спорів або аудиторських перевірок. У наукових роботах з управління електронними транзакціями зазначено, що прозорість і повнота журналів є ключовим елементом побудови довіри та механізмом постінцидентної оцінки ризиків [17]. Важливе місце у функціональних можливостях надавачів займає забезпечення високого рівня доступності сервісів - SLA не може допускати суттєвих простоїв, оскільки будь-яка зупинка OCSP, реєстрів або сервісів підписання спричиняє юридичні та фінансові наслідки для користувачів. Надавач має забезпечувати резервування каналів, дублювання критичних вузлів, географічно розподілені дата-центри та системи автоматичного перемикання при аваріях.

У дослідженнях цифрової стійкості підкреслюється, що саме відмовостійкість та доступність критичних сервісів визначають якість функціонування всієї екосистеми електронного документообігу [33].

Рисунок 2.1 - Структура технічних можливостей КНЕДП

Джерело: побудовано автором

Далі розглянемо ключові технічні можливості різних типів надавачів (умовних), що можна використати в роботі для аналітичного порівняння (табл. 2.1).

Таблиця 2.1 - Порівняльний аналіз технічних можливостей КНЕДП

Критерій	**Національні КНЕДП**	**Комерційні КНЕДП**	**Галузеві (банківські) КНЕДП**
Масштабованість систем	Висока, орієнтація на масові сервіси держави	Висока, залежно від інвестицій	Дуже висока, оптимізована під фінансові транзакції
Швидкість OCSP	Стабільна, але залежить від навантаження	Висока за рахунок оптимізованих кластерів	Максимальна, з жорсткими SLA
HSM-інфраструктура	Державні сертифіковані модулі	Комерційні FIPS-сертифіковані рішення	Корпоративні HSM рівня 3-4
Резервування та відмовостійкість	Висока, але менш гнучка	Гнучка, орієнтована на бізнес-ризики	Максимальна, з дублюванням у різних регіонах
Рівень сервісності	Стандартизований	Залежить від бізнес-моделі	Преміальний, з 24/7 підтримкою

Джерело: складено автором на основі [27]

Подальший аналіз технічних можливостей кваліфікованих надавачів електронних довірчих послуг неможливий без розгляду рівня їхньої інтегрованості з національною цифровою інфраструктурою, оскільки КНЕДП не є ізольованими організаціями, а працюють у середовищі, де кожна транзакція пов’язана з державними реєстрами, системами електронного урядування, сервісами «Дія», податковими кабінетами, банками, біржовими майданчиками та корпоративними платформами.

Якість інтеграції визначається тим, наскільки швидко та безпечно надавачі можуть передавати дані, перевіряти статуси сертифікатів і забезпечувати структуровані API для бізнесу та державних установ. У сучасних дослідженнях цифрової інфраструктури акцентується, що саме рівень інтеграційної сумісності формує можливість побудови наскрізних електронних процесів, у яких електронний підпис є лише одним із компонентів [17].

Надзвичайно важливим аспектом функціональних можливостей КНЕДП є підтримка різних форматів електронного підпису та електронної печатки, включаючи CAdES, XAdES та PAdES, що забезпечують юридичну силу документів у різних інформаційних середовищах.

Кожен з форматів виконує специфічну функцію: CAdES оптимізований для підписання файлів будь-якого типу, XAdES - для структурованих XML-документів, а PAdES - для PDF-документів, що найчастіше використовуються у публічному та корпоративному секторі. Підтримка цих форматів впливає на можливість взаємодії українських компаній із міжнародними контрагентами, оскільки ЄС використовує аналогічні стандарти. У наукових джерелах наголошується, що саме стандартизовані формати підпису забезпечують юридичну сумісність на глобальному рівні та мінімізують правові колізії при транскордонних операціях [29].

З технічного погляду важливо оцінити здатність КНЕДП забезпечувати масштабованість і стійкість до пікових навантажень. У періоди масового подання звітності, реєстрації податкових накладних або участі бізнесу в державних закупівлях навантаження на інфраструктуру різко зростає, і відмови сервісів OCSP чи реєстрів статусів можуть спричинити фінансові збитки для користувачів. Саме тому технічна архітектура КНЕДП має бути орієнтована не на середній рівень навантаження, а на найнесприятливіші сценарії роботи. Рекомендації експертів із цифрової стійкості вказують, що надавачі повинні застосовувати контейнеризацію, хмарну оркестрацію та балансування навантаження, щоб забезпечувати стабільність у періоди піків транзакцій [33].

Оцінюючи функціональні можливості надавачів, варто звернути увагу на рівень автоматизації внутрішніх процесів. Автоматизовані механізми видачі сертифікатів, управління життєвим циклом ключів, відстеження статусів та моніторинг подій інформаційної безпеки забезпечують зниження людського фактору, пришвидшують обробку запитів і мінімізують кількість технічних помилок.

Особливо важливою є автоматизація процесів, пов’язаних із перевіркою ідентичності користувачів, адже правильність ідентифікації визначає юридичну

достовірність майбутніх транзакцій. У публікаціях, присвячених трансформації ідентифікаційних систем, підкреслюється, що автоматизація є основою побудови швидкої, прозорої та безпечної моделі видачі довірчих послуг [26].

Іншою важливою складовою є здатність КНЕДП до оперативного оновлення криптографічних алгоритмів, інфраструктури та програмних компонентів відповідно до вимог регуляторів. Технологічний розвиток, поява нових загроз, перехід на постквантову криптографію та зміни в європейських стандартах вимагають від надавачів не лише підтримки актуального рівня захисту, а й готовності до швидкої модернізації. Зволікання у впровадженні нових алгоритмів або використання застарілих протоколів може створювати ризики компрометації ключів, що ставить під загрозу всю інфраструктуру довіри. Наукові роботи, присвячені кіберстійкості, вказують, що адаптивність криптографічних систем є ключем до їх надійності в умовах технологічних змін [39].

Технічний аналіз можливостей КНЕДП передбачає також оцінку їх готовності працювати відповідно до вимог eIDAS, що є стратегічно важливим для євроінтеграційних процесів. Це означає, що надавач має забезпечити взаємне визнання сертифікатів, відповідність форматам підпису, підтримку вимог ETSI та здатність пройти аудит у європейських органах оцінки відповідності. Відсутність такого рівня готовності може обмежувати можливість українських компаній використовувати національні електронні підписи у взаємодії з іноземними партнерами. Наукові дослідження цифрової інтеграції України вказують, що гармонізація з eIDAS є ключем до формування цифрових транснаціональних транзакцій і розвитку єдиного економічного простору [4].

Оцінюючи функціональність надавачів, не можна ігнорувати питання прозорості та відстежуваності операцій, які забезпечують довіру до транзакцій у цифровому середовищі. Система журналювання має бути побудована таким чином, щоб кожна дія могла бути відновлена та перевірена у межах нормативно визначених часових рамок. Це стосується як технічного фіксування подій, так і забезпечення неможливості їх коригування заднім числом. У роботах, присвячених цифровому праву, зазначено, що прозорість журналів є ключовим

елементом юридичної доказової бази у випадку спорів щодо підписаних документів або можливих інцидентів компрометації [25].

Загальний аналіз технічних та функціональних можливостей КНЕДП дозволяє зробити висновок, що їхня ефективність визначається не окремими технологічними функціями, а здатністю формувати комплексну, взаємопов'язану та відмовостійку інфраструктуру. Вона має включати криптографічну базу, реєстрову систему, статус-перевірку, автоматизовані процеси, масштабовані серверні рішення, резервні майданчики, інтеграційні API та здатність до міжнародної сумісності.

Саме синергія цих елементів формує можливість надавача забезпечувати юридично значимі транзакції у цифровому середовищі та створює підґрунтя для використання електронних довірчих послуг як інструменту корпоративного управління, державного регулювання та міжнародної економічної співпраці.

2.3. Виявлення проблем та перспектив розвитку систем надання електронних довірчих послуг

Аналіз функціонування систем надання електронних довірчих послуг в Україні свідчить про наявність структурних та технологічних бар'єрів, що стримують розвиток інфраструктури довіри та знижують ефективність цифрових транзакцій. Попри розвинену нормативну базу та поступову інтеграцію до європейського простору електронної ідентифікації, практична реалізація процесів залишається нерівномірною, а ринок - недостатньо конкурентним. Наявні дослідження у сфері правового регулювання електронної ідентифікації підтверджують, що слабка конкуренція у секторі довірчих послуг створює ризики технологічної стагнації та знижує рівень інноваційності сервісів [30].

Однією з найбільш суттєвих проблем є складність проходження акредитації КНЕДП та виконання технічних вимог, що охоплюють широкий спектр показників - криптографічний рівень HSM, відмовостійкість і резервування, якість журналювання, відповідність формату даних, процедури ідентифікації, політику управління ключами.

Чинна модель акредитації не враховує циклічний характер технологічних змін та часто орієнтована на перевірку статичних параметрів, хоча самі системи працюють у динамічному середовищі. Це створює «регуляторну інерцію», коли юридичні вимоги не встигають за технологічними оновленнями, що ускладнює роботу надавачів. Наукові джерела підкреслюють, що адаптивність нормативної бази є ключовою умовою інтеграції електронних довірчих послуг у сучасну цифрову економіку [4].

Другою проблемою є відсутність достатньо розвиненої інфраструктури інтеграції між КНЕДП та національними інформаційними системами. Хоча більшість надавачів забезпечують базові API, рівень їх стандартизації, продуктивності та безпеки суттєво відрізняється. Це впливає на можливість формування єдиної екосистеми електронних транзакцій, коли підпис, верифікація, перевірка статусу сертифіката та обмін структурованими документами здійснюються в автоматичному режимі. Дослідження трансформації державних цифрових сервісів підкреслюють необхідність створення високорівневої міжвідомчої інтеграційної платформи для стандартизації обміну між КНЕДП та державними реєстрами [25].

Серйозним викликом залишається проблема кіберстійкості довірчих сервісів, оскільки вони є об’єктом підвищеного ризику для зовнішніх атак. Компрометація ключів, доступ до реєстрів статусів або блокування OCSP-серверів можуть мати критичні наслідки, включно з паралізацією роботи банків, податкових органів, державних закупівель і великих підприємств. Це вимагає від надавачів застосування багаторівневих механізмів захисту, включно з постійним моніторингом, автоматизованим виявленням аномалій та швидким реагуванням на інциденти. У дослідженнях з управління інформаційною безпекою підкреслюється, що саме слабкі елементи інфраструктури довіри є головними точками вразливості національної кібербезпеки [39].

Нерозвиненість ринку надавачів електронних довірчих послуг також створює бар’єри для розвитку конкурентного середовища. Невелика кількість КНЕДП знижує динаміку оновлення сервісів та не стимулює впровадження інновацій, таких як мобільні апаратні модулі ключів, cloud-signing, постквантові

алгоритми, автоматизовані процеси remote onboarding або Smart-ID форматів підпису. Дослідження діджиталізації публічних послуг свідчать, що низький рівень конкуренції у сфері довірчих послуг призводить до уповільнення цифрової трансформації держави та бізнесу [27].

До важливих проблем належить і низький рівень цифрової грамотності користувачів, що ускладнює коректне застосування ключів та сертифікатів у щоденній діяльності підприємств. Неправильне використання підписів, передача носіїв, відсутність політики управління доступом та нерозуміння принципів юридичної відповідальності за електронні документи часто стають причиною внутрішніх інцидентів та порушення даних.

У роботах, присвячених цифровій компетентності організацій, наголошується, що успішність впровадження електронних довірчих сервісів залежить не лише від їх технічних властивостей, але й від здатності користувачів правильно інтегрувати їх у свої бізнес-процеси [16].

Виявлення перспектив розвитку інфраструктури електронних довірчих послуг показує, що ключовим напрямом є гармонізація української системи КЕП з вимогами європейського регламенту eIDAS. Це передбачає уніфікацію стандартів електронної ідентифікації, сертифікації, форматів підписів та протоколів OCSP/CRL, що у майбутньому створить умови для взаємного визнання електронних довірчих послуг.

Системи надання електронних довірчих послуг функціонують у специфічному середовищі, де правові та технічні вимоги є не зовнішнім обмеженням, а невід’ємною складовою архітектури програмного продукту. На відміну від більшості комерційних IT-рішень, у цій сфері неможливо відокремити програмну реалізацію від нормативного регулювання, оскільки саме відповідність законодавству визначає юридичну дійсність результатів роботи системи. Тому для глибокого аналізу проблем розвитку електронних довірчих послуг першочерговим є визначення їхнього місця серед інших інформаційних систем.

Сфера електронних довірчих послуг належить до категорії так званих високорегульованих сегментів IT-ринку. Під високорегульованими

інформаційними системами слід розуміти програмні комплекси та інфраструктурні рішення, діяльність яких жорстко регламентується державними або міжнародними нормами, стандартами й процедурами, а недотримання таких вимог призводить не просто до збоїв у роботі, а до юридичної нікчемності результатів функціонування системи або навіть створює загрози для держави та суспільства. Для таких систем характерною є обов’язкова сертифікація та проходження експертиз, зокрема отримання атестатів відповідності комплексних систем захисту інформації, без яких введення продукту в експлуатацію є неможливим. Їх функціонування супроводжується постійним жорстким аудитом з боку регуляторних органів, а толерантність до помилок є надзвичайно низькою, оскільки навіть одиничний технічний збій може мати серйозні юридичні наслідки, включно з анулюванням великої кількості електронних підписів.

Для кращого розуміння рівня регуляторного тиску, в якому працюють надавачі електронних довірчих послуг, доцільно порівняти цю сферу з іншими галузями ІТ, що мають подібний ступінь нормативної зарегульованості. Зокрема, до таких належить фінансово-технологічний сектор, де банківські та платіжні системи регулюються вимогами центральних банків і міжнародними стандартами безпеки, а будь-які зміни в програмному коді мають відповідати протоколам фінансового контролю. Аналогічний рівень вимог притаманний державним інформаційним системам у межах електронного урядування, зокрема державним реєстрам, виборчим системам і сервісам цифрової ідентифікації, де ключовим є збереження цілісності та достовірності державних даних. Високий ступінь регуляції характерний також для медичних інформаційних систем, які підпадають під дію законодавства про медичну таємницю й захист персональних даних, а також для систем критичної інфраструктури, зокрема енергетичних SCADA-комплексів, де технічний збій може мати катастрофічні наслідки. Окрему категорію становлять оборонні технології, що функціонують у режимі максимальної секретності та відповідають спеціалізованим національним і міжнародним стандартам.

Особливість систем кваліфікованих надавачів електронних довірчих послуг полягає в їх мультисферному характері. Вони одночасно перетинаються з кількома високорегульованими галузями, що створює ефект регуляторного накладання. З одного боку, такі системи є складовою GovTech, оскільки забезпечують ідентифікацію користувачів у державних електронних сервісах і мають відповідати вимогам до захисту державних інформаційних ресурсів. З іншого боку, електронний підпис є базовим інструментом фінансових операцій і дистанційного банківського обслуговування, що змушує надавачів довірчих послуг враховувати вимоги фінансового моніторингу та стандарти безпеки транзакцій. Крім того, відповідно до чинного законодавства такі надавачі часто відносяться до об’єктів критичної інфраструктури, що зумовлює застосування посилених заходів кіберзахисту. Саме необхідність одночасного дотримання розгалуженої та динамічної системи вимог формує ключову проблему розвитку КНЕДП. Класичні управлінські підходи та стандартні моделі розробки програмного забезпечення не здатні ефективно реагувати на синхронні зміни в суміжних регуляторних сферах. Цей мультисферний статус обґрунтовує потребу залучення юридичного аналітика як постійного учасника Agile-команди для превентивного вирішення конфліктів між технічною реалізацією та багатошаровим законодавчим регулюванням.

Специфіка високорегульованих систем особливо яскраво проявляється на етапі формування вимог. На відміну від традиційних програмних продуктів, де функціональні вимоги формуються переважно з бізнес-потреб замовника, у таких системах визначальну роль відіграють норми законодавства. Фактично закон стає первинним джерелом технічного завдання. У діяльності кваліфікованих надавачів електронних довірчих послуг законодавство прямо регламентує критично важливі функції, зокрема процедури ідентифікації користувачів, алгоритми видачі кваліфікованих сертифікатів, строки та порядок їх скасування у разі компрометації ключів, а також вимоги до інформаційної прозорості та наповнення офіційних вебресурсів надавача.

Основна складність полягає в тому, що ці вимоги зафіксовані у вигляді законів, підзаконних актів і постанов, які використовують специфічну юридичну

термінологію та складні нормативні конструкції. У більшості випадків традиційні команди розробки, включно з бізнес-аналітиками, не мають достатнього рівня юридичної підготовки для однозначного та коректного тлумачення таких норм. Помилка в розумінні навіть однієї правової вимоги може призвести до закладення хибного архітектурного рішення, яке зробить систему юридично нелегітимною незалежно від її технічної досконалості.

У зв'язку з цим відбувається трансформація ролей у процесі розробки програмного забезпечення. Якщо в класичній моделі «бізнес — IT» центральною фігурою у роботі з вимогами є бізнес-аналітик, який перекладає потреби замовника у технічні специфікації, то у високорегульованій моделі «законодавство — IT» виникає об'єктивна необхідність у юридичному аналітику. Саме він виконує роль критично важливої ланки між правом і технологіями, здійснюючи професійну декомпозицію правових норм у чіткі функціональні та нефункціональні вимоги. Це дозволяє команді розробки працювати з конкретними технічними параметрами, знижує ризики невідповідності законодавству та забезпечує успішне проходження державних експертиз і аудитів.

Рисунок 2.2. Порівняння моделей формування вимог у класичних та високорегульованих IT-системах

Джерело : розроблено автором

Перехід до моделі eIDAS 2.0 відкриває можливості для імплементації Європейського цифрового гаманця (European Digital Wallet), що дозволить забезпечити єдиний формат цифрової ідентифікації для громадян та бізнесу у взаємодії з державою. У роботах, присвячених інтеграції електронного підпису в європейську інфраструктуру, підкреслюється важливість синхронізації національної правової бази з регламентами ЄС для забезпечення повноцінної цифрової мобільності суб'єктів економіки [40].

З технічного боку перспективним напрямом є впровадження автоматизованих as-a-service моделей, які дозволяють використовувати електронний підпис без фізичного носія шляхом зберігання ключів у спеціалізованих хмарних модулях HSM та застосування багаторівневої аутентифікації.

Подібні моделі значно знижують ризики втрати ключів та забезпечують масштабованість для корпоративних і державних організацій. Міжнародні дослідження цифрової трансформації довірчих сервісів свідчать, що cloud-based signing є центральним елементом сучасної концепції електронного підпису як сервісу (Signing as a Service) [12].

Таблиця 2.2 - Основні проблеми та перспективи розвитку КНЕДП

Виявлена проблема	**Вплив на систему**	**Перспектива розвитку**
Невисокий рівень конкуренції між надавачами	Стагнація технологій, низька інноваційність	Розширення ринку, спрощення акредитації, залучення приватних провайдерів
Висока складність юридичних вимог	Ризик невідповідності, адміністративні бар'єри	Адаптація стандартів до eIDAS, створення гнучких регуляторних підходів
Слабка інтеграція з державними реєстрами	Повільні транзакції, збої в обміні даними	Єдина інтеграційна платформа державних сервісів
Недостатня кіберстійкість	Високі ризики компрометації	Постійний моніторинг, сучасні HSM, автоматизація безпеки
Низька цифрова грамотність користувачів	Втрати ключів, помилки у роботі	Освітні програми, корпоративні політики, автоматизовані інтерфейси

Джерело: складено автором на основі [29]

Розглянемо проблеми системи довірчих послуг (рис. 2.3).

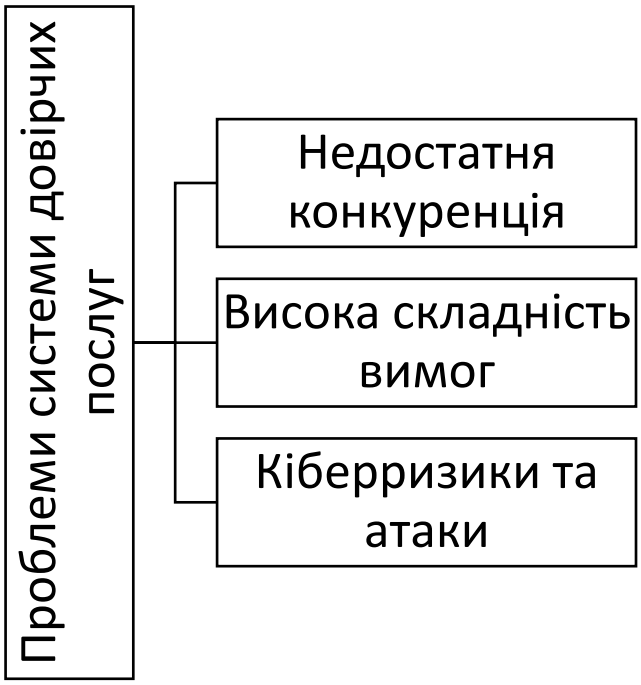

Рисунок 2.3 - Проблеми системи довірчих послуг

Джерело: розроблено автором

Подальший аналіз проблем і перспектив розвитку систем надання електронних довірчих послуг свідчить, що їх модернізація неможлива без формування нової моделі управління якістю сервісів, де ключовими параметрами стають не лише технічні характеристики, але й здатність надавачів забезпечувати прозорість, контрольованість і юридичну визначеність усіх етапів життєвого циклу електронного підпису.

Національна система КЕП потребує переходу від моделі «технічного реагування» до моделі «управління довірою», у якій на перший план виходять стандартизовані процеси взаємодії, постійний моніторинг інцидентів і превентивна аналітика ризиків. У дослідженнях сучасних підходів до управління інформаційною інфраструктурою наголошується, що довірчі послуги повинні розвиватися не лише як технологічний сервіс, а як комплексна система забезпечення відповідальності та цифрової безпеки [22].

Значну увагу у перспективах розвитку слід приділити появі нових ринкових моделей, які змінюють парадигму використання електронного підпису та відкривають можливість широкого застосування технологій, орієнтованих на бізнес-процеси.

Одним із перспективних напрямів є поширення концепції delegated signing - моделі, за якої підпис генерується у контрольованому середовищі і використовується від імені уповноваженої особи або організації, що дозволяє автоматизувати складні документообіги та масштабувати процеси погодження. Використання автоматизованих підписних сервісів у комплексі з електронною ідентифікацією створює передумови для формування інтелектуальних бізнес-рішень, де документи підписуються в рамках заздалегідь визначених бізнес-правил. Такі підходи вже практикуються у провідних країнах ЄС, що підтверджено дослідженнями з трансформації цифрових сервісів [12].

Суттєвим напрямом модернізації є також розвиток транскордонної взаємодії систем електронних довірчих послуг. Належне нормативне та технічне узгодження з європейськими інфраструктурами відкриває можливість використання українських кваліфікованих сертифікатів у міжнародних правовідносинах. Це стосується не лише укладення контрактів, але й участі у тендерах, подання фінансової документації, реєстрації іноземних представництв та інших процедур.

Юридична сила українського електронного підпису за кордоном є важливим показником довіри до країни як учасника цифрової економіки, а дослідження європейських регуляторів підтверджують, що взаємне визнання електронних ідентифікаційних засобів стимулює економічний розвиток і знижує транзакційні витрати [40].

Системою електронних довірчих послуг має бути подолана й проблема обмеженої адаптивності до швидких змін у законодавстві. Постійні оновлення нормативної бази потребують інтегрованих механізмів юридичного моніторингу, які дозволяли б автоматично відстежувати зміни у вимогах до форматів сертифікатів, процедур ідентифікації, рівнів криптографічної стійкості та технічних протоколів.

Саме тому у перспективі доцільно запровадити моделі regulatory-driven development - підхід, коли вимоги законодавства інтегруються у планування змін системи та формування беклогу оновлень. Наукові праці у сфері IT-комплаєнсу

підкреслюють, що саме інтеграція юридичного моніторингу у процеси розробки створює умови для сталого розвитку високорегульованих ІТ-систем [11].

Не менш важливим є розвиток комунікаційної та освітньої складової інфраструктури довірчих послуг, оскільки користувачі залишаються одним з ключових елементів надійності системи. Перспективним напрямом є формування навчальних модулів для бізнесу, інтеграція інструктивних матеріалів, автоматизованих підказок і систем інтелектуального супроводу користувача у процесі накладання підпису. Такі підходи дозволяють мінімізувати ризики людських помилок і підвищують ефективність використання сервісів. Наукові публікації у сфері цифрової компетентності підтверджують, що якість навчання користувачів має прямий вплив на рівень захищеності цифрових транзакцій [16].

Перспективи розвитку також охоплюють удосконалення механізмів аудиту діяльності КНЕДП. Сучасний аудит має стати не лише формальною процедурою перевірки відповідності технічним вимогам, а інструментом динамічної оцінки ризиків, що дозволяє прогнозувати можливі вразливості та оцінювати ефективність впроваджених заходів безпеки. Розвиток risk-based auditing у сфері довірчих послуг дозволить не лише підтримувати відповідність вимогам, але й завчасно реагувати на загрози. У літературі, присвяченій управлінню цифровими ризиками, зазначається, що ризик-орієнтовані моделі перевірки є ключем до забезпечення стійкості критичних ІТ-сервісів [22].

Підсумовуючи аналіз, можна зазначити, що сучасна система електронних довірчих послуг перебуває на етапі глибокої структурної трансформації. Її розвиток залежить від здатності надавачів адаптуватися до європейських стандартів, підтримувати високий рівень кіберстійкості, забезпечувати прозору роботу реєстрів, створювати зручні користувацькі сервіси та інтегрувати юридичний аналіз у технічні процеси. Від ефективності цих змін залежить не лише стабільність роботи національної цифрової інфраструктури, але й можливість України повноцінно інтегруватися у європейський та світовий цифровий простір. Перспективи розвитку КНЕДП охоплюють не тільки технічні та правові аспекти, але й управлінські: формування довіри, підвищення якості

сервісів та створення середовища, у якому електронний підпис стає універсальним інструментом цифрової взаємодії.

Висновки до розділу 2

Другий розділ поглибив розуміння того, якими є реальні можливості, обмеження та проблеми функціонування кваліфікованих надавачів електронних довірчих послуг в Україні. Аналіз організаційно-правових вимог показав, що діяльність КНЕДП є однією з найбільш зарегульованих сфер цифрового ринку, де кожен процес - від генерації ключів до управління статусами сертифікатів - визначений законодавством і підлягає суворому контролю. Це створює високий бар'єр входу на ринок та формує середовище з обмеженою конкуренцією, що, своєю чергою, впливає на швидкість розвитку технологій, якість сервісів та рівень інноваційності.

Функціональний аналіз технічної інфраструктури надавачів засвідчив, що здатність систем забезпечувати масштабованість, відмовостійкість, сумісність із державними реєстрами та відповідність міжнародним стандартам є ключовими передумовами для сталого розвитку електронних довірчих послуг. У роботі було доведено, що технічна інфраструктура КНЕДП має інтегрований характер і складається з взаємопов'язаних компонентів - криптографічних модулів, реєстрів статусів, інструментів автоматизованої перевірки, API-платформ та каналів обміну даними. Ефективність кожного з цих елементів безпосередньо впливає на надійність сервісів, що забезпечують юридично значимі транзакції.

У межах розділу було ідентифіковано системні проблеми ринку: складність акредитації, недостатність інтеграційних рішень, ризики кібербезпеки, нерозвинутість хмарних моделей підпису, низька цифрова компетентність користувачів і сповільнене впровадження європейських стандартів. Узагальнення цих проблем дозволило сформувати бачення перспектив розвитку інфраструктури довірчих послуг, серед яких центральне місце займає гармонізація з eIDAS, перехід до cloud-signing, автоматизація юридичних процесів, розвиток risk-based auditing та зміцнення кіберстійкості.

Загалом у розділі було доведено, що майбутній розвиток систем електронних довірчих послуг неможливий без комплексної модернізації як технічних, так і організаційно-правових компонентів. Лише поєднання стандартизованих технологічних рішень, адаптивного законодавчого регулювання, зростання компетентності користувачів та розвитку конкурентного середовища може забезпечити якісно новий рівень цифрової довіри в Україні. Виявлені проблеми та визначені перспективи є фундаментальною основою для подальшого формування моделі гнучкого управління розробкою системи КНЕДП, що буде розкрита у третьому розділі.

РОЗДІЛ 3
ГНУЧКЕ УПРАВЛІННЯ РОЗРОБКОЮ СИСТЕМИ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ З ВИКОРИСТАННЯМ AGILE-ПІДХОДУ

3.1. Особливості впровадження Agile-підходу у сфері електронних послуг. Інтеграція юридичного аналітика в Agile-команду

Розвиток системи електронних довірчих послуг в Україні відбувається в умовах постійної нормативної динаміки, технологічної модернізації та підвищених вимог до швидкості реагування на інциденти, що робить застосування традиційних моделей управління розробкою вкрай обмеженим.

Високорегульоване середовище, у якому працюють кваліфіковані надавачі електронних довірчих послуг (КНЕДП), передбачає одночасну відповідність технічним, правовим, процедурним і міжнародним стандартам, що унеможливлює використання жорстких каскадних моделей, орієнтованих на лінійність і фіксовані етапи [17]. Саме тому Agile-підхід розглядається як оптимальна методологія, що дозволяє інтегрувати швидкість розробки, гнучкість реакції на зміни та юридичну визначеність у межах одного проектного середовища.

Особливість впровадження Agile у сфері електронних довірчих послуг полягає в тому, що це середовище поєднує різнорідні вимоги, які стосуються криптографічної стійкості систем, безперервності реєстрових сервісів, відповідності eIDAS, захисту персональних даних, управління ризиками та документування процедур. На відміну від комерційних ІТ-проєктів, КНЕДП не мають можливості відкладати випуск функціоналу або вносити зміни до інфраструктури без обов’язкової юридичної оцінки та технічної атестації. У таких умовах Agile набуває функції не просто підходу до розробки, а моделі організації всієї діяльності, що забезпечує синхронізацію бізнес-процесів, технічних рішень і правових вимог [1].

Варто зазначити, що специфіка роботи КНЕДП вимагає особливого балансу між жорсткими регламентами безпеки та гнучкістю розробки. У цьому

контексті актуальним є застосування концепції «гібридної самоорганізації», дослідженої Д. Мігалем та О. Орловою-Куриловою. У своїй праці науковці доводять, що ефективність сучасних команд залежить від здатності поєднувати індивідуальну автономію працівників із колективною взаємодією. Для сфери довірчих послуг це означає, що технічні спеціалісти можуть мати автономію у виборі інструментів кодування, тоді як юридичні аспекти та питання безпеки залишаються під суворим колективним контролем та регламентацією, що дозволяє уникнути хаосу при збереженні високої швидкості реакції на зміни [46]

Ключовою перевагою Agile у контексті створення систем КНЕДП є можливість працювати в умовах високої невизначеності. Нормативна база України у сфері електронної ідентифікації регулярно оновлюється (зміни у Законі України «Про електронну ідентифікацію та електронні довірчі послуги», гармонізація з eIDAS 2.0, адаптація вимог ETSI), що потребує швидкого коригування функціоналу, політик безпеки та внутрішніх процесів. Каскадна модель не дозволяє враховувати нормативні зміни в режимі реального часу, натомість Agile базується на ітеративному вдосконаленні продукту, коли юридичні та технічні вимоги можуть бути інтегровані у кожен спринт. Як зазначає D. Rigby у дослідженні Agile at Scale, гнучкі моделі стають ефективними там, де зміна зовнішнього середовища є постійною і непередбачуваною [14].

Впровадження Agile у розробку систем довірчих послуг передбачає створення команд, що працюють за принципом міжфункціональності, тобто включають спеціалістів із різних галузей: розробників, DevOps-інженерів, спеціалістів із криптографії, експертів з інформаційної безпеки, бізнес-аналітиків та обов’язково юридичного аналітика. Саме така структура дозволяє забезпечити одночасну відповідність технічних модулів вимогам законодавства, стандартів безпеки та процедур управління ключами. У дослідженнях автономних Agile-команд зазначено, що найвища ефективність досягається тоді, коли команда має повний набір компетенцій для прийняття рішень без зовнішніх затримок і додаткової координації [15]. У випадку КНЕДП юридичний аналітик є невід’ємним учасником такої команди.

Інтеграція нових ролей, таких як юридичний аналітик, у технічну Agile-команду є складним управлінським викликом. Як підкреслюють у своєму дослідженні Д. Мігаль та О. Орлова-Курилова, традиційні методи адаптації персоналу часто виявляються надто інерційними для динамічних проєктів. Автори обґрунтовують доцільність застосування Agile-підходу до онбордингу, який передбачає ітеративність, гнучкість та постійний зворотний зв'язок. Впровадження такої моделі адаптації дозволить юридичному фахівцю швидше інтегруватися в процеси розробки, зрозуміти технічний контекст продукту та ефективніше взаємодіяти з розробниками, знижуючи ризики комунікаційних розривів на ранніх етапах проєкту [47].

Таблиця 3.1. Порівняння моделей залучення юриста в IT-проекти

Критерій порівняння	Юрист як сторонній консультант (традиційна модель)	Юридичний аналітик в Agile-команді (запропонована модель)
Характер залучення	Реактивний: підключається за запитом, коли проблема вже виникла	Проактивний: бере участь у плануванні та на кожному етапі розробки
Точка входу в процес	Етап виникнення інциденту, судового позову або фінального релізу	Етап формування Backlog та Refinement (уточнення вимог)
Комплаєнс (Compliance)	Реагування на комплаєнс-інциденти та штрафи від регуляторів	Continuous Compliance: безперервна перевірка коду та процесів на відповідність нормам
Інтелектуальна власність	Вирішення спорів щодо авторського права після завершення розробки	Перевірка авторського права та ліцензій безпосередньо в процесі розробки
Швидкість реакції	Низька через бюрократичні погодження між відділами або зовнішніми консультантами	Висока: миттєве консультування розробників під час спринту
Розуміння продукту	Поверхневе: обмежується юридичною документацією	Глибоке: розуміння архітектури БД, логіки КЕП та технічних обмежень
Кінцева мета	Захист компанії в суді або мінімізація збитків після інциденту	Створення юридично чистого продукту, готового до експертиз та аудитів

Джерело : розроблено автором

Юридичний аналітик виконує унікальну функцію - забезпечує зв'язок між Agile-підходом та нормативною природою довірчих сервісів. На відміну від

інших ІТ-проєктів, будь-яка зміна в архітектурі КНЕДП, алгоритмах, протоколах, форматах підписів, системах ідентифікації або реєстрах статусів повинна проходити правову перевірку на відповідність Закону № 2155-VIII, Регламенту 910/2014 та підзаконним актам НБУ і Держспецзв'язку [36; 38; 40].

Таблиця 3.2. Юридичний аналітик як частина Agile-команди

Роль	Основна функція	Відповідальність у проєкті КНЕДП
Product Owner (Власник продукту)	Визначає візію продукту та пріоритети Product Backlog	Максимізація бізнес-цінності сервісу та забезпечення відповідності ринковим запитам
Scrum Master	Фасилітатор процесів, усуває перешкоди для команди	Дотримання Agile-фреймворку та забезпечення ефективної комунікації між усіма учасниками
Development Team (Розробники)	Створюють технічний інкремент продукту (код)	Реалізація криптографічних алгоритмів, API та користувацьких інтерфейсів системи
QA Engineer (Тестувальник)	Перевірка якості та працездатності програмного забезпечення	Технічне тестування функціоналу на відповідність технічним і безпековим специфікаціям
Юридичний аналітик (нова роль)	Синхронізація процесу розробки з нормативно-правовим полем	Continuous Compliance: гарантування легітимності рішень, юридичний супровід експертиз та аудитів

Джерело : розроблено автором

Тому юридичний аналітик у складі Agile-команди не є стороннім консультантом, що підключається на окремих етапах, а постійним учасником спринтів, відповідальним за формування юридичних вимог до беклогу та оцінку нормативних ризиків. Як зазначає Puka у своїй роботі, юридичний контроль у high-compliance проєктах має бути інтегрованим, а не зовнішнім, оскільки він визначає легітимність усього продукту [11].

Особливість інтеграції юридичного аналітика в Agile-підхід полягає також у тому, що він бере участь не лише в оцінці вимог, але й у формуванні критеріїв приймання (Definition of Done), тестуванні функціоналу, розробці політик сертифікації, регламентації процедур ідентифікації та управління ключами.

У контексті КНЕДП юридична відповідність є частиною якості продукту, тому критерії закінчення задачі включають не лише технічну реалізацію, а й відповідність правовим нормам. Agile дозволяє вводити юридичну експертизу у форматі безперервного контролю, а не разового аудиту, як це відбувається у Waterfall-моделі, де правові недоліки виявляються вже після завершення розробки [3].

Для розробки систем електронних довірчих послуг важливо, що Agile забезпечує механізм швидкої реакції на події інформаційної безпеки. Критичні інциденти у сфері КЕП - компрометація ключів, відмова OCSP, збій реєстрів, невірні статуси сертифікатів - вимагають невідкладного оновлення системи.

В умовах каскадної моделі такі зміни потребували би переробки технічної документації, узгоджень і запуску нової ітерації, що призвело б до багатоденної або багатотижневої затримки. Agile ж дозволяє сформувати аварійний спринт, у межах якого команда оперативно випускає критичне оновлення. Як зазначає McKinsey, гнучкі команди забезпечують на 25-35 % швидшу реакцію на ризики критичної інфраструктури завдяки коротким циклам ухвалення рішень та автономності команди [1].

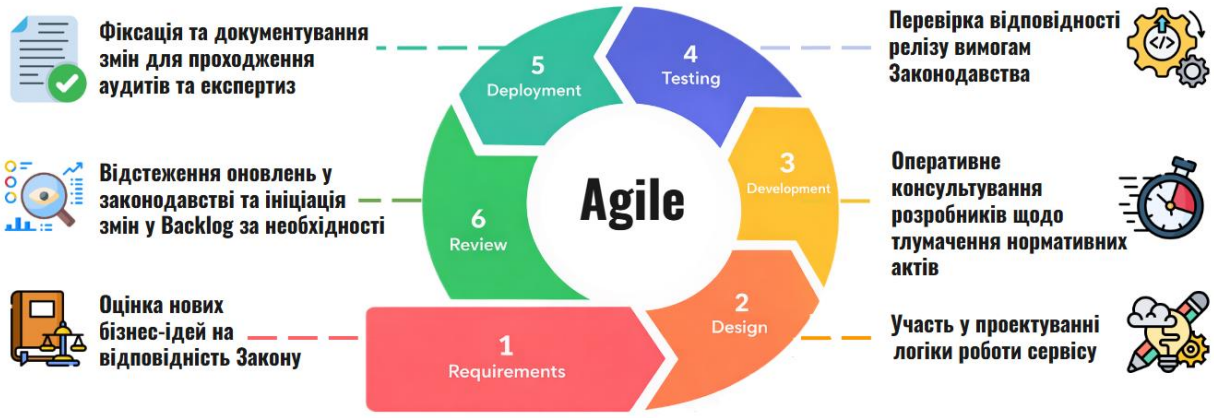

Рисунок 3.1 – Інтеграція бізнес-аналітика у цикл розробки

Джерело : Розроблено автором

Особливої ваги Agile набуває при роботі з криптографічними алгоритмами та їх оновленням відповідно до міжнародних стандарти. Перехід на постквантові алгоритми, впровадження нових політик ETSI EN 319 411-1/2, оновлення

процедур генерації ключів та логування подій є не разовими проєктами, а постійними процесами, які потребують адаптивності розробки. У цьому контексті Agile-філософія відповідає вимогам Lean-мислення, коли кожна зміна повинна додавати цінність і не створювати зайвих втрат ресурсів [8]. Застосування Agile у КНЕДП також дає змогу ефективно управляти ризиками правової невідповідності. У класичній IT-розробці ризики оцінюються переважно з технічної точки зору, однак у сфері електронних підписів відхилення від нормативних вимог призводять до втрати юридичної сили документів, анулювання сертифікатів та відповідальності надавача. Agile дозволяє впровадити risk-based backlog, коли ризик є ключовим критерієм пріоритетності задачі, а юридичний аналітик бере участь у формуванні рейтингу ризиків. Такий підхід використовується у моделях Safe та Large Scale Agile, де правові вимоги є частиною compliance-layer і інтегруються у кожен інкремент розробки [12].

Окрім організаційних методів, сучасне управління ризиками в IT-проєктах все частіше спирається на інтелектуальні технології. Дослідження І. Крискуна та О. Орлової-Курилової переконливо свідчать, що використання інструментів штучного інтелекту дозволяє перейти від реактивної до прогностично-адаптивної моделі керування ризиками. Зокрема, для системи КНЕДП, де ціна помилки є критичною, застосування алгоритмів машинного навчання для аналізу історичних даних та моніторингу поточних метрик дозволяє автоматично ідентифікувати потенційні загрози зриву термінів або перевищення бюджету ще до їх настання. Це дає змогу команді діяти проактивно, формуючи резерви часу та ресурсів на основі точних прогнозів, а не інтуїтивних припущень [48].

Також важливо, що Agile забезпечує прозорість взаємодії між стейкголдерами - державними органами, користувачами, банками, бізнесом, розробниками та аудиторами. У сфері довірчих послуг кожна зміна в системі має торкатися одразу багатьох груп користувачів, тому регулярна комунікація та постійний фідбек стають необхідною умовою. Agile-підхід вирішує цю проблему через інструменти daily-мітингів, review-сесій, демонстрацій інкрементів і відкритих backlog-обговорень. Як зазначає Stray у дослідженні автономних

команд, ключовим фактором успіху Agile є прозорість процесів, яка дозволяє виявляти помилки ще на стадії формування вимог [15].

Особливістю роботи Agile-команди у сфері довірчих послуг є взаємозалежність юридичних і технічних змін. Будь-які оновлення в алгоритмах підпису, розвитку мобільних ключів, запровадженні cloud-HSM чи механізмів remote onboarding повинні бути синхронізовані з правовими правилами видачі сертифікатів, рівнями ідентифікації, процедурами управління носіями та вимогами атестації засобів КЗІ. Тому юридичний аналітик в Agile-команді фактично виступає «контролером відповідності» у кожному спринті, забезпечуючи юридичну сталість продукту. Саме такий підхід підтримують сучасні дослідження у сфері інтеграції права й IT, де наголошується, що юридична експертиза має бути елементом agile-потоку, а не зовнішньою перевіркою після завершення розробки [11].

Значущою рисою Agile є також поєднання інкрементного розвитку з постійним тестуванням. У сфері довірчих сервісів тестування - це не лише технічна перевірка працездатності програмного забезпечення, а й оцінка відповідності формату сертифікатів, коректності CRL/OCSP, актуальності політик підпису та збереження юридичних властивостей транзакцій. Саме через це юридичний аналітик бере участь у розробці тест-кейсів, визначенні правових сценаріїв використання, відтворенні ситуацій втрати ключа, компрометації, некоректного статусу чи неправильної ідентифікації.

Таким чином, Agile у сфері електронних довірчих послуг не зводиться до гнучкої організації розробки, а перетворюється на комплексну методологічну основу управління якістю, юридичною відповідністю, безперервністю сервісів та інформаційною безпекою. Інтеграція юридичного аналітика в Agile-команду створює механізм, який дозволяє одночасно розвивати продукт, адаптувати його до нормативних змін і підтримувати юридичну силу електронних транзакцій. Це робить Agile не просто інструментом, а необхідною умовою модернізації системи КНЕДП в Україні.

3.2. Команда проєкту, стейкголдери проєкту, етичний кодекс, принципи та правила роботи в проєкті

Ефективне впровадження Agile-підходу в розробку систем електронних довірчих послуг вимагає не лише внутрішньої організації команди, але й глибокого аналізу стейкголдерів, користувацьких сценаріїв та бізнес-логіки сервісу. У середовищі КНЕДП усі ключові процеси - від реєстрації користувача до видачі та відкликання сертифікатів - нерозривно пов’язані з нормативними, технічними, організаційними й поведінковими аспектами. Тому моделювання системи через Business Model Canvas, User Persona та Use Case діаграми є необхідним інструментом, що дозволяє поєднати вимоги регуляторів, очікування користувачів та можливості команди розробки в єдиній структурі. Саме ці моделі створюють основу для формування беклогу Agile-проєкту та забезпечують прозорість взаємодії між юридичними та технічними процесами [1].

Одним із ключових етапів формування бачення продукту є визначення стейкголдерів та опис сценаріїв їхньої поведінки. У системах довірчих послуг користувачі поділяються на дві великі групи: кінцеві користувачі (фізичні та юридичні особи, які отримують КЕП і підписують документи) та адміністративно-технічний персонал КНЕДП, відповідальний за верифікацію особи, схвалення заявок, управління сертифікатами та реагування на інциденти. Взаємодія цих груп із системою формує підґрунтя для визначення бізнес-процесів, що мають бути реалізовані в продукті у форматі User Stories та Epics. Цю взаємодію наочно відображає Use Case діаграма, інтегрована у дослідження (рис. 3.2).

На ній представлено дві ключові ролі - «Користувач» та «Адміністратор системи». Користувач взаємодіє із системою через базові сценарії: реєстрація, авторизація, отримання КЕП, підписання документа та перевірка статусу підпису. Адміністратор виконує іншу групу функцій: ідентифікацію користувача, схвалення/відхилення заявки на КЕП та скасування сертифіката у разі потреби. Відображення цих дій у вигляді Use Case моделі є важливою

частиною бізнес-логіки, оскільки дозволяє Agile-команді визначати обсяг робіт, залежності між модулями та критичні точки юридичного контролю [12].

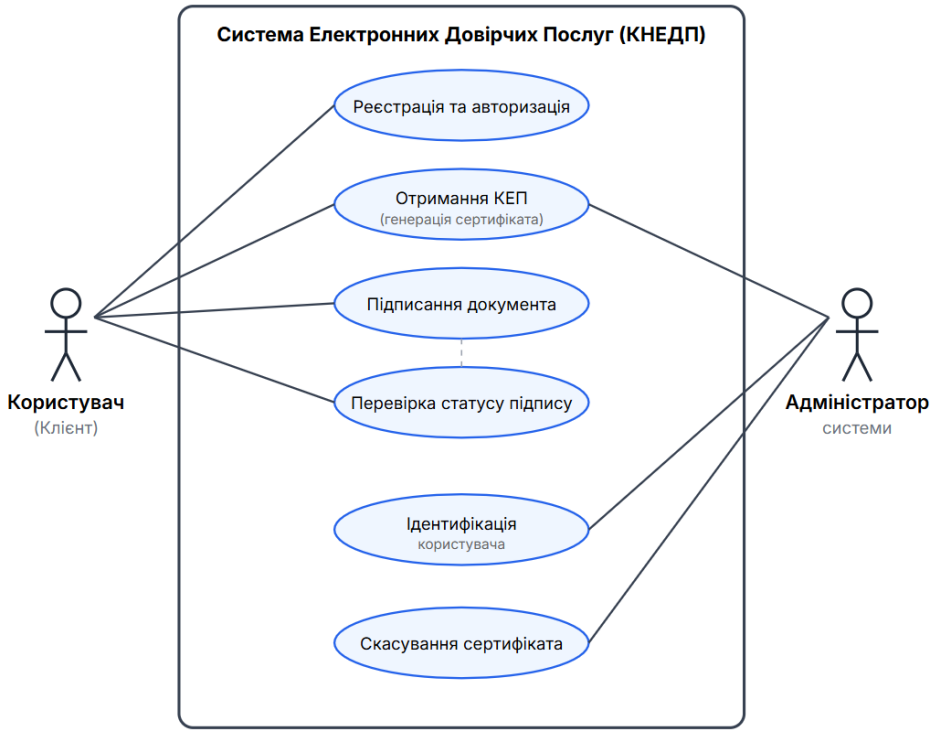

Рисунок 3.2 - Use Case діаграма системи електронних довірчих послуг

Джерело: побудовано автором

Однак для того, щоб система відповідала не лише нормативним вимогам, але й реальним потребам користувачів, важливо враховувати поведінкові характеристики та мотивацію конкретних користувацьких груп. Саме тому було інтегровано інструмент User Persona, представлений на рис. 3.3.

У дослідженні використано персону «Олена», 35 років, головний бухгалтер, для якої критичною є швидкість, безпека, зрозумілість інтерфейсу та юридична сила підпису. Вона схильна до скрупульозного аналізу, користується сучасними цифровими сервісами (Google Workspace, Дія, банківські додатки) та орієнтується на прозорі, надійні технологічні рішення.

З точки зору Agile-проєкту, така persona формує конкретні вимоги до особистого кабінету, інтерфейсу підписання, робочого процесу створення та використання КЕП, а також до змісту юридичних повідомлень, що супроводжують транзакції. Саме на основі таких персон формуються

пріоритетні User Stories, які лягають в основу беклогу і визначають сценарії тестування, що включають поведінкові та юридичні критерії.

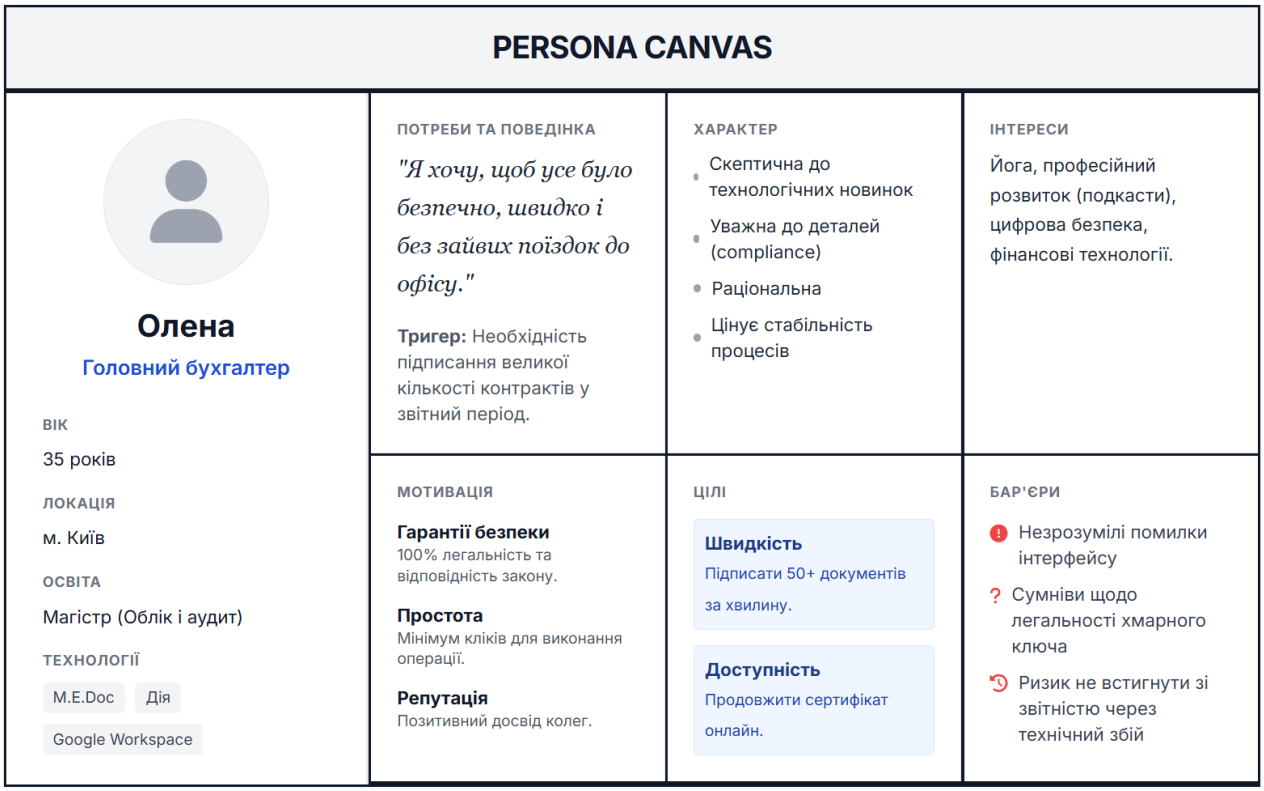

Рисунок 3.3 - Persona Canvas

Джерело: побудовано автором

User Persona працює у зв’язці з Use Case діаграмою: перша визначає мотивацію, страхи та очікування користувача, а друга - перелік дій, які система повинна йому надати. Саме така інтеграція дозволяє уникати технічного «тунельного бачення» та забезпечити клієнтоорієнтований підхід у високорегульованій системі. Це особливо важливо для КНЕДП, де будь-яка помилка інтерфейсу або непослідовність процесів може спричинити недовіру до системи, відмову від продукту або навіть юридичні наслідки, якщо некоректна дія призводить до неправильного статусу підпису чи помилки у верифікації особи [36].

Наступним елементом моделювання бізнес-логіки є Business Model Canvas, який дозволяє відобразити структуру системи, потоки цінності, ролі партнерів та ключові процеси. Інтеграція Canvas у розділ є методологічно обґрунтованою,

адже саме він дозволяє сформувати системне бачення того, які компоненти сервісу є найбільш критичними, які витрати формують основу функціонування, які ресурси є ключовими та як система створює юридично значущу цінність для користувачів. Це не лише бізнес-інструмент, але і стратегічна модель для Agile-команди, яка на основі Canvas формує епіки та визначає технічний обсяг спринтів (табл. 3.3).

Таблиця 3.3 - Business Model Canvas системи електронних довірчих послуг

Компонент	**Зміст**
Value Proposition	Юридично значущий електронний підпис; захищене зберігання ключів; довіра до транзакцій; відповідність eIDAS та Закону України «Про електронні довірчі послуги»
Customer Segments	Фізичні особи, бізнес-користувачі, бухгалтери, державні органи, банки, інтегратори, оператори електронних сервісів
Channels	Особистий кабінет, мобільний застосунок, API, фронтофіси, віддалена ідентифікація
Customer Relationships	Підтримка 24/7, чат-боти, SLA для корпоративних клієнтів, автоматичне повідомлення про статуси сертифікатів
Revenue Streams	Плата за випуск КЕП, інтеграційні послуги, корпоративні підписки, технічна підтримка, участь у тендерах
Key Resources	Сервери CA/RA/OCSP, HSM-модулі, криптографічні бібліотеки, команда розробників, юристи, політики безпеки, сертифікати відповідності
Key Activities	Генерація ключів, реєстрація користувачів, ведення реєстрів, моніторинг безпеки, оновлення криптографії, аудит
Key Partners	ДССЗЗІ, Мінцифра, НБУ, постачальники HSM, аудитори, банки, великі інтегратори
Cost Structure	Апаратні засоби, ліцензії, криптографія, дата-центри, аудит, зарплати фахівців, розробка та підтримка

Джерело: розроблено автором

Включення Business Canvas у структуру проєкту створює підґрунтя для планування Agile-спринтів: ціннісні блоки Value Proposition формують фундаментальні Epics, Key Activities - технічні задачі, Customer Segments - критерії UX-дизайну, а Key Partners - вимоги до нормативної відповідності. Таким чином модель Canvas виконує роль не лише бізнес-інструменту, а й фреймворку для стратегічних рішень у високоризиковому й високорегульованому середовищі [14].

3.3. Ресурсне забезпечення та оцінка економічної ефективності впровадження Agile-підходу

Впровадження системи надання електронних довірчих послуг вимагає чіткого планування ресурсів, оскільки Agile-підхід, на відміну від Waterfall, передбачає фінансування сталої команди, а не фіксованого обсягу робіт. Основною статтею витрат у проєкті є фонд оплати праці крос-функціональної команди, до якої, як було обґрунтовано раніше, входить юридичний аналітик.

Розрахунок кошторису проєкту базується на тривалості спринтів та складі команди. Припустимо, що для реалізації MVP (Minimum Viable Product) системи КНЕДП необхідно 6 місяців (12 спринтів по 2 тижні).

Кошторис витрат на команду розробки розраховується за формулою:

$$C_{total} = \Sigma\ (R_i * H_i) * T$$

де: C_{total} - загальні витрати на команду; R_i - погодинна ставка спеціаліста i-го профілю; H_i - кількість робочих годин у місяць (в середньому 160 годин); T - тривалість проєкту в місяцях (6 місяців).

Штатний розпис та розрахунок витрат на оплату праці наведено в табл. 3.4.

Таблиця 3.4 - Розрахунок бюджету Agile-команди проєкту (прогнозний)

Роль у команді	Кількість	Середня ставка (USD/год)*	Місячний фонд (USD)	Загальні витрати (6 міс.)
Project Manager / Scrum Master	1	30	4 800	28 800
Юридичний аналітик (Compliance)	1	35	5 600	33 600
Senior Backend Developer (Java/Crypto)	2	45	14 400	86 400
Frontend Developer	1	30	4 800	28 800
QA Engineer (Automation + Security)	1	25	4 000	24 000
DevOps Engineer	0.5 (part-time)	40	3 200	19 200
РАЗОМ	6.5	-	36 800	220 800

Джерело: розраховано автором на основі ринкових ставок IT-сектору України станом на 2025 рік

Крім прямих витрат на персонал, кошторис включає витрати на інфраструктуру (хмарні сервіси, ліцензії Jira/Confluence, сертифікати SSL, HSM-модулі). Орієнтовна вартість розгортання та підтримки інфраструктури складає близько 15% від фонду оплати праці, що становить 33 120 USD.

Загальна вартість реалізації проєкту за Agile-методологією складе: $220\,800 + 33\,120 = 253\,920\,USD$.

Економічна ефективність від впровадження Agile-підходу, порівняно з класичним каскадним методом, полягає у мінімізації ризиків «переробки» продукту. У сфері КНЕДП вартість помилки (наприклад, невідповідність вимогам eIDAS, виявлена на фінальному етапі) може призвести до необхідності переробки 40-60% коду. Застосування ітеративного підходу та інтеграція юридичного аналітика дозволяє заощадити до 30% бюджету, який у моделі Waterfall закладався б на виправлення критичних архітектурних помилок після аудиту.

$$E_{agile} = C_{risk_{waterfall}} - C_{risk_{agile}}$$

Якщо ризик переробки у Waterfall оцінюється у 30% від бюджету (76 176 USD), а в Agile завдяки постійному комплаєнсу він знижується до 5% (12 696 USD), то умовна економічна економія становить 63 480 USD, що підтверджує фінансову доцільність запропонованого підходу.

3.4. Перспективи впровадження Agile-підходу у сфері електронних послуг

Перспективи впровадження Agile-підходу у сфері електронних довірчих послуг визначаються потребою держави адаптуватися до швидких технологічних змін, підвищення вимог користувачів до зручності та безпеки сервісів, а також необхідністю гармонізації з європейськими підходами цифрового врядування. На відміну від традиційних каскадних моделей, які історично застосовувалися в розробці державних інформаційних систем, Agile дозволяє поєднати нормативну стабільність із гнучким реагуванням на зміну ризиків, кіберзагроз та очікувань користувача. Це особливо важливо для

КНЕДП, оскільки інфраструктура електронних довірчих послуг має одночасно відповідати нормам eIDAS та забезпечувати швидке оновлення функціональності [12].

Однією з ключових перспектив є можливість адаптивного розвитку сервісів на основі реальних поведінкових моделей користувачів, адже Agile дозволяє постійно перевіряти гіпотези, аналізувати дані використання підписів, ідентифікацій та транзакцій, а також швидко переносити ці висновки у продукт. Наприклад, використання User Persona, сформованої для типових сегментів на кшталт «головний бухгалтер» або «представник малого бізнесу», відкриває можливість коригувати процеси ідентифікації, інтеграцію з мобільними застосунками та алгоритми перевірки підпису відповідно до реальних потреб аудиторії. Такий підхід забезпечує орієнтацію на поведінкову аналітику замість абстрактних технічних вимог, що повністю узгоджується з концепцією клієнт-центрованого цифрового врядування [18].

Другою перспективою є можливість створення інкрементних оновлень електронних послуг без масштабних зупинок системи. Agile передбачає розробку функціоналу через короткі спринти, які завершуються готовим інкрементом. У системах електронного підпису це дає змогу впроваджувати нові модулі - наприклад, автоматичне відкликання сертифіката, додаткові канали ідентифікації або розширені API - без ризику порушення доступності сервісу. Таким чином, держава та приватні КНЕДП отримують механізм еволюційного розвитку, не порушуючи вимог до безперервності надання довірчих послуг [21].

Узгодження Agile із суворими нормативними вимогами є складним, проте перспективним напрямом. На рівні європейських практик, зокрема в межах регламенту eIDAS 2.0, активно розвивається підхід continuous compliance - безперервної відповідності, який не суперечить гнучким методологіям, а навпаки посилює їх. Україна, орієнтуючись на євроінтеграційний курс, може інтегрувати аналогічні механізми в державні електронні сервіси: автоматизовані тести відповідності, цифрові аудити, логування дій адміністраторів та криптографічний моніторинг. Це створює умови для того, щоб Agile-команди

могли впроваджувати зміни швидко, але у межах чітко визначених стандартів [9].

Застосування Use Case моделювання в Agile відкриває додаткові перспективи оптимізації бізнес-процесів. Діаграми прецедентів дозволяють не просто описати функціональні вимоги, а й визначити критичні точки взаємодії користувача з системою, де потенційно можуть виникати ризики кібербезпеки або юридичної невизначеності. Таким чином, команда отримує можливість проводити системний аудит сценаріїв: перевірку сертифіката, підписання документа, генерацію ключів, ідентифікацію користувача, відкликання сертифіката. Це створює основу для побудови стійкої моделі цифрової довіри, у якій ризики аналізуються не після розробки, а в процесі її виконання, що є сутністю Agile-підходу [15].

Важливим напрямом є можливість інтеграції Agile з сервісною моделлю розвитку електронних послуг. На основі Business Model Canvas можна створювати сценарії масштабування сервісів КЕП, орієнтуючись на нові сегменти користувачів: освітні заклади, бізнес-асоціації, міжнародні компанії, фізичних осіб-підприємців. Agile дозволяє швидко перевіряти, які саме елементи моделі - канали поширення, структура витрат, ключові партнери чи потоки цінності - потребують адаптації для різних груп користувачів. У такий спосіб електронні довірчі послуги перестають бути лише технічною інфраструктурою і перетворюються на адаптивний сервіс-продукт, здатний конкурувати з комерційними рішеннями на ринку електронного підпису [17].

Додаткову цінність Agile приносить у контексті кібербезпеки, оскільки гнучка методологія дає змогу інтегрувати моделі безперервного виявлення загроз у сам процес розробки. Команда може реагувати на вразливості ще до того, як вони вплинуть на користувачів, а всі критичні функції - зокрема генерація ключових пар, контроль доступів та управління сертифікатами - проходять багаторазові цикли тестування. Це не лише підвищує якість сервісу, а й сприяє формуванню довіри громадян до цифрових рішень держави, що є базовою умовою розширення використання електронних підписів [3].

Загалом перспективи впровадження Agile-підходу у сферу електронних послуг можна узагальнити у вигляді аналітичної таблиці (табл. 3.5).

Таблиця 3.5 - Основні перспективи використання Agile у сфері електронних довірчих послуг

Напрям розвитку	Сутність перспективи	Очікуваний ефект
Клієнт-центрований розвиток сервісів	Використання User Persona, моніторинг поведінки користувачів, адаптація UX	Підвищення доступності та зручності електронних підписів
Інкрементне оновлення функціоналу	Впровадження нових модулів через спринти без зупинки сервісу	Стабільність роботи та швидке реагування на зміни
Гармонізація Agile з eIDAS та законодавством України	Використання підходів continuous compliance	Зменшення юридичних ризиків і пришвидшення сертифікації
Оптимізація бізнес-процесів через Use Case моделювання	Системна ідентифікація критичних сценаріїв	Підвищення безпеки та зменшення операційних ризиків
Масштабування сервісів через BMC-аналітику	Визначення нових сегментів користувачів та каналів поширення	Розширення ринку електронних довірчих послуг
Вбудована кібербезпека	Безперервний аудит і тестування під час кожного спринту	Підвищення рівня цифрової довіри й зменшення інцидентів

Джерело: складено автором

Перспективи впровадження Agile-підходу у сфері електронних довірчих послуг свідчать про значний потенціал перетворення цифрових сервісів на динамічну, адаптивну та користувацько-орієнтовану систему. Agile забезпечує гнучкість, швидкість і точність прийняття рішень, дозволяє будувати електронні послуги відповідно до сучасних технологічних стандартів, збільшує конкурентоспроможність державних рішень і створює підґрунтя для розвитку цифрової економіки.

Загалом, запропонована трансформація підходів до створення систем довірчих послуг відповідає глобальним тенденціям розвитку управлінської думки. Як зазначають М. Кучма та О. Орлова-Курилова, еволюція концепцій менеджменту в умовах цифрової трансформації неминуче веде до переходу від традиційних ієрархічних моделей до гнучких, технологічно орієнтованих систем управління. Штучний інтелект та Agile-філософія у цьому процесі виступають

не просто інструментами, а ключовими драйверами змін, що дозволяють організаціям адаптуватися до вимог часу та забезпечувати конкурентоспроможність у цифровому просторі. Впровадження цих підходів у сферу КНЕДП є необхідним кроком для побудови сучасної, надійної та клієнт-орієнтованої інфраструктури електронної довіри в Україні [49].

Висновки до розділу 3

У третьому розділі було обґрунтовано, що впровадження Agile-підходу у розробку та модернізацію системи електронних довірчих послуг є не просто технологічним рішенням, а необхідною умовою підвищення адаптивності, безпеки та юридичної стійкості цифрової інфраструктури. На відміну від традиційних моделей проєктного управління, які передбачають лінійну реалізацію функціоналу, Agile дозволяє ефективно працювати у середовищі, де нормативні вимоги часто змінюються, кіберзагрози постійно ускладнюються, а користувачі очікують високої швидкості та простоти електронних сервісів. Саме тому гнучкі методології забезпечують баланс між інноваційністю та нормативною визначеністю, що має ключове значення для кваліфікованих надавачів електронних довірчих послуг.

Розглянувши особливості впровадження Agile у сфері КНЕДП, було встановлено, що критично важливою є інтеграція юридичного аналітика у роботу міжфункціональної команди. На практиці саме юридичний фахівець забезпечує відповідність функціональних інкрементів вимогам eIDAS, Закону України «Про електронні довірчі послуги», підзаконним актам ДССЗЗІ та НБУ, не дозволяючи технічним новаціям виходити за межі юридично допустимого. Такий підхід робить юридичну відповідність не зовнішнім етапом перевірки, а частиною Definition of Done, що значно підвищує керованість ризиками та якість розроблюваного функціоналу.

У ході дослідження було доведено, що для створення життєздатного цифрового продукту у сфері електронних довірчих послуг необхідним є використання бізнес-дизайн інструментів, зокрема Business Model Canvas, User

Persona та Use Case діаграм. Вони дозволяють поєднати технічні, правові та поведінкові аспекти продукту: чітко окреслити ключові сегменти користувачів, сформувати логіку їхньої взаємодії із системою, визначити джерела цінності сервісу, а також спрогнозувати сильні та слабкі сторони бізнес-моделі КНЕДП. Застосування таких інструментів в Agile-середовищі посилює фокус на потребах користувача, дає можливість тестувати гіпотези щодо поведінки різних категорій клієнтів та робить продукт більш конкурентоспроможним.

Важливою складовою аналізу стало визначення ролі Agile як інструменту управління ризиками. Гнучкі методології надають можливість реагувати на інциденти інформаційної безпеки в режимі, близькому до реального часу, формуючи аварійні спринти для ліквідації критичних вразливостей, оновлення криптографічних алгоритмів чи виправлення помилок у процедурах сертифікації. Замість того щоб чекати на завершення повного циклу розробки, команда може оперативно впроваджувати оновлення, зберігаючи безперервність роботи сервісу та юридичну силу електронних підписів.

Також, в рамках розділу було розраховано кошторис на утримання Agile-команди, до складу якої входить юридичний аналітик, що підтвердило економічну доцільність запропонованого підходу. Доведено, що витрати на постійний юридичний супровід та ітеративну розробку є меншими, ніж потенційні збитки від переробки системи у випадку виявлення невідповідності вимогам законодавства на фінальних етапах, що характерно для каскадних моделей.

Перспективи розвитку Agile у сфері електронних послуг засвідчили, що цей підхід є придатним не лише для внутрішньої оптимізації процесів, але й для системного масштабування ринку електронних довірчих сервісів. Agile забезпечує можливість поступового розширення функціоналу, залучення нових сегментів користувачів, інтеграцію з банківськими та державними системами, а також впровадження сервісної моделі розвитку КЕП, орієнтованої на цінність для кінцевого користувача. Поєднання інкрементності, високого рівня прозорості, постійної комунікації зі стейкголдерами та гнучкого управління

продуктовим беклогом створює сприятливе середовище для побудови сервісів, здатних відповідати сучасним вимогам цифрової економіки.

У підсумку, результати розділу засвідчили, що Agile-підхід має значний потенціал для модернізації та стратегічного розвитку системи електронних довірчих послуг в Україні. Він формує умови для підвищення правової відповідності, безпеки, швидкості розвитку сервісів, клієнт-орієнтованості та конкурентоспроможності. Поєднання гнучких методологій із сучасними інструментами цифрового дизайну дозволяє створити інноваційну модель управління розробкою, яка гармонійно інтегрує технічні, юридичні та поведінкові аспекти функціонування електронних послуг. Саме така модель є найбільш адекватною для майбутнього розвитку цифрової інфраструктури та реалізації принципів європейського цифрового врядування.

ВИСНОВКИ

Проведене дослідження підтвердило, що кваліфіковані електронні довірчі послуги є ключовим елементом сучасної цифрової інфраструктури держави та бізнесу. Стрімкий розвиток онлайн-сервісів, поява віддалених форм ідентифікації, електронного документообігу та безпечних транзакцій формують запит на технології, які здатні забезпечити юридично значущі дії без фізичної присутності. Саме такі технології - електронні підписи, криптографічні засоби захисту, системи ідентифікації користувачів та механізми гарантування цілісності даних - стали основою того, що сьогодні укладання угод і підпис документів можуть здійснюватися повністю онлайн, а КЕП в Україні зрівняний за юридичною силою з власноручним підписом.

У межах першого завдання було встановлено, що хоча потреба у КЕП постійно зростає, кількість кваліфікованих надавачів в Україні залишається вкрай малою. Обмежена конкуренція, високі регуляторні вимоги та відсутність технологічного оновлення багатьох КНЕДП створюють бар’єри для ринку та гальмують розвиток інновацій. Аналіз довів, що необхідність створення нової, сучасної системи надання довірчих послуг ґрунтується на запиті суспільства на швидкі, безпечні та зручні електронні сервіси, а також на потребі підвищення якості функціонування критичної цифрової інфраструктури.

У результаті аналізу структури та вимог до КНЕДП показано, що юридичні обмеження в цій сфері є значно жорсткішими, ніж у розробці звичайних ІТ-систем. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» фактично визначає структуру майбутнього програмного забезпечення, регламентуючи бізнес-процеси, способи ідентифікації користувачів, процедури видачі сертифікатів, порядок відкликання ключів та функціональні ролі персоналу. Також виявлено, що система КНЕДП повинна неодноразово проходити аудит відповідності, а будь-які зміни у законодавстві вимагають негайного оновлення технічних і організаційних процесів.

Визначення особливостей розробки системи показало, що класичні моделі, зокрема водоспадна модель, не відповідають специфіці цього ринку, оскільки не

дозволяють швидко реагувати на нормативні зміни, кіберінциденти та вимоги аудиту. Було встановлено, що розробка систем цього типу потребує постійної участі юридичного фахівця, який здатний забезпечити дотримання eIDAS, національного законодавства та технічних регламентів у кожному етапі життєвого циклу продукту. Також проаналізовано, що система КНЕДП потребує інтегрованої моделі управління ризиками, постійного тестування та адаптивності до зовнішніх змін.

Запропоновано оптимізацію процесу розробки системи КНЕДП шляхом впровадження адаптивної моделі Agile, яка враховує особливості регульованого середовища. Доведено, що саме Agile найбільш ефективно інтегрується з вимогами системи електронних довірчих послуг, оскільки забезпечує безперервну юридичну оцінку, швидке реагування на законодавчі зміни та гнучке управління вимогами. Важливою практичною пропозицією стала модель командної інтеграції юридичного аналітика як постійного учасника спринтів, що дозволяє уникати розсинхронізації між технічним і правовим блоком продукту. Використання інструментів User Persona, Use Case та Business Model Canvas дало можливість структурувати процес розробки не лише з технічного, але й з бізнесового та поведінкового погляду.

Розроблено план реалізації системи КНЕДП із використанням Agile-підходу через опис гнучкої, ітераційної, ризик-орієнтованої моделі керування розробкою. Визначено структуру Agile-команди, ролі, правила комунікації, планування спринтів, критерії приймання, порядок тестування та механізми забезпечення відповідності законодавству. Розраховано бюджет проєкту, який склав 253 920 USD, та обґрунтовано економічну ефективність впровадження Agile-підходу за рахунок зниження ризиків переробки системи на 25%.

Таким чином, досягнення кожного із завдань дало можливість сформувати цілісне уявлення про те, як має функціонувати сучасна система надання електронних довірчих послуг в Україні та яким чином Agile може стати інструментом її стратегічного розвитку. У роботі доведено, що поєднання гнучких методологій, юридичної експертизи та бізнес-аналітики забезпечує

можливість створення інноваційного, безпечного та конкурентоспроможного сервісу, відповідного міжнародним стандартам та очікуванням користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Aghina W., Handscomb Ch., Salo O., Thaker Sh. The impact of agility: how to shape your organization to compete. McKinsey & Company. 2021. URL: https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-impact-of-agility-how-to-shape-your-organization-to-compete (дата звернення: 17.11.2025).

2. Agile Essentials: Agile 101. What is Agile? Agile Alliance. URL: https://www.agilealliance.org/agile101/ (дата звернення: 21.11.2025).

3. Agile Vs. Waterfall: Which Project Management Methodology Is Best For You? Forbes Advisor. 2022. URL: https://www.forbes.com/advisor/business/agile-vs-waterfall-methodology/ (дата звернення: 16.11.2025).

4. Agile-маніфест розробки програмного забезпечення / J. Sutherland, K. Schwaber, K. Beck та ін. URL: https://agilemanifesto.org/iso/uk/manifesto.html (дата звернення: 15.11.2025).

5. Daraojimba C., Nwasike Ch. N., Adegbite A. O., Ezeigweneme Ch. A. A comprehensive review of agile methodologies in project management. Computer Science & IT Research Journal. 2024. Vol. 5(1). P. 190-218. DOI: 10.51594/csitrj.v5i1.717.

6. Hamanyuk I. M. Agile flexible development manifesto from the customer’s point of view. Connectivity. 2024. Vol. 168, no. 2. URL: https://doi.org/10.31673/2412-9070.2024.020308 (date of access: 25.11.2025).

7. How’s Ralabs different from anyone else? 2024. URL: https://ralabs.org/why-work-at-ralabs/ (дата звернення: 19.11.2025).

8. LEAN мислення / LEAN Production / LEAN Manufacturing. Lean Institute Ukraine. URL: https://lean.org.ua/olean (дата звернення: 20.11.2025).

9. Mishenina H., Pavlenko D. Features and prospects of agile application in the activity of public authorities in terms of Ukraine’s public administration transformations. Vìsnik Sums′kogo deržavnogo unìversitetu. 2020. No. 4. P. 139-151. URL: https://doi.org/10.21272/1817-9215.2020.4-16 (date of access: 25.11.2025).

10. Navigating the Agile Umbrella: Unveiling the Essence of Agile Methodologies. 2023. URL: https://guides.visual-paradigm.com/navigating-the-agile-umbrella-unveiling-the-essence-of-agile-methodologies/ (дата звернення: 18.11.2025).

11. Puka M. P. Legal regulation of electronic contracts: problems of authentication and legal validity of electronic signature. Scientific notes of Taurida National V.I. Vernadsky University. Series: Juridical Sciences. 2025. No. 3. P. 173-178. URL: https://doi.org/10.32782/tnu-2707-0581/2025.3/27 (date of access: 25.11.2025).

12. Putta A., Uludağ Ç., Paasivaara M., Hong Sh.-L. Benefits and challenges of adopting SAFe - an empirical survey. Agile Processes in Software Engineering and Extreme Programming (XP 2021). 2021. P. 172-187.

13. Riedl R., Oettl Ch., Stangl F. J., Hevner A. R. How an agile software process increases developers' job satisfaction: a stress perspective based on the effort-reward-imbalance model. Business & Information Systems Engineering. 2025. Vol. 67. P. 83-107. URL: https://link.springer.com/article/10.1007/s12599-024-00919-x (дата звернення: 22.11.2025).

14. Rigby D. K., Sutherland J., Noble A. Agile at scale. Harvard Business Review. 2018. Vol. 96(3). P. 88-96. URL: https://hbr.org/2018/05/agile-at-scale (дата звернення: 20.11.2025).

15. Stray V., Moe N., Hoda R. Autonomous agile teams: challenges and future directions for research. Proceedings of the 19th International Conference on Agile Software Development: Companion. 2018. P. 1-5.

16. Understanding Lean Methodology and Its Applications. Indeed. 2023. URL: https://ca.indeed.com/career-advice/career-development/lean-methodology (дата звернення: 22.11.2025).

17. Waterfall Methodology: A Comprehensive Guide. Atlassian. URL: https://www.atlassian.com/agile/project-management/waterfall-methodology (дата звернення: 19.11.2025).

18. What is Scrum? An overview of Scrum and The Agile Journey. PM-partners. 2024. URL: https://www.pm-partners.com.au/insights/the-agile-journey-a-scrum-overview/ (дата звернення: 23.11.2025).

19. What to expect in 2025: key FDA regulatory trends impacting importers and food businesses. FDAImports.com. 2025. URL: https://www.fdaimports.com/what-to-expect-in-2025/?utm_source (дата звернення: 19.11.2025).

20. Вміння бачити бізнес-процеси: створення цінності та зменшення втрат / М. Ротер, Д. Шук; пер. з англ. К. Гуменюк. Київ: Пабулум, Lean Institute Ukraine, 2017. 132 с.

21. Воронкова В. Г., Нікітенко В. О., Васильчук Г. М. Agile-філософія як чинник форсайту цифрової економіки. Цифрова економіка та економічна безпека. 2022. № 3. С. 109-117. DOI: 10.32782/dees.3-19.

22. Галушка В. Теоретико-методичні засади управління проєктами. Підприємництво, господарство і право. 2020. № 7. С. 430-434.

23. Дідковська М. Технології проектування програмного забезпечення / Марина Дідковська. КПІ, 2020. URL: http://mmsa.kpi.ua/sites/default/files/disciplines/didkovska_m_v (дата звернення: 17.11.2025).

24. Дрогозюк К. Б. Нормативно-правове регулювання електронного підпису в цивільному судочинстві України та Франції. Часопис цивілістики. 2019. Вип. 34. С. 74-84.

25. IT-індустрія забезпечила $2 млрд експортних надходжень в умовах війни. 2022. URL: https://itukraine.org.ua/the-it-industry-provided-a-record-$-2-billion-in-exportearnings-during-the-war.html (date of access: 25.11.2025).

26. КЕП чи УЕП? Що вимагати у Учасників закупівель в Прозорро. Інформаційний ресурс - Інфобокс Прозорро. URL: https://infobox.prozorro.org/articles/yakiy-elektronniy-pidpis-maye-naklasti-uchasnik-na-svoyu-propoziciyu (дата звернення: 17.11.2025).

27. Ковальчук Н., Комарова К. Гнучкі підходи в управління командами. Економіка та суспільство. 2023. № 47. DOI: 10.32782/2524-0072/2023-47-20.

28. Крикавська І. В., Ткачук Л. В. Актуальні питання правового регулювання використання електронного підпису. Юридичний науковий електронний журнал. 2021. № 11. С. 447-449.

29. Ланкастер Д. Лідерство в стилі Lean: шлях до постійного вдосконалення вашого бізнесу / Джим Ланкастер. Київ: K.Fund, 2023. 240 с.

30. Новосад Р. В. Правовий статус електронного підпису в Україні: від ідеї до реалізації. Право та державне управління. 2023. № 3. С. 112-116.

31. Нормативно-правові акти у сфері електронних довірчих послуг. ДПСУ. URL: https://acsk.dpsu.gov.ua/normative-documentation (дата звернення: 18.11.2025).

32. Особливості використання кваліфікованого електронного підпису під час роботи з програмним РРО. Державна Податкова Служба. URL: https://nvp.tax.gov.ua/media-ark/news-ark/601102.html (дата звернення: 18.11.2025).

33. Особливості електронного підпису та переваги його використання. Згурівський районний суд Київської області. URL: https://zg.ko.court.gov.ua/sud1011/pres-centr/news/1383907 (дата звернення: 19.11.2025).

34. Петруненко Я. В., Сиротко М. В., Тройніков В. В. Правове регулювання електронної комерції в умовах розвитку цифрової економіки в Україні. Науковий вісник Ужгородського Національного Університету. Серія Право. 2023. Вип. 79. Ч. 1. С. 278-285.

35. Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації: Закон України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2801-20#Text (дата звернення: 18.11.2025).

36. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#n534 (дата звернення: 18.11.2025).

37. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 21.11.2025).

38. Про затвердження Положення про використання електронного підпису та електронної печатки: постанова Національного банку України від 20.12.2023 № 172. URL: https://zakon.rada.gov.ua/laws/show/v0172500-23#Text (дата звернення: 23.11.2025).

39. Псарьов О., Дружинін Є. Agile-фреймворк як каталізатор ефективного впровадження систем управління інформацією. Інформаційні технології та суспільство. 2024. № 4. С. 108-114. DOI: 10.32689/maup.it.2024.4.17.

40. Регламент Європейського парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку від 23 липня 2014 року. URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення: 15.11.2025).

41. Смолич Д. В. Інноваційні методи управління проектами. Економічний форум. 2019. № 4. С. 50-53.

42. Тітова Г. О. Проблеми правового регулювання використання електронного підпису при укладанні правочинів в сфері електронної комерції. Інформаційні технології у судочинстві: матер. всеукр. наук.-практ. конф. (Одеса, 18 квітня 2017 р.). Одеса: Фенікс, 2017. С. 95-98.

43. Швабер К., Сазерленд Д. Авторитетний посібник зі Скраму: Правила гри. Scrum.org & ScrumInc, 2014. 18 с.

44. Шевченко В. С. Синергія agile-підходу та low-code технологій як чинник підвищення адаптивності підприємств до кризових умов. Development Service Industry Management. 2025. № 2. С. 142-148. DOI: 10.31891/dsim-2025-10(17).

45. Ядуха С., Дурач А., Семенченко В., Яблонський Т. Управління проєктною діяльністю підприємства на засадах agile-менеджменту та сучасних інформаційних технологій. Development Service Industry Management. 2023. № 4. С. 95-100. DOI: 10.31891/dsim-2023-4(15).

46. Мігаль Д. Гібридна самоорганізація як підхід до гнучкого управління командною роботою / Д. Мігаль, О. Орлова-Курилова // Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку: матеріали VI міжнародної конференції (Київ, 05 грудня 2024 р.). – Київ: Університет «КРОК», 2024. – URL: https://dspace.krok.edu.ua/server/api/core/bitstreams/0fb93e1b-07ce-4913-9b3b-b5da7b770f49/content?trackerId=333cfc67967e5018

47. Мігаль Д. Agile-підхід до адаптації нових співробітників: переваги та виклики / Д. Мігаль, О. Орлова-Курилова // Вчені записки Університету «КРОК». – 2025. – № 1 (77). – С. 289–298. – URL: https://dspace.krok.edu.ua/server/api/core/bitstreams/bec3a661-d925-4ec7-81ac-8c2a1af890f8/content?trackerId=333cfc67967e5018

48. Крискун І. Керування ризиками в управлінні ІТ-проєктами з використанням інструментів штучного інтелекту / І. Крискун, О. Орлова-Курилова // Вчені записки Університету «КРОК». – 2025. – № 2 (78). – С. 315–325. – URL: https://dspace.krok.edu.ua/server/api/core/bitstreams/64e56129-6452-41f5-9557-e077acde7179/content?trackerId=333cfc67967e5018

49. Кучма М. Еволюція концепцій менеджменту в умовах цифрової трансформації: роль штучного інтелекту / М. Кучма, О. Орлова-Курилова // Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку: матеріали VI міжнародної конференції (Київ, 05 грудня 2024 р.). – Київ: Університет «КРОК», 2024. – С. 447. – URL: https://dspace.krok.edu.ua/server/api/core/bitstreams/44520826-e42c-46d6-a0c9-b4461d684c89/content?trackerId=333cfc67967e5018