

Кафедра фінансів, банківської справи та страхування

«Цифрові фінансові послуги: сучасний стан та перспективи розвитку»

Галузь знань: 07 «Управління та адміністрування»

Освітня програма **ФІНАНСИ, БАНКІВСЬКА СПРАВА, СТРАХУВАННЯ ТА ФОНДОВИЙ РИНОК**

Освітньо-кваліфікаційний рівень: магістр

Виконавець:

Верютін Олександр Михайлович
Студент 2 курсу, гр. ЕФ-61

Науковий керівник:

Глущенко Ольга Вікторівна
Доктор економічних наук,
професор

Кваліфікаційна робота магістра допущена до захисту рішенням кафедри фінансів, банківської справи та страхування

Протокол № _____ від « ____ » _____ 2025 р.
Зав. кафедри _____ проф.
підпис _____

Харків 2025

АНОТАЦІЯ

Верютін О.М. Цифрові фінансові послуги: сучасний стан та перспективи розвитку. – Рукопис

Кваліфікаційна робота магістра.

Харківський національний університет імені В. Н. Каразіна. – Харків, 2025.

У кваліфікаційній магістерській роботі досліджено стан і перспективи розвитку цифрових фінансових послуг в Україні в умовах відновлення та євроінтеграції. Уточнено зміст поняття «цифрові фінансові послуги» як екосистеми продуктів, платформ і інфраструктур банківського, небанківського та фінтех-секторів, що забезпечують дистанційну фінансову взаємодію між домогосподарствами, бізнесом і державою. Запропоновано класифікацію цифрових послуг за функціональними блоками, технологічними підходами та рівнем регуляторної взаємодії, що дає змогу виокремити напрями зростання, потенціал масштабування й ключові групи ризиків для фінансової стабільності та споживачів.

Методологія дослідження базується на системному підході, статистичному й порівняльному аналізі даних НБУ та міжнародних організацій. Проаналізовано динаміку безготівкових і миттєвих платежів, розвиток дистанційних каналів обслуговування, мобільного й інтернет-банкінгу, становлення відкритого банкінгу та цифрових екосистем, включно з government-as-a-platform. Показано, що повномасштабна війна одночасно прискорила цифровізацію роздрібних платежів і державних сервісів та загострила проблеми кіберзагроз, цифрової нерівності, захисту даних і стійкості платіжної інфраструктури та критичних фінансових сервісів.

На основі порівняння з ЄС, США та окремими азійськими ринками сформовано бенчмарки для оцінювання рівня інклюзії, інноваційності й регуляторної зрілості цифрових фінансових послуг в Україні. Запропоновано візію розвитку до 2030 року та комплекс рекомендацій для НБУ, органів державної влади й учасників ринку щодо переходу до data-driven регулювання,

посилення кіберстійкості, розширення фінансової включеності населення, підвищення довіри споживачів, інтеграції ESG-параметрів і використання цифрових фінансових інструментів як драйвера сталого економічного зростання.

Ключові слова: цифрові фінансові послуги; фінансова стабільність; фінтех-екосистема; платіжні інновації; сталий розвиток.

ABSTRACT

Veriutin O. M. Digital financial services: current state and prospects for development. – Manuscript.

Master's qualification thesis

V. N. Karazin Kharkiv National University. – Kharkiv, 2025.

The master's qualification thesis examines the current state and prospects for the development of digital financial services in Ukraine under conditions of post-war recovery and European integration. The concept of “digital financial services” is clarified as an ecosystem of products, platforms and infrastructures of the banking, non-banking and fintech sectors that enable remote financial interaction between households, businesses and the state. A classification of digital services is proposed by functional blocks, technological approaches and the level of regulatory interaction, which makes it possible to identify growth areas, scaling potential and key groups of risks for financial stability and consumers.

The research methodology is based on a systemic approach and on statistical and comparative analysis of data from the National Bank of Ukraine and international organisations. The thesis analyses the dynamics of cashless and instant payments, the development of remote service channels, mobile and Internet banking, as well as the emergence of open banking and digital ecosystems, including government-as-a-platform solutions. It is shown that the full-scale war has simultaneously accelerated the digitalisation of retail payments and public services and exacerbated problems of cyber threats, digital inequality, data protection, and the resilience of payment infrastructure and critical financial services.

Based on comparison with the EU, the United States and selected Asian markets, benchmarks are developed to assess the level of inclusion, innovativeness and regulatory maturity of digital financial services in Ukraine. The thesis proposes a vision of development up to 2030 and a set of recommendations for the National Bank of Ukraine, public authorities and market participants regarding the transition to data-

driven regulation, strengthening cyber-resilience, expanding financial inclusion of the population, increasing consumer trust, integrating ESG parameters, and using digital financial instruments as a driver of sustainable economic growth.

Keywords: digital financial services; financial stability; fintech ecosystem; payment innovations; sustainable development.

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ РОЗВИТКУ ЦИФРОВИХ ФІНАНСОВИХ ПОСЛУГ	10
1.1. Сутність, структура та класифікація цифрових фінансових послуг.....	10
1.2. Теоретичні підходи до цифровізації та її вплив на фінстабільність	19
1.3. Технологічні інновації та цифрова трансформація інститутів.....	28
РОЗДІЛ 2. СУЧАСНИЙ СТАН ТА РОЗВИТОК РИНКУ ЦИФРОВИХ ФІНАНСОВИХ ПОСЛУГ	37
2.1. Огляд ключових тенденцій, ризиків та бар'єрів розвитку цифрових фінансових послуг в Україні	37
2.2. Оцінка поточного рівня та динаміки розвитку цифрових фінансових послуг в Україні	47
2.3. Порівняльний аналіз міжнародного досвіду цифровізації фінансових систем (ЄС, США, Азія та Україна)	57
РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА НАПРЯМИ УДОСКОНАЛЕННЯ РОЗВИТКУ ЦИФРОВИХ ФІНАНСОВИХ ПОСЛУГ В УКРАЇНІ	69
3.1. Стратегічні пріоритети розвитку цифрових фінансових послуг в Україні	69
3.2. Підвищення ефективності регулювання та впровадження інновацій у сфері цифрових фінансових послуг	77
3.3. Імплементація цифрових фінансових інструментів у стратегію сталого розвитку фінансового сектору.....	86
ВИСНОВОК.....	98
Список використаних джерел	101
ДОДАТКИ	127

ВСТУП

Актуальність обраної теми зумовлена стрімкою цифровізацією фінансового сектору України, яка відбувається на тлі воєнних викликів, структурних змін в економіці та євроінтеграційного курсу держави. За останні роки цифрові платіжні сервіси, дистанційне банківське обслуговування, мобільні гаманці, миттєві перекази, «необанки» та інші фінтех-рішення перетворилися з додаткового сервісу на базовий канал взаємодії між споживачами, бізнесом і фінансовими установами. В цих умовах від якості, надійності та доступності цифрових фінансових послуг безпосередньо залежать фінансова включеність населення, швидкість відновлення економіки, конкурентоспроможність банківського сектору та рівень довіри до фінансової системи в цілому.

Разом з тим швидке поширення цифрових сервісів супроводжується низкою проблем: нерівномірним доступом різних груп населення до сучасних каналів обслуговування, посиленням кіберзагроз, появою нових моделей шахрайства, а також потребою в оновленні регуляторної бази відповідно до стандартів ЄС та кращих світових практик. Це створює наукову й практичну проблему – оцінити сучасний стан ринку цифрових фінансових послуг, виявити основні тенденції й ризики, визначити бар'єри розвитку та обґрунтувати напрями вдосконалення державної політики й бізнес-моделей учасників ринку. Саме тому дослідження цифрових фінансових послуг, їхнього сучасного стану та перспектив розвитку є своєчасним і має як теоретичне значення для поглиблення розуміння трансформації фінансової системи, так і прикладну цінність для регуляторів, фінансових установ і користувачів цих послуг.

Огляд літератури. У сучасних зарубіжних дослідженнях цифрові фінансові послуги розглядаються як результат поєднання блокчейн-технологій, децентралізованих фінансів, цифрової економіки та фінтех-інновацій. Е. Abad-Segura та співавт. аналізують фактори формування довіри до облікових систем на базі блокчейну, підкреслюючи значення прозорості й захищеності даних для сприйняття цифрових сервісів користувачами [1]. W. Al-Zoubi, спираючись на бібліометричний огляд, показує, що дослідження цифрової економіки дедалі частіше концентруються на платіжних інноваціях та цифрових платформах [5].

А. Alamsyah з колегами систематизують екосистеми DeFi та пропонують таксономію блокчейн-рішень у фінансовій сфері [6; 7], тоді як М. Asif та співавт. демонструють, як фінтех-та цифрові фінансові послуги сприяють фінансовій інклюзії в Індії [13]. N. Azeez та співавт. пропонують методологічну рамку вимірювання «цифрової» фінансової інклюзії [17], а Т. Babina, S. Bahaj та ін. на основі перших результатів впровадження open banking показують вплив доступу до клієнтських даних на вхід фінтех-компаній і конкуренцію [18]. У роботах Т. Bas та співавт., а також S. Daud, S. Hasan і їхніх колег, простежується зв'язок між розвитком цифрових фінансів, індексами CBDC, фінансовою стабільністю та економічним зростанням [20; 34; 68; 142].

Важливе місце займають дослідження нормативно-інституційних засад цифрових фінансових послуг і механізмів підтримки інновацій. Досвід регуляторних «пісочниць» узагальнено у звіті Світового банку (S. Appaya, H. Gradstein та ін.), де показано, як тестування фінтех-продуктів у контрольованому середовищі дозволяє збалансувати інновації та ризики [12]. Спеціальні доповіді ADA, REDCAMIF та Alliance for Financial Inclusion висвітлюють роль фінтех-рішень у «зеленій» фінансовій інклюзії та підтримці вразливих груп, зокрема МСП, що належать вимушено переміщеним особам [4; 8–10]. У працях V. Brühl та авторів NBER-дослідження (Т. Babina та ін.) акцентується, що відкритий банкінг і платформи BigTech змінюють структуру ринку та підходи до регулювання цифрових фінансів [18; 23]. На наднаціональному рівні ключові орієнтири задають Банк міжнародних розрахунків щодо сталої фінансової політики центральних банків [19], Асоціація європейських банків і європейські наглядові органи, які через настанови з ICT-та кіберризиків, DORA і PSD2 формують вимоги до цифрової операційної стійкості, доступу до даних та захисту споживачів [21; 26; 39; 41; 45–47; 49; 51–53; 56–58; 59; 69; 71; 92; 95; 161; 168].

Окремий кластер літератури присвячений впливу цифрової трансформації на бізнес-моделі, ефективність і ризики фінансових установ. S. Fang і G. Wen досліджують стійкість інноваційної взаємодії між банками та фінтех-компаніями, обґрунтовуючи переваги коопераційних моделей над суто

конкурентними [61]. I. Gálík, A. Kaščáková та ін. порівнюють індекси цифрової конкурентоспроможності та розвитку ШІ, показуючи, що цифрова трансформація фінансового сектору тісно пов'язана з рівнем цифрових компетентностей суспільства [64]. D. Dolbnieva, Y. Antypin та їхні колеги аналізують, як інноваційна трансформація фінансових установ впливає на управління соціальними конфліктами в умовах цифровізації [38], тоді як M. Mavlutova та співавт. доводять, що цифрова трансформація сприяє як фінансовій інклюзії, так і операційній ефективності [99]. Q. Li та X. Zhang, Z. Liu з колегами, а також M. Iatzaz Ul Hassan і співавт. на матеріалі Китаю та інших країн, що розвиваються, показують, що розвиток цифрового фінансування та inclusive FinTech позитивно корелює з продуктивністю банків, але водночас генерує нові канали системних ризиків [72; 96; 97]. Для українського корпоративного та роздрібного сегменту релевантними є висновки D. Kretov, O. Kretova, A. Metelski, D. Dylewski та інших авторів щодо управління цифровізацією, KPI DeFi-проектів і використання методів аномалій-детекції в цифрових фінансових системах [94; 101; 148].

Український науковий та аналітичний дискурс фокусується на специфіці цифрової трансформації фінансового сектору в умовах війни, енергетичних шоків та євроінтеграції. Оглядові роботи O. Dovhan, M. Tymots, O. Iorgachova, R. Miroshnyk і I. Kukhta висвітлюють еволюцію цифрових інновацій на фінансовому ринку України, розвиток цифрового банкінгу та фінтех-сектору в 2010–2025 рр. [40; 84; 100; 108; 162]. Статистичну базу для аналізу становлять дані DataReportal щодо рівня цифровізації, профілів цифрового розвитку ITU, обстеження фінансової грамотності та інклюзії NBU й OECD/INFE, а також індикатор 9.6.1 Держстату про охоплення інтернет-послугами [33; 81; 82; 118; 141; 158; 175–177]. На рівні інфраструктури ключовими є звіти НБУ про роботу банківського сектору, карткового ринку, СЕП-4.1, впровадження ISO 20022, миттєвих переказів, BankID та ризику шахрайства [114; 116–121; 123–124; 127–139; 160]. Дослідження L. Robochenko, O. Prokopenko, N. Shmygol, V. Smal, O. Totska, O. Urikova, Y. Verheliuk та ін. окреслюють ризики інвестування у фінтех, напрями покращення взаємин із клієнтами через цифрові сервіси, загрози

кібербезпеки в умовах воєнного стану, роль цифрових грошових переказів і перспективи розвитку української фінтех-індустрії [149; 151; 156; 157; 159; 166; 167; 169]. Водночас законодавчі акти щодо платіжних послуг та відкритого банкінгу, а також каталоги UAFIC і опитування Visa про рівень довіри до безготівкових розрахунків демонструють, що нормативна рамка та ринкова практика в Україні ще перебувають у процесі гармонізації з європейським цифровим фінансовим простором [163; 164; 170; 171; 173; 178], що й зумовлює необхідність комплексного дослідження сучасного стану й перспектив розвитку цифрових фінансових послуг.

Мета кваліфікаційної роботи полягає в розробці теоретичних положень і практичних рекомендацій щодо формування та розвитку стійкої екосистеми цифрових фінансових послуг в Україні з урахуванням узагальнення вітчизняного й зарубіжного досвіду та пріоритетів фінансової стабільності й сталого розвитку.

Завдання дослідження

Для досягнення поставленої мети в роботі передбачено розв'язання таких основних завдань:

1. Узагальнити теоретичні підходи до визначення сутності, структури та класифікації цифрових фінансових послуг і їх зв'язку з фінансовою стабільністю.
2. Проаналізувати сучасний стан і динаміку розвитку ринку цифрових фінансових послуг в Україні, виявити основні ризики та бар'єри їх поширення.
3. Систематизувати міжнародний досвід розвитку цифрових фінансових послуг (ЄС, США, Азія) та на цій основі сформулювати бенчмарки для України.
4. Обґрунтувати стратегічні пріоритети й розробити практичні рекомендації щодо розвитку та регулювання цифрових фінансових послуг в Україні та їх інтеграції в стратегію сталого розвитку фінансового сектору.

Об'єкт дослідження – процеси формування та функціонування екосистеми цифрових фінансових послуг в Україні.

Предмет дослідження – теоретичні, організаційні та прикладні засади розвитку стійкої екосистеми цифрових фінансових послуг в Україні та її впливу на фінансову стабільність і сталий розвиток.

У дипломній роботі використано комплекс загальнонаукових та спеціальних **методів** дослідження. Теоретико-методичну базу сформовано за допомогою аналізу, синтезу, індукції та дедукції для узагальнення підходів вітчизняних і зарубіжних науковців до сутності та класифікації цифрових фінансових послуг. Для оцінювання сучасного стану й динаміки розвитку ринку застосовано економіко-статистичні методи (групування, порівняльний аналіз, аналіз трендів) на основі офіційних даних НБУ, міжнародних організацій і галузевої аналітики. Системно-структурний підхід дозволив виявити взаємозв'язки між учасниками цифрової фінансової екосистеми, а графічні методи – наочно представити ключові показники та тенденції розвитку цифрових фінансових послуг в Україні.

Інформаційну базу дослідження становлять нормативно-правові акти України, що регулюють розвиток платіжного ринку, цифрових фінансових послуг та фінансового сектору загалом, зокрема закони України, постанови Кабінету Міністрів, нормативні документи Національного банку України, профільних міністерств і регуляторних органів. Використано офіційні статистичні та аналітичні матеріали НБУ, Державної служби статистики України, міжнародних організацій (Світовий банк, МВФ, OECD, ITU, ЄЦБ), а також результати репрезентативних опитувань щодо фінансової грамотності, інклюзії та довіри до цифрових платежів. Аналітичну складову доповнюють галузеві звіти міжнародних і національних асоціацій (фінтех-об'єднань, банківських та платіжних організацій), відкриті дані цифрових платформ та платіжних систем, а також емпіричні дослідження, опубліковані в українських і зарубіжних наукових виданнях, що індексуються у провідних наукометричних базах.

Наукова література. Важливе місце посідають аналітичні матеріали міжнародних організацій і професійних асоціацій, які узагальнюють глобальні тренди розвитку цифрових платежів, інклюзивних фінансів та ESG-орієнтованих

фінансових продуктів. Додаткові відомості отримано з електронних наукових журналів і баз даних Scopus, Web of Science та інших наукометричних ресурсів, що дозволило поєднати сучасні теоретичні підходи з актуальними статистичними та кейс-орієнтованими дослідженнями.

Наукова новизна одержаних результатів полягає в подальшому розвитку теоретико-методичних засад дослідження цифрових фінансових послуг. У роботі уточнено зміст поняття «цифрові фінансові послуги» як багаторівневої системи сервісів, що базуються на поєднанні платіжної інфраструктури, даних та цифрових каналів взаємодії, а не лише на технологічній формі їх надання. Запропоновано авторську класифікацію цифрових фінансових послуг за критеріями технологічної основи (API, блокчейн, штучний інтелект, хмарні рішення), функціонального призначення (платежі, кредитування, інвестиції, страхування, ідентифікація, RegTech/InsurTech) та ступеня регуляторної інтегрованості з традиційною фінансовою системою. Удосконалено підхід до трактування цифрової фінансової екосистеми через виділення ключових груп учасників (регулятори, фінансові установи, фінтех-компанії, провайдери критичної інфраструктури, BigTech, користувачі) та їх взаємозв'язків в умовах воєнних ризиків і євроінтеграційного курсу України.

Практичне значення одержаних результатів полягає в тому, що розроблені в роботі підходи до класифікації та оцінювання цифрових фінансових послуг можуть бути використані регуляторами та учасниками ринку для перегляду стратегій цифрової трансформації. Запропонована система показників дає змогу комплексно оцінювати рівень розвитку окремих сегментів (миттєві платежі, карткові операції, дистанційний банкінг, цифрова ідентифікація, open banking), виявляти «вузькі місця» інфраструктури, дисбаланси між швидкістю зростання операцій та рівнем операційної стійкості, а також приймати більш обґрунтовані рішення щодо інвестицій у технології, кіберзахист і клієнтський досвід. Практичні рекомендації можуть бути використані Національним банком України, профільними міністерствами, банками та фінтех-компаніями при розробленні дорожніх карт розвитку цифрових фінансових сервісів, політик

управління ризиками та програм підвищення довіри до безготівкових розрахунків.

Практична складова отриманих результатів полягає в розробленні системи показників та аналітичного інструментарію для комплексної оцінки сучасного стану й перспектив розвитку цифрових фінансових послуг в Україні. У роботі сформовано узагальнений індекс розвитку цифрових фінансових послуг, який поєднує параметри охоплення (penetration), інтенсивності використання, операційної стійкості, рівня довіри та інклюзивності, що дозволяє зіставляти динаміку окремих сегментів ринку (миттєві платежі, карткові операції, дистанційний банкінг, цифрова ідентифікація) у часовому розрізі. На основі проведеного аналізу обґрунтовано авторські пропозиції щодо пріоритетних напрямів державної політики й стратегій фінансових установ у сфері цифрових фінансових послуг, адаптованих до умов повоєнного відновлення та інтеграції в європейський цифровий фінансовий простір.

Результати дослідження мають прикладну цінність і для фінансових установ, які впроваджують або масштабують цифрові продукти. Запропонований алгоритм оцінювання готовності до поглиблення цифрової трансформації може бути використаний як інструмент внутрішнього аудиту для порівняння поточного стану з найкращими практиками щодо організації ІТ-архітектури, управління даними, відкритих API, відповідності вимогам інформаційної безпеки та інтеграції ESG-орієнтованих сервісів. Окремі висновки та узагальнення можуть бути використані в освітньому процесі закладів вищої освіти під час викладання дисциплін, пов'язаних із фінтехом, цифровими фінансами та банківським менеджментом, а також у програмах підвищення кваліфікації працівників фінансового сектору.

Структура і обсяг кваліфікаційної роботи. Робота складається із вступу, трьох розділів, висновків, списку використаних джерел із 178 найменування на 15 сторінках, містить 5 рисунків на 5 сторінках та 9 таблиць на 13 сторінках, кількість додатків 1. Загальний обсяг роботи – 127 сторінок. Основний зміст дипломної роботи викладено на 99 сторінках.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ РОЗВИТКУ ЦИФРОВИХ ФІНАНСОВИХ ПОСЛУГ

1.1. Сутність, структура та класифікація цифрових фінансових послуг

У термінологічному полі доцільно розрізняти «цифрові фінансові послуги» та ширше вживані в практиці «електронні/онлайн-послуги». Під цифровими фінансовими послугами розумітимемо фінансові продукти і процеси, що проектуються, реалізуються та масштабуються як цифрові з моменту задуму (digital-by-design), використовують програмні інтерфейси (API), хмарні платформи, аналітику даних і алгоритмічні механізми прийняття рішень на всьому життєвому циклі послуги – від ідентифікації клієнта до післяпродажного супроводу. Натомість електронні або онлайн-послуги нерідко відображають лише канал доступу до традиційного продукту (web/mobile-фронт) без глибинної перебудови бек-офісних процесів і даних, тобто є радше «оцифрованою вітриною» паперово-центричної моделі. Така розвідка понять дозволяє фіксувати різницю між косметичною цифровізацією і платформною трансформацією бізнес-моделі [99; 145].

Ключовою характеристикою є дистанційність: укладення договору, верифікація особи (eKYC/біометрія), надання згод на обробку даних, виконання платежів/виплат і комунікація з клієнтом здійснюються без фізичної присутності сторін через омніканальні інтерфейси. Дистанційність водночас задає вимоги до надійної ідентифікації, юридичної значущості електронних підписів/печаток, а також до цілодобової доступності сервісів із гарантованим рівнем безвідмовності. Вона виступає передумовою інклюзивності, розширюючи охоплення на віддалені регіони та групи з обмеженим доступом до відділень.

Другий вимір – автоматизація у форматі straight-through processing (STP), що означає наскрізне, безперервне проходження операції без ручних втручань. STP спирається на формалізацію бізнес-правил, використання скорингових/ризикових моделей, RPA у бек-офісі, а в окремих кейсах – на смарт-

контракти для тригерних виплат. Ефектами виступають скорочення часу прийняття рішень, зниження операційних помилок, реплікативність комплаєнс-процедур і можливість масштабувати обсяги без пропорційного зростання витрат. На відміну від «онлайн-подання заявки», STP передбачає, що і перевірки, і маршрутизація, і розрахунки виконуються машинно у єдиному конвеєрі.

Третя характеристика – клієнтоцентричність/UX як принцип проектування сервісів. Йдеться про персоналізацію пропозицій на основі поведінкових та контекстних даних, прозору подачу умов (plain-language disclosure), інклюзивний дизайн інтерфейсів, а також вбудовані інструменти фінансового добробуту (бюджетування, нотифікації ризиків, освітні підказки). Клієнтоцентричність нерозривно пов'язана з безшовністю (seamlessness): можливістю почати взаємодію в одному каналі та продовжити в іншому без втрати статусу чи даних. Безшовність досягається завдяки єдиному профілю клієнта, подієвим шинам даних і узгодженим SLA між фронт- та бек-сервісами, що мінімізує «тертя» (friction) і підвищує конверсію [73; 151].

Наступний елемент – орієнтація на дані (data-centricity): дані розглядаються як первинний актив, а послуги – як похідні від даних та аналітики. Це означає наявність єдиної моделі даних, керованих сховищ, каталогу метаданих, політик якості та походження даних (data lineage), а також механізмів контролю доступу й мінімізації даних відповідно до принципів privacy-by-default. Даноцентрична архітектура забезпечує трасованість рішень, можливість аудиту, адаптивну аналітику ризиків і відповідність вимогам звітності в реальному часі.

Нарешті, compliance-by-design – вбудованість регуляторних, етичних і безпекових вимог у дизайн продукту й процесів від початку, а не їх накладання «зверху» на завершену систему. У практиці це проявляється у конфігурованих правилах AML/CTF і санкційного скринінгу, KYC-контролях на рівні подій, журналюванні та незмінності логів, сегрегації обов'язків, управлінні згодами суб'єктів даних, а також у регулярному тестуванні надійності й кіберстійкості. Поєднання compliance-by-design із дистанційністю, STP, UX і даноцентричністю

формує цілісний стандарт якості цифрових фінансових послуг і задає рамки для подальшої класифікації та аналізу їх інституційної організації.

Цифрові фінансові послуги розвиваються як мережа взаємодіючих суб'єктів із розподіленими ролями, де створення цінності відбувається не в межах однієї установи, а завдяки координації платформ, стандартів і даних. До ключових учасників належать банки (універсальні та спеціалізовані), небанківські фінансові установи (платіжні установи, мікрофінансові організації, кредитні спілки, страховики, інвесткомпанії, небанківські емітенти електронних грошей), компанії FinTech і BigTech із їхніми маркетплейсами/суперзастосунками, оператори платіжних систем і технологічні процесингові центри. Вагоме місце посідають регулятори та органи нагляду (центральный банк, ринкові комісії, органи захисту персональних даних і конкуренції), які встановлюють правила доступу на ринок, ліцензування, стандарти відкритих інтерфейсів, вимоги до капіталу, ризик-менеджменту та захисту прав споживачів. Підтримувальну роль відіграють провайдери кібербезпеки, інсорсингові/аутсорсингові ІТ-компанії, а також професійні асоціації, що координують саморегулювання та розробку галузевих кодексів [23; 172].

Канальна архітектура екосистеми вибудовується за принципами омніканальності й «API-first». Традиційні web- і mobile-інтерфейси доповнюються відкритими прикладними інтерфейсами (API) для машинної взаємодії між провайдерами, партнерами та агрегаторами, що уможливорює сценарії вбудованих фінансів – коли фінансова послуга «вшивається» у нефінансовий сервіс (маркетплейс, транспорт, телемедицина тощо). Канали включають також чат- та voice-асистентів, платежі з контексту (in-app/in-game), інтеграції з POS/SoftPOS і «інтернетом речей». Критично важливими є узгоджені SLA між каналами та бек-сервісами, механізми збереження контексту сесії й єдиний клієнтський профіль, що забезпечують безшовність переходів між каналами та стабільну якість обслуговування.

Інфраструктурний шар – це «транспорт і комунікації» цифрових фінансів. До нього входять сервіси електронної ідентифікації та верифікації (eID, eKYC,

біометрія, кваліфіковані е-підписи), платіжні рейли (миттєві та пакетні перекази, карткові схеми, кліринг/неттинг, процесинг), бюро кредитних історій і скорингові провайдери, а також хмарні платформи з керуванням даними (data lakes/warehouses, каталоги метаданих, подієві шини). На інфраструктурному рівні реалізуються механізми комплаєнсу (AML/CTF-скринінг, санкційні списки, моніторинг транзакцій), журнали незмінних подій для аудиту, сервіси токенизації платіжних даних, шифрування та керування ключами, а також засоби безперервності бізнесу та відновлення після інцидентів. Саме цей шар забезпечує сумісність, інтеоперабельність і масштабованість, виступаючи спільним ресурсом для багатьох провайдерів [45; 128].

Продуктовий вимір екосистеми охоплює чотири базові кластери, які часто комбінуються в пакети та «життєві сценарії» клієнта. Платежі включають рахункові та безрахункові перекази, миттєві платежі, еквайринг/SoftPOS, електронні гроші й цифрові гаманці з функціями P2P і P2M. Кредит – від мікрокредитування та BNPL до споживчих/іпотечних продуктів із динамічним ціноутворенням на базі ризик-моделей і відкритих даних; сюди ж належать кредитні ліміти в торгових додатках і кредитування в точці продажу. Інвестиційний блок охоплює брокерські сервіси, робот-радіників, керовані портфелі, цифрові облігації та краудфандингові/краудінвестиційні майданчики. Страхування представлено як класичними полісами (майнові, особисті, медичні), так і мікрополісами та вбудованим страхуванням із тригерними виплатами (parametric/usage-based), що активуються даними із сенсорів або зовнішніх орієнтирів [84; 163].

Структура екосистеми передбачає різні моделі взаємодії: B2C і B2B доповнюються B2B2C та платформними оркестраторами, де один із гравців виконує роль «маркетплейс-ядра» й забезпечує правила підключення, маршрутизацію трафіку, білінг, розподіл ризиків і вирішення спорів. Управління даними та доступом реалізується через політики даноцентричності й «compliance-by-design»: сегрегацію обов’язків, мінімізацію даних, контроль згод, версіонування моделей і відтворюваність рішень. У такій конструкції суб’єкти, канали, інфраструктура й продуктові кластери утворюють цілісний каркас, на

якому надалі вибудовуються класифікаційні підходи, метрики ефективності та механізми регуляторної взаємодії у наступних підрозділах.

Класифікацію цифрових фінансових послуг доцільно здійснювати за кількома ортогональними осями, що відображають технологічну основу, модель надання, функціональне призначення та логіку монетизації. Такий підхід дозволяє уникнути редукації складних платформних рішень до «каналів збуту» та забезпечує узгодженість подальшого аналізу ефективності, ризиків і регуляторних вимог. З огляду на описані вище принципи даноцентричності та compliance-by-design, кожна вісь класифікації взаємодіє з іншими через інтероперабельність даних, стандарти API та наскрізну автоматизацію процесів.

За технологічною ознакою виділяються класи (див. табл. 1.1): (1) сервіси на базі API/open banking, що забезпечують стандартизований доступ до рахунків, ініціювання платежів і обмін фінансовими даними між провайдерами; (2) рішення, побудовані на AI/ML, включно з кредитним і поведінковим скорингом, антифрод-аналітикою, персоналізацією пропозицій та робот-радниками; (3) сервіси з використанням DLT/блокчейн (розподілений реєстр для клірингу/розрахунків, токенизація активів, смарт-контракти для тригерних виплат у страхуванні); (4) RPA/процесна автоматизація, що оркеструє бек-офісні процедури (KYC/AML, звітність, супровід кредитів) у форматі STP; (5) біометричні технології для ідентифікації та аутентифікації клієнтів (обличчя, голос, відбиток), включно з liveness-контролями та багатофакторними схемами. На практиці продукти часто є гібридними: наприклад, кредитування в точці продажу може поєднувати відкриті API, ML-скоринг, RPA-бек-офіс і біометрію в онбордингу.

Таблиця 1.1

Класи цифрових фінансових послуг за технологічною ознакою

Клас технологій	Сутність / короткий опис	Типові приклади застосування	Приклади сервісів / функцій
1. API / Open Banking	Стандартизований доступ сторонніх провайдерів до рахунків, платіжних	Ініціювання платежів, агрегування рахунків, обмін даними між банками та фінтехами, PIS/AIS-сервіси.	AIS (account information services), PIS (payment initiation services), open-data-інтерфейси, «банківські шлюзи» для партнерських продуктів.

	інструментів та фінансових даних.		
2. AI / ML-системи у фінансах	Автоматизована аналітика великих масивів даних для оцінки ризиків, прогнозування та персоналізації.	Кредитний та поведінковий скоринг, антифрод, рекомендаційні системи, робот-радіники (robo-advisors).	ML-скоринг, anomaly detection, NLP-боти, предиктивна аналітика, моделі LTV/propensity to buy.
3. DLT / Blockchain-рішення	Розподілені реєстри, смарт-контракти, токенизація активів, прозорі та незмінні записи транзакцій.	Кліринг/розрахунки, транскордонні платежі, DeFi-моделі, страхові смарт-контракти з тригерними виплатами, токенизація цінних паперів.	DeFi-протоколи, stablecoins, токенизовані депозити, on-chain кліринг, permissioned blockchain у банках.
4. RPA / Процесна автоматизація	Автоматизоване виконання типових бек-офісних процесів у форматі STP (straight-through processing).	KYC/AML-перевірки, обробка заявок, формування звітності, супровід кредитних договорів, workflow-автоматизація.	RPA-боти для перевірки документів, автоматичне заповнення форм, тригерна генерація звітів.
5. Біометричні технології	Ідентифікація та аутентифікація за фізіологічними та поведінковими характеристиками.	Онбординг клієнтів, верифікація платежів, доступ до мобільних застосунків, KYC із liveness-контролем.	FaceID/фотоідентифікація, голосова біометрія, відбитки пальців, поведінкова біометрія (keystroke, gait).
6. Гібридні фінансові продукти	Комбінація декількох технологій для створення комплексних продуктів та «цифрових потоків».	BNPL та кредитування в точці продажу, миттєвий скоринг і випуск карт, embedded finance у маркетплейсах.	Open API + ML-скоринг + RPA-бекофіс + біометричний онбординг.

Джерело: складено автором за матеріалами [44; 88; 95; 115; 140]

За моделями надання розрізняють B2C (пряме обслуговування кінцевих споживачів через мобільні/веб-застосунки), B2B (технологічні й фінансові сервіси для банків, небанківських установ, мерчантів, інституційних інвесторів), а також B2B2C/embedded-моделі, у межах яких фінансова послуга вбудовується в нефінансовий клієнтський шлях (маркетплейси, телемедицина, транспорт, ритейл). У B2B2C-конфігураціях виникають ролі оркестратора платформи, провайдера ліцензійної «бек-енджин»-інфраструктури (Banking-/Insurance-as-a-Service) та бренд-фронту, який відповідає за UX і комунікацію з кінцевим

клієнтом; саме тут найбільш виразно проявляються вимоги до безшовності, SLA та керування згодами на обмін даними.

Функціональна класифікація за призначенням охоплює чотири базові кластери: платіжні послуги (миттєві перекази, еквайринг/SoftPOS, гаманці, P2P/P2M, токенизація платіжних даних); заощадження та інвестиції (депозити, брокерські сервіси, цифрові облігації, краудфандинг/краудінвестинг, робот-радники); кредитні послуги (мікрокредитування, BNPL, споживчі/іпотечні продукти з динамічним ціноутворенням, кредитні ліміти у суперзастосунках); страхові сервіси (онлайн-поліси, usage-/parametric-insurance, мікрополіси, вбудоване страхування). Кожен кластер може мати як самостійні продукти, так і бути складовою «життєвих сценаріїв» клієнта, що komponує фінансові рішення через API-орієнтовані каталоги.

З погляду монетизації виділяються моделі: комісійна (fee-based) – фіксовані або відсоткові комісії за транзакції, обслуговування рахунків чи преміальні функції; інтерчейндж-модель – частка від міжбанківських комісій в еквайрингу/карткових схемах; підписка – регулярні платежі за пакет сервісів, відсутність/зниження окремих комісій та доступ до розширених можливостей; data-driven-монетизація, що включає використання анонімізованої/агрегованої аналітики для ціноутворення, ризик-менеджменту або партнерських програм (за суворого дотримання принципів privacy-by-design і нормативних вимог до персональних даних). У складних платформних моделях доходи диверсифікуються між кількома потоками, і вибір конкретної схеми пов'язаний з еластичністю попиту, регуляторними обмеженнями та вартістю залучення клієнта [60; 91; 103].

Запропонована багатовимірна класифікація забезпечує інструментарій для зіставлення продуктів і провайдерів за рівнем технологічної зрілості, глибиною автоматизації та якістю клієнтського досвіду, а також дозволяє коректно вибудувати карти ризиків і регуляторних вимог у подальшому аналізі моделі ринку. Вона є також практичним каркасом для порівняння бізнес-стратегій і вибору релевантних метрик ефективності на рівні окремих кластерів і всієї екосистеми.

Оцінювання якості цифрових фінансових послуг доцільно здійснювати через систему критеріїв, що відображають суспільно значущі результати та техніко-організаційну зрілість провайдера. Базовим орієнтиром виступає фінансова інклюзія: розширення охоплення раніше недообслуговуваних груп, зменшення територіальних і соціальних бар'єрів, можливість самообслуговування для осіб з обмеженими можливостями. Практичні індикатори: частка активних цифрових клієнтів у загальному портфелі, кількість відкритих рахунків/полісів дистанційно, коефіцієнт завершення онбордингу (conversion to onboard), рівень використання простих продуктів першого контакту (гаманці, P2P), а також питомі витрати клієнта на базову транзакцію. Позитивний ефект інклюзії проявляється у зростанні економічної активності домогосподарств і МСП, які отримують швидший доступ до платежів і мікрофінансування [17; 176; 177].

Другий блок критеріїв охоплює доступність/вартість і швидкість. На пропозиційній стороні йдеться про зменшення сукупної вартості володіння сервісом для клієнта (комісії, приховані витрати часу, кількість кроків у сценарії), на стороні оператора – про зниження одиничної собівартості обслуговування за рахунок STP, RPA і хмарних масштабувань. Вимірювання включає середній час виконання ключових процесів (time-to-yes/time-to-cash у кредитуванні; end-to-end time у страхових виплатах), частку операцій, що проходять без ручних втручань (STP rate), продуктивність каналів (TPS/здатність до пікових навантажень), доступність сервісу за SLA (uptime) та еластичність ціноутворення. Ефект матеріалізується у скороченні транзакційних витрат економіки та зростанні конкуренції завдяки легшому переходу між провайдерами [99; 145].

Прозорість, безпека та конфіденційність становлять третій вимір якості. Прозорість визначається зрозумілістю тарифів і умов (plain-language disclosure, вбудовані калькулятори повної вартості), а також відтворюваністю рішень алгоритмів (traceability, модельні карти й логи). Безпека включає багатоваровий захист: сильну автентифікацію (MFA/біометрія з liveness), сегментацію мереж, шифрування даних у русі та спокої, управління ключами, тестування на

проникнення і програму виявлення вразливостей. Конфіденційність забезпечується принципами *privacy-by-design/default*: мінімізацією даних, керуванням згодами, аудитом доступів, псевдонімізацією/анонімізацією для аналітики. Ключові метрики: частота інцидентів і їхній середній час відновлення (MTTR), рівень шахрайства на 1000 транзакцій, частка хибнопозитивних спрацювань антифроду, повнота журналювання та результати незалежних аудитів.

Четвертий критерій – довіра як інтегральний показник сприйняття клієнтом якості сервісу і надійності провайдера. Вона формується не лише через UX і безпеку, а й через етичність використання даних, справедливість алгоритмічних рішень і коректне врегулювання спорів. Індикаторами виступають NPS/CSAT, частота скарг і їхній час розв’язання, прозорість комунікацій у разі інцидентів, а також наявність сертифікацій, участь у схемах гарантування/страхування та підключення до галузевих кодексів поведінки. Підтримка довіри вимагає процесної дисципліни: регулярної переоцінки моделей (*model risk management*), зрозумілих механізмів оскарження рішень і можливості «людського перегляду» у чутливих кейсах.

Паралельно з ефектами виникає поле ризиків, що має бути керованим у логіці *enterprise risk management*. Операційні ризики (відмова хмарних компонентів, збої інтеграцій, помилки релізів) потребують зрілих практик *DevSecOps*, резервування, *chaos testing* та планів безперервності бізнесу. Кіберризики включають фішинг/соціальну інженерію, атаки на ланцюг постачання, експлойти в мобільних клієнтах і API; відповіді – *Zero Trust*, *WAF/API security*, *EDR/XDR*, *bug bounty* та постійний моніторинг. Комплаєнс-ризики походять з AML/санкційних вимог, захисту даних і споживача; інструменти – *compliance-by-design*, журналювання незмінних подій, тестування моделей на упередженість, регуляторна звітність у майже реальному часі. Поведінкові ризики пов’язані з гіперперсоналізацією і «надто зручним» UX (перевитрати, імпульсні кредити, асиметрія інформації); їх пом’якшують прозорі попередження, ліміти за замовчуванням, освітні підказки та можливість «паузи» перед ризиковими операціями. Синхронізація критеріїв якості з картою ризиків

дозволяє інтегрувати показники ефективності (KPI) з показниками стійкості (KRI) і забезпечити кероване зростання цифрових сервісів на наступних етапах аналізу [66; 168].

1.2. Теоретичні підходи до цифровізації та її вплив на фінстабільність

Неоінституційний підхід пропонує розглядати цифровізацію як зміну «правил гри» та механізмів координації в фінансовому секторі. Інститути – формальні (регулювання, стандарти, контракти) й неформальні (норми довіри, очікування) – визначають транзакційні витрати доступу до послуг, моніторингу, виконання зобов’язань і вирішення спорів. Поява електронної ідентифікації, стандартизованих API і цифрових слідів знижує витрати пошуку, переговорів і контролю, водночас підвищуючи вимоги до прав власності на дані, механізмів згод та інституційного забезпечення кіберстійкості. У цій логіці цифрові платформи виступають «інституційними інноваціями»: вони перерозподіляють контроль над інформацією, модифікують структуру стимулів для банків і небанківських установ і змінюють баланс між централізованим наглядом та саморегулюванням ринку [18; 39].

Концепція транзакційних витрат (Коуз–Вільямсон) уточнює мікроекономічний механізм цих зрушень. Алгоритмічний скоринг, смарт-контракти, RPA/STP і цифрова документація скорочують витрати вимірювання ризику та примусу до виконання, що сприяє масштабуванню «тонких» маржинальних продуктів (мікрокредитування, BNPL, мікрострахування). Разом із тим нові види витрат – інтеграційні, верифікаційні та пов’язані з кіберзагрозами – можуть частково компенсувати виграш, а в окремих нішах формувати бар’єри входу через необхідність інвестицій у безпеку, управління даними та відповідність регуляторним стандартам. Вимір і баланс цих витрат визначають, чи виникатиме дезінтермедіація на користь прямих платформ або, навпаки, перерозподіл функцій у бік «бек-енджин»-провайдерів (Banking-/Insurance-as-a-Service).

У теорії інновацій Шумпетера цифрові фінанси постають як хвиля «творчого руйнування», що перебудовує комбінації ресурсів у поєднанні з даними як новим виробничим фактором. Підприємницькі інновації – від відкритих банківських інтерфейсів до дата-орієнтованого ціноутворення – створюють тимчасові монопольні ренти, які стимулюють інвестування в технології, але одночасно запускають процес імітації й стандартизації. Коли технологічний цикл дозріває, ренти зменшуються, а конкуренція зміщується у площину якості даних, UX та ефективності ризик-менеджменту. Для фінансової стабільності важливе питання темпу: надто швидка дифузія інновацій без адаптації нагляду і практик управління ризиками підвищує ймовірність помилок моделей і операційних збоїв, тоді як поступова – дозволяє «вбудовувати» вимоги до кіберстійкості та комплаєнсу у дизайн продуктів [20; 142].

Мережеві ефекти та платформна економіка пояснюють концентраційні тенденції цифрових ринків. Зі зростанням числа користувачів збільшується корисність платформи, що знижує середні витрати на залучення клієнта, підсилює даноцентричні переваги (кращі моделі, нижчі втрати від шахрайства) і може створювати бар'єри для менших гравців. Перехресні (multi-sided) ефекти між споживачами, мерчантами та постачальниками ліквідності формують позитивні зворотні зв'язки, які одночасно підвищують ефективність і ризик «надмірної» концентрації даних та операцій на кількох вузлах. Паралельно виникає залежність від інтерфейсів та стандартів домінантних платформ, що впливає на структуру системної важливості та канали передачі шоків у разі технічних чи кіберінцидентів.

Теорія «ринків, що можуть бути оскаржені» (contestable markets) додає рамку для аналізу конкурентного тиску: навіть за високої частки великих гравців потенційна загроза входу з боку інноваційних платформ здатна стримувати ціни та маржі за умови низьких незворотних витрат і доступності ключових інфраструктур (платіжні рейли, ідентифікація, хмари, відкриті API). Якщо ж доступ до цих інфраструктур обмежений або стандарти неінтероперабельні, «оскаржуваність» падає, зростають інформаційні ренти, а бар'єри виходу/входу підвищують системні ризики. Таким чином, дизайн відкритості та переносимості

даних безпосередньо пов'язаний із конкурентною динамікою і, опосередковано, зі стійкістю сектору.

Поведінкові фінанси фокусуються на тому, як цифровий UX, нотифікації, «фрикційний дизайн» і персоналізовані «підштовхування» (nudges) впливають на рішення споживачів. Зменшення транзакційного тертя і гіперперсоналізація можуть покращувати планування витрат і заощаджень, однак водночас підсилюють імпульсивність, короткозорість і «ефект спрощення» при складних продуктах (кредит, інвестиції). На рівні провайдерів евристики та упередження проявляються у надмірній довірі до моделей і «ілюзії стабільності» при рідкісних ризиках (кіберподії з великим збитком). Усі ці аспекти визначають потребу в механізмах етичного дизайну, прозорих розкриттях і «людському перегляді» чутливих рішень, що в подальшому буде відображено в каналах впливу на фінансову стабільність та інструментах їхнього вимірювання.

Перший канал проходить через конкуренцію і маржинальність. Відкриті інтерфейси, низькі витрати переключення між провайдерами та зниження транзакційних витрат схиляють ринок до цінового тиску й «тонких маржин», особливо у платежах і стандартних роздрібних продуктах. Для окремих установ це означає стиснення чистого процентного та комісійного доходу, що за відсутності достатньої операційної ефективності і масштабів може послаблювати внутрішнє генерування капіталу і здатність покривати неочікувані збитки. Водночас конкуренція, що зберігає «оскаржуваність ринку», покращує ефективність розподілу ресурсів і стимулює інвестиції у керування ризиками; отже, стабілізаційний або дестабілізаційний ефект залежить від того, чи супроводжується тиск на маржі підвищенням продуктивності (STP, хмари) і вдосконаленням управління витратами на ризик [72; 142].

Другий канал – дезінтермедіація і перерозподіл функцій посередництва. Платформні моделі B2B2C та «вбудовані фінанси» переносять частину взаємодії з клієнтом до нефінансових інтерфейсів, тоді як банківський/страховий «бек-енджин» перетворюється на постачальника ліцензійної інфраструктури. Наслідки двоїсті: з одного боку, розширюється охоплення і знижується вартість залучення, з іншого – виникає ризик концентрації ринкової влади у фронтових

платформ і зменшення лояльності до балансоутримувача ризику. Це здатне посилювати чутливість до репутаційних шоків і змін алгоритмів платформи, а також створює непрямі канали зараження між на перший погляд несуміжними сегментами через спільних оркестраторів або провайдерів «беку».

Третій, критичний для макростійкості канал – ліквідність і фандинг. Цифрові канали підвищують швидкість перетікання коштів між інститутами й інструментами, знижуючи тертя у разі панічних реакцій (ефект «цифрових забігів» на депозити або інші зобов'язання, миттєві перекази між гаманцями/рахунками). Позитивно впливає те, що гнучкі інструменти управління ліквідністю, динамічне ціноутворення і раннє попередження на базі аналітики підвищують готовність до відтоків; негативно – те, що однакова швидкість діє і в протилежний бік, скорочуючи час на коригування позицій і підвищуючи потребу у високоякісних ліквідних активах. На рівні показників це відображається в волатильності LCR/NSFR, чутливості до ритміки миттєвих платежів і залежності від оптового/платформного фандингу.

Четвертий канал стосується кібер- та операційних ризиків. Підвищена взаємопов'язаність через API, використання спільних хмарних інфраструктур і широка автоматизація формують «вузли системної важливості» поза балансами традиційних банків. Збої або кібератаки на критичні компоненти (ідентифікація, процесинг, платіжні рейли, провайдери хмар) здатні призвести до одночасних порушень у багатьох установах, трансформуючись із ідіосинкратичних у системні події. Окрім негайних втрат і простоїв, наслідками стають різкі зміни поведінки клієнтів (обмеження довіри до каналів), правові претензії та підвищення витрат на відповідність вимогам, що опосередковано тисне на капітал і ліквідність.

П'ятий канал – концентрація даних і залежність від моделей, що поєднується з мережевими ефектами. Дані як виробничий фактор генерують економію на масштабі у прогнозуванні ризиків і протидії шахрайству, але водночас сприяють концентрації інформаційної ренти у кількох гравців, які контролюють ключові потоки й стандарти. Така асиметрія може знижувати «оскаржуваність ринку» і підвищувати перешкоди для нових учасників,

посилюючи вразливість до збоїв і помилок у домінантних вузлах. На рівні стабільності це проявляється через синхронізацію дій багатьох провайдерів, які спираються на подібні дата-пайплайни, зовнішні оркестратори або моделі.

Шостий канал – проциклічність і модельні ризики AI/ML. Дані та моделі, натреновані на «спокійних» періодах, схильні недооцінювати хвости розподілів і змінювати поведінку у стресі: кредитні ліміти, ціноутворення ризику, антифрод-пороги синхронно затягуються, що посилює стискання кредиту та загальну ліквіднісну напруженість. Крім того, фідбек-петлі (менше видач - менше «свіжих» даних - гірша калібровка) та однотипні джерела альтернативних даних спричиняють «стадну» реакцію. Практичні наслідки – посилення циклу втрат/резервів, більш різкі коливання NPL та маржі, а також ризик дискримінаційних упереджень, що викликають правові/репутаційні шоки і додаткові вимоги до капіталу.

Зведення цих каналів у єдину систему причинно-наслідкових зв'язків (див табл. 1.2.) дозволяє пов'язати мікромеханізми цифровізації з ключовими показниками фінстабільності – капіталом і ліквідністю, якістю активів, концентрацією та операційною стійкістю.

Таблиця 1.2

Канали впливу цифрових фінансів на фінансову стабільність

№	Канал / цифровий драйвер	Причинно-наслідковий опис	Наслідки для фінансової стабільності
1	Конкуренція та маржі (open API, низькі витрати переключення)	Відкриті інтерфейси й низькі витрати переключення підсилюють цінову конкуренцію, знижують транзакційні витрати та стискають маржі, роблячи критичною операційну ефективність.	Ризик ослаблення капіталізації установ із низькою продуктивністю; водночас потенційне підвищення ефективності системи завдяки тиску на витрати.
2	Дезінтермедіація, B2B2C та embedded finance	Перенесення взаємодії з клієнтом на платформи й нефінансові інтерфейси перетворює банки/страховиків на бек-енд-постачальників і концентрує ринкову владу у фронтових гравців.	Розширення охоплення та зниження вартості залучення клієнтів за одночасного зростання системної залежності від платформ і їхніх репутаційних та алгоритмічних шоків.
3	Ліквідність і фандинг (миттєві платежі, цифрові канали)	Миттєві цифрові канали прискорюють перетікання коштів між установами й інструментами, у стресових	Зростання волатильності показників ліквідності, потреби в високоякісних ліквідних активах та

		умовах це проявляється як швидкі відтоки та «цифрові забіги».	чутливості до змін у платіжній інфраструктурі.
4	Кібер- та операційні ризики (API, хмари, спільні провайдери)	Глибока інтеграція через API, спільні хмарні та процесингові рішення формує кілька критичних інфраструктурних вузлів, від яких одночасно залежать багато установ.	Перетворення локальних кібер- та технічних інцидентів на системні події з впливом на доступність сервісів, довіру клієнтів, доходи та капітал.
5	Концентрація даних і моделей (мережеві ефекти)	Концентрація великих масивів даних і ключових моделей у небагатьох гравців посилює їхню інформаційну ренту та уніфікує поведінку інших учасників, що спираються на ті самі дата-пайплайни.	Послаблення конкуренції, концентрація системного ризику в домінантних дата-та модельних платформах, посилення ефекту «єдиної точки відмови».
6	Проциклічність і модельні ризики AI/ML	Моделі AI/ML, налаштовані на докризові дані, у стресових умовах різко посилюють вимоги до клієнтів і скорочують ризикові експозиції, підсилюючи кредитну та ліквіднісну проциклічність.	Більш різкі коливання кредитної активності, частки NPL і резервів; підвищений ризик правових та регуляторних шоків через упереджені чи некоректно калібровані моделі.

Джерело: складено автором за матеріалами [18; 23; 58; 142; 168]

Така карта стане основою для вибору аналітичного інструментарію в наступному підрозділі (індикаторні панелі, мережевий аналіз, стрес-тести кібер- та операційних шоків, DSGE/ABM-моделі), де окремі канали будуть переведені у вимірювані метрики і сценарії.

Практичне вимірювання каналів впливу цифровізації доцільно починати з індикаторних панелей, що поєднують мікро- та макропоказники у єдиній системі моніторингу. Базове «ядро» становлять показники капіталу та якості активів: CET1/Tier 1/CAR, леверидж-рейшо, частка NPL і покриття резервами, очікувані кредитні збитки (ECL) та динаміка маржі (NIM) у розрізі цифрових/традиційних продуктів. Ліквідність вимірюється LCR/NSFR, коефіцієнтами «стрес-нетто-стікання» (run-off rates) за різними джерелами фінансування, часткою миттєвих платежів у загальному обсязі, волатильністю денних залишків і залежністю від платформного/оптового фінансування. Окремий блок формують операційні та кібер-KPI: доступність сервісів (uptime/SLA), середній час відновлення (MTTR), частота критичних інцидентів, рівень шахрайства на 1000 транзакцій, частка STP-операцій, показники якості моделей

(AUC, PD-калібрування, частка відхилення через антифрод). Панель має підтримувати щонайменше щоденну/тижневу частоту для операційних показників і місячну/квартальну – для регуляторних метрик, із можливістю дрілдауну до рівня продукту/каналу/платформи [119; 142].

Для оцінки системних зв'язків цифрової екосистеми застосовується мережевий аналіз. Конструюються щонайменше три граfi: (1) граfi платіжних/розрахункових потоків між установами; (2) граfi залежностей від спільної інфраструктури (процесинг, хмари, eID, провайдери API); (3) граfi спільності даних/моделей (спільні бюро даних, антифрод-хаби, зовнішні оракули). На цих графах оцінюються центральності (in/out-degree, betweenness, eigenvector), щільність, кластеризація, ННІ за ролями вузлів та «мости» між кластерами; для кожного критичного вузла – показник системної важливості (Systemic Importance Score) з урахуванням ваги трафіку й можливості заміни. Імітаційні процедури на мережі дозволяють моделювати каскадні ефекти відмови вузла (операційна аварія, кіберінцидент, збої API), оцінюючи втрату функціональності сервісів і вторинні ефекти для ліквідності/платоспроможності.

Третій блок – стрес-тестування кібер- та операційних шоків із прив'язкою до балансів і ліквідності. Сценарії включають: тривалу недоступність хмарного регіону; компрометацію ключів/токенів і масове блокування транзакцій; відмову платіжних рейлів/процесингу у пікові періоди; модельні помилки AI/ML з різким ростом false-positive у антифроді або «надмірним затягуванням» кредитних порогів. Для кожного сценарію визначаються припущення щодо тривалості, частки уражених операцій, швидкості «цифрового відтоку» пасивів, параметри відновлення (RTO/RPO), а також трансляція операційних втрат у P&L/капітал (через AMA/стандартні підходи до операційного ризику) та LCR/NSFR. Важливо інтегрувати поведінкові реакції клієнтів (зміна частоти логінів, підвищення готівкових зняттів, міграція до альтернативних каналів) і контрзаходи установи/регулятора (тимчасові ліміти, повідомлення, ліквідні буфери, вікна рефінансування) [119; 168].

Для поглибленого аналізу макроефектів використовуються DSGE та ABM-моделі як взаємодоповнювальні інструменти. У DSGE цифровізація вводиться

через зниження транзакційних витрат, зміну конкуренції і маржі посередництва, підвищення швидкості перетоку заощаджень/кредиту та ймовірності «цифрових забігів». Окремими шоками моделюються операційні втрати і тимчасова втрата продуктивності інтермедіації; калібрування спирається на фактичні еластичності маржі до конкуренції, емпіричні run-off-коефіцієнти та частоти інцидентів. ABM доцільні для захоплення гетерогенності поведінки домогосподарств/SME і платформної динаміки: включаються агенти-банки, провайдери інфраструктури, фронтові платформи, з мережевими ефектами, алгоритмічними політиками ціноутворення та «adaptive expectations». У контексті модельного ризику AI/ML ABM дозволяє явно врахувати проциклічні фідбек-петлі (менше видач - менше даних - жорсткіші моделі) і перевірити ефекти політик «анти-проциклічності» (наприклад, буфери даних, обмеження на синхронні пороги).

Для повноти картини інструментарій доповнюється ранніми попереджувальними індикаторами та ризик-апетитом, що зв'язують моніторинг із управлінськими діями. До перших належать сигнали різкої зміни швидкості коштів (velocity), «аномалії довіри» в цифрових каналах (сплески відмов MFA, стрибки звернень у підтримку), розриви між антифрод-тригерами та фактичними втратами, синхронні корекції лімітів у кількох провайдерів. Рамка ризик-апетиту встановлює пороги KPI/KRI (наприклад, мінімальні LCR/NSFR для різних сценаріїв, максимальні MTTR/частоти інцидентів, ліміти на залежність від окремого провайдера хмари або процесингу) і «сигнальні світлофори» на панелі. Візуально результати доцільно подавати як теплові мапи ризиків і матриці «канал - показник - відповідальна дія», а мережеві вразливості – як карти центральності з маркуванням вузлів критичної важливості. Така комбінація дашбордів, мережових імітацій, стрес-тестів та макромоделей забезпечує зв'язок від операційної події до її капітально-ліквіднісних наслідків і політичних імплікацій, які розглядатимуться у наступному підпункті.

Провідним принципом державної політики у добу цифрових фінансів виступає proportionality – пропорційність регулювання до масштабу, ризик-профілю й системної значущості учасника. Ідеться не про «м'якше» ставлення

до новачків, а про ризик-орієнтоване накладання вимог: однакові за суттю правила (капітал, ліквідність, кіберстійкість, захист даних) застосовуються через диференційовані інструменти й пороги. Для малих, вузькоспеціалізованих провайдерів – спрощені звітні пакети, пропорційні вимоги до governance та моделювання ризиків; для платформних оркестраторів і критичної інфраструктури – посилений операційний нагляд, тестування на стійкість, підвищена прозорість моделей і концентраційні ліміти щодо зовнішніх залежностей (хмари, процесинг). Така градація зберігає «оскаржуваність» ринку, не нівелюючи базових запобіжників для фінансової стабільності [45; 172].

Інструментально пропорційність підсилюється регуляторними «пісочницями» (sandboxes) і режимами поетапного впровадження новацій. Пісочниця забезпечує контрольоване середовище для тестування продуктів/моделей з обмеженою вибіркою клієнтів, визначеними порогамі ризику, ex ante умовами виходу з експерименту та прозорою методикою вимірювання ефектів. У межах таких режимів можливе тимчасове звільнення від окремих процедур (за умови функціональних еквівалентів контролю), що знижує бар'єри інновацій і дозволяє наглядати отримувати «дані з поля» для подальшої стандартизації. Після завершення випробування вимоги до безпеки, комплаєнсу й розкриттів масштабуються до повного регуляторного периметра, а уроки експерименту трансформуються у типовий набір правил і технічних стандартів.

Ключовою опорою політики стає RegTech/SupTech – цифрові технології дотримання та наглядової аналітики. На боці ринку RegTech означає автоматизацію KYC/AML, керування ризиками моделей (включно з перевітками на упередженість і стабільність), «machine-readable» політики, журналювання незмінних подій і трасованість рішень AI/ML. На боці нагляду SupTech включає поточкову звітність, API-доступ до агрегованих показників, мережеву аналітику залежностей, ранні індикатори операційних/кіберінцидентів і інструменти сценарного аналізу. Спряження RegTech і SupTech скорочує регуляторні лаги, уможлиблює майже реальний час моніторингу ключових показників (LCR/NSFR, інциденти, fraud rate) та підвищує передбачуваність наглядових рішень для учасників ринку.

Баланс між інноваціями та захистом споживача/даних вимагає інституційного дизайну «ethics & safety by design». Йдеться про обов'язковість plain-language розкриттів повної вартості продукту, механізмів інформованої згоди на обробку даних, права на переносимість/видалення і контроль над алгоритмічними рішеннями з можливістю людського перегляду у чутливих кейсах. Для AI/ML доцільні вимоги до документації моделей (data lineage, карти ризиків, метрики стабільності), A/B-протоколів змін і незалежних валідацій. У площині кіберстійкості політика має фокусуватися на обов'язкових тестах типу «червоних команд»/threat-led penetration (для критичних вузлів), планах безперервності бізнесу з часовими орієнтирами RTO/RPO та дисципліні повідомлень про інциденти з чіткими дедлайнами і форматами взаємодії з клієнтами [55; 56].

Окремий вимір політичних імплікацій – відкритість та інтероперабельність. Стандартизовані API, уніфіковані довідники та протоколи безпеки знижують транзакційні витрати, зберігаючи конкуренцію «на рівні сервісу», а не «на рівні замкнених даних». При цьому політика має протидіяти надмірній концентрації інформаційної ренти: симетричний доступ до ключових інфраструктур (платіжні рейли, eID, кредитні бюро, хмари), вимоги до переносимості даних, обмеження «пакування» сервісів платформами, що можуть витіснити незалежних провайдерів. Така конфігурація правил сполучає стимул до інновацій із мінімізацією системних вразливостей, готуючи підґрунтя для наступного підрозділу, де технологічні рішення будуть показані як механізми інституційної трансформації на рівні процесів, продуктів і архітектури ринку.

1.3. Технологічні інновації та цифрова трансформація інститутів

Сучасна хвиля цифрової трансформації у фінансовому секторі спирається на низку загальнотехнологічних платформ, що виконують роль «загальних виробничих факторів» для створення та масштабування послуг. Штучний інтелект і машинне навчання (AI/ML) формують аналітичне ядро прийняття

рішень – від кредитного та поведінкового скорингу до антифрод-моніторингу, персоналізації пропозицій, оптимізації ціноутворення ризику і прогнозування відтоків ліквідності. У практиці інститутів це означає перехід від статичних правил до адаптивних моделей з безперервним донавчанням, розгортання ML-операцій (MLOps) із контролем якості даних, версіонуванням моделей і картами ризиків (model risk). Паралельно Big Data забезпечує збір, збагачення та уніфікацію структурованих і неструктурованих джерел (транзакції, логи взаємодії, альтернативні дані), що створює базу для аналітики в реальному часі та побудови клієнтоцентричних сервісів [44; 66].

Хмарні обчислення та мікросервіси виконують роль операційної платформи для масштабування й швидкої еволюції продуктів. Моделі IaaS/PaaS/SaaS, контейнеризація й оркестрація (Kubernetes), подієві шини та асинхронні інтеграції дозволяють відокремити бізнес-логіку від інфраструктури, прискорити випуски (CI/CD) і досягти еластичності під пікові навантаження. Мікросервісна архітектура спрощує модульну модернізацію «соге»-систем: окремі домени (платежі, кредит, андеррайтинг, розрахунки) можуть оновлюватися незалежно, з чіткими SLA та контрактами API, що знижує ризики «великих релізів» і скорочує time-to-market.

Розподілені реєстри (DLT) і смарт-контракти створюють альтернативні механізми довіри в процесах, де потрібна прозорість, незмінність і автоматизоване виконання умов. У фінансах це – токенизація активів, прискорений кліринг/розрахунки, синдиковане кредитування з прозорим workflow, параметричне страхування з тригерними виплатами та забезпечення простежуваності прав вимоги. Хоча DLT не є універсальним рішенням для всіх задач, його цінність проявляється у багатосторонніх взаємодіях і там, де зменшення операційного тертя компенсує витрати на інтеграцію й зміну процесів.

API/open finance забезпечують інтероперабельність і «шлюзи» між провайдерами, клієнтами та партнерами. Стандартизовані прикладні інтерфейси підтримують сценарії відкритого банкінгу (доступ до рахунків/ініціювання платежів), агрегування портфелів і даних, а також моделі B2B2C та вбудованих

фінансів (embedded) у нефінансові платформи. На практиці це означає каталогізовані API з керуванням життєвим циклом (API management), політиками безпеки та моніторингом продуктивності, що є критичним для безшовності клієнтського шляху й контролю операційних ризиків інтеграцій.

Електронна ідентифікація/eKYC та біометрія формують фундамент дистанційного онбордингу й підтвердження операцій. Поєднання документ-сканування, перевірок у довірчих реєстрах, біометричної автентифікації з liveness-detection і кваліфікованого е-підпису забезпечує юридичну значущість процесів без фізичної присутності. У поєднанні з ризик-орієнтованими сценаріями (risk-based approach) це знижує шахрайство й скорочує час залучення клієнта, водночас ставлячи вимоги до точності, недискримінаційності та захисту біометричних шаблонів.

RPA/low-code інструменти пришвидшують автоматизацію бек-офісу та «закриття розривів» між старими й новими системами. Роботизовані сценарії обробляють рутинні операції (KYC/AML-перевірки, звірки, звітність, супровід кредитів і врегулювання), зменшуючи помилки та підвищуючи STP-rate. Платформи low-/no-code дозволяють бізнес-командам швидко збирати внутрішні сервіси та прототипи, структуруючи їх через централізовану службу архітектури й контроль зміни процесів.

Безпековий каркас задає Zero Trust і сучасна кіберстійкість. Модель «нікому не довіряй, завжди перевіряй» передбачає мікросегментацію, найменші привілеї, постійну верифікацію ідентичностей і пристроїв, шифрування «в русі та спокої», а також телеметрію подій із виявленням аномалій (EDR/XDR, SIEM). У комплексі з практиками DevSecOps, керуванням ключами, політиками секретів, тестами типу threat-led penetration та планами безперервності (RTO/RPO) Zero Trust знижує ризик каскадних інцидентів у взаємопов'язаній екосистемі. Сукупно перелічені технології утворюють взаємодоповнюваний стек, у межах якого дані стають центральним активом, а модульна архітектура, автоматизація та відкриті інтерфейси – засобами швидкої адаптації операційних моделей фінансових інститутів.

Переорієнтація на product-centric логіку означає, що центр тяжіння організації зміщується від функціональних «силосів» до кросфункційних продукт-тімів із повним циклом відповідальності (discovery - delivery - run). Agile-підходи (Scrum/Kanban, PI-планування, DevSecOps) закріплюють ритм коротких ітерацій, метрики прогнозованості та якості (lead time, deployment frequency, change fail rate) і формують «спільну мову» бізнесу, IT та ризик-функцій. У такій моделі продуктові власники (Product Owners) керують беклогами з урахуванням ризик-апетиту, тоді як платформи (ідентифікація, платежі, дані, безпека) управляються як внутрішні продукти з договірними SLA. Це дає змогу синхронізувати time-to-market із вимогами комплаєнсу та кіберстійкості, уникаючи розриву між швидкістю релізів і зрілістю контролів [94; 145].

Стійкість product-centric операційної моделі напрядується на data governance. У центрі – єдина цільова модель даних, каталог метаданих, полі data owner/data steward, політики якості, лінійка походження даних (data lineage) і регламенти доступу. Для масштабів застосовується підхід «data mesh»: доменні команди володіють «data-продуктами» (наприклад, «клієнт», «ризик», «транзакція») з чіткими контрактами якості, а централізована функція задає стандарти, інструменти MDM/DQ і контроль відповідності (privacy-by-design, мінімізація даних, журналювання запитів). Це скорочує транзакційні витрати на інтеграцію, підвищує відтворюваність рішень AI/ML та забезпечує прозорість для наглядових SupTech-інтерфейсів.

Omnichannel перетворюється з «узгоджених фронтів» на подієво-керовану архітектуру клієнтського шляху. Єдиний профіль клієнта, спільні правила авторизації, подієві шини та черги дозволяють зберігати контекст між web, mobile, contact-center, POS/SoftPOS і партнерськими каналами. Канальна незалежність бізнес-логіки досягається через API-оркестрацію і явні контракти; це мінімізує «тертя» у сценаріях онбордингу, платежів, кредитування та страхових виплат і дає змогу вбудовувати фінансові сервіси у нефінансові платформи без дублювання процесів. Для керованості застосовують показники

STP-rate, uptime/MTTR, конверсію кроків і когортні NPS/retention у розрізі каналів [151; 94].

Вектор масштабування задають партнерські моделі – Banking-/Insurance-as-a-Service (BaaS/IaaS), white-label, дистрибуція через маркетплейси. Інститут виступає провайдером ліцензійної «бек-енджин»-платформи з відкритими API, тоді як фронт та бренд може належати партнеру. Операційна модель при цьому включає каталог партнерських API, «угоди рівня ризику» (risk-SLA), механізми continuous assurance (реєстри інтеграцій, постійний моніторинг продуктивності та безпеки), а також процедури виходу/замінності (reversibility) для зниження концентраційних ризиків. White-label-схеми вимагають чіткої сегрегації ролей у KYC/AML, прозорого атрибутування інцидентів і узгоджених сценаріїв повідомлень клієнтам.

Ключовою передумовою всіх перелічених змін є модернізація core-систем. Типова траєкторія – «strangler pattern»: навколо наявного core формуються доменні мікросервіси з чіткими API-контрактами, дані поступово виносяться у сучасні сховища (data lake/warehouse), критичні функції відокремлюються в незалежні модулі (платіжний хаб, скоринг, андеррайтинг, розрахунки). Після стабілізації навантажень проводиться міграція на хмарні платформи з автоматизованим тестуванням (CI/CD, інфраструктура як код), blue-green/канарковими релізами та вимогами до нульового або мінімального простою. Така еволюція знижує ризики «великих переїздів», підтримує пропорційність контролів і відкриває простір для швидкої інтеграції партнерів, утримуючи в фокусі показники cost-to-income, операційну надійність і відповідність ризик-апетиту, окресленому в попередніх підрозділах.

Платежі (миттєві та QR). Миттєві платежі реалізуються через подієву архітектуру з низькими затримками, токенизацією платіжних реквізитів та сильну клієнтську автентифікацію (MFA/біометрія з liveness). Оркестрація каналів API дозволяє ініціювати переказ із мобільного застосунку, web чи партнерського фронту з однаковим SLA; QR-платежі доповнюють екосистему як недорогий інструмент еквайрингу для МСП (динамічні QR із сумою та метаданими замовлення). Ключові показники: середній час авторизації/клірингу,

частка STP-операцій, рівень відмов на 1 тис. транзакцій, fraud rate, доступність сервісу (uptime). На бек-офісі операційні розриви закриваються RPA-сценаріями (reconciliation, chargeback), а ризики концентрації зменшуються завдяки мульти-рейлам (миттєві схеми, карткові мережі, внутрішньобанківські розрахунки) з автоматичним маршрутизатором за ціною та надійністю [63; 120].

Кредит (скоринг і BNPL). Алгоритмічний скоринг поєднує традиційні бюро з альтернативними даними (транзакційні профілі, поведінкові патерни, дані пристрою) та explainable ML-моделями, задокументованими в MLOps-контурах (версії, фічі, контроль дрейфу, стабільність PD). Видача «в один клік» забезпечується straight-through processing: eKYC/біометрія, API до рахунків для підтвердження доходів/витрат, динамічне ціноутворення за ризиком і миттєве відкриття ліміту. У BNPL додатково діють модулі «merchant risk» і анти-фрагментаційні правила, що запобігають надмірній заборгованості через агрегування лімітів між провайдерами. Вимірювання ефективності спирається на time-to-yes/time-to-cash, скорингові метрики (AUC, KS), динаміку NPL/ECL та повноту пояснюваності відхилень, а також поведінкові індикатори (prepayment, roll-rate). Ризик проциклічності моделей пом'якшується «антициклічними» політиками – буфери даних, консервативні пороги в періоди стресу, ручний перегляд маржинальних кейсів.

Ризик/AML (AI-моніторинг). Переорієнтація з правил на ризик-орієнтовану аналітику включає комбінацію графових алгоритмів, аномалій у потоках подій і профілювання клієнтів/пристроїв. Сценарії AML та санкційного скринінгу підсилюються ML-модулями пріоритезації алертів, що знижують частку хибнопозитивних спрацювань і прискорюють розслідування. Усі моделі проходять незалежну валідацію та документуються в «model cards» з таргетами на стабільність, упередженість і відтворюваність, а рішення логуються для подальшого аудиту (traceability). KPI: false positive rate, average handling time кейсу, частка автоматично закритих «низького ризику», покриття санкційних/PEP-джерел, виконання SLA для підозрілих активностей, збитки від шахрайства у розрахунку на 1 тис. транзакцій. Операційні ризики зменшуються

завдяки сегрегації середовищ даних, Zero Trust-доступу аналітиків та чітким «червоним лініям» щодо використання персональних даних [44; 148].

Інвестиції (робо-адвайзинг). Робо-радники будуються на багаторівневій моделі: оцінка ризик-профілю клієнта (анкета + поведінкові маркери), стратегія алокації активів, ребалансування за правилами та пояснювані рекомендації у plain language. Для гібридних моделей (цифровий + людський консультант) використовуються task-рутинги: складні кейси передаються до радника разом із контекстом даних і попередніми симуляціями. Прозорість забезпечується «інвестиційними паспортами» портфеля, симуляціями історичної волатильності й стрес-сценаріями. Оцінювання: показники дохідності з урахуванням ризику (Sharpe/Sortino), відхилення від цільових алокацій, час відповіді на запити, рівень завершення онбордингу та NPS/retention інвест-клієнтів. Контроль включає обмеження на складні/ілюквідні інструменти для нефахових інвесторів, тест на доречність та етичні вимоги до розкриттів.

Страховання (usage-based і телеметрика). Продукти з оплатою «за використання» покладаються на телеметрію (авто, гаджети, смарт-пристрої) і смарт-контракти/тригери для оперативних виплат. Андеррайтинг перетворюється на безперервний процес: профілі ризику оновлюються за подіями, премія та ліміти коригуються динамічно, а клієнт отримує превентивні підказки щодо зменшення ризику. Для параметричного страхування використовуються зовнішні оракули (погода, гео, логістика) з чіткими SLA джерел і журналюванням для оскарження. Вимірюються loss ratio, час врегулювання збитку, частка автоматичних виплат, точність тригерів, churn та частка активних користувачів телеметрії. Ризики приватності адресуються мінімізацією даних, агрегацією, прозорими політиками згод і можливістю відмови від окремих сенсорів без втрати базового покриття.

Залежність від постачальників (vendor lock-in). Масштабування на хмарних і платформних сервісах підвищує ризик технологічної «пришитості» до конкретного вендора інфраструктури, даних або ядра процесингу. Контрольна рамка передбачає політики reversibility/portability: контрактні зобов'язання на експорт даних у відкритих форматах, сумісність контейнерних образів, пруф-оф-

екзит (proof-of-exit) під час онбордингу та щорічні «сухі» міграції критичних доменів (data/ID/payments) у тестовому середовищі. Для сервісів «місії критично» – подвійний інтеніт (active-active/active-standby) у різних зонах або провайдерах, каталог залежностей (software bill of materials, карта інтеграцій), ліміти на частку трафіку через одного постачальника та регулярна переоцінка ТСО з урахуванням прихованих витрат на вихід [45; 56].

Кібервитривалість та операційна безпека. Ризик-менеджмент і безпека інтегруються в DevSecOps, де кожна зміна проходить статичний/динамічний аналіз, секрети зберігаються централізовано, а доступи оформлено за принципом найменших привілеїв. Модель Zero Trust із мікросегментацією, постійною валідацією ідентичностей і телеметрією подій (EDR/XDR, SIEM) зменшує площину атаки, а керування ключами та шифрування «в русі й спокої» забезпечують конфіденційність. Для критичних вузлів застосовуються threat-led penetration й «червоні команди», регулярні tabletop-сесії з імітаціями фішингу, DDoS, компрометації токенів API та відмови хмарного регіону. KRI: MTTR, частота інцидентів за критичністю, відсоток багів, знайдених до продакшну, coverage журналювання, частка сервісів із $SLO \geq 99,9\%$ [66; 168].

Моделний ризик AI/ML. Алгоритмічні рішення створюють додаткові канали технічних і поведінкових вразливостей – від дрейфу даних і «розвалу» калібровок до упередженості у відмовах. Система контролю охоплює Model Risk Management: карти моделей (model cards), валідацію незалежною другою лінією, контроль дрейфу фіч/параметрів, бек-тестинг стабільності PD/скорингових метрик, моніторинг false-positive/false-negative та explainability для рішень, що впливають на права споживачів. Впроваджуються антициклічні гвардірейли: мінімальні буфери даних, «пауза-правила» на синхронне затягування порогів, обов'язковий людський перегляд маржинальних кейсів у стрес-періоди, з фіксацією причин і навчальних датасетів у репозиторіях MLOps.

Комплаєнс: KYC/AML і приватність даних. Ризики дотримання зумовлені дистанційністю процесів і мультиплікацією інтеграцій. Контрольна система вибудовується як compliance-by-design: ризик-орієнтовані сценарії eKYC (еквіваленти надійності, liveness, перехресні реєстри), санкційний та PER-

скринінг з оновленням списків у близькому до реального часу, графові моделі в AML з журналюванням рішень та SLA на розслідування. Захист даних базується на мінімізації, розмежуванні доступів, псевдонімізації для аналітики, керуванні згодами, аудиті запитів до персональних даних і праві на переносимість/видалення. Для зовнішніх партнерів – «risk-SLA», DPIA для нових інтеграцій, тест на еквівалентність контролів і договір на відповідальність за інциденти [55; 65].

Операційна безперервність (BCP/DR). Зростання швидкості цифрових потоків робить критичними RTO/RPO, сценарну готовність і комунікації з клієнтами. План безперервності включає георезервування, «гарячі» копії, автоматизовані відновлення інфраструктури як коду, blue-green/канаркові релізи, runbooks із чіткими ролями та матрицею ескалацій. Проводяться повноциклові відмовостійкі тести з відсіченням залежностей (chaos-engineering), стреси пікових навантажень, тренування з відключення ключових провайдерів, а також репетиції повідомлень клієнтам і регулятору із заздалегідь погодженими форматами. KPI/KRI: відсоток покриття сервісів планами DR, частота та успішність тестів, середній рівень сервісу під час інцидентів, виконання SLO в дні пікових навантажень.

Операційна модель контролю. Для керованості ризику відображаються у ризик-апетиті та перев'язуються з метриками продуктів: пороги STP-rate, fraud per 1k txn, мінімальні LCR/NSFR на сценаріях «цифрового відтоку», ліміти залежності від окремого вендора/хмари, допустимі вікна простою й відмов API. Три лінії захисту працюють у режимі «безперервного забезпечення» (continuous assurance): перша – вбудовані технічні контролі, друга – незалежна валідація моделей і процесів, третя – внутрішній аудит із фокусом на концентраційних вузлах і виконанні планів виходу. Така конструкція дозволяє інтегрувати швидкість релізів і партнерські моделі з вимогами стійкості, зберігаючи основу для наступного підпункту щодо KPI та візуалізацій дорожньої карти трансформації.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ТА РОЗВИТОК РИНКУ ЦИФРОВИХ ФІНАНСОВИХ ПОСЛУГ

2.1. Огляд ключових тенденцій, ризиків та бар'єрів розвитку цифрових фінансових послуг в Україні

Український ринок швидко переходить до безготівкових розрахунків: у 2024 р. частка безготівкових операцій за сумою досягла 64,5 %, а за кількістю – 94,6 %. За рік українці здійснили 8 184,8 млн безготівкових операцій на 4 243,5 млрд грн. Такі значення свідчать, що цифрові платежі стали «звичною поведінкою» для побутових та комерційних транзакцій, а мережевий ефект (ширша приймальна інфраструктура, онлайн-торгівля, Р2Р-перекази) далі підсилює попит на дистанційні фінансові сервіси. Джерела НБУ також фіксують подібну динаміку протягом 2024 р. за дев'ять місяців: 64,8 % за сумою та 94,5 % за кількістю, що підкреслює сталість тренду, а не одиничний сплеск [129; 131].

Поведінка клієнтів характеризується принципом «mobile-first»: переважна більшість карткових операцій відбувається без фізичного контакту з відділенням, а зростання частки безготівкових транзакцій за кількістю до 94–95 % корелює з активним використанням інтернет-банкінгу, мобільних гаманців, QR/NFC-оплат і р2р-переказів. Публікації НБУ про розвиток системи електронних платежів (СЕП) додатково відображають «цифрову нормальність» на рівні міжбанківських розрахунків: СЕП забезпечує ≈ 97 % гривневих міжбанківських переказів у режимі RTGS, що опосередковано підтримує швидкі кінцеві платежі для користувачів і бізнесу [117; 128].

Технологічна база попиту – масовий доступ до інтернету та смартфонів. На початок 2024 р. в Україні було 29,64 млн користувачів інтернету (79,2 % населення), причому показник за 2023–2024 рр. зріс на 1,1 млн. Профілі ІТУ фіксують охоплення принаймні 3G/4G не менше ніж 91 % населення станом на 2022 р., а кількість активних 4G-користувачів зросла до 29,8 млн на кінець 2023 р. Це означає, що цифрові канали вже доступні більшості домогосподарств, а бар'єр входу у fintech-сервіси (мобільні банківські додатки, е-гаманці, страховки

онлайн) переважно зводиться до цифрової грамотності й довіри, а не до фізичної інфраструктури [33; 82].

Фінансова інклюзія відображає, наскільки «цифровий попит» перетворюється на формальну участь у фінансовій системі. За даними Global Findex (Світовий банк), у 2021 р. в Україні частка дорослих із рахунком у фінансовій установі або мобільному провайдері становила близько 84 % (проти ≈ 63 % у 2017 р.), тобто за чотири роки приріст склав понад 20 в.п. Оновлення хвилі 2025 р. ще публікується, однак уже оприлюднені гендерні зрізи на порталах Світового банку свідчать про високий рівень охоплення як серед жінок, так і чоловіків. Сукупно це підтверджує: цифрові канали стали основним способом доступу до платежів, заощаджень і базових банківських послуг, а подальше зростання залежатиме від довіри, якості UX та регуляторної підтримки віддаленої ідентифікації та захисту прав споживачів.

Українська пропозиція цифрових фінансових послуг швидко розширюється як за інфраструктурою, так і за продуктовою лінійкою. На рівні екосистеми Національний банк реалізує перехід СЕП на версію 4.1 із функціональністю миттєвого кредитового переказу (граничний час виконання – до 10 секунд, ліміт однієї операції – 100 тис. грн), що з 1 грудня 2024 р. створило технічну основу для масових «instant» платежів 24/7. За 2024 р. через СЕП опрацьовано близько 483 млн платежів на суму майже 241 трлн грн (+14 % р/р), а СЕП забезпечує майже 99 % міжбанківських платежів у гривні. У середньому система обробляє 1,5 млн платежів на добу, маючи значний запас пропускну здатності. Таке оновлення інфраструктури підштовхує банки й платіжні установи до запуску нових швидких сервісів та інтеграцій у канали торговців і державних виплат [120; 137].

Продуктова динаміка у платіжному сегменті відображається в структурі безготівкових операцій картками (див. рис. 2.1). У 2024 р. розрахунки в торговельній/сервісній мережі дали майже половину суми безготівкових операцій (49,9 % у I півріччі 2025 р.), інтернет-платежі – 14,7 %, а Р2Р-перекази – 31,1 % за сумою (8,2 % за кількістю). На тлі розвитку безконтактних сценаріїв зростає «токенізація»: кількість токенизованих платіжних карток у 2024 р.

досягла приблизно 14,9 млн (+19 % від початку року). Паралельно НБУ стандартизував QR-механізми для передавання реквізитів і ініціювання кредитових переказів, що спрощує приймання платежів офлайн та в онлайн-каналах, а також прискорює розрахунки малого бізнесу без дорогого обладнання [129; 131; 126].

Сегмент «миттєві платежі/P2P/QR» отримав додатковий імпульс завдяки переходу платіжної інфраструктури на ISO 20022 і запуску миттєвих переказів у СЕП-4.1: граничний час виконання переказу – до 10 секунд, що істотно («реального часу») змінює дизайн продуктів (моментальні поповнення гаманців, розрахунки торговців, миттєві повернення/виплати). За дев'ять місяців 2024 р. через СЕП проведено ≈ 347 млн платежів (+13,4 % р/р), а у 2025 р. НБУ підкреслює готовність СЕП-4 закладати підґрунтя для подальшої інтеграції з європейським простором платежів (SEPA). У підсумку миттєві/QR-сценарії стають базовим очікуванням користувачів, що зумовлює появу нових сервісів «on-top» (касові лінки, pay-by-link, push-to-card, миттєві P2P-refunds).

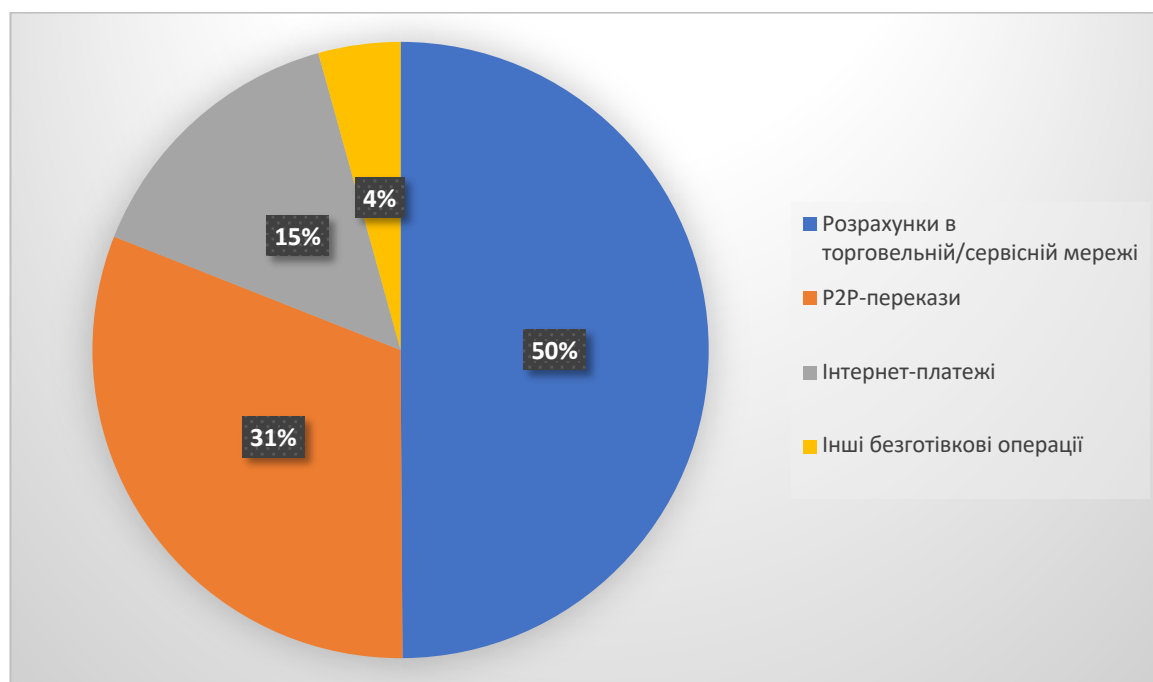


Рис. 2.1 Структура безготівкових операцій за платіжними картками за сумою, I півріччя 2025 р., %

Джерело: складено автором за матеріалами [129; 131]

Фінтех-пропозиція поза платежами також еволюціонує, але нерівномірно. Моделі BNPL в Україні переважно реалізуються як банківські продукти

розстрочки («Оплата частинами», «Миттєва розстрочка» тощо), для яких є верифіковані звітні орієнтири: обсяг виданих споживчих кредитів, включно з розстрочками, у провідних банків відображається у звітності та публічній статистиці (напр., у 2020–2021 рр. один з найбільших банків звітував про 42,3 млрд грн виданих кредитів за відповідними продуктами). Натомість автоматизоване інвестиційне консультування (robo-advice) перебуває на ранній стадії через регуляторні та ринкові обмеження; розвиток цього сегмента більше пов’язаний із загальними ініціативами щодо цифровізації ринку капіталу, тоді як масових офіційних статистичних вимірів robo-advice наразі немає. З боку інвестицій в екосистему, профіль УАФІК 2024 (за підтримки Мінцифри, НБУ, IFC/SECO тощо) фіксує 256 активних фінтех-компаній, з яких 79 % фінансуються власним коштом і 47 % працюють на міжнародних ринках; додатково міжнародні інституції (IFC, EBRD) оголошують інструменти підтримки технологічного підприємництва, зокрема й фінтех-напрямку, в межах програм відновлення та розвитку венчурного середовища [150; 163; 79].

Цифрова нерівність залишається системним бар’єром для масштабування фінтех-послуг (див. рис. 2.2). Попри загальне зростання покриття, індикатор ЦСР 9.6.1 фіксує: рівень охоплення інтернет-послугами зріс із 46 абонентів на 100 жителів у 2019 р. до 62 у 2023 р., причому статистика воєнних років подається без тимчасово окупованих територій і може уточнюватися. Це означає, що значна частина домашніх господарств досі не має стабільного доступу до якісного зв’язку, особливо у сільській місцевості, де оптика й досі розгорнута нерівномірно. Зафіксована в урядових оглядах логіка політики (пріоритет «сільської оптики» та доінвестування у ВШД) залишається актуальною, адже без базової конективності користувачі не доходять до етапу встановлення мобільних банків, е-гаманців чи страхових застосунків. Окремо ІТУ у країновому профілі підкреслює високе (90%+) покриття населення принаймні 3G/4G, але саме якість і стабільність каналу (а не лише «наявність сигналу») визначає реальну готовність до дистанційної ідентифікації, платежів і підписання е-договорів. Джерела офіційної статистики таким чином вказують: «цифровий доступ» покращується, але шов нерівності за місцевістю та доходом ще відчутний,

особливо для складніших фінансових сценаріїв (кредит онлайн, інвестиційні сервіси).

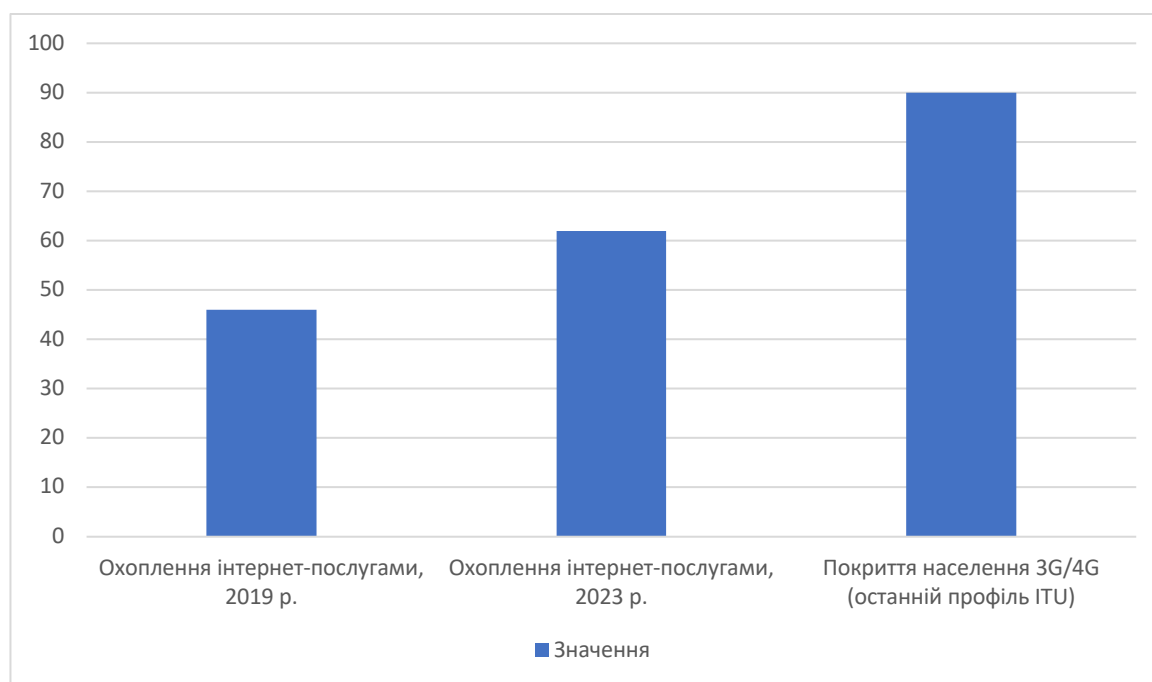


Рис. 2.2 Охоплення інтернет-послугами та мобільним зв'язком в Україні, 2019–2023 рр., % населення / абонентів на 100 жителів

Джерело: складено автором за матеріалами [33; 82]

Низька фінансова грамотність знижує конверсію «підключених» користувачів у регулярних користувачів фінтех-продуктів. Останнє комплексне вимірювання НБУ за методологією OECD/INFE (2021) зафіксувало індекс 12,3 із 21 можливого балу (проти 11,6 у 2018 р.), тобто прогрес є, але до цільових орієнтирів розвинених країн ще далеко (див рис.2.3.) . Світовий зріз OECD/INFE 2023 додатково показує: у середньому лише 38% дорослих, які керують продуктами онлайн, досягають мінімального порогу цифрової фінансової грамотності—це важливий орієнтир і для України, де швидка диджиталізація випереджає освітні зміни. Свіжа Національна стратегія розвитку фінансової грамотності до 2030 р. прямо пов'язує поведінкові моделі домогосподарств із рівнем фінансової культури та передбачає масштабування освітніх кампаній, однак для зняття бар'єрів входу в більш «просунуті» сервіси (інвестиції онлайн, страхові продукти on-demand) потрібні тривалі інтервенції в освіту дорослих, а також дизайн «за замовчуванням безпечний» у самих продуктах [118; 141].

Довіра до цифрових фінансових сервісів уразлива до шахрайства та кіберризиків. За даними НБУ, у 2024 р. збитки від незаконних операцій з платіжними картками зросли на 37% – до понад 1,1 млрд грн; при цьому переважна частка інцидентів припадає на інтернет-канали, а більшість втрат спричинена методами соціальної інженерії (розголошення реквізитів, кодів авторизації). Спільне опитування НБУ та OpenDataBot свідчить: із початку воєнного стану кожен дев'ятий респондент ставав жертвою шахраїв, найчастіше – під час купівлі/продажу товарів онлайн. Наявність швидких платіжних «рейлів» (миттєві перекази, токени, QR) безпосередньо підвищує вимоги до комплаєнсу, а також до UX-рішень проти «людського фактору»: фрикційні перевірки, in-app попередження, ліміти за ризиковими сценаріями та «червоні екрани» при виявленні ймовірного фішингу. Умовно «висока» довіра до банківської системи на макрорівні (зростання строкових депозитів) тут не гарантує побутового відчуття безпеки: без системної просвіти та проактивних технічних запобіжників користувачі уникають складніших цифрових фінансових продуктів, обмежуючись P2P і простими платежами.

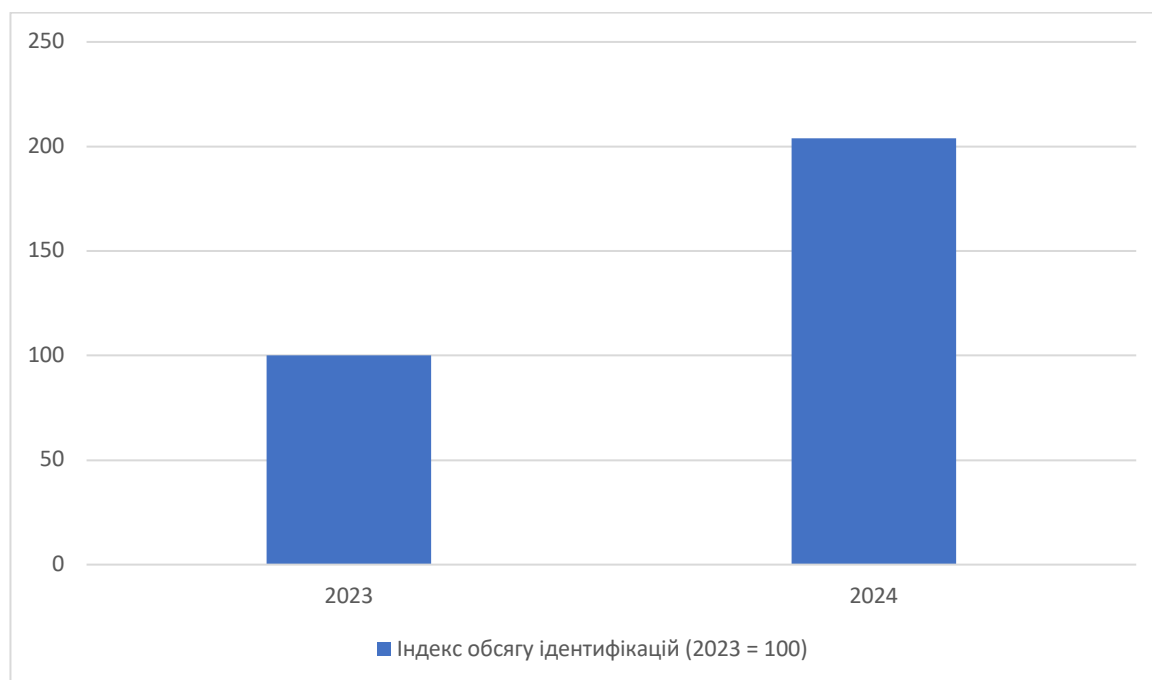


Рис. 2.3 Індекс фінансової грамотності населення України, 2018 та 2021 рр. (максимум 21 бал)

Джерело: складено автором за матеріалами [118]

Дефіцит кадрів обмежує швидкість виводу нових продуктів та масштабування цифрових операцій. За результатами офіційного онлайн-опитування роботодавців Мінекономіки у 2024 р., 43% компаній уже зіткнулися зі складнощами із заповненням вакансій; у міністерських щомісячних оглядах і прогнозних матеріалах брак кваліфікованих працівників прямо названо структурним обмеженням відновлення економіки у 2025–2027 рр. Для фінсектору й фінтеху це означає дефіцит інженерів платіжної безпеки, аналітиків даних/AML, розробників мобільних застосунків і фахівців з UX-доступності. Паралельно НБУ повідомляє про кратне зростання використання дистанційної ідентифікації (BankID НБУ: 87,7 млн успішних ідентифікацій за 2024 р., +104% р/р), що підвищує навантаження на суміжні компетенції (KYC, кіберзахист, протидія шахрайству). Вирішення кадрового вузького місця потребує трикутника «освіта-індустрія-держава»: прискорених програм перепідготовки, спрощеного імпорту експертизи та гнучких режимів працевлаштування для фахівців, що повертаються/релокуються [106; 107; 136].

Кіберінциденти залишаються одним із найсуттєвіших ризиків для цифрових фінансових послуг. Урядова команда CERT-UA у 2024 р. опрацювала 4 315 кіберінцидентів, із домінуванням атак на критичну інфраструктуру та державний сектор; у звітах Держспецзв'язку також фіксується сотні інцидентів, атрибутованих конкретним загрозливим кластерам (зокрема UAC-0006), що посилює навантаження на фінансові установи через ланцюгові залежності постачальників ІКТ-послуг. Національний регулятор оновлює вимоги до організації кіберзахисту в банківській системі, посилюючи контроль і підвищуючи стандарти операційної стійкості, а галузева CSIRT-NBU забезпечує рекомендації щодо виявлення та реагування. Такі дані підтверджують: навіть за наявності підвищеної готовності сектору, загальний фон загроз залишається високим, а профілактика та тестування стійкості (red-teaming, threat-led testing) мають бути системними практиками [22; 134; 156].

Витоки даних і конфіденційність формують окремий контур ризиків – як через компрометацію кінцевих пристроїв і хмарних сервісів, так і через вплив інформаційно-психологічних операцій, що підривають довіру до державних і

фінансових платформ. У 2025 р. Мінцифри публічно спростувало повідомлення про «масовий витік» із застосунку «Дія», наголошуючи на фальсифікації поширених файлів і відсутності компрометації державних систем; водночас інформаційні хвилі довкола «витоків» демонструють, що репутаційні ризики й потреба у прозорих процедурах верифікації інцидентів не менш критичні, ніж власне технічні вади. Для надавачів фінпослуг це означає необхідність посиленого управління ризиками третіх сторін, шифрування «за замовчуванням», журналювання доступів і готовності до публічних повідомлень про інциденти за уніфікованими схемами.

Шахрайство в цифрових каналах зростає разом із масовістю онлайн-операцій. За даними НБУ, у 2024 р. сума збитків від незаконних дій та шахрайських операцій із платіжними картками зросла на 37 % – до 1,1 млрд грн, головню через соціальну інженерію й зростання середнього чека однієї незаконної операції. Високошвидкісні «рейли» (миттєві перекази 24/7, токенизовані платежі, QR) підвищують вимоги до превенції: поведінкових тригерів у застосунках, адаптивних лімітів, відкладених виплат для ризикових сценаріїв, поглиблених KYC/AML-процедур і централізованого звітування про інциденти. Практичний висновок для ринку: без «фрикції там, де потрібна безпека» (warning-екрани, підтвердження наміру, contextual-risk scoring) зберігати прийнятний рівень втрат буде дедалі складніше [132; 133].

Модельний ризик AI та залежність від критичної інфраструктури формують подвійний системний виклик. На рівні ЄС регулятори прямо вказують: рішення, ухвалені з використанням AI (скоринг, андеррайтинг, робо-адвайзинг), залишаються відповідальністю органів управління фінансових установ; запроваджується режим DORA для ICT-ризиків і нові орієнтири щодо AI-систем, включно з вимогами до оцінки ризиків, тестування, логування та повідомлення про серйозні інциденти. Для України, що переживає масовані атаки на енергетичну інфраструктуру, стійкість фінансових сервісів додатково залежить від електро- й телеком-каналів: регулярні аварійні відключення електроенергії та пошкодження об'єктів генерації/передачі у 2024–2025 рр. демонструють, що без георезервування дата-центрів, офлайн-планів

безперервності (fallback-процедур), автономного живлення вузлів і мультиканальної телеком-резерви ризик недоступності платежів і дистанційних сервісів залишається матеріальним.

Регуляторна рамка підтримки цифрових фінансових послуг в Україні фокусується на поєднанні відкриття ринку й модернізації інфраструктури. Базовим актом є Закон України «Про платіжні послуги» № 1591-IX від 30.06.2021 р., який відкрив можливість діяльності нових категорій надавачів платіжних послуг (у т.ч. небанківських фінустанов, платіжних установ, операторів послуг платіжної інфраструктури), заклав понятійний апарат для open banking та гармонізував низку норм із європейським правом. НБУ, спираючись на цей закон, у серпні 2023 р. затвердив Концепцію відкритого банкінгу з дорожньою картою впровадження API-доступу до рахунків і стандартів взаємодії між банками та фінтех-провайдерами. У липні 2025 р. НБУ перейшов від концепції до повноцінного регуляторного режиму, ухваливши Положення про відкритий банкінг в Україні (постанова Правління № 80), яке визначає коло учасників, вимоги до безпеки, формати даних та строки приведення діяльності банків/PSP у відповідність – це формує «твердий каркас» для масштабування сервісів на основі відкритих API.

Політики й програми Мінцифри доповнюють регуляторні кроки НБУ, створюючи загальні умови для розвитку цифрової економіки та технологічного бізнесу, включно з фінтехом. Ключовий інструмент – правовий режим Дія.City, запроваджений Законом № 1667-IX, зі спрощеними податковими й корпоративними моделями для IT-компаній та стартапів (зниження податкового навантаження, гіг-контракти, опціони тощо). Офіційний портал Дія.City містить електронну процедуру набуття статусу резидента, а також статистику щодо кількості резидентів та створених робочих місць. Процедура резидентства передбачає онлайн-подання заяви до Мінцифри і розгляд протягом 10 робочих днів за принципом «мовчазної згоди», що знижує адміністративні бар'єри для технологічного бізнесу, у тому числі для фінтех-компаній, які розробляють цифрові платіжні, кредитні та страхові рішення.

Ринкові ініціативи й партнерські програми виконують роль «м'якої» інфраструктури, поєднуючи компанії, регуляторів та інвесторів. Українська асоціація фінтех та інноваційних компаній (UAFIC) за підтримки Мінцифри, НБУ, IFC, SECO, GGF та Українського фонду стартапів у 2024 р. підготувала Ukrainian Fintech Catalog 2024, який фіксує структуру екосистеми, надає публічний реєстр фінтех-компаній і використовується як довідник для інвесторів та партнерів. Каталог прямо позиціонується як частина офіційної фінтех-екосистеми України, що відображає системну співпрацю між державою, регуляторами та бізнес-об'єднаннями. Паралельно функціонує Український фонд стартапів (USF), який реалізує грантові програми для технологічних компаній на стадіях pre-seed/seed, у тому числі для фінтех-проектів, – це здешевлює вхід на ринок та дає доступ до нефінансової підтримки (менторство, акселерація, інтеграція з європейськими програмами) [163; 164].

Попри наявність карти політик і програм, низка прогалин гальмує масштабування цифрових фінансових послуг. По-перше, значна частина норм Закону «Про платіжні послуги» та Положення про відкритий банкінг потребує повної імплементації через підзаконні акти НБУ, типові угоди, технічні стандарти API та наглядову практику (авторизація нових типів постачальників, моделі відповідальності, процедури відкликання дозволів). По-друге, режим Дія.City, попри привабливі умови, не є універсальним рішенням для всіх фінтех-компаній (особливо малих команд із невеликою виручкою), а отже вимагає доповнення іншими формами підтримки (податкові стимули для R&D, пілотні регуляторні «пісочниці» для фінпослуг). По-третє, ринкові каталоги й програми грантової підтримки поки що не розв'язують проблеми «останніх миль» – браку доступного капіталу на стадіях growth/scale-up, нестачі спеціалізованих фінтех-інвесторів і нерозвиненості виходу на ринок капіталу. Сукупно це означає, що формальні рамки підтримки вже існують, але їхня повна реалізація й координація між НБУ, Мінцифрою та ринком залишаються критичними передумовами для виходу українських цифрових фінансових сервісів на стійкі масштаби.

2.2. Оцінка поточного рівня та динаміки розвитку цифрових фінансових послуг в Україні

Ринок цифрових каналів банківського обслуговування в Україні у 2022–2024 рр. де-факто став масовим: доступ до фінансових послуг для більшості домогосподарств забезпечується саме через мобільні та інтернет-застосунки банків і небанків. За даними «ПриватБанку», його послугами у 2024 р. користувалися понад 18 млн активних роздрібних клієнтів, причому цифрові сервіси (Приват24 для фізичних осіб та бізнесу, нефінансові онлайн-сервіси) демонструють стійке зростання й охоплюють сотні тисяч підприємців і юридичних осіб. Оцінка незалежного медіа Fintech Insider на основі річного звіту банку за 2022 р. показує, що кількість активних користувачів інтернет-банкінгу «Приват24» досягла 13,1 млн осіб, збільшившись на 11 % з початку повномасштабної війни. Паралельно швидко розвиваються цифрові небанки: кількість клієнтів monobank на кінець січня 2024 р. досягла 8 млн, а в публічних коментарях менеджменту компанії у вересні 2024 р. йдеться вже про «майже 9 мільйонів клієнтів». Сукупно лише два найбільших мобільних сервіси (Приват24 та monobank), попри перетин клієнтських баз, охоплюють аудиторію, співмірну з більшістю економічно активного населення країни, що підтверджує домінування мобільного та інтернет-банкінгу як ключових каналів доступу до цифрових фінансових послуг [150; 163].

Транзакційна активність у цих каналах добре простежується через офіційну статистику Національного банку щодо операцій з платіжними картками, які є основною «транспортною шиною» для мобільного та інтернет-банкінгу. За 2024 р. кількість операцій з платіжними картками, емітованими українськими банками та фінансовими установами, становила 8 654,4 млн на загальну суму 6 577,4 млрд грн, причому 8 184,8 млн операцій на суму 4 243,5 млрд грн були безготівковими. Частка безготівкових операцій сягнула 94,6 % за кількістю та 64,5 % за сумою, що свідчить про стійку переорієнтацію платежів у цифрові канали навіть в умовах повномасштабної війни. Інфраструктурно цю динаміку підтримує зростання кількості платіжних терміналів у торговельній та сервісній мережі на 10,5 % за рік (до 496,6 тис., з яких 97,5 % – безконтактні), а

також збільшення емісії платіжних карток до 132 млн (+15 % до 2023 р.) і активних карток – до 58,8 млн (+13 % до 2023 р.). Фактично це означає, що більшість економічно активних українців не лише мають платіжну картку, а й регулярно здійснюють видаткові операції через цифрові канали, що є проксі-показником високих MAU для мобільного й інтернет-банкінгу [129; 131].

Окрему групу каналів становлять P2P-перекази та оплата товарів і послуг онлайн, які реалізуються як через застосунки банків, так і через інтеграцію з електронними гаманцями та платіжними сервісами. За даними аналітичного огляду НБУ за 2024 р., найчисельнішим видом безготівкових операцій залишаються розрахунки платіжними картками в торговельній мережі (73,4 % за кількістю та 46,8 % за сумою), однак перекази з картки на картку вже формують 31,1 % від суми всіх безготівкових операцій (1 318,4 млрд грн) і 8,2 % від їх кількості. Оплата товарів та послуг в інтернеті становить 13,6 % за кількістю безготівкових операцій та 14,7 % за сумою (622 млрд грн), із середньою сумою однієї операції 561 грн, тоді як середня сума P2P-переказу – 1 958 грн. Це вказує, що P2P-канали й онлайн-еквайринг перерозподіляють значну частку грошових потоків домогосподарств у цифровий простір. На тлі посилення регулювання електронних грошей та скорочення кількості емітентів у 2019–2021 рр., зафіксованого дослідженнями на основі статистики НБУ (зменшення кількості електронних гаманців із 79 до 23 млн та обсягів операцій майже вдвічі), роль карткових P2P-переказів і токенизованих карток у мобільних гаманцях лише посилилася [129; 159].

Оцінка показників ARPU та DAU/MAU для українських цифрових фінансових сервісів ускладнена тим, що такі метрики, як правило, не розкриваються у відкритій офіційній звітності банків і небанків, однак окремі джерела дозволяють окреслити їх порядок величини. Наприклад, за даними Fintech Insider, які спираються на річний звіт «ПриватБанку», чистий комісійний дохід банку за 2022 р. становив 20,4 млрд грн при 13,1 млн активних користувачів Приват24, що дає орієнтовний рівень комісійного ARPU близько 1,5–1,6 тис. грн на активного клієнта на рік (з урахуванням того, що цей дохід формується не лише цифровими, але й традиційними каналами). У 2024 р. банк

звітує також про майже 1 млн цифрових «конвертів» для накопичень із сумарними поповненнями 7,5 млрд грн та 3,5 млн користувачів програми лояльності «Привіт», що демонструє здатність мобільного застосунку генерувати додану вартість через перехресні продажі та кешбек-програми. Для monobank офіційно озвучена цифра 8 млн клієнтів станом на січень 2024 р. у поєднанні з високою транзакційною активністю, яку видно на публічному дашборді сервісу, свідчить про формування однієї з найбільших в Європі баз користувачів мобільного необанкінгу з високою часткою щоденних активних користувачів, хоча конкретні DAU/MAU та ARPU публічно не розкриваються [150; 163].

Платіжна інфраструктура України протягом 2023–2025 рр. пройшла суттєве оновлення завдяки модернізації Системи електронних платежів НБУ. Перехід СЕП на стандарт ISO 20022 та запуск роботи у режимі 24/7 (СЕП 4.0 з квітня 2023 р.) забезпечили можливість обробки міжбанківських переказів у реальному часі. З 1 грудня 2024 р. введено СЕП 4.1 із функціональністю миттєвих кредитових переказів: кошти мають надходити одержувачу в межах приблизно 10 секунд, за умови доступності отримувача у системі. Така модернізація створює «швидкі платіжні рейли» для масштабування fintech-продуктів – зокрема серверних P2P-сервісів, e-commerce-еквайрингу та миттєвих виплат.

Другим ключовим блоком інфраструктури є цифрова ідентифікація. Система BankID НБУ забезпечує віддалену ідентифікацію фізичних осіб через банки-ідентифікатори та використовується державними й приватними сервісами. BankID дозволяє користувачеві дистанційно відкривати рахунки, активувати фінансові сервіси, підписувати угоди онлайн. НБУ зазначає, що сервіс є «зручним, надійним та безпечним інструментом ідентифікації», однак публічно доступна кількісна статистика (кількість ідентифікацій, підключених провайдерів, частка фінпослуг) поки що обмежена, що ускладнює повну кількісну оцінку впливу на ринок.

Розвиток API-економіки та відкритого банкінгу формує наступний рівень інфраструктурної зрілості. На рівні правової рамки open banking ґрунтується на

Законі України «Про платіжні послуги» та підзаконних актах Секторального регулятора. 25 липня 2025 р. НБУ ухвалив Положення про відкритий банкінг (Постанова № 80), що визначає вимоги до API-інтерфейсів, форматів обміну даними, ролей учасників (ASPSP, AISP, PISP), безпеки доступу та строків впровадження. З 1 серпня 2025 р. режим відкритого банкінгу офіційно набрав чинності. Це фактично запускає механізм регульованого доступу третіх сторін до рахунків користувачів через стандартизовані інтерфейси, що має вирівняти українську модель з європейською (PSD2/PSD3), стимулювати розвиток API-платформ, кредитних маркетплейсів та нових платіжних сценаріїв [170; 171].

Попри модернізацію інфраструктури, залишаються важливі прогалини. У сфері миттєвих платежів поки що бракує публічних агрегованих даних щодо кількості банків, що технічно реалізували instant-функціональність, та обсягів операцій у новому режимі СЕП 4.1. У сфері open banking навіть після прийняття Положення № 80 необхідні активні кроки з боку банків та платіжних установ – розгортання та тестування API-інтерфейсів, ліцензування AISP/PISP, впровадження стандартів безпеки доступу. Також є технічні бар'єри для інтеграції BankID із небанківським сектором (страхові послуги, інвестиційні сервіси, мікрофінансові продукти). Нарешті, стійкість інфраструктури сильно залежить від зовнішніх факторів – телекомунікаційних каналів і енергопостачання, що особливо критично в умовах воєнних загроз.

Банківський сектор залишається «ядерним» гравцем ринку цифрових фінансових послуг, забезпечуючи масштаб, довіру та регуляторну стабільність. Станом на кінець III кв. 2024 р. в Україні діяло 62 платоспроможні банки; частка державних банків у чистих активах становила 53,3 %, а топ-20 банків концентрували понад 90 % активів сектору, що створює високу концентрацію ресурсів для інвестицій у цифрові сервіси (мобільний/інтернет-банкінг, миттєві перекази, цифрові карти). Саме найбільші банки – насамперед державні, а також приватні та іноземні групи – задають стандарти UX, швидкості платежів, рівня безпеки та інтеграції з державними сервісами (Дія, е-довірчі послуги). На цій основі формується конкурентне поле для необанківських проєктів (monobank на базі АТ «Універсал Банк») та банківських екосистем, які комбінують класичні

продукти з маркетплейсом сервісів й інтеграцією з платіжними й RegTech-платформами [116; 119].

Другий контур ринку – небанківські фінансові установи та учасники платіжного ринку, які нарощують свою роль у сегментах P2P-переказів, електронних гаманців, масових платежів і торговельного еквайрингу. За даними НБУ, станом на 1 жовтня 2024 р. на ринку небанківських фінансових послуг функціонувало 926 установ (509 фінансових компаній, 64 ризикових страховиків, 11 лайф-страховиків, 113 ломбардів, 110 кредитних спілок тощо), а на платіжному ринку – 16 платіжних систем, створених резидентами, та 15 міжнародних платіжних систем. У сфері надання платіжних послуг працюють 18 платіжних установ, 12 фінансових установ, що мають право на платіжні послуги, один банк-емітент електронних грошей, один поштовий оператор, 48 комерційних агентів і 30 технологічних операторів платіжних послуг. Саме ці гравці, співпрацюючи з банками й торговельними мережами, забезпечують масштабування цифрових гаманців, овердрафт-рішень «у чек-ауті», масових виплат (зарплатні, соціальні, маркетплейси) та P2P-переказів із мінімальним тертям для користувача [14; 15].

Динамічно зростає прошарок спеціалізованих фінтех-компаній, які працюють як у форматі самостійних провайдерів, так і в моделі B2B/BaaS для банків та небанківських ФК. Згідно з «Ukrainian fintech catalog 2024», на ринку ідентифіковано 256 фінтех-компаній, з яких 75 % уже вийшли на точку беззбитковості, 47 % працюють на міжнародних ринках, 79 % базуються в Києві, а 79 % фінансуються переважно власними коштами засновників. Значна частина цих компаній працює в сегментах платежів, еквайрингу та онлайн-торгівлі (платіжні шлюзи та процесингові платформи на кшталт Fondy), миттєвих переказів, BNPL-рішень, мікрокредитування, факторингу, сервісів для МСП і маркетплейсів. Показовим кейсом є NovaPay, яка поєднує логістичну та платіжну інфраструктуру: станом на 1 жовтня 2024 р. вона є єдиним небанківським емітентом платіжних карток, який обслуговується НБУ, із 212,2 тис. активних карток. Такі гравці підсилюють конкуренцію в цифрових

платежах, знижують вартість сервісів для торговців і підвищують доступність онлайн-платежів для домогосподарств [163; 116].

Окремий сегмент складають інфраструктурні платіжні системи та RegTech/SupTech-рішення, що забезпечують стійкість і відповідність ринку регуляторним вимогам. На рівні платіжної інфраструктури ключову роль відіграють Система електронних платежів (СЕП-4) НБУ, що з 2023 р. працює 24/7 на стандарті ISO 20022, та національна платіжна система PROSTIR: станом на кінець 2023 р. в системі налічувалося близько 460 тис. емітованих карток (254 тис. активних), а їх приймання забезпечувалося у 458 тис. POS-терміналів (майже 100 % мережі) і 15 тис. банкоматів (94 % мережі). На рівні RegTech важливими стейкхолдерами стали приватні платформи YouControl (комплексна перевірка компаній, KYC/AML-скоринг, API YouScore) та Опендатабот (моніторинг реєстрів, судових рішень, податкових боргів, сервіс оплати IBAN-рахунків), які інтегруються в процеси банків, небанківських ФК, страхових і великих корпорацій для автоматизації комплаєнсу та управління ризиками. З боку регулятора запроваджено SupTech-концепцію розвитку наглядових рішень на 2023–2028 рр. та інтегровану платформу супервізії, що поєднує дані щодо банків та небанківських установ. У сукупності це формує багаторівневу екосистему, де банки залишаються центральними операторами рахунків і регульованими провайдерами, а небанківські ФК, платіжні системи, процесинг і RegTech-компанії виступають каталізаторами інновацій, забезпечуючи спеціалізацію, нішеві продукти та технологічну гнучкість [123; 137; 144; 178; 119].

Економічні ефекти цифровізації фінансових послуг в Україні проявляються насамперед через підвищення операційної ефективності банківського сектору. За даними НБУ, у I кв. 2024 р. cost-to-income ratio (CIR) банків становив 35,9 % (проти 35,6 % у I кв. 2023 р.), а в III кв. 2024 р. – 37,9 % проти 33,0 % роком раніше, що свідчить про збереження високої операційної результативності навіть за зростання витрат. Одночасно чистий процентний дохід зріс на 20,3 % р/р, а чистий комісійний дохід – на 4,5 % р/р, причому НБУ прямо пов'язує це зі зростанням обсягів безготівкових платежів та карткових

операцій, які здійснюються переважно через дистанційні канали. У 2024 р. чистий прибуток банківського сектору досяг близько 103,7 млрд грн (+20 % до 2023 р.), причому 85 % прибутку сформовано топ-10 банків, серед яких Universal Bank (monobank) уже входить до десятки найприбутковіших установ. Це вказує, що цифрові моделі обслуговування (масштабні мобільні сервіси, онлайн-екосистеми) стали важливим фактором доходності, доповнюючи «воєнні» чинники – високі ставки за ОВДП та значні обсяги ліквідності [116; 119].

На рівні витрат та якості сервісу цифрові фінпослуги скорочують транзакційні витрати й час обробки операцій, одночасно підвищуючи доступність. Дослідження цифрового банкінгу за 2019–2023 рр. показує, що частка безготівкових операцій з платіжними картками в Україні в середньому становила близько 89,1 % від кількості транзакцій, а в 2023 р. досягла 93,5 %; кількість операцій із картками зросла за 2019–2023 рр. на 43,2 %, а обсяг у грошовому вимірі – на 54,6 %, паралельно збільшувалася кількість POS-терміналів. Це означає, що основний потік платежів перемістився у цифровий простір, де граничні витрати на проведення додаткової операції є низькими. Кейс ПриватБанку демонструє масштаби ефекту: у 2023 р. банк мав 18,35 млн активних роздрібних клієнтів, 51,3 % частки на ринку платежів і 1,3 млрд P2P-переказів на суму понад 2,8 трлн грн; понад 98 % платежів та переказів здійснювались через канали самообслуговування. Така концентрація операцій у мобільних та інтернет-каналах знижує потребу в утриманні розгалуженої мережі відділень і касових операцій та дозволяє перерозподіляти ресурси на розвиток UX, антифроду й аналітики [100; 150].

Для економіки в цілому цифрові фінтех-рішення посилюють конкуренцію та розширюють вибір для користувача, але водночас зберігаються ознаки високої концентрації на ринку. Наукові дослідження фінтех-індустрії в Україні підкреслюють, що застосування фінансових технологій зменшує вартість фінансових транзакцій для бізнесу та домогосподарств, створює нові канали виходу на ринок і змушує традиційні банки підвищувати технологічний рівень сервісу. Однак емпіричні огляди показують, що конкуренція досі не є «досконалою»: значна частина прибутку й активів сконцентрована в декількох

найбільших державних і приватних банках, а частка чисто фінтех-компаній у кредитуванні та роздрібних платежах залишається відносно невеликою, попри швидке зростання. Показовим є те, що, за оцінками оглядів банківського сектору та медіа-аналітики, частина надприбутків банків у 2023–2024 рр. пояснюється не лише ефективністю цифрових бізнес-моделей, а й монетизацією надлишкової ліквідності через ОВДП і сертифікати НБУ. Водночас державне підвищення податку на прибуток банків до 25 % та рекордні податкові відрахування (понад 83 млрд грн за 2024 р.) означають, що частина економічних вигід від цифровізації опосередковано повертається в державний бюджет [166; 116].

Зміни в якості сервісу та поведінці клієнтів мають і соціально-економічний вимір. Дослідження розвитку цифрових інновацій на ринку фінансових послуг України за 2010–2024 рр. показує, що впровадження онлайн-банкінгу, мобільних застосунків, fintech-стартапів і державних цифрових сервісів (зокрема, інтеграція фінооперацій у застосунок «Дія») підвищили доступність, швидкість і безпеку фінансових транзакцій, а також сприяли фінансовій інклюзії. Окремі праці підтверджують, що цифрові фінтех-послуги зменшують інформаційну асиметрію, полегшують доступ до кредитів МСП і дозволяють бізнесу краще керувати грошовими потоками, хоча й створюють нові ризики кібербезпеки та операційної стійкості. Журналістські розслідування та експертні інтерв'ю при цьому звертають увагу, що, попри рекордні прибутки банків, корпоративне кредитування залишається стриманим через воєнні ризики, а вигоди для домогосподарств часто проявляються більше у зручності та швидкості платежів, ніж у суттєвому здешевленні фінансових продуктів. Сукупно це дозволяє зробити висновок: цифрові фінансові послуги вже істотно підвищили операційну ефективність сектору, конкуренцію за сервіс і зручність для споживачів, однак структурні ефекти для вартості фінансових ресурсів та глибини кредитування поки що обмежені макрофінансовими та воєнними факторами.

На найближчі 1–3 роки головними «больовими точками» для цифрових фінансових послуг залишаються воєнні ризики, енергетичний дефіцит та високі ставки, які звужують простір для інвестицій у розвиток. За базовим прогнозом НБУ, економіка України у 2025–2027 рр. має потенціал зростання на рівні

близько 3–4 % на рік за умови стабілізації енергосистеми та збереження зовнішнього фінансування, але восени 2025 р. регулятор уже був змушений знизити прогноз зростання ВВП через нову хвилю атак на енергетичну інфраструктуру й дефіцит робочої сили. Центральний банк тримає облікову ставку на підвищеному рівні 15,5 %, щоб стримати інфляцію й профінансувати дефіцит бюджету, що одночасно стримує кредитування та зменшує апетит банків до ризикових інноваційних проєктів. У такому середовищі цифрові фінпослуги з одного боку стають опорою безперервності розрахунків і підтримують економічну активність, з іншого – їх подальше масштабування прямо залежить від того, наскільки швидко буде вирішено проблеми із «фізичною» інфраструктурою та регуляторною визначеністю.

Операційна стійкість цифрових каналів залишається вразливою до енергетичних та телекомунікаційних шоків, і це одна з ключових зон, де потрібні швидкі інтервенції. Офіційні огляди цифрового розвитку фіксують, що з 2022 р. в Україну вкладено значні ресурси у генератори, акумулятори, публічні точки Wi-Fi та резервні канали зв'язку, завдяки чому телеком-оператори здатні підтримувати роботу мережі годинами навіть під час відключень світла. Водночас дослідження розвитку фінтех-ринку вказують, що нестабільна робота енергомереж і доступу до Інтернету залишається серед головних перешкод для подальшого розвитку цифрових сервісів. Приклад масового збою електронних платежів у квітні 2025 р., коли через технічну проблему тимчасово не працювали термінали в частині ресторанів, відділеннях пошти, у київському метро та спостерігались збої в окремих банківських застосунках і сервісі «Дія», показав, наскільки уразливою є екосистема до «точкових» відмов критично важливих банківських і платіжних систем. У відповідь НБУ розвиває програму «Power banking», а мобільні оператори масово інвестують у резервне живлення, але в найближчі 1–3 роки пріоритетом має стати більш глибока диверсифікація процесингу, розвиток офлайн-сценаріїв (offline-токени, резервні карти, кеш-фолбек) та обов'язкові плани безперервності для ключових учасників платіжного ринку.

Другий великий блок «больових точок» – регуляторна невизначеність та структурні обмеження фінансування й кадрів, особливо для фінтех-компаній. Сучасні дослідження fintech-індустрії України за 2025 р. показують, що попит на цифрові фінпослуги й далі зростає, однак основними викликами залишаються регуляторна невизначеність, кібербезпека, нестача фінансових ресурсів і дефіцит кваліфікованих спеціалістів. Воєнний конфлікт звузив ринок, посилив відтік кадрів і ускладнив залучення довгострокового капіталу: інвестори очікують більшої синхронізації правил з ЄС (зокрема у сферах відкритого банкінгу, захисту даних, AI-скорингу) та прозорі дорожньої карти гармонізації регулювання. Сам НБУ у Звіті про фінансову стабільність за 2025 р. підкреслює, що зосереджений на набутті статусу «еквівалентної третіх країн» за банківським регулюванням, впровадженні європейських буферів капіталу й оновленні підходів до покриття операційних ризиків, що в середньостроковій перспективі вивільнить частину капіталу банків. Проте в короткостроковому горизонті поточна висока ставка, воєнні ризики й підвищене податкове навантаження (windfall-податок) обмежують готовність банків масштабно фінансувати ризикові цифрові інновації, а фінтех-сектор змушений більше покладатися на власний капітал і зовнішні грантові програми [166; 119].

Третя група трендів стосується довіри, фінансової грамотності й поведінкових ризиків, які можуть або підштовхнути, або загальмувати подальшу цифровізацію. Дослідження Visa Stay Secure 2025 показує, що 95 % опитаних українців уже користуються цифровими платежами, 80 % «переважно» чи «повністю» їм довіряють, 39 % очікують збільшення частки цифрових оплат у найближчі 12 місяців; водночас 98 % переживають, що їхні рідні можуть стати жертвою шахрайства, а 97 % уже вживають певні заходи безпеки. Це поєднання високого проникнення й високої тривожності створює запит на системні освітні програми та «дизайн безпеки за замовчуванням» у продуктах (попередження, обмеження за ризиковими сценаріями, прозорі механізми відшкодування). Паралельно стрімке зростання використання системи BankID НБУ (87,7 млн успішних ідентифікацій у 2024 р., +104 % р/р) вказує на швидке зміщення критичних процесів (відкриття рахунків, активація сервісів, укладення

договорів) в онлайн. Це посилює вимоги до захисту персональних даних, кіберстійкості державних і приватних платформ і створює вікно можливостей для RegTech-рішень у сфері KYC/AML.

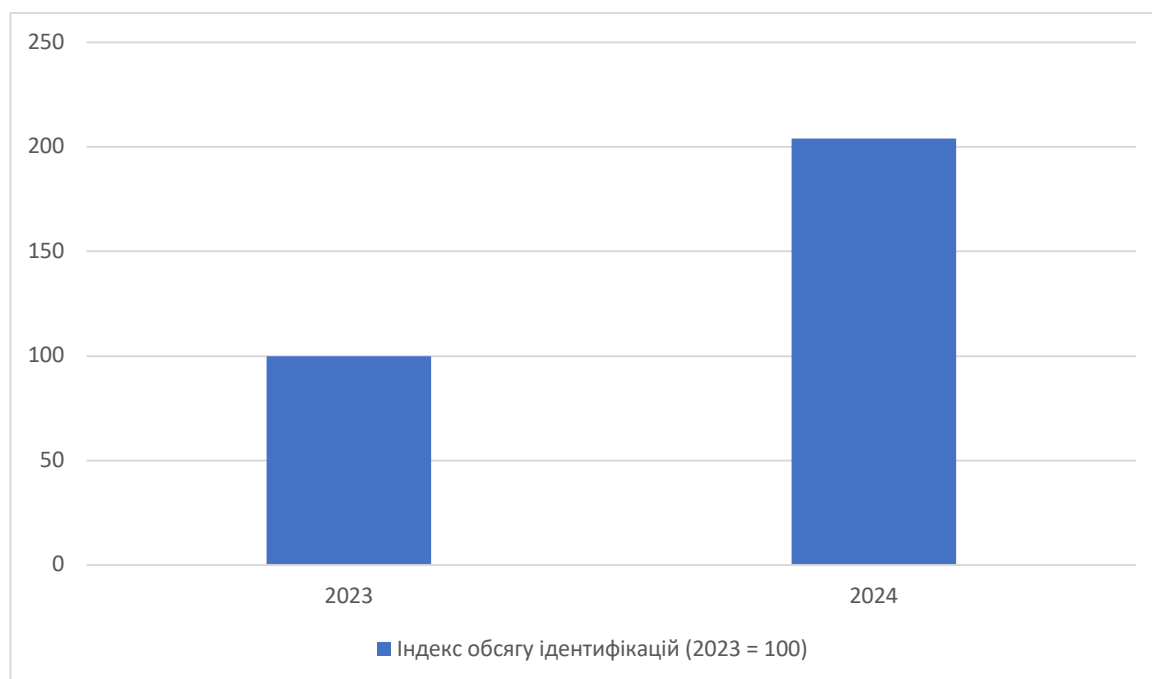


Рис. 2.4 Зростання обсягу ідентифікацій через BankID НБУ, 2023–2024 рр. (індекс)

Джерело: складено автором за матеріалами [112; 136]

У найближчі 1–3 роки швидкі інтервенції потрібні насамперед у трьох напрямках: масштабування програм цифрової фінансової грамотності; впровадження єдиного підходу до повідомлень про інциденти та прозорих процедур відшкодування для споживачів; а також прискорене формування рамок для етичного й безпечного використання AI у скорингу, андеррайтингу й антифроді.

2.3. Порівняльний аналіз міжнародного досвіду цифровізації фінансових систем (ЄС, США, Азія та Україна)

У європейській моделі цифрових фінансових послуг ядром стратегії виступає нормативно закріплений open banking з поступовим переходом до open finance. Директива PSD2 запровадила обов’язковий доступ третіх сторін до платіжних рахунків через стандартизовані API та посилену аутентифікацію (SCA), але її імплементація виявила низку прогалин (нерівна якість API, безпека,

роль BigTech). У відповідь Єврокомісія в червні 2023 р. представила пакет PSD3 + Payment Services Regulation (PSR), спрямований на оновлення платіжної рамки, підвищення конкуренції та захисту споживачів. Паралельно запропоновано Regulation on a Framework for Financial Data Access (так званий FiDA / open finance framework), який має розширити обмін даними далеко за межі платіжних рахунків – на страхування, інвестиційні продукти, пенсійні накопичення та кредитні дані, створивши єдиний режим «відповідального доступу» до фінансових даних. Фактично ЄС рухається від галузевого open banking до горизонтальної open finance-екосистеми, де дані стають окремим регульованим активом із чіткими правами та обов’язками для всіх учасників.

У Великій Британії, де історично зародився «еталонний» open banking, стратегія еволюціонує від проєкту, нав’язаного конкурентним регулятором (CMA Order і Open Banking Implementation Entity), до постійної ринкової інституції. Спільний наглядовий комітет JROC (FCA + CMA + HM Treasury + PSR) у 2023–2024 рр. сформував бачення так званої Future Entity – нової структури, яка має підтримувати технічні стандарти API, розвивати інфраструктуру й поступово розширювати сферу відкритих даних від платіжних рахунків до ширшого спектра фінансових продуктів, тобто де-факто рухатися в бік open finance. Британська модель демонструє, як жорстко регульований старт (обов’язкові API для великих банків) із часом трансформується в більш ринково орієнтовану екосистему, де нормативна база забезпечує конкуренцію та інтероперабельність, а бізнес моделі формуються самим ринком [143; 47].

США історично йдуть іншим шляхом – «market-driven APIs» з поступовою додатковою регуляцією. Довгий час відкритому банкінгу передували хаотичний ринок screen-scraping та двосторонніх угод між банками й агрегаторами даних (Plaid, MX тощо): доступ до даних спирався на приватні API та контракти, а не на єдиний законодавчий мандат. Першим кроком до більш регульованої моделі стала реалізація §1033 Закону Dodd-Frank: у жовтні 2024 р. Бюро фінансового захисту споживачів (CFPB) фіналізувало Personal Financial Data Rights Rule, яка встановлює право споживача доступати та ділитися своїми даними (банківські рахунки, картки, мобільні гаманці, платіжні застосунки тощо) через

стандартизовані механізми. Однак уже у 2025 р. правило опинилося під сильним політичним та судовим тиском: суд тимчасово заблокував його застосування, а нове керівництво CFPB ініціювало перезапуск rulemaking із наміром істотно переробити «відкритобанківське» регулювання. Паралельно Visa закрила свій open-banking-підрозділ у США на тлі конфліктів між банками й фінтехами щодо оплати за доступ до даних, що підкреслює: американська модель і далі значною мірою залишається ринково-договірною, з фрагментованими стандартами й сильною роллю окремих корпорацій.

Азійські фінансові центри, зокрема Сінгапур, демонструють більш проактивний «pro-innovation» підхід, поєднуючи гнучке регулювання та активну роль центрального банку як «архітектора екосистеми». Грошово-кредитне управління Сінгапуру (MAS) запустило FinTech Regulatory Sandbox ще у 2016 р., а нині підтримує кілька варіантів sandbox-режимів, які дозволяють фінансовим установам і стартапам тестувати інноваційні продукти в обмеженому середовищі з тимчасовим послабленням окремих вимог. Паралельно MAS активно розвиває стратегію токенизованих фінансів: у 2025 р. оголошено плани пілотувати токенизовані MAS-bills, розширювати використання wholesale-CBDC у міжбанківських операціях і запроваджувати повноцінні правила для стейблкоїнів із 2026 р. Цей підхід поєднує високі стандарти нагляду й захисту споживачів із цілеспрямованим стимулюванням експериментів – від AI-рішень до децентралізованих інфраструктур [119; 132].

Китайська модель цифрових фінансів базується на поєднанні потужних ринкових гравців (BigTech-екосистеми на кшталт Alipay, WeChat Pay) із сильно централізованим державним контролем. Open-banking-подібні рішення тут розвивалися в першу чергу як комерційні інтеграції між банками та платформами електронної комерції, тоді як єдиного всеосяжного закону про відкритий банкінг досі немає – на що прямо вказують дослідження правового режиму open banking у КНР. Натомість НБК (PBOC) та інші регулятори поступово вибудовують рамку цифрового нагляду: у 2023 р. опубліковано Financial Digitalisation Capability Maturity Guidelines із моделлю зрілості цифрових фінансів, а спільні нормативні акти PBOC, NDRC, CSRC та інших регуляторів окреслюють завдання щодо

посилення цифрового нагляду, захисту споживачів і управління ризиками у фінтех-секторі. У результаті формується модель, де інновації великих платформ стимулюються, але дедалі жорсткіше вбудовуються в державну стратегію «керованої цифровізації» фінансової системи.

На цьому тлі Україна стратегічно орієнтується саме на європейсько-британську, а не американську чи китайську траєкторію. Закон «Про платіжні послуги» та комплекс підзаконних актів НБУ, включно з Положенням про відкритий банкінг, створюють PSD2-подібну модель доступу третіх сторін до рахунків через стандартизовані API, а з 1 серпня 2025 р. в Україні офіційно стартував режим open banking, прямо позиціонований як крок до гармонізації з правом ЄС. На відміну від США, де багато чого залишається на рівні приватних угод, українська модель ближча до ЄС/UK: регульовані типи постачальників (AISP/PISP), обов’язкові вимоги до кібербезпеки, довірчих е-послуг і SCA. Водночас, спостерігаючи за європейською дискусією щодо FiDA/open finance, Україна потенційно може «перестрибнути» етап часткових рішень і одразу дизайнувати майбутню open finance-рамку з урахуванням уроків PSD2/PSD3, американського досвіду ринкових API та азійських sandbox-практик.

Для узагальнення підходів різних юрисдикцій до відкритих фінансів у таблиці 2.1 наведено порівняння основних регуляторних рамок і моделей доступу до фінансових даних.

Таблиця 2.1

Порівняння моделей відкритих фінансів у вибраних юрисдикціях

Юрисдикція	Ключові акти / рамки	Тип моделі відкритих даних	Статус open banking / open finance
ЄС	PSD2, пакет PSD3+PSR, проєкт FiDA (open finance framework)	Регуляторно зумовлений open banking із переходом до горизонтального open finance	ОБ діє, OF формується; дані розглядаються як окремий регульований актив
Велика Британія	CMA Order, Open Banking Implementation Entity, JROC, концепція Future Entity	Спочатку жорстко регульований ОБ, далі – ринково орієнтована екосистема під наглядом спільного органу	Перехід від ОБ до ширшого режиму відкритих даних (де-факто open finance)
США	§1033 Dodd-Frank, Personal Financial Data Rights Rule (CFPB)	Market-driven APIs з частковою	Спроба створити єдине правило доступу до даних; у 2025 р. – судові

		регуляторною надбудовою	й політичні блокування, зберігається фрагментація
Сінгапур	Sandbox-режими MAS, рамка токенизованих фінансів, правила для стейблкоїнів	Pro-innovation: sandbox + активна роль центрального банку як «архітектора екосистеми»	Тестування інновацій (AI, DeFi, wholesale-CBDC, стейблкоїни) у контрольованих режимах
Китай	Акти PBOC, NDRC, CSRC; Financial Digitalisation Capability Maturity Guidelines	BigTech-платформи + централізований цифровий нагляд; без єдиного закону про ОБ	Комерційні «open-banking-подібні» інтеграції під посиленням державним контролем
Україна	Закон «Про платіжні послуги», Концепція open banking, Положення про відкритий банкінг НБУ (постанова № 80)	PSD2-подібна модель: регульовані AISP/PISP, стандартизовані API, SCA	З 1.08.2025 – офіційний режим open banking; стратегічна орієнтація на майбутній open finance

Джерело: складено автором за матеріалами [24; 28; 80; 119; 160]

З табл. 2.1 випливає, що Україна свідомо зближається з європейсько-британською моделлю регуляторно зумовленого open banking, отримуючи можливість одразу проектувати майбутню open finance-рамку з урахуванням уроків ЄС (PSD2/PSD3+FiDA), ринково-договірного американського підходу та азійських sandbox-практик.

Регуляторні моделі країн ЄС та Великої Британії демонструють найбільш структурований та формалізований підхід до доступу до фінансових рахунків і даних. У ЄС друга платіжна директива (PSD2) закріпила право третіх сторін – AISP та PISP – на доступ до платіжних рахунків через стандартизовані API, а вимога Strong Customer Authentication (SCA) підвищила рівень захисту кінцевого користувача. Водночас проблемна імплементація PSD2 (неоднорідність API, бар'єри доступу, низька інтероперабельність) стала причиною для реформування підходів: у 2023–2025 рр. Єврокомісія розробила пакет PSD3 + PSR із посиленими правилами для доступу до рахунків і вимогами до якості API, включно з тестовими середовищами, зобов'язанням банків усувати необґрунтовані перешкоди та уніфікованою схемою сертифікації. Одночасно надзвичайно важливим є Regulation on a Framework for Financial Data Access (FiDA), який поширює регуляторну логіку «відкритого доступу» на ширший спектр фінансових даних (страхування, інвестиції, кредити), фактично

створюючи перехід до open finance. Так ЄС формує модель, де доступ до фінансових даних став окремим регульованим правом, а обмін даними – предметом суворих технічних та безпекових вимог [24; 28; 119].

Британська модель відрізняється від європейської тим, що правила формувалися не директивою, а рішенням конкурентного регулятора (UK CMA) та реалізацією через Open Banking Implementation Entity (OBIE). Хоча у 2018–2022 рр. саме OBIE відповідало за стандарти API, порядок доступу та тестові середовища, надалі ініціатива перейшла до спільного наглядового комітету JROC (FCA + CMA + HM Treasury + PSR). Нове бачення передбачає створення постійної Future Open Banking Entity, яка матиме ширший мандат: забезпечення інтероперабельності API, розвиток стандартів, впровадження нових use-cases (variable recurring payments, enhanced data APIs) та поступову інтеграцію принципів open finance. Британська модель, на відміну від ЄС, є більш «практичною» – фокус на стабільності API, тестах відповідності, SLA та схемах оплати за інфраструктуру, що робить її однією з найзрілих у світі за якістю реалізації та ринковим використанням.

США демонструють іншу логіку – «ринкова» модель доступу до даних із поступовим переходом до регуляторного формату. Десятиліттями взаємодія між банками та фінтех-агрегаторами даних (Plaid, Yodlee, MX) базувалася на приватних API та screen-scraping без єдиної правової норми. Зрушення почалося з імплементації §1033 Dodd-Frank Act: у жовтні 2024 р. CFPB фіналізувало Personal Financial Data Rights Rule, яке встановлювало право споживача на доступ і передачу фінансових даних, вимоги до стандартизації API, заборону screen-scraping та критерії для Data Providers і Data Recipients. Проте у 2025 р. реалізацію правила блокував федеральний суд, а CFPB розпочало перезапуск rulemaking, визнавши потребу в більш збалансованій моделі участі банків, фінтехів та BigTech. Дебати у США підкреслюють фундаментальну різницю від ЄС/UK: навіть за наявності законодавчої рамки, американська модель залишається фрагментованою, з домінуванням великих приватних API-платформ та відсутністю централізованої інституції, відповідальної за стандарти API [41; 134; 150].

У країнах Азії підходи до регулювання більш експериментальні та проінноваційні, із центробанками, що виконують роль «архітекторів» технологічних екосистем. У Сінгапурі Грошово-кредитне управління (MAS) запровадило низку режимів Regulatory Sandbox (Sandbox, Sandbox Express, Sandbox Plus), які дозволяють тимчасово пом'якшувати ліцензійні вимоги для інноваційних продуктів і одночасно забезпечувати наглядовий контроль у реальному часі. MAS також активно просуває стандартизацію API через API Playbook, формує правила для стейблкоїнів (з 2026 р.) і пілотує токенозовані MAS-bills та wholesale-CBDC для міжбанківських розрахунків. У Китаї регулятори рухаються у бік централізованої моделі: існує кілька паралельних регуляторів (PBOC, NDRC, CSRC), які формують спільні вимоги до цифрового нагляду, Cyber-security Law та PIPL встановлюють високі бар'єри для передачі даних, а open-banking-подібні рішення розвиваються переважно як комерційні інтеграції між банками й BigTech (Ant Group / Tencent). Нові документи – Digitalisation Capability Maturity Guidelines та «вказівки щодо розвитку якісних цифрових фінансів» – координують вимоги до API, безпеки, тестування та наглядових процедур, формуючи модель «керованої інновації» [42; 138; 139].

Порівняно з провідними моделями, Україна йде шляхом глибокої гармонізації з ЄС/УК. Закон «Про платіжні послуги» та підзаконні акти НБУ щодо відкритого банкінгу наближають українську рамку до PSD2/PSD3: передбачено регульовані API, чіткі ролі AISP/PISP, вимоги до безпеки, SCA, сертифікацію постачальників та обов'язок банків забезпечувати недискримінаційний доступ. НБУ також застосовує елементи SupTech-моделі, готує підходи до RegTech-інтеграції та розвиває вимоги до кібер- та операційної стійкості відповідно до стандартів ЄС (DORA-подібні вимоги до управління ІКТ-ризиками). На відміну від США, українська модель не спирається на приватні договори, а на інтегровану нормативну рамку; а на відміну від Азії – не передбачає широких sandbox-режимів, хоча окремі пілоти Мінцифри та НБУ можуть стати основою для їх розвитку в майбутньому. У перспективі 2–4 років Україна потенційно може запровадити open finance-елементи, використовуючи

досвід ЄС та британського JROC, доповнений азійськими підходами до тестування інновацій.

Цифрове середовище розвинутих країн формується під впливом високих показників проникнення фінтех-послуг та мобільних платежів (рис.2.5). Дані EY Global FinTech Adoption Index показують, що вже у 2019 р. рівень фінтех-адопшену становив: 87 % у Китаї, 71 % у Великій Британії, 67 % у США, а європейські країни Центральної та Північної Європи демонстрували близькі значення – 70–75 %. Хоча звіт не оновлювався після 2019 р., усі подальші регіональні дослідження (включно з оглядами ЄС та даними FCA/UK Finance) підтверджують: частка користувачів, що регулярно застосовують фінтех-застосунки для платежів, бюджетування, кредитування чи інвестування, у цих країнах лише зростає. У Великій Британії понад 90 % дорослого населення використовує цифровий банкінг, а частка транзакцій у цифрових каналах перевищує 80 % усіх роздрібних платежів. У США, за оцінкою Pew Research Center, близько 67 % користувачів здійснюють регулярні банківські операції через мобільні застосунки. Така динаміка формує «платформену нормальність», де fintech-рішення стають базовим каналом доступу до фінансових послуг [36; 121; 122].

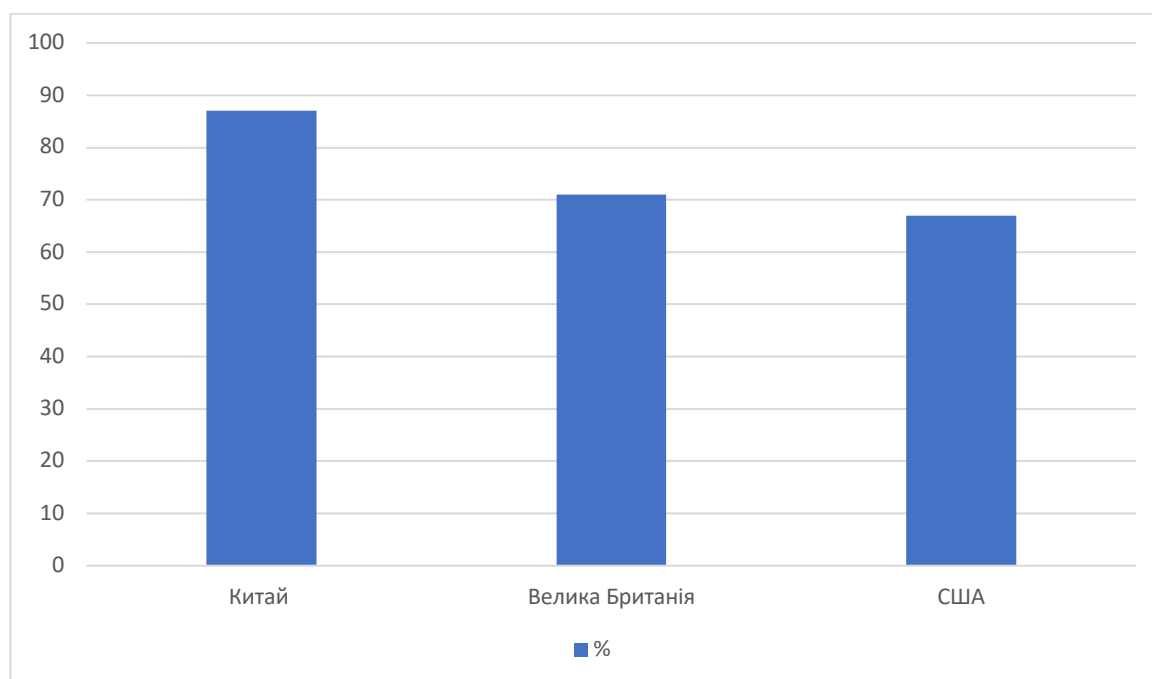


Рис. 2.5 Рівень fintech-adoption у вибраних країнах, %, 2019 р.

Джерело: складено автором за матеріалами [36; 121; 122]

Рівень цифрової готовності інфраструктури також демонструє значний розрив між регіонами. За даними ITU Digital Development Country Profiles, цифрова зрілість країн ЄС та Сінгапуру оцінюється у високих категоріях («advanced»), що означає стабільне покриття якісним мобільним інтернетом 95–99 % населення, високий рівень цифрових компетенцій та активну е-ідентифікацію (eIDAS, SingPass). У США мобільний інтернет охоплює понад 97 % населення, але зберігаються нерівності між штатами, що враховується у стратегіях реформування Federal Communications Commission. У Сінгапурі рівень цифрової готовності практично максимальний: понад 98 % домогосподарств мають широкосмуговий інтернет, держава підтримує екосистему API-платформ, а цифрова ідентифікація SingPass використовується в понад 2 700 сервісах. У Китаї цифрова готовність інфраструктури оцінюється ITU як «high and improving», що відповідає масовій електронній комерції, домінуванню супердодатків (Alipay, WeChat) та централізованій державній стратегії цифровізації [47; 118; 124].

Сегмент миттєвих платежів (instant payments) є найпоказовішим індикатором цифрової динаміки економіки. За глобальним рейтингом ACI Worldwide «Prime Time for Real-Time Payments» (2024), Китай обробив найбільшу кількість миттєвих платежів у світі – 28,1 млрд транзакцій на рік, тоді як Індія утримує абсолютне лідерство у довгостроковій перспективі завдяки системі UPI. У ЄС лідерами впровадження SEPA Instant Payments є Нідерланди, Естонія, Литва та Фінляндія, де понад 90 % кредитових переказів можуть проходити в режимі SCT Inst. У Великій Британії Faster Payments обробляє понад 4,2 млрд операцій на рік (2023), забезпечуючи практично повну покритість банків. Американська система FedNow, запущена у 2023 р., поки працює обмежено: у 2024 р. у ній брали участь близько 400 установ, але кількість транзакцій і обсяг миттєвих операцій ще далекі від рівня ЄС чи Азії. У Сінгапурі система FAST забезпечує майже повний охоплення банків та миттєві P2P/P2B-сценарії, а інтеграція з системами Таїланду й Індії формує біржові коридори для міжнародних миттєвих платежів [52; 100; 117].

Фінансова інклюзія є кінцевим інтегральним індикатором цифрового розвитку. За Global Findex (Світовий банк), у 2021 р. рівень доступу до рахунків становив: 100 % у Данії та Фінляндії, 99 % у Норвегії, 95 % у Великій Британії, 94 % у США та 88 % у Китаї. У Сінгапурі, згідно з даними MAS, доступ до рахунків та цифрових платіжних рішень практично універсальний (≈ 100 %). Водночас зберігається розрив у якості інклюзії: у США близько 4,5 % домогосподарств залишаються *unbanked*, а 14 % – *underbanked*. У ЄС виклики стосуються радше цифрової компетентності та вікових груп 65+, ніж доступу до рахунків. Китай демонструє високу інклюзію завдяки інтеграції фінансів у супердодатки, але тут значною мірою обмежена конкуренція й висока централізованість. Ці відмінності визначають гнучкість ринку: у країнах зі зрілою інфраструктурою (ЄС, UK, SG) цифрові фінансові послуги стали не лише інструментом доступу, а й драйвером інновацій, тоді як у США й Китаї ключовими факторами залишаються ринок API та BigTech-екосистеми [39; 88; 121].

Порівняння з практиками ЄС та Великої Британії показує, що частину інструментів Україна вже практично імплементувала «як є». Запуск відкритого банкінгу з 1 серпня 2025 р. фактично відтворює архітектуру PSD2: Закон «Про платіжні послуги» та Положення про відкритий банкінг закріплюють ролі постачальників послуг з інформації про рахунки та ініціювання платежів, вимоги до API, електронних довірчих послуг і страхування відповідальності, а також принципи безпечного обміну даними на основі згоди користувача. Аналітичні огляди юристів і бізнес-асоціацій прямо вказують, що українська рамка з 1.08.2025 р. узгоджується зі стандартами PSD2 і готує ґрунт для приєднання до SEPA, тобто у сфері доступу до рахунків, SCA, ролей учасників та базових вимог до API Україна може й надалі копіювати європейські рішення майже без модифікацій, фокусуючись на своєчасному прийнятті підзаконних актів та технічній стандартизації.

Водночас навіть у рамках європейського вектору значна частина практик потребує адаптації під воєнний стан, розмір ринку та стан інфраструктури. Стратегія розвитку фінансового сектору до 2025 р. декларує інтеграцію з правом

ЄС і розвиток «відкритої архітектури» ринку, однак її реалізація відбувається в умовах повномасштабної війни, енергетичних атак та обмеженого інвестиційного ресурсу. Якщо для ЄС і Великої Британії пріоритетом у нових актах PSD3/PSR та FiDA є поглиблення конкуренції і розширення переліку відкритих даних, то для України нагальним є поєднання цих підходів із підвищенням кібер- та операційної стійкості (резервні дата-центри, вимоги до безперервності бізнесу, сценарії роботи за відсутності електроенергії). Наприклад, система BankID НБУ у 2024 р. зафіксувала 87,7 млн успішних електронних ідентифікацій (+104 % p/p), що свідчить про дуже високий рівень цифрової інклюзії, але одночасно різко підвищує критичність цієї інфраструктури та вимоги до її захисту в умовах воєнних ризиків. Отже, пряме копіювання норм ЄС щодо відкритого доступу до даних без «українізації» операційних та кібер-вимог могло б посилити вразливість фінансової системи [111; 160; 171].

Практики регуляторних «пісочниць» і стимулювання інновацій, які демонструє, зокрема, Сінгапур, для України радше слід сприймати як модель для адаптації, а не прямого перенесення. MAS sandbox побудована на припущенні високої інституційної спроможності регулятора, стабільності ринку та наявності великого пулу приватного капіталу; учасникам тимчасово пом'якшуються окремі вимоги, але вони проходять інтенсивний супервізійний супровід, а успішні кейси масштабуються. Українські дослідження fintech-індустрії фіксують інший контекст: ключовими викликами залишаються регуляторна невизначеність, кіберризик, дефіцит фінансових ресурсів і кваліфікованих кадрів, тоді як попит на цифрові послуги та інтеграція з міжнародними ринками є драйверами зростання. Це означає, що українська «пісочниця», якщо її розвивати, має бути жорсткіше сфокусована на пріоритетних напрямках (платежі, RegTech, кібербезпека, AI-скоринг), поєднувати регуляторні послаблення з грантовою/донорською підтримкою та тісною координацією між НБУ, Мінцифрою та донорами, а не просто відтворювати азійську конфігурацію.

Досвід США та Китаю в частині ринково-договірних API та домінування BigTech-екосистем практично неможливо перенести в Україну «як є» без ризику

структурних дисбалансів. Американська модель спирається на велику кількість приватних угод між банками й агрегаторами даних, наднаціональний вплив корпорацій та розвинений ринок венчурного капіталу; китайська – на гігантські екосистеми Alipay/WeChat Pay під щільним державним контролем. Для українського ринку, що одночасно орієнтується на європейське право та відновлення після війни, пріоритетом є уникнути надмірної концентрації даних і ринкової влади в окремих приватних гравців та зберегти керованість процесу цифровізації. На це прямо вказують як наукові публікації про перспективи й виклики fintech-індустрії України, так і праці, присвячені порівняльному аналізу регулювання відкритого банкінгу з правом ЄС: автори наголошують, що імплементація відкритого банкінгу має відбуватися з урахуванням воєнного стану, рівня фінансової грамотності, цифрової нерівності та обмежень на стороні регуляторних інституцій. У цьому сенсі для України «як є» можна запозичувати європейські стандарти захисту споживачів, кіберстійкості, управління даними та фінансової інклюзії, але бізнес-моделі (масштабні супердодатки, агресивні BNPL, необмежений AI-скоринг) та інструменти стимулювання інновацій повинні проходити глибоку адаптацію до локальних ризиків, цілей відбудови та курсу на вступ до ЄС.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА НАПРЯМИ УДОСКОНАЛЕННЯ РОЗВИТКУ ЦИФРОВИХ ФІНАНСОВИХ ПОСЛУГ В УКРАЇНІ

3.1. Стратегічні пріоритети розвитку цифрових фінансових послуг в Україні

Візія розвитку цифрових фінансових послуг України до 2030 року полягає у формуванні відкритої, інклюзивної та стійкої фінансової екосистеми, у якій цифрові сервіси виступають не додатковим каналом, а базовим форматом взаємодії домогосподарств, бізнесу та держави. До цього часу цифрові фінансові послуги мають забезпечувати безшовний доступ до платежів, заощаджень, кредитування, страхування та інвестицій незалежно від місця проживання, типу пристрою чи рівня доходу користувача. Така візія передбачає не лише технологічне оновлення сектору, а й глибинну трансформацію бізнес-моделей, регулювання та поведінки учасників ринку.

Ключовим стратегічним орієнтиром є фінансова інклюзія, що розуміється як фактична можливість користувачів активно та безпечно застосовувати цифрові сервіси для повсякденних потреб. До 2030 року пріоритетом має стати зменшення «цифрового розриву» між міськими та сільськими територіями, молодшими та старшими віковими групами, а також підвищення доступності ЦФП для МСП та вразливих категорій населення. Це передбачає масштабування віддаленої ідентифікації, розвиток простих за дизайном і тарифами продуктів, а також системну підтримку цифрової та фінансової грамотності, що інтегрується в державні та освітні програми.

Другим блоком візії є посилення конкуренції та інноваційності фінансового сектору. До 2030 року цифрова інфраструктура (миттєві платежі, стандартизовані API, відкриті дані) має забезпечувати рівні умови доступу до ринку для банків, небанківських установ, фінтех-компаній та BigTech-платформ. Цілями виступають скорочення time-to-market для нових цифрових продуктів, зростання частки операцій, що здійснюються в повністю автоматизованому режимі (STP), та розвиток моделей open finance і embedded finance. Розширення конкуренції має супроводжуватися стимулюванням

експериментів у контрольованих режимах (пісочниці, пілоти) та підтримкою стартап-екосистеми через регуляторні, податкові й інвестиційні стимули [111; 152; 171].

Нарешті, візія до 2030 року неможлива без пріоритету безпеки (див. табл. 3.1.), операційної витривалості та довіри. Цифрові фінансові послуги мають розвиватися на основі принципів кіберстійкості, управління ризиками третіх сторін, захисту даних і прозорого використання алгоритмів, зокрема за участю штучного інтелекту. Стратегічними цілями є гармонізація вимог із DORA-подібними підходами, поступове запровадження risk-based нагляду за цифровими сервісами та підвищення рівня сприйнятої довіри користувачів до ЦФП. Довіра виступає інтегральним показником успішності візії: саме відчуття прозорості, передбачуваності та справедливості цифрових продуктів визначатиме глибину й сталість їх використання в економіці.

Таблиця 3.1

Вимір візії	Ціль до 2030 року	Основні завдання / напрями реалізації
Фінансова інклюзія	Цифрові фінпослуги доступні та безпечні для домогосподарств, МСП і вразливих груп незалежно від місця проживання та доходу	Зменшення цифрового розриву «місто–село»; масштабування дистанційної ідентифікації; прості продукти за дизайном і тарифами; інтеграція digital/financial literacy у держта освітні програми
Конкуренція та інновації	Відкрита й конкурентна екосистема, де цифрові сервіси є основним каналом і драйвером інновацій	Розвиток миттєвих платежів і стандартизованих API; запуск та розвиток open finance і embedded finance; скорочення time-to-market; підтримка стартап-екосистеми та sandbox/pilot-режимів
Безпека, операційна витривалість і довіра	Високий рівень кіберстійкості та прозорості, що забезпечує стійку довіру користувачів до ЦФП	Гармонізація з DORA-подібними вимогами; risk-based нагляд за цифровими сервісами; управління ризиками третіх сторін; захист даних і відповідальне використання алгоритмів (у т.ч. ШІ); підвищення сприйнятої довіри клієнтів

Джерело: складено автором за матеріалами [95; 98; 111; 152; 160; 171]

Першим пріоритетним напрямом виступає подальший розвиток миттєвих платежів 24/7 як базової «транспортної мережі» для цифрових фінансових послуг. До 2030 року інстант-платежі мають стати стандартом для розрахунків між фізичними особами, бізнесом і державою, інтегрованим у мобільні

застосунки банків, платіжні сервіси, маркетплейси та державні платформи. Це вимагає розширення функціоналу платіжної інфраструктури (адресні платежі за номером телефону, e-mail, ID, QR-коди), високої доступності сервісів (SLA на рівні 99,9 % і вище) та уніфікації схем тарифоутворення. Миттєві платежі виступають не лише зручним інструментом для користувача, а й критично важливою передумовою для масштабування open finance та embedded-моделей.

Другим стратегічним вектором є формування повноцінної моделі Open Finance, яка виходить за межі класичного open banking. Йдеться про створення екосистеми відкритого доступу до фінансових і суміжних даних (рахунки, кредити, страхові продукти, інвестиційні портфелі, пенсійні накопичення) на основі стандартизованих API та чітко визначених режимів згоди користувача. До 2030 року пріоритетами мають стати: запровадження єдиних технічних стандартів API; розвиток ринку TPR-провайдерів (постачальників платіжних та інформаційних послуг); побудова прозорих моделей розподілу відповідальності та ризиків між учасниками. Це дасть змогу створювати персоналізовані фінансові сервіси, сервіси фінансового планування, агрегатори рахунків і платформні рішення для МСП.

Третій пріоритет пов'язаний із масовим впровадженням цифрової ідентичності та ID-гаманців як ядра взаємодії користувача з фінансовою екосистемою. Цифровий ID має забезпечувати уніфіковану схему KYC/AML, електронний підпис, зберігання цифрових документів та сертифікатів, а також керування згодами на обробку даних. ID-гаманець, у свою чергу, повинен стати інтерфейсом не лише для документів, а й для токенизованих активів, платіжних інструментів, страхових полісів, доступу до пільг і соціальних програм. Пріоритетами до 2030 року є взаємосумісність державних і комерційних рішень, висока стійкість до кібератак та інтеграція цифрового ID в ключові фінансові й нефінансові процеси (кредитування, страхування, e-commerce, публічні послуги) [95; 98].

Четвертим ключовим напрямом виступає розвиток embedded finance для МСП, коли фінансові послуги вбудовуються безпосередньо в бізнес-процеси та цифрові платформи підприємств. До 2030 року вектором має стати зміщення від

традиційної моделі «клієнт - банк» до моделі «послуга в моменті потреби»: кредитування в точці продажу, інтегровані факторингові й страхові продукти в системах обліку, платіжні та касові рішення, вбудовані в CRM/ERP та маркетплейси. Це потребує розвитку партнерств між банками, небанківськими фінустановами, фінтех-платформами та провайдерами бізнес-ПЗ, а також адаптації регулювання під моделі «Banking-as-a-Service» і «Finance-as-a-Feature». Для МСП це означатиме спрощений доступ до фінансування, зниження транзакційних витрат і можливість масштабувати діяльність у цифровому середовищі.

Реалізація стратегічних пріоритетів розвитку цифрових фінансових послуг до 2030 року неможлива без чітко структурованої дорожньої карти, яка задає послідовність кроків, відповідальних інституцій та очікувані результати на кожному етапі. Така карта має включати короткостроковий горизонт (1–2 роки) з фокусом на нормативні зміни, запуск пілотів та базових інфраструктурних рішень; середньостроковий (3–5 років) – масштабування успішних моделей, поширення стандартів та інтеграцію систем; а також довгостроковий (до 2030 року) – повноцінну імплементацію open finance, розвиток embedded-моделей та стійкої екосистеми цифрових талантів. Дорожня карта має бути інтегрована з національними стратегіями цифрової економіки, фінансової інклюзії та євроінтеграційними зобов'язаннями.

Для узагальнення стратегічного бачення розвитку цифрових фінансових послуг до 2030 року доцільно виділити ключові пріоритети, очікувані результати та індикатори їх досягнення (табл. 3.2).

Таблиця 3.2

Стратегічні пріоритети та індикатори реалізації до 2030 року

Стратегічний пріоритет	Результат до 2030 р.	Ключові індикатори
Миттєві платежі 24/7	Instant-платежі як стандарт для P2P, P2B, G2P	Частка інстант-платежів; середній час виконання; uptime; STP-rate у платежах
Open Finance	Повноцінна екосистема відкритих фінансових даних та TPP	Кількість/частка активних TPP; обсяг операцій через API; час підключення до API

Цифрова ідентичність та ID-гаманець	Єдиний цифровий ID як базовий інтерфейс для фінансових і держпослуг	Кількість користувачів ID / ID-гаманця; частка операцій з eKYC; кількість інтегрованих сервісів
Embedded finance для МСП	Фінансові послуги вбудовані у ключові бізнес-процеси МСП	Частка МСП, що користуються embedded-рішеннями; обсяг фінансування через embedded-канали
Партнерства та PPP-інфраструктура	Спільно розвинута базова інфраструктура ЦФП	Кількість PPP-проектів; охоплення спільними сервісами; зниження дублювання інвестицій
Екосистема талантів	Стійкий «кадровий контур» для цифрових фінансів	Кількість випускників і сертифікованих фахівців; рівень закриття критичних вакансій

Джерело: складено автором за матеріалами [95; 98; 111; 160; 161; 152]

Для оцінки прогресу впровадження цієї дорожньої карти необхідно сформувати систему ключових показників ефективності (KPI), що відображатимуть не лише формальне прийняття рішень, а їхній реальний вплив на ринок та користувачів. Одним із базових індикаторів виступає STP-rate (Straight-Through Processing rate) – частка транзакцій і процесів, які виконуються повністю автоматизовано, без ручного втручання. Зростання STP-rate у платежах, кредитуванні, відкритті рахунків та онбордингу клієнтів свідчатиме про реальну цифрову трансформацію, а не про поверхневу автоматизацію окремих етапів.

Другий клас показників пов'язаний із динамікою впровадження інновацій, насамперед через time-to-market цифрових продуктів та cost-to-income у контексті ЦФП. Скорочення time-to-market демонструє, наскільки регуляторне середовище, інфраструктура, стандарти даних і внутрішні процеси фінансових установ дозволяють швидко виводити на ринок нові сервіси (наприклад, модулі миттєвих платежів, open API, цифрові кредити). Зниження cost-to-income для цифрових каналів сигналізує про підвищення операційної ефективності та робить можливими моделі з нижчими тарифами для кінцевого користувача, зберігаючи при цьому стійку дохідність для постачальників послуг.

Третя група KPI орієнтована на користувацький досвід та реальне використання цифрових продуктів. Тут ключову роль відіграють NPS (Net Promoter Score) як інтегральний індикатор задоволеності й лояльності клієнтів та DAU/MAU (Daily Active Users / Monthly Active Users) як показники активності

й залученості користувачів у цифрових каналах. Зростання DAU/MAU у поєднанні з позитивною динамікою NPS свідчить про те, що цифрові рішення є не лише доступними, а й зручними та цінними для клієнта. Вбудування цих показників у систему моніторингу на рівні регулятора і учасників ринку дає змогу оперативно коригувати дорожню карту, фокусуючись на тих ініціативах, які справді змінюють поведінку користувачів та структуру ринку.

Досягнення стратегічних цілей розвитку цифрових фінансових послуг до 2030 року потребує переходу від фрагментарних ініціатив окремих гравців до системних партнерств, у яких держава, регулятори, фінансовий сектор і технологічні компанії виступають співтворцями спільної інфраструктури. Ключовим інструментом тут є моделі публічно-приватного партнерства (PPP), що дозволяють поєднати нормативний мандат і довіру до державних інституцій із гнучкістю, технологічною експертизою та інвестиційним потенціалом приватного сектору. У форматі PPP можуть розвиватися платформи миттєвих платежів, стандартизовані API-шлюзи, спільні KYC/AML-рішення, центри обміну кіберінформацією та інші елементи базової інфраструктури ЦФП [95; 160].

У межах таких партнерств банки зберігають роль системних фінансових посередників і носіїв ліцензійних функцій, фінтех-компанії виступають драйверами інноваційних моделей (open banking, embedded finance, neobanking), а інфраструктурні провайдери (платіжні системи, процесингові центри, хмарні та телеком-оператори) забезпечують безперервність і масштабованість сервісів. Оптимальною є модель, коли регулятор задає рамкові правила гри та стандарти безпеки, а учасники ринку через PPP-проекти спільно реалізують конкретні цифрові рішення. Це скорочує дублювання інвестицій, пришвидшує створення стандартизованих рішень та зменшує бар'єри входу для малих гравців.

Окрему, недооцінену в багатьох юрисдикціях, але критично важливу для України роль відіграють академічне середовище та індустріяльні асоціації. Університети та науково-дослідні центри мають виступати не лише «постачальниками» кадрів, а й партнерами в аналітиці, моделюванні регуляторних змін, тестуванні нових підходів до оцінки ризиків, ESG-

компонентів, поведінки користувачів. Спільні лабораторії (labs), магістерські програми з FinTech/RegTech/SupTech, інкубатори стартапів при університетах можуть стати інструментом системного апскілла та генерації інновацій, що напряду підживлюють розвиток цифрових фінпослуг.

Індустрійні асоціації (банківські, фінтех, платіжні, страхові тощо) виступають каналом самоорганізації ринку й важливим контрагентом для регулятора у формуванні політики. Через робочі групи, спільні стандарти, кодекси практик і консультації вони здатні агрегувати позиції учасників, виявляти регуляторні «вузькі місця», пропонувати узгоджені технічні та правові рішення. Для реалізації візії до 2030 року доцільно інституціоналізувати формат постійних тристоронніх платформ «регулятор – ринок – академія», що забезпечуватимуть безперервний діалог, спільне формування дорожньої карти ЦФП та регулярний перегляд її КРІ з урахуванням технологічної динаміки та євроінтеграційних зобов'язань України.

Стратегічний розвиток цифрових фінансових послуг до 2030 року неможливий без цілісної екосистеми талантів, яка забезпечує постійне відтворення та оновлення компетенцій у секторі. Йдеться не лише про підготовку окремих фахівців, а про формування стійкого «кадрового контуру», де формальна освіта, корпоративне навчання, професійні сертифікації й участь у проєктах створюють безперервний ланцюг розвитку знань і навичок. Візія передбачає, що до 2030 року базове розуміння цифрових фінансових сервісів, ризиків та можливостей стане стандартом для економістів, фінансистів, менеджерів, а спеціалізовані цифрові компетенції – ядром для нових професійних ролей у фінансовому секторі [96; 159].

Ключовим елементом екосистеми є модернізація освітніх програм на рівні університетів і професійної освіти. Програми з фінансів, банківської справи, страхування, економіки мають системно інтегрувати модулі з FinTech, цифрових платформ, регулювання цифрових фінансових ринків, open finance, цифрових валют центральних банків, RegTech/SupTech. Паралельно необхідне оновлення змісту ІТ-освіти з урахуванням специфіки фінансового сектору: робота з чутливими даними, вимоги нагляду, моделювання ризиків, кіберзагрози.

Важливо, щоб такі програми розроблялися у співпраці з регуляторами та ринком, відображаючи реальну практику та очікування роботодавців.

Другий блок стосується розвитку системи професійних сертифікацій та апскілли для діючих фахівців. Для кадрів фінансових установ, регуляторів, інфраструктурних провайдерів необхідно запроваджувати спеціалізовані сертифікаційні треки з напрямів: кібербезпека фінансових сервісів, управління даними (data governance, data analytics), управління цифровими продуктами (product management), UX/UI у фінансах, а також регуляторний комплаєнс у цифровому середовищі. Такі програми можуть реалізовуватися на базі університетів, бізнес-шкіл, галузевих центрів компетенцій і самих фінансових груп. Апскілл і рескілл мають бути не разовою ініціативою, а постійним елементом HR-стратегії, підтриманим як внутрішніми ресурсами, так і стимулюючими політиками держави.

Третім виміром є формування критичної маси фахівців у кібербезпеці, роботі з даними та продукт-менеджменті— сферах, де наразі спостерігається найбільший дефіцит. Для кібербезпеки це означає підготовку спеціалістів, здатних працювати з DORA-подібними вимогами, тестуванням операційної витривалості, керуванням ризиками третіх сторін, побудовою SOC-центрів для фінансових груп. У сфері даних потрібні фахівці з аналітики, машинного навчання, управління якістю даних, які можуть розробляти скорингові моделі, персоналізовані пропозиції, системи виявлення шахрайства. Продукт-менеджери мають володіти як фінансовим, так і технологічним мисленням, відповідати за повний життєвий цикл цифрового продукту: від гіпотези й дизайну до вимірювання KPI та масштабування.

Завершальним елементом побудови екосистеми талантів є створення платформ взаємодії між освітою, ринком і державою: галузеві консорціуми, спільні лабораторії, хакатони, акселераційні програми для студентів і молодих фахівців, стажування в регуляторах і фінансових установах. Такі інструменти дозволяють забезпечити швидкий обмін знаннями, валідацію навчальних програм практикою та ранній вхід молодих спеціалістів у сектор цифрових фінансових послуг. У результаті до 2030 року кадрова екосистема має

стати одним із головних факторів конкурентоспроможності України на мапі глобального фінтеху, забезпечуючи не лише підтримку поточних сервісів, а й здатність генерувати й масштабувати нові моделі цифрових фінансів.

3.2. Підвищення ефективності регулювання та впровадження інновацій у сфері цифрових фінансових послуг

Системне підвищення ефективності регулювання цифрових фінансових послуг вимагає переходу від фрагментованих IT-рішень регулятора до єдиної RegTech/SupTech-платформи, яка поєднує збір, зберігання й аналітику даних для наглядових цілей. RegTech у цьому контексті забезпечує інструменти для фінансових установ, що автоматизують виконання регуляторних вимог (звітність, KYC/AML, управління ризиками), тоді як SupTech фокусується на цифровізації процесів самого нагляду – від ліцензування і звітності до моніторингу ринкової поведінки та споживчого захисту. Така платформа стає «цифровим ядром» взаємодії між регулятором і ринком, дозволяючи перейти від повільних, шаблонних форм звітності до гнучкого, даних-орієнтованого, проактивного нагляду [109; 121].

Базовою передумовою для функціонування RegTech/SupTech-платформи є впровадження єдиних форматів даних і стандартів звітності (див. табл. 3.3) . Йдеться про поступову відмову від розрізнених табличних шаблонів на користь уніфікованих, машинозчитуваних структур (granular data), які дозволяють збирати інформацію на рівні окремих транзакцій, договорів, клієнтських профілів. Узгоджені формати, схеми довідників, єдині ідентифікатори суб'єктів і продуктів, а також централізовані «data lakes» регулятора зменшують дублювання звітності, знижують витрати учасників ринку та підвищують якість даних. Для України це означає побудову архітектури, у якій дані подаються один раз у стандартизованому вигляді й надалі використовуються для різних наглядових, статистичних та аналітичних задач.

Наступний компонент – real-time або near real-time моніторинг, який радикально змінює можливості нагляду за цифровими фінансовими послугами. SupTech-рішення дозволяють регулятору отримувати потоки операційних даних

від платіжних систем, банків, небанківських установ, провайдерів інноваційних сервісів, автоматично їх очищувати, агрегувати та візуалізувати у вигляді дашбордів і карт ризиків. Використання аналітичних модулів, включно з методами машинного навчання, дає змогу переходити від ретроспективного аналізу до раннього виявлення аномалій (аномальні патерни транзакцій, концентрація ризику, підозріла поведінка постачальників послуг, сплески скарг споживачів). Такий підхід підсилює фінансову стабільність і споживчий захист, особливо в умовах стрімкого росту цифрових каналів.

Таблиця 3.3

Компоненти RegTech/SupTech-платформи та їх ефекти

Компонент	Що це означає	Основні інструменти	Ефект для регулятора	Ефект для учасників ринку
RegTech для установ	Автоматизація виконання вимог (звітність, KYC/AML, ризики)	Reg-reporting модулі, KYC/AML-платформи, risk-engines	Якісніші, швидші дані, менше помилок	Менше ручної роботи, нижчі витрати комплаєнсу, прозорість вимог
SupTech	Цифровізація процесів нагляду	Портали звітності, аналітичні дашборди, ML-модулі	Перехід до risk-based та проактивного нагляду	Більш прогнозований, даних-орієнтований нагляд
Granular-дані і стандарти	Єдині формати даних, ідентифікатори, data lakes регулятора	XBRL/ін. формати, каталоги довідників, єдині ID продуктів	Крос-секційна аналітика, менше дублювання, краща якість даних	«Подати один раз» – використання для кількох регуляторних та статистичних цілей
Real-time / near real-time моніторинг	Потоки даних і онлайн-дашборди ризиків	Потокові інтеграції, тригери аномалій, карти ризиків	Раннє виявлення проблем, стресових патернів	Менше «раптових» перевірок, зрозумілі критерії ризиків

Джерело: складено автором за матеріалами [109; 113; 121; 136]

На основі уніфікованих даних і можливостей оперативного моніторингу реалізується risk-based модель нагляду як ключовий принцип регулювання інновацій. RegTech/SupTech-платформа дозволяє формувати для кожної установи та окремих типів продуктів профілі ризику, які враховують фінансові показники, операційні інциденти, кіберподії, поведінку клієнтів, результати стрес-тестів і патерни скарг. Це дає змогу пріоритизувати наглядові ресурси:

поглиблені інспекції та стрес-тести зосереджуються на високоризикових гравцях і продуктах, тоді як для низькоризикових, але інноваційних моделей (фінтех-стартапи, sandbox-проекти, провайдери open finance) застосовується пропорційний, полегшений режим, орієнтований на превентивний контроль, а не на «каральний» підхід. У результаті risk-based нагляд, технічно підтриманий SupTech, стає не бар'єром для інновацій, а рамкою їхнього безпечного та контрольованого розвитку.

Одним із ключових інструментів підвищення ефективності регулювання цифрових фінансових послуг є регуляторні пісочниці та пов'язані з ними інноваційні хаби. Регуляторна пісочниця – це контрольоване, обмежене в часі середовище, у якому фінтех-компанії та фінансові установи можуть тестувати нові продукти з частковим пом'якшенням або адаптацією вимог за умови посиленого нагляду з боку регулятора. Світовий банк та інші міжнародні інституції трактують пісочниці як спосіб збалансувати цілі інновацій, конкуренції та споживчого захисту, особливо в країнах, що розвиваються, де традиційні регуляторні рамки часто не встигають за технологічними змінами [45; 96].

Функціонування пісочниць органічно поєднується з принципом пропорційності регулювання, коли рівень регуляторного навантаження коригується відповідно до масштабів, складності та ризиковості конкретної діяльності. Міжнародні рекомендації пропонують застосовувати пропорційність як загальний підхід до інноваційних фінтех-моделей, зокрема мікропровайдерів, платформ peer-to-peer, інноваційних платіжних сервісів: регуляторні вимоги можуть бути спрощені на етапі тестування, за умови обмеженого кола клієнтів, лімітів операцій та чітких механізмів виходу з пісочниці. Такий режим дозволяє зменшити бар'єри входу для стартапів, одночасно зберігаючи контроль над ключовими ризиками для споживачів та фінансової стабільності.

Другим критичним елементом є формування спеціального регуляторного режиму для API-провайдерів та third-party providers (TPP) в екосистемі open banking / open finance. Європейська модель PSD2 запровадила категорії

постачальників платіжних ініціаційних та інформаційних послуг (PISP/AISP), для яких передбачено окремі вимоги до ліцензування, безпеки та доступу до рахунків через стандартизовані інтерфейси, а банки зобов'язані забезпечити безпечні канали комунікації з такими учасниками. Для України аналогічні підходи імплементуються через законодавство про платіжні послуги та регулювання open banking, де НБУ встановлює вимоги до ідентифікації та сертифікації TPP, безперервного доступу до рахунків і публікації технічної документації API. Це створює прозорі правила гри для нових гравців і зменшує правову невизначеність для банків як власників рахунків.

З режимом для TPP безпосередньо пов'язане стимулювання відкритих технічних стандартів, насамперед стандартів API. Приклади Великої Британії та ЄС демонструють, що централізовано розроблені Open Banking API Specifications, які охоплюють питання ідентифікації, безпеки, структури даних та сценаріїв використання, значно знижують транзакційні витрати інтеграції та підвищують інтероперабельність між учасниками ринку. Для України стратегічним завданням є гармонізація національних стандартів відкритих інтерфейсів із європейськими підходами, що закріплені у регуляції НБУ щодо open banking, та підтримка галузевих ініціатив (API-хаби, профільні асоціації), які можуть розробляти рекомендації й best practices. Це дозволить уникнути «зоопарку» несумісних рішень, прискорити розвиток open finance і створити передумови для масштабування вітчизняних фінтех-рішень на зовнішні ринки.

Розвиток цифрових фінансових послуг неминуче підвищує залежність фінансового сектору від ІКТ-інфраструктури, що робить операційну витривалість (digital operational resilience) одним із ключових вимірів регулювання. У ЄС цю рамку кодифіковано в Регламенті DORA (Digital Operational Resilience Act), який встановлює єдині вимоги до управління ІКТ-ризиками, інцидент-менеджменту, тестування стійкості та управління ризиками критичних ІКТ-провайдерів для всіх фінансових установ. Для України, яка рухається в напрямі євроінтеграції, гармонізація підходів до операційної витривалості з DORA-подібними вимогами є не лише зобов'язанням з точки зору

імплементції *acquis* ЄС, але й практичною передумовою стабільності цифрових фінансових сервісів у умовах зростаючих кіберзагроз [43; 111].

Гармонізація з DORA означає системне посилення рамки управління ІКТ-ризиками на рівні фінансових установ і регулятора. Регламент вимагає від суб'єктів фінансового ринку наявності інтегрованої політики ІКТ-ризиків, чітких ролей та відповідальності, інвентаризації критичних функцій і пов'язаних із ними ІКТ-активів, впровадження процесів виявлення, реагування та відновлення після інцидентів. Для НБУ та інших регуляторів це означає потребу адаптувати власні наглядові керівництва й методики до стандартів DORA, як це вже робить Європейський банківський орган (ЕБА), оновлюючи свої настанови з ІКТ- та безпекових ризиків у світлі набрання чинності DORA. На практиці це дозволяє уникнути фрагментації вимог, забезпечити взаємне визнання результатів тестування та зменшити регуляторне навантаження для установ, що працюють у кількох юрисдикціях.

Другим структурним елементом операційної витривалості є регулярне тестування кіберстійкості. DORA формалізує підхід до цифрового операційного тестування: від внутрішнього тестування безпеки та планів безперервності до більш просунутих форм *threat-led penetration testing* (TLPT), коли сценарії атак наближаються до реальних загроз. Для українського фінансового сектору імплементція DORA-подібних вимог означає встановлення обов'язкових мінімальних стандартів щодо частоти, глибини та периметра тестувань, інтеграцію результатів тестів у процес управління ризиками, а також координацію з національними центрами кібербезпеки та CERT/CSIRT-структурами. Для *digital-first* установ і фінтех-компаній це створює стимули інвестувати в побудову зрілих процесів *secure-by-design* і регулярного «стрес-тестування» своїх платформ.

Третій критично важливий вимір операційної витривалості пов'язаний з управлінням ризиками третіх сторін (*third-party / ICT third-party risk*). DORA прямо визнає, що концентрована залежність фінансових установ від обмеженої кількості ІКТ-провайдерів (зокрема хмарних) створює системні ризики, і запроваджує окремий наглядовий режим для критичних постачальників ІКТ-

послуг та суворі вимоги до управління їхнім ризиком. Для фінансових установ це означає необхідність комплексного due diligence постачальників, включно з оцінкою їх кіберзахищеності, планів безперервності, відповідності стандартам, переддоговірному аналізу та постійного моніторингу. Контракти з ІКТ-вендорами мають містити чіткі положення щодо SLA, управління інцидентами, права аудиту, умов субпідряду та exit-стратегій на випадок припинення співпраці. Для України адаптація цих підходів потребує оновлення настанов із аутсорсингу та ІКТ-ризиків для банків і небанківських фінансових установ, визначення критеріїв «критичності» ІКТ-провайдерів та посилення координації між фінансовими регуляторами й органами, відповідальними за кібербезпеку.

У підсумку, операційна витривалість у цифровій фінансовій екосистемі має розглядатися як безперервний цикл, що поєднує гармонізовані з DORA вимоги до управління ІКТ-ризиками, системне тестування кіберстійкості та зріле управління third-party risk. Побудова такої системи дозволяє не лише реагувати на окремі інциденти, а й запобігати їх ескалації до рівня системних криз, підтримуючи довіру користувачів до цифрових фінансових послуг та інтеграцію України до єдиного європейського фінансового простору.

Етичний вимір регулювання цифрових фінансових послуг дедалі більше зосереджується навколо того, як саме збираються, обробляються й використовуються дані, особливо в умовах масової цифровізації та застосування алгоритмів ШІ. Базовим принципом для фінансових установ стає підхід data protection / privacy by design and by default, закріплений у GDPR: захист даних має бути інтегрований у продукт з етапу проєктування, а за замовчуванням обробляється мінімально необхідний обсяг персональної інформації, із обмеженим доступом і строками зберігання. Для цифрових фінансових сервісів це означає, що архітектура продукту, UX-рішення, логіка роботи бекенду, журналювання операцій та управління згодами клієнтів повинні спочатку проходити «фільтр» захисту даних, а не коригуватися постфактум у відповідь на інциденти або санкції регулятора [28; 151].

У цьому контексті важливу роль відіграють privacy-enhancing technologies (PETs) – технологічні рішення, що дозволяють аналізувати й обмінюватися

даними між суб'єктами ринку без розкриття повної персональної інформації. OECD визначає PETs як інструменти, які уможливають збір і використання даних із збереженням конфіденційності, доповнюючи правові рамки захисту приватності. До таких технологій належать, зокрема, багатосторонні обчислення, гомоморфне шифрування, zero-knowledge proofs, федеративне навчання тощо; їх застосовують для виявлення шахрайства, спільного скорингу, аналізу транзакційних патернів у кількох банках без прямого обміну сирими даними. Для України інтеграція PETs у регуляторні підходи дає змогу одночасно розширювати використання даних у фінансовій аналітиці й зменшувати ризики порушення приватності.

Наступний рівень етичного виміру – це AI-governance, тобто система політик, процедур та інституційних ролей, які забезпечують відповідальне використання штучного інтелекту у фінансових продуктах. Сучасні огляди підкреслюють, що відповідальний ШІ включає набір принципів – прозорість, пояснюваність, підзвітність, справедливість, людський нагляд, безпека й надійність – які мають бути формалізовані у внутрішніх стандартах компаній і наглядових очікуваннях регулятора. На рівні ЄС це доповнюється AI Act, який вводить ризик-орієнтований підхід до систем ШІ, класифікуючи їх за рівнем ризику та встановлюючи посилені вимоги до «систем високого ризику», зокрема кредитного скорингу та оцінки кредитоспроможності фізичних осіб. Для України це означає необхідність синхронізувати майбутні вимоги до ШІ у фінансах із європейськими рамками, включаючи обов'язкову документацію моделей, прозорість критеріїв прийняття рішень, механізми human-in-the-loop та внутрішні комітети з етики даних.

Особливе значення у фінансовому секторі має аудит алгоритмів і запобігання дискримінації. Кредитні, страхові та аналітичні моделі, побудовані на основі ШІ, можуть ненавмисно відтворювати або посилювати упередження, закладені в даних (за віком, статтю, регіоном, соціально-економічним статусом тощо). Європейський парламент у своїх аналітичних матеріалах щодо AI Act і GDPR наголошує, що боротьба з дискримінацією потребує обробки певних «чутливих» категорій даних для виявлення й корекції упередженості, але така

обробка має відбуватися в чітких правових рамках із посиленими гарантіями безпеки. Практика фінансового сектору поступово рухається до впровадження систематичних bias- та fairness-тестів кредитних моделей, що включають оцінку впливу на різні групи населення, незалежну валідацію, періодичний перегляд параметрів та документування рішень щодо балансування між точністю й справедливістю. Для України адаптація таких підходів до національного контексту (антидискримінаційне законодавство, захист прав споживачів фінпослуг, вимоги НБУ) має стати невід’ємною частиною стратегії розвитку цифрових фінансових послуг, підсилюючи довіру до нових технологій з боку суспільства.

Модель оцінки впливу регуляторних змін у сфері цифрових фінансових послуг має спиратися на підхід Regulatory Impact Assessment (RIA) як стандарт «розумного регулювання». У міжнародній практиці RIA розглядається як структурований процес, який щонайменше включає: визначення проблеми, постановку цілей, опис регуляторної пропозиції, аналіз альтернатив (включаючи нерегуляторні), оцінку витрат і вигід, вибір переважного варіанта та формування рамки моніторингу й оцінки результативності. Для України, де у сфері регуляторної політики вже застосовуються методики аналізу регуляторного впливу, важливо адаптувати їх до специфіки цифрових фінансових сервісів – високої динаміки інновацій, значної ролі даних та мережевих ефектів [119; 160].

У фінансовому секторі ефект на інновації має оцінюватися не абстрактно, а через конкретні показники: зміна бар’єрів входу для нових гравців (час і вартість отримання ліцензій, вимоги до капіталу та IT-інфраструктури), вплив на time-to-market нових цифрових продуктів, інтенсивність запуску пілотних проєктів і використання регуляторних пісочниць, динаміка інвестицій у фінтех та RegTech-рішення. Рекомендації OECD і Світового банку підкреслюють, що RIA має системно порівнювати декілька регуляторних опцій з точки зору їхнього впливу на інноваційну активність і трансакційні витрати для бізнесу, а не зосереджуватися лише на формальному дотриманні вимог. Для цифрових фінансових послуг доцільно включати до RIA індикатори, пов’язані з розвитком

open finance, доступністю API, поширенням миттєвих платежів та впровадженням нових цифрових ідентифікаційних рішень.

Другий вимір моделі RIA стосується безпеки та операційної витривалості. Оцінюючи нові регуляторні акти, що впливають на цифрові сервіси, регулятор має аналізувати очікуваний ефект на рівень кіберзахищеності, управління ІКТ-ризиками, частоту та масштаб інцидентів, здатність установ підтримувати безперервність критичних функцій. Це передбачає *ex ante* моделювання: як запропоновані вимоги (наприклад, щодо DORA-подібних стандартів, тестування кіберстійкості, управління ризиками третіх сторін) змінять профіль ризику окремих установ і системи в цілому. У рамках RIA важливо співставляти додаткові витрати на комплаєнс із потенційним зменшенням ймовірності й тяжкості інцидентів, а також включати плани збору даних для подальшого *ex post* аналізу (динаміка кіберінцидентів, відмов у сервісі, втрат клієнтів).

Третій ключовий блок – конкуренція та ринкова структура. Сучасні підходи до RIA в країнах ОЕСР пропонують розглядати вплив регулювання на конкурентоспроможність через три взаємопов'язані компоненти: вартісна конкурентоспроможність, інноваційність та міжнародна конкурентоспроможність. Для цифрових фінансових послуг це означає, що в рамках RIA слід оцінювати: як нові правила вплинуть на структуру ринку (концентрацію, індекси ННІ), умови входу/виходу для МСП і фінтехів, можливість кросбордерної діяльності, рівень тарифів і комісій, прозорість продуктів, а також на поведінку споживачів (перемикання між постачальниками, рівень скарг, NPS). Окремо доцільно аналізувати ризик небажаного посилення позицій окремих великих гравців через надмірно складні або дорогі для менших учасників регуляторні вимоги. Ключові виміри аналізу регуляторного впливу представлені у таблиці 3.4 .

Таблиця 3.4

Ключові виміри аналізу регуляторного впливу (RIA) для цифрових фінпослуг

Вимір RIA	Що оцінюється	Приклади показників / запитань
-----------	---------------	--------------------------------

Інновації та розвиток ринку	Як нові правила впливають на запуск/масштабування цифрових продуктів	Час і вартість отримання ліцензії; вимоги до ІТ; кількість пілотів і учасників пісочниць; динаміка інвестицій у фінтех/RegTech; доступність API
Безпека та операційна витривалість	Вплив на кіберзахищеність, ІКТ-ризик, безперервність критичних функцій	Очікувана зміна частоти/масштабу інцидентів; покриття DORA-подібними вимогами; витрати на комплаєнс vs зменшення ризику; наявність планів BCP/DR
Конкуренція та структура ринку	Як регулювання впливає на конкуренцію, вартість послуг і поведінку споживачів	Зміна концентрації (ННІ), частка фінтехів/МСП, рівень тарифів/комісій, бар'єри входу/виходу, кросбордерна активність, динаміка скарг, NPS, легкість зміни постачальника

Джерело: складено автором за матеріалами [24; 83; 119; 151; 160]

В українському контексті модель RIA для цифрових фінансових послуг може спиратися на вже чинну Методику проведення аналізу впливу та відстеження результативності регуляторного акта, затверджену постановою Кабінету Міністрів України, але потребує її «оцифрування» з урахуванням специфіки фінансового сектору: granular-дані, API, алгоритмічні моделі, кіберризик. Це означає, що для кожного істотного регуляторного рішення у сфері ЦФП мають готуватися RIA-документи з чіткою структурою: опис проблеми (наприклад, недостатня безпека миттєвих платежів чи асиметрія інформації в open finance), окреслення цілей (інновації, безпека, конкуренція), перелік альтернатив (у тому числі «м'які» інструменти – рекомендації, стандарти), кількісна й якісна оцінка впливів на інновації, безпеку та конкуренцію, а також план подальшого моніторингу й коригування регулювання. Такий підхід робить регуляторну політику в цифровому фінансовому секторі більш прозорою, передбачуваною та орієнтованою на довгостроковий розвиток ринку.

3.3. Імплементація цифрових фінансових інструментів у стратегію сталого розвитку фінансового сектору

Імплементація цифрових фінансових інструментів у стратегію сталого розвитку передбачає перехід від суто «декларативного» ESG до ESG-вбудованих

продуктів, де екологічні та соціальні параметри безпосередньо впливають на дизайн, ціну та умови користування послугами. Фінтех-інновації у сфері сталих фінансів розглядаються як один із ключових механізмів перенаправлення капіталу в проєкти з позитивним екологічним ефектом, зниження бар'єрів входу для дрібних інвесторів та підвищення прозорості ESG-даних. У цій логіці особливе значення мають цифрові продукти на стику retail-фінансів і зеленої трансформації – «зелені» BNPL-рішення для енергоефективності, мікроінвестиційні платформи для «зелених» інструментів, а також usage-based страхування, яке винагороджує екологічно відповідальну поведінку [83; 119; 145].

«Зелений» BNPL (Buy Now, Pay Later) для енергоефективності можна розглядати як цільовий різновид розстрочених цифрових кредитних продуктів, прив'язаних до фінансування заходів із підвищення енергоефективності домогосподарств та МСП (сонячні панелі, теплові насоси, модернізація опалення, утеплення тощо). Такі рішення вже реалізуються через спеціалізовані «green finance» платформи, які дозволяють клієнтам оформити онлайн-фінансування енергоефективних проєктів із диференційованими ставками та пільговими періодами, часто у співпраці з виробниками обладнання та енергосервісними компаніями. З ESG-позиції ключовими елементами дизайну «зеленого» BNPL є верифікація відповідності товару/послуги екологічним стандартам (таксономія), прив'язка умов фінансування до очікуваного скорочення споживання енергії чи викидів та прозора звітність щодо профінансованих «зелених» активів. У перспективі для України це може стати інструментом масової модернізації житлового фонду й МСП при мінімальних транзакційних витратах для користувачів через повністю цифровий онбординг.

Другим напрямом є платформи мікроінвестицій у «зелені» інструменти, які використовують можливості цифрових каналів для демократизації доступу до ESG-активів. Дослідження з фінтеху та сталих фінансів показують, що цифрові інвестиційні сервіси здатні знижувати вхідні пороги для інвесторів, дозволяючи інвестувати невеликі суми в зелені облігації, фонди ESG, проєкти відновлюваної енергетики чи «зелені» інфраструктурні ініціативи, поєднуючи

автоматизований скоринг, мобільний UX та інтегровану ESG-аналітику. Через такі платформи користувачі можуть, наприклад, направляти «дрібні залишки» (round-up investments) або регулярні невеликі внески у портфелі, структуровані відповідно до ESG-критеріїв. Для фінансових установ це відкриває можливість формування масових «зелених» продуктів на роздрібному рівні, а для регулятора – канал накопичення статистики щодо запиту населення на сталі інвестиції.

Третя група рішень – usage-based страхування (UBI), насамперед у автострахуванні та страхуванні майна, яке безпосередньо вбудовує ESG-інcentиви в тарифну структуру. Використання телематики, IoT-сенсорів та аналітики даних дозволяє страховикам формувати індивідуальні премії на основі фактичної поведінки клієнта (стиль водіння, пробіг, тип транспортного засобу, інтенсивність використання), одночасно оцінюючи й кліматичний вплив (викиди, ефективність). ESG-орієнтовані UBI-продукти винагороджують екологічно відповідальну поведінку – керування електромобілем чи малолітражним авто, дотримання еко-режимів, скорочення непотрібних поїздок – через знижені тарифи, бонуси або «зелений кешбек». Таким чином цифрові страхові сервіси перетворюються з інструменту простого перерозподілу ризиків на механізм активного управління поведінкою клієнтів у напрямі зниження дорожньо-транспортних і кліматичних ризиків.

У сукупності зелений BNPL, мікроінвестиційні платформи для ESG-активів та usage-based страхування формують ядро ESG-вбудованих продуктів (див табл. 3.5), які можуть бути масштабовані через цифрові канали в українському фінансовому секторі. Їхня поява й розвиток мають бути інтегровані в стратегію сталого розвитку банків та небанківських установ, з урахуванням національної таксономії сталого фінансування, цілей декарбонізації та програм енергоефективності. Для регулятора вони створюють як нові можливості (мобілізація приватного капіталу на «зелені» цілі, підвищення фінінклюдії), так і нові виклики – потребу в стандартизації ESG-даних, запобіганні «greenwashing» та забезпеченні прозорості й справедливості умов для споживачів.

Таблиця 3.5

ESG-вбудовані роздрібні продукти в цифрових фінпослугах

Тип продукту	Ціль/призначення	ESG-механізм (що «вбудовано»)	Цільові сегменти	Ключові дані / таксономія	Приклади КРІ
«Зелений» BNPL для енергоефективності	Фінансування утеплення, ВДЕ, модернізації житла та МСП	Знижені ставки/пільги за «зелені» товари; прив'язка до економії енергії/CO ₂	Домогосподарства, МСП	Таксономія «зелених» товарів, енергоаудит, дані про споживання	Обсяг профінансованих проектів, оцінене скорочення кВт·год / т CO ₂
Мікроінвестиції в «зелені» інструменти	Доступ дрібних інвесторів до ESG-активів	Автоматичні дрібні внески, портфелі з ESG-фільтрами	Роздрібні інвестори	ESG-рейтинг інструментів, дані про фонди / «зелені» облігації	Кількість інвесторів, сума під управлінням, частка ESG-активів
Usage-based страхування (UBI)	Тарування премій за реальною поведінкою	Знижки/бонуси за еко-водіння, електротранспорт, менший пробіг	Водії, власники майна	Телеметрія, тип ТЗ, пробіг, еко-параметри	Loss ratio, частка «зелених» ТЗ, частка policy з UBI

Джерело: складено автором за матеріалами [83; 119; 145; 146; 147]

Дані для сталості в цифрових фінансових послугах – це окрема «інфраструктура», без якої ESG-продукти й регулювання залишаються деклараціями. Базою для такої інфраструктури виступають таксономії сталих видів діяльності, які уніфікують визначення «зелених» активів і зменшують ризики грінвошингу. Прикладом є EU Taxonomy – класифікаційна система, що визначає критерії для економічних видів діяльності, узгоджених із траєкторією до «NET ZERO-2050» і шістьма екологічними цілями ЄС, та слугує «наріжним каменем» європейської системи сталих фінансів і ключовим інструментом прозорості ринку. Для України адаптація принципів Європейської таксономії (із урахуванням секторної структури економіки та післявоєнної відбудови) може стати основою для побудови національного «словника» сталих проектів, на який

спиратимуться банки, небанківські установи, ринок капіталу й державні програми.

На рівні продуктів і клієнтів наступним кроком виступають еко-скоринги – інтегральні показники, що в одній метриці агрегують дані про викиди, енергоефективність, використання ресурсів та циркулярність. У ЄС активно обговорюється запровадження єдиного екологічного скорингу для транспортних засобів (vehicle eco-score) як стандартизованого індикатора екологічної ефективності авто, який можна використовувати для інформування споживачів, податкових стимулів та диференціації екоподатків. Подібні підходи розвиваються й у сфері ремонту: система Eco Repair Score оцінює вплив конкретної операції з ремонту авто на навколишнє середовище на основі повного життєвого циклу (виробництво й транспортування деталей, енергія майстерні, переробка відходів), надаючи єдину шкалу А–Е, якою можуть користуватися страхові компанії, автосервіси та клієнти. Для України релевантною є побудова власних моделей еко-скорингу для кредитування «зелених» МСП, оцінки житлових будинків за енергоефективністю, страхування «зеленого транспорту» тощо з подальшим їхнім включенням у скорингові карти й тарифні сітки.

Верифікація впливу потребує стандартизованої, порівнюваної та регулярно оновлюваної нефінансової звітності. Міжнародним стандартом де-факто є рамка TCFD, яка структурує розкриття кліматичних ризиків за блоками «управління – стратегія – ризик-менеджмент – метрики й цілі» і вже підтримана тисячами організацій у понад 100 юрисдикціях. ЄЦБ і національні центральні банки Євросистеми з 2023 року щороку публікують кліматичні розкриття щодо портфелів активів, використовуючи гармонізовану методологію, узгоджену з рекомендаціями TCFD; розкриття охоплюють вуглецевий слід, кліматичні ризики та прогрес декарбонізації на шляху до цілей Паризької угоди. Міжнародні фінансові інституції (зокрема IFC у своїх кліматичних звітах за 2025 рік) показують, як кліматичні метрики інтегруються в прийняття інвестиційних рішень, таргетування зелених бондів, підтримку МСП та оцінку впливу на природу й біорізноманіття. Для українського фінансового сектору це означає необхідність поступового переходу до повноцінної ESG-звітності, інтеграції

кліматичних та екологічних індикаторів у кредитні політики й ризик-менеджмент, а також розробки єдиних методичних рекомендацій регуляторів щодо RIA для «зелених» ініціатив.

Ключовим каталізатором розвитку «даних для сталості» стають відкриті дані та API. У Європі та світі формується окрема ніша «green fintech»: компанії, які поєднують транзакційні дані банків (через open banking API), відкриті кліматичні й ESG-бази та моделі викидів, щоб будувати сервіси оцінки вуглецевого сліду за витратами, «зелені» платіжні й інвестиційні рішення, платформи для аналізу сталості ланцюгів постачання. Open banking-сервіси вже сьогодні демонструють, як з однієї транзакції можна отримати дані про тип купівлі, транспорт, енергоспоживання й на їх основі обчислювати CO₂-слід, пропонувати клієнтам варіанти його зменшення або автоматичний офсет. Для України імплементація «зелених» use-case'ів у майбутній архітектурі Open Finance (скоринг за викидами для кредитів, «еко-дашборди» в мобільному банкінгу, API для доступу до державних екоданих) дозволить інтегрувати сталість у масові цифрові фінпослуги, зробивши ESG-метрики звичним елементом UX для громадян і бізнесу.

У сучасних підходах до сталого розвитку фінансова інклюзія розглядається як складова не лише соціального блоку ESG, а й як необхідна умова економічної стійкості домогосподарств та МСП. Цифрові фінансові послуги відкривають доступ до платежів, заощаджень, кредитів і страхування для мільйонів людей, які раніше користувалися лише готівкою або не мали стосунку до формального сектору. Для України, де воєнні події додатково загострили вразливість окремих груп (ВПО, ветерани, домогосподарства з тимчасово окупованих чи прифронтових територій), інклюзія через цифрові канали стає не тільки соціальним, а й безпековим пріоритетом [83; 119].

Окремий вимір – продукти, орієнтовані на уразливі групи: малозабезпечені домогосподарства, жінки, жителі сільських територій, люди з інвалідністю, вимушено переміщені особи та біженці. Міжнародна практика показує, що поєднання цифрових рахунків, мобільних гаманців і цифрових G2P-платежів дає

змогу переводити людей із готівкового «тіні» у формальний сектор та посилювати їхню шокостійкість. Водночас дослідження фіксують типові бар'єри: відсутність документів у частини населення, гендерні розриви у доступі до смартфонів та мобільного інтернету, слабе покриття у сільських територіях, вищу уразливість до шахрайства. Тому інклюзивні цифрові продукти для таких груп мають передбачати спрощені процедури відкриття рахунку (за підтримки спрощеного KYC, e-ID), адаптовані ліміти й тарифи, інтеграцію з програмами соціальної підтримки, а також захисні «запобіжники» від надмірної заборгованості.

Другий компонент інклюзивності – UX-доступність цифрових каналів. Навіть формально «дешевий» та доступний рахунок не буде по-справжньому інклюзивним, якщо мобільний застосунок чи вебінтерфейс не пристосовано для людей із порушеннями зору, слуху, моторики, когнітивними особливостями або низькими цифровими навичками. Сучасні рекомендації для банків та фінтеху наголошують на необхідності проєктування за принципами WCAG 2.1/2.2 (Web Content Accessibility Guidelines): достатній контраст, масштабування інтерфейсу, коректна робота з читачами екрана, навігація з клавіатури, альтернативні описи зображень, доступні форми тощо. Практика показує, що інвестування в доступність зменшує відтік клієнтів, розширює базу користувачів і знижує репутаційні та регуляторні ризики, а отже є елементом довгострокової стійкості бізнес-моделі.

Третя опора інклюзії як сталості – системні програми digital- та financial-literacy. Недостатня фінансова й цифрова грамотність часто виявляється не менш серйозною перешкодою, ніж низький дохід чи відсутність відділень. В українському контексті важливу роль відіграють Національна стратегія розвитку фінансової грамотності до 2030 року НБУ, яка прямо включає підвищення обізнаності щодо цифрових фінансових сервісів і захисту від кібершахрайства, а також екосистема онлайн-ресурсів – платформи «Дія.Цифрова освіта», освітні серіали з фінансової грамотності й «цифрових грошей», спеціалізовані сайти НБУ («Harazd», «TALAN») для різних вікових і цільових груп. У поєднанні зі шкільними курсами підприємництва та фінансової грамотності це створює

основу для масового апскілли населення, без якого масштабування цифрових фінпослуг може лише поглибити нерівність.

Отже, інклюзія як складова сталості цифрового фінансового сектору потребує цілісного підходу: таргетованих продуктів для уразливих груп із урахуванням їхніх життєвих контекстів; технічно доступних і зручних цифрових каналів, спроектованих за принципами доступності; а також розгалуженої системи програм цифрової та фінансової грамотності, що охоплюють різні вікові й соціальні групи. Лише за умови поєднання цих трьох елементів цифрові фінансові інструменти сприятимуть не тільки зростанню ринку, а й зменшенню бідності, розширенню можливостей для жінок, молоді, ВПО та інших уразливих груп, посилюючи стійкість суспільства в цілому.

У контексті інтеграції цифрових фінансових інструментів у стратегію сталого розвитку логічно виділяти поетапний підхід: від пілотних кейсів (quick wins) до масштабування на рівень сектору. Міжнародна практика «inclusive green finance» показує, що пілоти дозволяють протестувати попит, технологічну життєздатність та ризиковий профіль ESG-орієнтованих продуктів (зелений кредит, еко-страхування, кліматичні мікрофінансові продукти) в обмеженому середовищі, перш ніж ухвалюється рішення про їх широке впровадження. У низці країн центральні банки й регулятори прямо вбудовують пілотні фази в дорожні карти «зелених» фінансів як обов'язковий етап між концепцією та національними програмами [83; 151].

На горизонті 12–18 місяців доцільно фокусуватися на quick wins, які спираються на вже наявну цифрову інфраструктуру (миттєві платежі, мобільний банкінг, базові open API) та мають чітко вимірюваний ефект. Для України до таких пілотів можна віднести: запуск «зелених» BNPL-продуктів для енергоефективних товарів у партнерстві з виробниками та енергосервісними компаніями; модулі «вуглецевого сліду» в мобільних застосунках банків на основі аналізу транзакцій; мікроінвестиційні сервіси, що дозволяють невеликими сумами інвестувати в «зелені» облігації чи фонди; usage-based страхування для електротранспорту та еко-водіння. Усі ці кейси можуть запускатися в обмеженій кількості банків/страховиків, на вибраних регіонах або

сегментах клієнтів, що знижує ризики та дає змогу швидко отримати зворотний зв'язок.

На етапі масштабування (2–3 роки) акцент зміщується від тестування окремих продуктів до розбудови екосистеми та інтеграції з публічною політикою. Це означає: поширення успішних пілотів на всю клієнтську базу та всю країну; інтеграцію «зелених» продуктів із національними програмами енергоефективності, відбудови, підтримки МСП; узгодження критеріїв продуктів із національною таксономією сталих видів діяльності; підключення до міжнародних ринків (green bonds, blended finance). Досвід енергетичних і «зелених» програм Світового банку показує, що переходу від пілота до масштабного впровадження зазвичай заважають нестача довгострокового фінансування, слабка координація між державною політикою та банківським сектором, а також обмежені аналітичні дані щодо ефективності перших хвиль проєктів. Врахування цих факторів на етапі планування дає змогу уникнути «застрягання» інновацій у вічному статусі пілоту.

Для того щоб пілоти перетворилися на реальні драйвери сталості, необхідно заздалегідь визначити критерії успіху вбудувати їх у дизайн проєктів. На рівні інновацій та ринку це: кількість активних користувачів, динаміка DAU/MAU, частка цифрових операцій, показники утримання клієнтів, unit economics продукту (дохідність, cost-to-income у цифровому каналі). На рівні сталості – обсяги профінансованих «зелених» інвестицій, оцінене скорочення викидів або енерговитрат, підвищення стійкості до кліматичних ризиків (наприклад, через кліматичне страхування чи адаптаційні кредити), частка ESG-критеріїв, інтегрованих у скоринг. На рівні інклюзії – охоплення уразливих груп, частка клієнтів із сільських територій, жінок-підприємниць, ВПО тощо. Міжнародні огляди пілотів «green & inclusive finance» підкреслюють, що саме чітко визначені метрики дозволяють оцінити, які моделі варто масштабувати, а які – залишити на рівні експерименту.

В українському контексті доцільно також закладати в кожен пілот компонент навчання для регулятора і ринку: документування уроків (lessons learned), розробку типових договорів і процедур, уточнення підходів до

управління ризиками, кібербезпеки та споживчого захисту. Результати успішних пілотів мають лягати в основу оновлених регуляторних актів (наприклад, вимог до відкритих API для еко-сервісів, стандартів розкриття ESG-інформації в цифрових продуктах, підходів до RIA у сфері зеленої та інклюзивної цифрової фінансизації). Такий зворотний зв'язок «пілот - регулювання - масштабування» забезпечує еволюційний розвиток ринку, коли регуляторні рамки базуються не лише на теорії та зовнішньому досвіді, а й на власних емпіричних кейсах.

Фінансова модель сталості для цифрових фінансових послуг означає, що ESG-фактори інтегруються безпосередньо в управління ризиками, дохідністю та розвитком продуктового портфеля, а не існують як «паралельний» звіт. На практиці це реалізується через систему ESG-KPI, які доповнюють класичні показники рентабельності (ROE, RAROC, NPL) метриками вуглецевого сліду, ресурсоефективності, соціального охоплення та якості управління. Міжнародні огляди підкреслюють, що ESG-KPI стають інструментом не лише нефінансової звітності, а й драйвером довгострокової вартості бізнесу: вони впливають на вартість капіталу, доступ до інвесторів та оцінку кредитного рейтингу. Для українських банків і небанківських установ це означає необхідність розробки інтегрованих дашбордів, де фінансові та ESG-показники аналізуються спільно – наприклад, співставлення маржинальності «зелених» продуктів із їхнім впливом на скорочення ризиків [83; 119; 151].

З погляду ризиків і дохідності зелена фінансова модель базується на емпіричному факті: кліматичні та екологічні ризики поступово трансформуються у кредитний, ринковий та операційний ризики для фінансових установ. Дослідження для країн ASEAN+4 показують, що розвиток green finance може підвищувати фінансову стабільність та пом'якшувати негативний вплив кліматичних ризиків на банківський сектор. Інші роботи демонструють, що екологічний кредитний ризик безпосередньо корелює з фінансовими результатами банків: портфелі, концентровані в «вуглецево-інтенсивних» секторах, мають вищу волатильність та потенційно гірший профіль дохідність/ризик у середньостроковій перспективі. У фінансовій моделі сталості це відображається через: включення кліматичних чинників у PD/LGD,

диференціацію цінових надбавок для «коричневих» активів, окремі ліміти на експозиції до секторів з високими перехідними ризиками та розрахунок risk-adjusted return on capital (RAROC) з урахуванням ESG-параметрів.

Другий блок – зниження вуглецевого сліду портфеля як окремий вимір KPI сталості. Сучасні підходи спираються на методики оцінки financed emissions (викиди, профінансовані через кредити й інвестиції), які дають змогу банкам і інвесторам вимірювати та відслідковувати вуглецевий профіль своїх портфелів. Стандарти на кшталт PCAF пропонують як абсолютні показники (тонни CO₂e, «закріплені» за портфелем), так і інтенсивні (CO₂e на одиницю виручки, активів чи виробленої енергії). OECD і низка міжнародних організацій наголошують, що такі метрики є базою для моніторингу прогресу щодо net-zero-цілей фінансових установ. У фінансовій моделі сталості для українських установ доцільно закладати: цільові траєкторії зниження financed emissions, ліміти на вуглецево-інтенсивні портфелі, KPI для «зеленого» кредитування (частка портфеля, що відповідає таксономії) та прив'язку бонусних схем менеджменту до досягнення кліматичних орієнтирів.

Третій вимір – показники охоплення (coverage), які відображають, наскільки сталі фінансові продукти реально досягають цільових сегментів економіки та населення. Міжнародні практики impact-інвестування й сталого фінансування пропонують використовувати так звані reach- та outcome-KPI (див. табл. 3.): кількість клієнтів, охоплених «зеленими» чи інклюзивними продуктами; обсяг виданого фінансування для МСП у «зелених» секторах; частка уразливих груп (жінки-підприємці, ВПО, мікробізнес) серед користувачів ESG-продуктів; регіональне охоплення тощо. Такі індикатори поєднуються з якісними показниками – зміною доступу до базових фінансових послуг, рівнем фінансової стійкості домогосподарств, розвитком «зелених» бізнес-моделей у регіонах. Для цифрових фінансових сервісів додатковою перевагою є можливість вимірювати ці метрики майже в реальному часі (через транзакційні дані, usage-поведінку в мобільних застосунках та аналітику open API), що дозволяє швидко коригувати продуктові стратегії.

Структура КРІ сталості для цифрових фінансових послуг

Вимір	Приклади КРІ	Джерела даних / інструменти
Ризик і дохідність	RAROC з урахуванням ESG, частка «коричневих» активів, NPL у «зелених» vs звичайних портфелях	Внутрішні ризик-системи, PD/LGD-моделі з кліматичними чинниками
Вуглецевий слід портфеля	Financed emissions (тонни CO ₂ e), інтенсивність CO ₂ e/грн виручки, частка портфеля, що відповідає таксономії	PCAF-методики, дані клієнтів, галузеві бенчмарки, еко-скоринги
Охоплення та інклюзія	Кількість користувачів ESG-продуктів, частка уразливих груп, частка «зелених» МСП, регіональне покриття	Транзакційні дані, CRM, аналітика мобільних застосунків, open API

Джерело: складено автором за матеріалами [15; 83; 95; 119; 151]

У підсумку фінансова модель і система КРІ сталості для українського фінансового сектору мають будуватися як інтегрована панель показників: (1) ризик/дохідність портфелів із урахуванням кліматичних і екологічних чинників; (2) траєкторії скорочення вуглецевого сліду (операційного та профінансованого) у відповідності до національних і глобальних цілей; (3) охоплення реального сектору й населення ESG-вбудованими продуктами, особливо уразливих груп та «зелених» секторів економіки. Саме така архітектура КРІ дозволяє цифровим фінансовим інструментам бути не лише технологічною інновацією, а й механізмом реального зниження системних ризиків, підвищення дохідності в довгостроковій перспективі та досягнення кліматичних і соціальних цілей.

ВИСНОВОК

У роботі уточнено зміст поняття «цифрові фінансові послуги» як digital-by-design сервісів, що надаються повністю дистанційно на базі API, хмарної інфраструктури та аналітики даних у режимі, близькому до реального часу. Відмежовано власне цифрові послуги від традиційних продуктів, що лише продаються онлайн, що дозволило розглядати цифрову фінансову екосистему як сукупність продуктового, інфраструктурного та даноцентричного вимірів.

На цій основі сформовано широку класифікацію цифрових фінансових послуг: за суб'єктами (банки, небанківські установи, платіжні та фінтех-компанії, BigTech), за функціями (платежі, кредитування, заощадження, страхування, інвестиції) і за технологічними моделями (мобільні додатки, маркетплейси, embedded finance, DeFi-рішення). Показано, що цифрові послуги поступово стають не «додатком» до класичного банкінгу, а самостійним структуроутворюючим сегментом фінансового ринку.

Розкрито взаємозв'язок цифровізації з фінансовою стабільністю через канали впливу на ліквідність, структуру фінансування, операційні та кіберризики, концентрацію критичної інфраструктури й даних. Обґрунтовано, що цифрові фінансові послуги можуть одночасно підвищувати стійкість (швидкі платежі, краща аналітика ризиків) та генерувати нові системні ризики, що потребує інтегрованого підходу до політики фінансової та цифрової стабільності.

Аналіз статистики свідчить про швидкий перехід України до безготівкових розрахунків і мобільних каналів. Частка безготівкових операцій картками перевищує дев'ять десятих за кількістю й понад половину за сумою, а мережа POS-терміналів і кількість активних карток стабільно зростають. Мобільний та інтернет-банкінг стали основним каналом взаємодії клієнтів із фінансовими установами, а миттєві платежі 24/7 перетворилися на стандарт.

Паралельно посилюються позиції небанківських платіжних установ і фінтех-компаній, розвиваються електронні гарантії, платіжні сервіси в екосистемах електронної комерції, інтеграція фінансових продуктів у державні цифрові платформи. Це свідчить про формування конкурентного, технологічно

розвиненого сегмента цифрових фінансових послуг, який відіграв важливу роль у підтриманні економічної активності в умовах війни.

Разом із тим виявлено низку бар'єрів: цифрову нерівність між регіонами й соціальними групами, недостатню фінансову та цифрову грамотність, поширеність шахрайства й кіберінцидентів, дефіцит кваліфікованих кадрів, залежність від окремих технологічних провайдерів. Ці фактори обмежують глибину використання складніших цифрових продуктів і формують «вузькі місця» подальшого розвитку ринку.

Узагальнено європейську модель розвитку цифрових фінансових послуг, у центрі якої – нормована модель open banking / open finance, поєднана з високими вимогами до кіберстійкості, захисту споживачів і конкуренції. Показано, що завдяки стандартизованим API, наглядовим рамкам на кшталт DORA та розвитку цифрової ідентичності ЄС формує цілісне середовище для масштабування інновацій.

Порівняння з США та провідними азійськими юрисдикціями продемонструвало різні траєкторії: від ринково керованої моделі доступу до даних у США до «архітектурного» підходу Сінгапуру з активним використанням sandbox-режимів і експериментів із новими формами грошей. Окремо окреслено уроки китайського досвіду BigTech-платформ, які поєднують масову цифрову інклюзію з концентрацією ризиків.

На цій основі сформовано систему бенчмарків для України: рівень penetration миттєвих платежів, стандартизація відкритих API, розвиток цифрової ідентичності, масштаби регуляторних пісочниць, показники цифрової інклюзії. «Картка розривів» показує, що Україна досягла суттєвого прогресу в платежах і мобільних сервісах, але відстає щодо повноцінної моделі open finance, розгортання SupTech-рішень та інтеграції ESG-параметрів у цифрову фінансову екосистему.

Запропоновано візію до 2030 року, згідно з якою Україна формує відкриту, інклюзивну та стійку цифрову фінансову екосистему, де цифрові сервіси є базовим форматом взаємодії домогосподарств, бізнесу та держави. Визначено ключові пріоритети: розвиток миттєвих платежів та інфраструктури високої

доступності, формування моделі open finance, масштабування цифрової ідентичності, підтримка embedded finance та платформних рішень для МСП.

Рекомендації в сфері регулювання передбачають перехід до даних-орієнтованого, проактивного нагляду із широким використанням RegTech і SupTech, розширення практики регуляторних пісочниць, посилення операційної стійкості учасників ринку та комплексний захист прав споживачів у цифровому середовищі. Наголошено на необхідності пропорційного підходу до фінтех-моделей і синхронізації національної рамки з європейськими стандартами.

Особливу увагу приділено інтеграції цифрових фінансових інструментів у стратегію сталого розвитку. Сформульовано підходи до розробки ESG-вбудованих продуктів (зелені BNPL-рішення, мікроінвестиції в «зелені» активи, usage-based страхування), використання таксономій, еко-скорингу та відкритих даних для верифікації впливу. Запропоновано базові контури системи KPI сталості, що враховують вплив цифрових продуктів на ризики, дохідність, вуглецевий слід та охоплення вразливих груп, що підтверджує потенціал цифрових фінансових послуг як інструменту стійкого відновлення українського фінансового сектору.

Список використаних джерел

1. Abad-Segura E., Infante-Moro A., González-Zamar M. D., López-Meneses E. Influential factors for a secure perception of accounting management with blockchain technology // Journal of Open Innovation: Technology, Market, and Complexity: електрон. наук. журн. 2024. Т. 10, № 2. Article 100264. URL: <https://doi.org/10.1016/j.joitmc.2024.100264> (дата звернення: 16.11.2025).
2. ACI Worldwide. Prime Time for Real-Time Payments 2024 // ACI Worldwide: analytical report, electronic resource. URL: <https://www.aciworldwide.com/> (дата звернення: 16.11.2025).
3. ACI Worldwide. Prime Time for Real-Time Payments 2024: global report on the growth of instant payments // ACI Worldwide: електрон. ресурс. 2024. URL: <https://www.aciworldwide.com/> (дата звернення: 16.11.2025). (Bank for International Settlements)
4. ADA; REDCAMIF. Sustainability, FinTech and Financial Inclusion: Lessons from 19 green financial service projects // ADA: електрон. ресурс. Luxembourg, 2020. URL: <https://www.ada-microfinance.org/en/our-resources/media-center/sustainability-fintech-and-financial-inclusion> (дата звернення: 15.11.2025). (IDEAS/RePEc)
5. Al-Zoubi W. K. Economic Development in the Digital Economy: A Bibliometric Review // Economies: електрон. наук. журн. 2024. Т. 12, № 3. Article 53. URL: <https://doi.org/10.3390/economies12030053> (дата звернення: 16.11.2025). (Directory of Open Access Journals)
6. Alamsyah A., Kusuma G. N. W., Ramadhani D. P. A Review on Decentralized Finance Ecosystems // Future Internet: електрон. наук. журн. 2024. Т. 16, № 3. Article 76. URL: <https://doi.org/10.3390/fi16030076> (дата звернення: 16.11.2025). (figshare.utas.edu.au)
7. Alamsyah A., Syahrir S. The Taxonomy of Blockchain-based Technology in the Financial Industry // F1000Research: електрон. наук. журн. 2023. Т. 12. Article 457. URL: <https://doi.org/10.12688/f1000research.133518.2> (дата звернення: 16.11.2025). (MDPI)

8. Alliance for Financial Inclusion. Access to Finance for Forcibly Displaced Person-led MSMEs: special report // AFI: електрон. ресурс. Kuala Lumpur, 2023. URL: https://www.afi-global.org/wp-content/uploads/2024/10/AFI_Access-to-Finance-for-Forcibly-Displaced-Person-led-MSMEs.pdf (дата звернення: 15.11.2025). (IDEAS/RePEc)
9. Alliance for Financial Inclusion. Leveraging Digital Financial Services to Advance Inclusive Green Finance Policies: special report // AFI: електрон. ресурс. Kuala Lumpur, 2022. URL: https://www.afi-global.org/wp-content/uploads/2024/10/Leveraging-Digital-Financial-Services-to-Advance-Inclusive-Green-Finance-Policies_03092022_isbn.pdf (дата звернення: 15.11.2025). (Directory of Open Access Journals)
10. Alliance for Financial Inclusion. Roadmap for Inclusive Green Finance Implementation: country case studies on IGF policy implementation // AFI: електрон. ресурс. Kuala Lumpur, 2023. URL: <https://www.afi-global.org/wp-content/uploads/2024/09/Roadmap-for-Inclusive-Green-Finance-Implementation.pdf> (дата звернення: 15.11.2025). (figshare.utas.edu.au)
11. Anderson J., Caimi G. A Three-Part Game Plan for Delivering Sustainability Digitally // Bain & Company: електрон. аналіт. ресурс. 2022. URL: <https://www.bain.com/insights/a-three-part-game-plan-for-delivering-sustainability-digitally/> (дата звернення: 16.11.2025).
12. Appaya S., Gradstein H., та ін. Global Experiences from Regulatory Sandboxes // World Bank: електрон. ресурс. Washington, DC, 2020. URL: <https://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf> (дата звернення: 15.11.2025).
13. Asif M., Khan M. N., Tiwari S., Wani S. K., Alam F. The Impact of Fintech and Digital Financial Services on Financial Inclusion in India // Journal of Risk and Financial Management: електрон. наук. журн. 2023. Т. 16, № 2. Article 122. URL: <https://doi.org/10.3390/jrfm16020122> (дата звернення: 16.11.2025).
14. Association of Ukrainian Banks (AUB). In the non-bank financial services market, the number of participants decreased by 20 in September // Association of Ukrainian Banks: електрон. новин. ресурс. 18.10.2024.

URL: <https://aub.org.ua/en/press-center-en/financial-sector-news/14895-na-rynku-nebankivskykh-finansovykh-posluh-u-veresni-kilkist-uchasnykiv-zmenshyasia-na-21> (дата звернення: 15.11.2025).

15. Association of Ukrainian Banks (AUB). In the non-bank financial services market, the number of participants decreased by 20 in September: news item of 18.10.2024 // AUB: official website, electronic resource. URL: <https://aub.org.ua/en/press-center-en/financial-sector-news/14895-na-rynku-nebankivskykh-finansovykh-posluh-u-veresni-kilkist-uchasnykiv-zmenshyasia-na-21> (дата звернення: 15.11.2025).

16. AVERE. Setting up a vehicle eco-score: policy paper // AVERE – The European Association for Electromobility: електрон. аналіт. ресурс. 2025. URL: <https://www.emobilityeurope.org/wp-content/uploads/2025/05/AVERE-Setting-up-a-vehicle-eco-score-5.pdf> (дата звернення: 15.11.2025).

17. Azeez N. P. A., Haque M. I., Akhtar S. M. J., Banu M. N. Methodological framework to define and measure “digital” financial inclusion // International Journal of Financial Engineering: електрон. наук. журн. 2025. Т. 12, № 2. Article 2450016. URL: <https://doi.org/10.1142/S2424786324500166> (дата звернення: 15.11.2025).

18. Babina T., Bahaj S. A., Buchak G., De Marco F., Foulis A. K., Gornall W., Mazzola F., Yu T. Customer Data Access and Fintech Entry: Early Evidence from Open Banking // NBER Working Paper: електрон. наук. ресурс. 2024. Working Paper No. 32089. URL: <https://www.nber.org/papers/w32089> (дата звернення: 15.11.2025). creditonline.eu

19. Bank for International Settlements. IFC Report No. 14 – Sustainable Finance and the Role of Central Banks // Bank for International Settlements: електрон. ресурс. Basel, 2021. URL: https://www.bis.org/ifc/publ/ifc_report_14.pdf (дата звернення: 15.11.2025).

20. Bas T., Malki I., Sivaprasad S. Connectedness between central bank digital currency index, financial stability and digital assets // Journal of International Financial Markets, Institutions and Money: електрон. наук. журн. 2024. Т. 92. Article 101981. URL: <https://doi.org/10.1016/j.intfin.2024.101981> (дата звернення: 15.11.2025).

21. Bitsight. DORA Compliance Checklist & Guide // Bitsight: електрон. метод. ресурс. 13.08.2025. URL: <https://www.bitsight.com/learn/dora-compliance-checklist> (дата звернення: 15.11.2025).
22. Bondarenko S., Makeieva O., Usachenko O., Veklych V., Arifkhodzhaieva T., LERNYK S. The Legal Mechanisms for Information Security in the Context of Digitalization // Journal of Information Technology Management: електрон. наук. журн. 2022. Т. 14 (Special Issue: Digitalization of Socio-Economic Processes). С. 25–58. URL: https://jitm.ut.ac.ir/article_88868.html (дата звернення: 15.11.2025).
23. Brühl V. Big Tech, the Platform Economy and the European Digital Markets // Intereconomics: Review of European Economic Policy: електрон. наук. журн. 2023. Т. 58, № 5. С. 274–282. URL: <https://doi.org/10.2478/ie-2023-0056> (дата звернення: 15.11.2025).
24. Bublyk Ye., Shapoval Yu., Shpanel-Yukhta O., Brus S. Effect of financial access on cashless economy: The case of Ukraine // Banks and Bank Systems: електрон. наук. журн. 2023. Т. 18, № 1. С. 91–102. URL: [https://doi.org/10.21511/bbs.18\(1\).2023.08](https://doi.org/10.21511/bbs.18(1).2023.08) (дата звернення: 15.11.2025).
25. Chand S. A., Singh B., Narayan K., Chand A. The Impact of Financial Technology (FinTech) on Bank Risk-Taking and Profitability in Small Developing Island States: A Study of Fiji // Journal of Risk and Financial Management: електрон. наук. журн. 2025. Т. 18, № 7. Article 366. URL: <https://doi.org/10.3390/jrfm18070366> (дата звернення: 15.11.2025).
26. CM-Alliance. EU DORA requirements for ICT service providers – all you need to know // CM-Alliance: електрон. аналіт. ресурс. 12.09.2024. URL: <https://www.cm-alliance.com/cybersecurity-blog/eu-dora-requirements-for-ict-service-providers-all-you-need-to-know> (дата звернення: 15.11.2025).
27. Congressional Research Service. Access to Consumer Financial Data: Open Banking and the CFPB’s Section 1033 Rule (IF13117) // Congressional Research Service: електрон. аналіт. ресурс. 30.09.2025. URL: <https://www.congress.gov/crs-product/IF13117> (дата звернення: 15.11.2025).

28. Congressional Research Service. Open banking and the CFPB's Section 1033 rule (IF13117). 30.09.2025 // CRS: electronic resource. URL: <https://www.congress.gov/crs-product/IF13117> (дата звернення: 15.11.2025).

29. Consumer Financial Protection Bureau. CFPB finalizes Personal Financial Data Rights Rule to boost competition, protect privacy, and give families more choice in financial services // Consumer Financial Protection Bureau: електрон. новин. ресурс. 22.10.2024. URL: <https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-personal-financial-data-rights-rule-to-boost-competition-protect-privacy-and-give-families-more-choice-in-financial-services/> (дата звернення: 15.11.2025).

30. Consumer Financial Protection Bureau. CFPB finalizes Personal Financial Data Rights Rule to boost competition, protect privacy, and give families more choice in financial services. 22.10.2024 // CFPB: official website, electronic resource. URL: <https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-personal-financial-data-rights-rule-to-boost-competition-protect-privacy-and-give-families-more-choice-in-financial-services/> (дата звернення: 15.11.2025).

31. CreditOnline. Green Finance Loan Software – Solar & Sustainable Energy // CreditOnline: електрон. ресурс. URL: <https://www.creditonline.eu/green-finance/> (дата звернення: 15.11.2025).

32. CSE. Driving Sustainability: The Critical Role of Telematics in Insurance // CSE: електрон. ресурс. 2024. URL: <https://www.cse.com.my/blog/2024/02/02/driving-sustainability-the-critical-role-of-telematics-in-insurance/> (дата звернення: 15.11.2025).

33. DataReportal. Digital 2024: Ukraine // DataReportal: електрон. аналіт. звіт. 23.02.2024. URL: <https://datareportal.com/reports/digital-2024-ukraine> (дата звернення: 15.11.2025).

34. Daud S. N. M., Ahmad A. H., Trinugroho I. Financial inclusion, digital technology, and economic growth: Further evidence // Research in International Business and Finance: електрон. наук. журн. 2024. Vol. 70. Article 102361. URL: <https://doi.org/10.1016/j.ribaf.2024.102361> (дата звернення: 15.11.2025).

35. Diia.Education. Digital Money: online course // Diia.Education: електрон. освіт. ресурс. 2020. URL: <https://osvita.diia.gov.ua/en/courses/digital-money> (дата звернення: 15.11.2025).

36. DiXi Group. Almost 40% of Ukrainians have been manipulated about the causes of power outages: social survey results // DiXi Group: analytical brief, electronic resource. 19.12.2024. URL: <https://dixigroup.org/en/almost-40-of-ukrainians-have-been-manipulated-about-the-causes-of-power-outages-social-survey-results/> (дата звернення: 15.11.2025).

37. Dmytrenko T., Volkova V., Havrylenko S., Parkhomenko Yu. Overview of the new proposals regarding the regulation of the cryptoassets market in Europe and the ways of their implementation in Ukraine // RFI Scientific Papers: електрон. наук. журн. 2023. № 1. Р. 30–42. DOI: 10.33763/npndfi2023.01.030. URL: https://npndfi.org.ua/docs/NP_23_01_030_uk.pdf (дата звернення: 15.11.2025).

38. Dolbnieva D., Antypin Y., Kolisnyk O., та ін. Innovative transformation of a financial institution in the context of digitalisation and its impact on social conflict management // Financial and Credit Activity: Problems of Theory and Practice: електрон. наук. журн. 2024. Vol. 2(55). Р. 75–88. DOI: <https://doi.org/10.55643/fcaptr.2.55.2024.4386> (дата звернення: 15.11.2025).

39. Donnelly S., Ríos Camacho E., Heidebrecht S. Digital sovereignty as control: the regulation of digital finance in the European Union // Journal of European Public Policy: електрон. наук. журн. 2024. Vol. 31(8). Р. 2226–2249. DOI: <https://doi.org/10.1080/13501763.2023.2295520> (дата звернення: 15.11.2025).

40. Dovhan O. Analysis of the development of digital innovations in the financial services market in Ukraine in 2010–2024 // Економіка та суспільство: електрон. наук. журн. 2025. Вип. 71. С. 146–150. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/5492> (дата звернення: 15.11.2025).

41. Earnix. Leveraging Technology to Fulfill Insurers' Climate Change Commitments // Earnix: електрон. аналіт. ресурс. 2023.

URL: <https://earnix.com/assets/leveraging-technology-to-fulfill-insurers%27-climate-change-commitments.pdf>(дата звернення: 15.11.2025).

42. EcoActiveTech. Understanding ESG KPIs: Key Performance Indicators for Sustainable Success // EcoActiveTech: електрон. аналіт. ресурс. 03.07.2024. URL: <https://ecoactivetech.com/understanding-esg-kpis-key-performance-indicators-for-sustainable-success/> (дата звернення: 15.11.2025).

43. Ellex. EU payments legislation in transition: PSD3 and PSR status // Ellex: електрон. правовий ресурс. 15.09.2025. URL: <https://ellex.legal/eu-payments-legislation-in-transition-psd3-psr/> (дата звернення: 15.11.2025).

44. Eskandarany A. Adoption of artificial intelligence and machine learning in banking systems: a qualitative survey of board of directors // Frontiers in Artificial Intelligence: електрон. наук. журн. 2024. Т. 7. Article 1440051. URL: <https://doi.org/10.3389/frai.2024.1440051> (дата звернення: 16.11.2025). (ResearchGate)

45. European Banking Authority (EBA). Guidelines on ICT and security risk management (draft updated guidelines) // EBA: official website, electronic resource. 15.07.2025. URL: <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-ict-and-security-risk-management> (дата звернення: 15.11.2025).

46. European Banking Authority. Guidelines on ICT and security risk management (EBA/GL/2019/04) // European Banking Authority: офіц. сайт, електрон. ресурс. 2019. URL: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf (дата звернення: 15.11.2025).

47. European Banking Federation. Guidance for implementation of the revised Payment Services Directive: PSD2 Guidance // European Banking Federation: електрон. аналіт. документ. 2016. URL: https://www.ebf.eu/wp-content/uploads/2017/05/EBF_PSD2_guidance_September_2016.pdf (дата звернення: 15.11.2025).

48. European Business Association. A new era in financial services: open banking officially launched in Ukraine // European Business Association: news item, electronic resource. 04.08.2025. URL: <https://eba.com.ua/en/nova-era-finansovyyh-poslug-vidbuvsya-zapusk-vidkrytoho-bankingu-v-ukrayini/> (дата звернення: 16.11.2025).

49. European Central Bank. Climate-related financial disclosures // European Central Bank: офіц. сайт, електрон. ресурс. 2025. URL: <https://www.ecb.europa.eu/ecb/climate/climate-related-financial-disclosures/html/index.en.html> (дата звернення: 15.11.2025).

50. European Circular Economy Stakeholder Platform. Eco Repair Score®: a solution for informed and environmentally friendly vehicle repair choices // European Circular Economy Stakeholder Platform: електрон. ресурс. 2023. URL: <https://circulareconomy.europa.eu/platform/en/good-practices/eco-repair-score-solution-informed-and-environmentally-friendly-vehicle-repair-choices> (дата звернення: 15.11.2025).

51. European Commission. EU taxonomy for sustainable activities // European Commission: офіц. сайт, електрон. ресурс. 2025. URL: https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/eu-taxonomy-sustainable-activities_en (дата звернення: 15.11.2025).

52. European Commission. Framework for Financial Data Access (FiDA) // European Commission: official website, electronic resource. URL: https://finance.ec.europa.eu/digital-finance/framework-financial-data-access_en (дата звернення: 15.11.2025).

53. European Commission. Payment Services Directive (PSD2): Regulatory Technical Standards on strong customer authentication and secure communication // European Commission: прес-реліз, електрон. ресурс. 27.11.2017. URL: https://europa.eu/rapid/press-release_MEMO-17-4961_en.htm (дата звернення: 15.11.2025).

54. European Commission. Recommendations on complying with the AI Act for AI models with systemic risks (requirements for risk assessment, testing, reporting) // Reuters: electronic article. 18.07.2025.

URL: <https://www.reuters.com/sustainability/boards-policy-regulation/ai-models-with-systemic-risks-given-pointers-how-comply-with-eu-ai-rules-2025-07-18/> (дата звернення: 15.11.2025).

55. European Commission. What does data protection ‘by design’ and ‘by default’ mean? // European Commission: офіц. сайт, електрон. ресурс. 2025. URL: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (дата звернення: 15.11.2025).

56. European Insurance and Occupational Pensions Authority (EIOPA). Digital Operational Resilience Act (DORA) // EIOPA: офіц. сайт, електрон. ресурс. 2024. URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en (дата звернення: 15.11.2025).

57. European Parliamentary Research Service. Algorithmic discrimination under the AI Act and the GDPR // European Parliament: аналіт. записка, електрон. ресурс. 26.02.2025. URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769509/EPRS_ATAG\(2025\)769509_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769509/EPRS_ATAG(2025)769509_EN.pdf) (дата звернення: 15.11.2025).

58. European Securities and Markets Authority (ESMA). Statement on the use of AI in financial services: management responsibility and investor protection // Reuters: electronic article. 30.05.2024. URL: <https://www.reuters.com/business/finance/eu-watchdog-says-banks-must-take-full-responsibility-when-using-ai-2024-05-30/> (дата звернення: 15.11.2025).

59. ExecViva. ESG KPIs: The Executive Guide to Driving Sustainable Performance // ExecViva: електрон. ресурс. 19.09.2025. URL: <https://execviva.com/executive-hub/esg-kpis> (дата звернення: 15.11.2025).

60. EY. EY Global FinTech Adoption Index 2019 // EY: електрон. звіт. 2019. URL: https://www.ey.com/en_gl/ey-global-fintech-adoption-index (дата звернення: 16.11.2025).

61. Fang Y., Wen G. Stability Analysis of Innovation Collaboration between Commercial Banks and Fintech Companies // Mathematics: електрон. наук. журн.

2024. Т. 12, № 17. Стаття 2724. DOI: <https://doi.org/10.3390/math12172724> (дата звернення: 15.11.2025).

62. FAO. Rural women and financial inclusion: Technical Guidance Note // Food and Agriculture Organization of the United Nations: електрон. ресурс. Rome, 2024. DOI: <https://doi.org/10.4060/cc9522en> (дата звернення: 15.11.2025).

63. Faster Payments. Faster Payments Annual Report 2023 (UK) // Faster Payments / Pay.UK: електрон. ресурс. 2024. URL: <https://www.fasterpayments.org.uk/> (дата звернення: 16.11.2025).

64. Gálik I., Kaščáková A., Kajanová J. Digitalization and Artificial Intelligence: A Comparative Study of Indices on Digital Competitiveness // Information: електрон. наук. журн. 2025. Vol. 16, No. 4. Article 286. DOI: <https://doi.org/10.3390/info16040286> (дата звернення: 15.11.2025).

65. GDPR-info.eu. Privacy by Design – General Data Protection Regulation (GDPR): електрон. ресурс. 2024. URL: <https://gdpr-info.eu/issues/privacy-by-design/> (дата звернення: 15.11.2025).

66. Ghenai C., Belayadi M., Benidris M., та ін. AI, machine learning and deep learning in cyber risk management // Discover Sustainability: електрон. наук. журн. 2025. Vol. 6. Article 389. DOI: <https://doi.org/10.1007/s43621-025-01012-3> (дата звернення: 15.11.2025).

67. Green Digital Finance Alliance; Swiss Green Fintech Network. A Green Fintech Taxonomy and Data Landscaping / Green Fintech Classification: електрон. ресурс. 2021–2022. URL: <https://www.greenfinanceplatform.org/research/green-fintech-taxonomy-and-data-landscaping-0>; <https://www.greendigitalfinancealliance.org/news-and-events/the-worlds-first-green-fintech-taxonomy> (дата звернення: 15.11.2025).

68. Hasan M. та ін. FinTech and sustainable development: A systematic review // International Review of Economics & Finance: електрон. наук. журн. 2024. Vol. 92. P. 320–337. DOI: <https://doi.org/10.1016/j.iref.2023.12.012> (дата звернення: 15.11.2025).

69. Hassani A., Klingberg A. The EU AI Act and Its Implications for Credit Risk Models in Banking // Advisense: електрон. версія статті. 19.03.2025.

URL: <https://advisense.com/2025/03/19/the-eu-ai-act-and-its-implications-for-credit-risk-models-in-banking/> (дата звернення: 15.11.2025).

70. HES FinTech. Green finance lending software: електрон. ресурс. URL: <https://hesfintech.com/green-finance-software/> (дата звернення: 15.11.2025).

71. Hutukka P. Fintech law in the European Union, the United States and China: Regulation of financial technology in comparative context // Maastricht Journal of European and Comparative Law: електрон. наук. журн. 2024. DOI: <https://doi.org/10.1177/1023263X241298416> (дата звернення: 15.11.2025).

72. Iatzaz Ul Hassan M., Wu M., Lu J., Sohu J. M., Ali S., Anjum H. N., Bilal M. Financial technology and banking performance in developing countries: evidence from an advanced quantile regression approach // Humanities and Social Sciences Communications: електрон. наук. журн. 2025. Vol. 12. Article 1455. DOI: <https://doi.org/10.1057/s41599-025-05571-8> (дата звернення: 15.11.2025).

73. IdeaSoft. Online Banking Accessibility: How Fintech Products Can Become Inclusive: електрон. ресурс. 05.06.2025. URL: <https://ideasoft.io/blog/online-banking-accessibility/> (дата звернення: 15.11.2025).

74. Implementation of FinTech is the bank's competitive advantage // Financial and Credit Activity: Problems of Theory and Practice: електрон. наук. журн. 2024. № 3 (56). DOI: <https://doi.org/10.55643/fcaptp.3.56.2024.4368> (дата звернення: 15.11.2025).

75. Independent Evaluation Group. World Bank Group Support to Demand-Side Energy Efficiency: Effectiveness, Scale-Up Challenges, and Factors of Success: електрон. ресурс. Washington, DC: World Bank, 2023. URL: <https://ieg.worldbankgroup.org/evaluations/world-bank-group-support-demand-side-energy-efficiency/effectiveness-scale-challenges> (дата звернення: 15.11.2025).

76. Insurtech Digital. Tackling ESG Issues for a Green Future: електрон. ресурс. 01.11.2024. URL: <https://insurtechdigital.com/articles/tackling-esg-issues-for-a-green-future> (дата звернення: 15.11.2025).

77. International Banker. Unlocking the Power of Privacy-Enhancing Technologies in Financial Services: електрон. ресурс. 02.01.2024. URL: <https://internationalbanker.com/technology/unlocking-the-power-of-privacy-enhancing-technologies-in-financial-services/> (дата звернення: 15.11.2025).

78. International Finance Corporation (IFC). IFC 2025 Climate-related Disclosures. Washington, D.C., 2025. [Електронний ресурс]. – Режим доступу: <https://www.ifc.org/content/dam/ifc/doc/2025/ifc-ar25-climate-related-disclosures.pdf> (дата звернення: 15.11.2025).

79. International Finance Corporation. IFC Announces New Initiatives to Accelerate Ukraine's Reconstruction at Ukraine Recovery Conference // IFC: прес-реліз, електрон. ресурс. 10.07.2025. URL: <https://www.ifc.org/en/pressroom/2025/ifc-announces-new-initiatives-to-accelerate-ukraine-s-reconstruction-at-ukraine-re> (дата звернення: 15.11.2025).

80. International Finance Corporation. Technical Guidance for Financial Institutions on Greenhouse Gas Accounting. Washington, DC : IFC, 2023. [Електронний ресурс]. – Режим доступу: <https://www.ifc.org/content/dam/ifc/doc/2023-delta/technical-guidance-ghg.pdf> (дата звернення: 15.11.2025).

81. International Telecommunication Union. Digital Development Country Profile – Singapore, EU, US, China (2024–2025) // ITU: official website, electronic resource. URL: <https://www.itu.int/> (дата звернення: 16.11.2025).

82. International Telecommunication Union. Ukraine – Digital Development Country Profile (Advanced draft) // ITU: електрон. ресурс. 2023. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/Digital%20Development%20Country%20Profiles/Ukraine%20Digital%20Development%20Country%20Profile_Advanced%20Draft_V1%201_03.25.pdf (дата звернення: 16.11.2025).

83. Intuition. What are DORA's five pillars? Digital Operational Resilience Act. 07.05.2025. [Електронний ресурс]. – Режим доступу: <https://www.intuition.com/what-are-doras-five-pillars-digital-operational-resilience-act/> (дата звернення: 15.11.2025).

84. Iorgachova M., Kovalova O. Financial technologies in the development of banking activities in Ukraine's financial market // Economic Forum. 2025. Vol. 15, No. 1. P. 8–24. DOI: <https://doi.org/10.62763/ef/1.2025.08>.
85. Irving S., та ін. Understanding Banks' Disclosure of Emissions Reduction Targets [Електронний ресурс] // Association for Financial Markets in Europe (AFME), 2024. – Режим доступу: <https://www.afme.eu/our-work/sustainable-finance/afme-briefing-note-understanding-banks-disclosure-of-emissions-reduction-targets/> (дата звернення: 15.11.2025).
86. Javaid M., Haleem A., Singh R.P., Suman R., Khan S. A review of Blockchain Technology applications for financial services // BenchCouncil Transactions on Benchmarks, Standards and Evaluations. 2022. Vol. 2, No. 3. Article 100073. DOI: <https://doi.org/10.1016/j.tbench.2022.100073>.
87. Jia K., Wang L., Chen L. Bank Digital Transformation, Bank Competitiveness and Systemic Risk // Frontiers in Physics. 2023. Vol. 11. Article 1297912. DOI: <https://doi.org/10.3389/fphy.2023.1297912>.
88. Kálmán H. FinTech Sandboxes and the Expansion of Open Banking into Open Finance // FinTech. 2025. Vol. 4, No. 2. Article 26. DOI: <https://doi.org/10.3390/fintech4020026>.
89. Kinstellar. Open Banking in Ukraine enters a new stage of payments market digital transformation [Електронний ресурс]. 2025. – Режим доступу: <https://www.kinstellar.com/news-and-insights/detail/3646/open-banking-ukraine-enters-new-stage-of-payments-market-digital-transformation> (дата звернення: 15.11.2025).
90. Koval Y.O. Implementation of open banking in Ukraine: a comparative legal analysis with EU legislation // Uzhhorod National University Herald. Series: Law. 2025. Vol. 90, Part 5. P. 166–171. [Електронний ресурс]. – Режим доступу: <https://visnyk-pravo.uzhnu.edu.ua/article/view/340846> (дата звернення: 16.11.2025). DOI: <https://doi.org/10.24144/2307-3322.2025.90.5.20>.
91. KPMG China. China Fintech 50 Report 2023. 2024 // KPMG: analytical report, electronic resource.

URL: <https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2024/01/china-fintech-50-2023.pdf> (дата звернення: 15.11.2025).

92. KPMG. Setting the ground rules: the EU AI Act [Електронний ресурс]. 2024. – Режим доступу: <https://kpmg.com/xx/en/our-insights/ecb-office/setting-the-ground-rules-the-eu-ai-act.html> (дата звернення: 15.11.2025).

93. KPMG. Sustainable Finance: It's Action Time. Luxembourg : KPMG, 2019. [Електронний ресурс]. – Режим доступу: <https://assets.kpmg.com/content/dam/kpmg/lu/pdf/esg-brochure-2-web.pdf> (дата звернення: 15.11.2025).

94. Kretov D., Kretova O., Zherdetska L., Chaikovskiy Y. Digitalization Management in the Corporate Banking Sector of Ukraine // Economics. Ecology. Socium. 2024. Vol. 8, No. 3. P. 92–103. DOI: <https://doi.org/10.61954/2616-7107/2024.8.3-8>.

95. Li J., Maiti A., Fei J. Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things // Future Internet: електрон. наук. журн. 2023. Т. 15, № 8. Article 256. URL: <https://doi.org/10.3390/fi15080256> (дата звернення: 16.11.2025). (Bank for International Settlements)

96. Li Q., Zhang X. Digital finance development in China: A scientometric review // Heliyon: електрон. наук. журн. 2024. Vol. 10, No. 16. Article e36107. DOI: <https://doi.org/10.1016/j.heliyon.2024.e36107> (дата звернення: 15.11.2025).

97. Liu Z., Li X., Li Z. Inclusive FinTech, open banking, and bank performance: evidence from China // Financial Innovation: електрон. наук. журн. 2024. Vol. 10. Article 149. DOI: <https://doi.org/10.1186/s40854-024-00679-3> (дата звернення: 15.11.2025).

98. MAS – Monetary Authority of Singapore. Regulatory Sandbox // MAS: official website, electronic resource. URL: <https://www.mas.gov.sg/development/fintech/regulatory-sandbox> (дата звернення: 15.11.2025).

99. Mavlutova I., Spilbergs A., Verdenhofs A., Natrins A., Arefjevs I., Volkova T. Digital Transformation as a Driver of the Financial Sector Sustainable

Development: An Impact on Financial Inclusion and Operational Efficiency // Sustainability: електрон. наук. журн. 2023. 15(1):207. DOI: <https://doi.org/10.3390/su15010207> (дата звернення: 15.11.2025).

100. Medvid A., Dmitrishyn D. Digital banking in the financial services market of Ukraine // Visnyk of Sumy State University. Economics Series: електрон. наук. журн. 2024. Issue 2. P. 18–27. URL: https://visnyk.fem.sumdu.edu.ua/issues/2_2024/2.pdf (дата звернення: 15.11.2025).

101. Metelski D., Dylewski M., Tomczyk Ł. Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations // International Journal of Financial Studies: електрон. наук. журн. 2022. 10(4):108. DOI: <https://doi.org/10.3390/ijfs10040108> (дата звернення: 15.11.2025).

102. Mhlanga D., Dlamini S., Moloi T. Blockchain Technology for Digital Financial Inclusion in the Industry 4.0, Towards Sustainable Development? // Frontiers in Blockchain: електрон. наук. журн. 2023. Vol. 6. Article 1035405. DOI: <https://doi.org/10.3389/fbloc.2023.1035405> (дата звернення: 15.11.2025).

103. Microfinance Centre. The Fintech Market in Ukraine: Fintech Case Study. Warsaw: Microfinance Centre, 2020. 22 p. URL: https://mfc.org.pl/wp-content/uploads/2020/03/UKRAINE_FINTECH-CASE-STUDY_FEB2020.pdf (дата звернення: 15.11.2025).

104. Ministry of Digital Transformation of Ukraine. Application for obtaining Diia.City resident status // Diia Portal – “Guide to Public Services”: electronic resource. URL: <https://diia.gov.ua/services/zayava-pro-nabuttya-statusu-rezidenta-diya-city> (дата звернення: 15.11.2025).

105. Ministry of Digital Transformation of Ukraine. Diia.City: official web portal of the special legal regime for the IT industry // Diia.City: electronic resource. URL: <https://city.diia.gov.ua/> (дата звернення: 15.11.2025).

106. Ministry of Economy of Ukraine. Forecast 2025–2027: structural constraints to growth (shortage of skilled labour) // Ministry of Economy of Ukraine: analytical report, electronic resource. 2025.

URL: <https://me.gov.ua/download/39b49ee0-bf04-4fa3-bddc-47505dd2b444/file.pdf> (дата звернення: 15.11.2025).

107. Ministry of Economy of Ukraine. Survey of employers on the situation in the labour market (2024): 43% face difficulties filling vacancies // Ministry of Economy of Ukraine: official website, electronic resource. 03.06.2024. URL: <https://me.gov.ua/News/Detail?id=e9317d6b-282f-4346-bc90-2cc7b70a45b5&lang=uk-UA> (дата звернення: 15.11.2025).

108. Miroshnyk R., Kukhta I. Digitalization of the banking system of Ukraine in modern conditions // Economy and Society: електрон. наук. журн. 2023. Вип. 49. DOI: <https://doi.org/10.32782/2524-0072/2023-49-39> (дата звернення: 15.11.2025).

109. Monetary Authority of Singapore. Digital Readiness & FAST Payments // MAS: official website, electronic resource. URL: <https://www.mas.gov.sg/> (дата звернення: 16.11.2025).

110. Monetary Authority of Singapore. Overview of Regulatory Sandbox // MAS: official website, electronic resource. URL: <https://www.mas.gov.sg/development/fintech/regulatory-sandbox> (дата звернення: 16.11.2025).

111. Nagesh K. C., Murugan K. S. FinTech and Sustainable Finance: Impact of Digital Finance in Promoting Green Investments // mLAC Journal for Arts, Commerce and Sciences (m-JACS): електрон. наук. журн. 2025. Т. 3, № 1. DOI: <https://doi.org/10.59415/mjacs.v3i1.246> (дата звернення: 15.11.2025).

112. National Bank of Ukraine; Ukrainian News. BankID NBU system in 2024: number of identifications more than doubled over the year // National Bank of Ukraine: news item of 06.02.2025; Ukrainian News: news report “Identifications using BankID double in 2024”. URLs: <https://bank.gov.ua/ua/news/all/sistema-bankid-nbu-u-2024-rotsi-kilkist-identifikatsiy-za-rik-zroslo-bilshe-nij-udvichi>

113. National Bank of Ukraine. “Prosto pro ekonomiku” (Simply about the economy) based on the April 2025 Inflation Report: news item of 13.05.2025 // National Bank of Ukraine: official website, electronic resource. URL: <https://bank.gov.ua/en/news/all/prosto-pro-ekonomiku-na-osnovi-materialiv-inflyatsiynogo-zvitu-kviten-2025-roku> (дата звернення: 15.11.2025).

114. National Bank of Ukraine. Annual Report 2023: Financial fortress. Kyiv: NBU, 2024. 152 p. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2023_eng.pdf (дата звернення: 15.11.2025).

115. National Bank of Ukraine. BankID NBU // National Bank of Ukraine: official website, electronic resource. URL: <https://bank.gov.ua/en/bank-id-nbu> (дата звернення: 15.11.2025).

116. National Bank of Ukraine. Banking Sector Review. November 2024: analytical overview. Kyiv: NBU, 2024. 14 p. URL: https://bank.gov.ua/admin_uploads/article/Banking_Sector_Review_2024-11_eng.pdf (дата звернення: 15.11.2025).

117. National Bank of Ukraine. Card Market in First Nine Months of 2024: Share of Cashless Card Transactions Keeps Rising // National Bank of Ukraine: official website, electronic resource. 03.12.2024. URL: <https://bank.gov.ua/en/news/all/kartkoviy-rinok-za-devyat-misyatsiv-2024-roku-chastka-bezgotivkovih-operatsiy-prodovjuye-zrostaty> (дата звернення: 15.11.2025).

118. National Bank of Ukraine. Financial literacy, financial inclusion and financial well-being in Ukraine (OECD/INFE methodology) // National Bank of Ukraine: research report, electronic resource. 2021. URL: https://bank.gov.ua/admin_uploads/article/Research_Financial_Literacy_Inclusion_Welfare_2021_en.pdf (дата звернення: 15.11.2025).

119. National Bank of Ukraine. Financial Stability Report. June 2025. Kyiv: NBU, 2025. 48 p. URL: https://bank.gov.ua/admin_uploads/article/FSR_2025-H1_eng.pdf (дата звернення: 15.11.2025).

120. National Bank of Ukraine. From 1 December 2024 a new version of SEP with instant payments functionality has been launched in Ukraine // National Bank of Ukraine: official website, electronic resource. 01.12.2024. URL: <https://bank.gov.ua/en/news/all/z-01-grudnya-2024-roku-v-ukrayini-zapratsyuvala-nova-versiya-sep-z-funktsionalnistyu-mittyevih-perekaziv> (дата звернення: 15.11.2025).

121. National Bank of Ukraine. In 2024 SEP Continued Smooth Operations and Innovative Development // National Bank of Ukraine: official website, electronic resource. 13.01.2025. URL: <https://bank.gov.ua/en/news/all/u-2024-rotsi-sep-prodovjuvala-bezperebiyno-pratsyuvati-ta-innovatsiyno-rozvivatisya> (дата звернення: 15.11.2025).

122. National Bank of Ukraine. Instant payments and open banking: information page (links to the Law “On Payment Services”, Open Banking Concept and Regulation) // National Bank of Ukraine: official website, electronic resource. URLs: <https://bank.gov.ua/ua/payments/open-banking>; <https://bank.gov.ua/en/payments/open-banking> (дата звернення: 15.11.2025).

123. National Bank of Ukraine. ISO 20022 project and transition to the new SEP standard // National Bank of Ukraine: official website, electronic resource. URL: <https://bank.gov.ua/en/payments/project-iso20022> (дата звернення: 15.11.2025).

124. National Bank of Ukraine. NBU 2024 Consolidated Management Report (Consolidated financial statements for the year ended 31 December 2024). Kyiv: NBU, 2025. 144 p. URL: https://bank.gov.ua/admin_uploads/article/NBU_2024_consolidated_fsu_eng.pdf (дата звернення: 15.11.2025).

125. National Bank of Ukraine. Open Banking // National Bank of Ukraine: official website, electronic resource. URL: <https://bank.gov.ua/en/payments/open-banking> (дата звернення: 15.11.2025).

126. National Bank of Ukraine. QR-код для передавання реквізитів / Платежі стають зручнішими з новим QR-кодом // Національний банк України: офіц. сайт, електрон. ресурс. 09.02.2021. URL: <https://bank.gov.ua/ua/news/all/plateji-stayut-zruchnishimi-z-novim-qr-kodom> (дата звернення: 15.11.2025).

127. National Bank of Ukraine. Strategy of Ukrainian financial sector development until 2025. Kyiv: NBU, 2020. 40 p.

URL: https://bank.gov.ua/admin_uploads/article/Strategy_FS_2025_eng.pdf (дата звернення: 16.11.2025).

128. National Bank of Ukraine. System of Electronic Payments (SEP) // National Bank of Ukraine: official website, electronic resource. URL: <https://bank.gov.ua/en/payments/sep> (дата звернення: 15.11.2025).

129. National Bank of Ukraine. Безготівкові розрахунки у 2024 році суттєво переважали серед операцій з платіжними картками // Національний банк України: офіц. сайт, електрон. ресурс. 03.03.2025. URL: <https://bank.gov.ua/ua/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo-perevajali-sered-operatsiy-z-platijnimi-kartkami> (дата звернення: 15.11.2025).

130. National Bank of Ukraine. З 01 грудня 2024 року в Україні запрацювала нова версія СЕП з функціональністю миттєвих переказів // Національний банк України: офіц. сайт, електрон. ресурс. 01.12.2024. URL: <https://bank.gov.ua/ua/news/all/z-01-grudnya-2024-roku-v-ukrayini-zapratsyuvava-nova-versiya-sep-z-funktsionalnistyu-mittyevih-perekaziv> (дата звернення: 15.11.2025).

131. National Bank of Ukraine. Картковий ринок за дев'ять місяців 2024 року: токенизовані картки (+19 %, до 14,9 млн) // Національний банк України: офіц. сайт, електрон. ресурс. 03.12.2024. URL: <https://bank.gov.ua/ua/news/all/kartkoviy-rinok-za-devyat-misyatsiv-2024-roku-chastka-bezgotivkovih-operatsiy-prodovjuye-zrostaty> (дата звернення: 15.11.2025).

132. National Bank of Ukraine. Кількість випадків шахрайства з картками знизилася, збитки за ними – зросли (підсумки 2024 р.) // National Bank of Ukraine: official website, electronic resource. 12.05.2025. URL: <https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli> (дата звернення: 15.11.2025).

133. National Bank of Ukraine. Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами (підсумки 2023 р.) // National Bank of Ukraine: official website,

electronic resource. 02.04.2024. URL: <https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami> (дата звернення: 15.11.2025).

134. National Bank of Ukraine. Проєкт Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачів фінансових послуг (роль керівництва, інцидент-менеджмент) // National Bank of Ukraine: draft regulation, electronic resource. 10.03.2025. URL: https://bank.gov.ua/admin_uploads/article/proekt_2025-03-10.pdf (дата звернення: 15.11.2025).

135. National Bank of Ukraine. Результати опитування від НБУ та OpenDataBot: кожен дев'ятий опитаний ставав жертвою шахраїв з початку воєнного стану // National Bank of Ukraine: official website, electronic resource. 09.10.2023. URL: <https://bank.gov.ua/ua/news/all/rezultati-opituvannya-vid-nbu-ta-opendatabot-kojen-devyatiy-opitaniy-stavav-jertvoyu-shahrayiv-z-pochatku-voennogo-stanu> (дата звернення: 15.11.2025).

136. National Bank of Ukraine. Система BankID НБУ у 2024 році: кількість ідентифікацій за рік зросла більш ніж удвічі (до 87,7 млн) // National Bank of Ukraine: official website, electronic resource. 06.02.2025. URL: <https://bank.gov.ua/ua/news/all/sistema-bankid-nbu-u-2024-rotsi-kilkist-identifikatsiy-za-rik-zroslo-bilshe-nij-udvichi> (дата звернення: 15.11.2025).

137. National Bank of Ukraine. Система електронних платежів (СЕП): факти та цифри; середньодобові обсяги; реалізація миттєвих переказів у СЕП-4.1 // Національний банк України: офіц. сайт, електрон. ресурс. Б/д (оновл.). URL: <https://bank.gov.ua/ua/payments/sep> (дата звернення: 15.11.2025).

138. National Bank of Ukraine. У 2024 році СЕП продовжувала безперебійно працювати та інноваційно розвиватися // Національний банк України: офіц. сайт, електрон. ресурс. 13.01.2025. URL: <https://bank.gov.ua/ua/news/all/u-2024-rotsi-sep-prodovjuvala-bezperebiyno-pratsyuvati-ta-innovatsiyno-rozvivatisya> (дата звернення: 15.11.2025).

139. National Bank of Ukraine. Упровадження стандарту ISO 20022: параметри миттєвих переказів СЕП-4.1 // Національний банк України: офіц. сайт,

електрон. ресурс. Б/д (оновл.). URL: <https://bank.gov.ua/ua/payments/project-iso20022> (дата звернення: 15.11.2025).

140. Nelaturu K., Pathak N., Ali A. A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions // *Cryptography: електрон. наук. журн.* 2022. 6(2):18. DOI: <https://doi.org/10.3390/cryptography6020018> (дата звернення: 15.11.2025).

141. OECD/INFE. 2023 International Survey of Adult Financial Literacy (global results) // OECD: electronic resource. 2023. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/12/oecd-infe-2023-international-survey-of-adult-financial-literacy_8ce94e2c/56003a32-en.pdf (дата звернення: 15.11.2025).

142. Okoli T. T. Gauging the Impact of Digital Finance on Financial Stability in the Presence of Multiple Unknown Structural Breaks: Evidence from Developing Economies // *Economies: електрон. наук. журн.* 2025. 13(7):187. DOI: <https://doi.org/10.3390/economies13070187> (дата звернення: 15.11.2025).

143. Open Banking Limited. JROC programme and future entity // Open Banking: official website, electronic resource. URL: <https://www.openbanking.org.uk/jroc/> (дата звернення: 15.11.2025).

144. Opendatabot. Open data on companies, private entrepreneurs, courts and real estate in Ukraine: official website // Opendatabot: electronic resource. URL: <https://opendatabot.ua/> (дата звернення: 15.11.2025).

145. Papathomas D., Karousos I. N., Tsihrizis G., та ін. Financial institutions digital transformation in the European Union: stages of maturity along with indicators and results // *SN Business & Economics: електрон. наук. журн.* 2024. Vol. 4. Article 242. DOI: <https://doi.org/10.1057/s41264-023-00223-x> (дата звернення: 15.11.2025).

146. People's Bank of China. Notice on promoting high-quality digital finance development // People's Bank of China: official website, electronic resource. URL: <https://www.pbc.gov.cn/en/3688253/3689009/4180845/5576773/index.html> (дата звернення: 15.11.2025).

147. Pew Research Center. Mobile Banking Statistics 2023–2024 // Pew Research Center: electronic resource. URL: <https://www.pewresearch.org/> (дата звернення: 16.11.2025).
148. Pinto S. O., Sobreiro V. A. Literature review: Anomaly detection approaches on digital business financial systems // Digital Business: електрон. наук. журн. 2022. 2(2):100038. DOI: <https://doi.org/10.1016/j.digbus.2022.100038> (дата звернення: 15.11.2025).
149. Pobochenko L., та ін. Risks of investing in FinTech at the global and national levels // CEUR Workshop Proceedings. 2025. Vol. 4024. P. 468–478. URL: <https://ceur-ws.org/Vol-4024/paper30.pdf> (дата звернення: 16.11.2025).
150. PrivatBank. Підсумки роботи ПриватБанку (довідкова інформація щодо продуктів розстрочки в складі роздрібного кредитування) // PrivatBank: офіц. сайт, електрон. ресурс. Б/д (оновл.). URL: <https://privatbank.ua/cpa/pidsumky> (дата звернення: 15.11.2025).
151. Prokopenko O., Pliushch V., Kyslyi V., Kononova K. Improving customer relations via digital banking products and services for Ukrainian banks // Banks and Bank Systems: електрон. наук. журн. 2022. 17(3):12–21. DOI: [https://doi.org/10.21511/bbs.17\(3\).2022.02](https://doi.org/10.21511/bbs.17(3).2022.02) (дата звернення: 15.11.2025).
152. Reuters. Singapore to trial tokenised bills, bring in stablecoin laws, central bank chief says. 13.11.2025 // Reuters: electronic article. URL: <https://www.reuters.com/world/asia-pacific/singapore-trial-tokenised-bills-bring-stablecoin-laws-central-bank-chief-says-2025-11-13/> (дата звернення: 15.11.2025).
153. Reuters. Some electronic payments systems in Ukraine disrupted // Reuters: electronic article. 26.04.2025. URL: <https://www.reuters.com/technology/some-electronic-payments-systems-ukraine-disrupted-2025-04-26/> (дата звернення: 15.11.2025).
154. Reuters. Ukraine keeps key rate on hold, cuts growth forecast amid energy challenges // Reuters: electronic article. 23.10.2025. URL: <https://www.reuters.com/world/europe/ukraine-keeps-key-rate-hold-cuts-growth-forecast-amid-energy-challenges-2025-10-23/> (дата звернення: 15.11.2025).

155. Reuters. US judge blocks consumer agency's "open banking" rules for now. 29.10.2025 // Reuters: electronic article. URL: <https://www.reuters.com/sustainability/boards-policy-regulation/us-judge-blocks-consumer-agencys-open-banking-rules-now-2025-10-29/> (дата звернення: 15.11.2025).

156. Shmygol N., Polyezhayev Y., Shtyrov D., та ін. Financial security of economic processes in the context of digital technologies: cybersecurity threats to Ukrainian banking system under the conditions of martial law // *Financial and Credit Activity: Problems of Theory and Practice*: електрон. наук. журн. 2025. 4(63). DOI: <https://doi.org/10.55643/fcaptp.4.63.2025.4790> (дата звернення: 15.11.2025).

157. Smal V., Vdovychenko A. How digital remittances help Ukraine during crises // *Geopolitics under Globalization*: електрон. наук. журн. 2024. 5(1):67–78. DOI: [https://doi.org/10.21511/gg.05\(1\).2024.05](https://doi.org/10.21511/gg.05(1).2024.05) (дата звернення: 15.11.2025).

158. State Statistics Service of Ukraine. Indicator 9.6.1 "Population coverage with Internet services, subscribers per 100 inhabitants" // *SDG National Reporting Platform*: electronic resource. 2019–2023. URL: <https://sdg.ukrstat.gov.ua/uk/9-6-1/> (дата звернення: 15.11.2025).

159. Totska O. Fintech market in Ukraine: analysis and development prospects // *Economic Innovations*: electronic journal. 2023. (cited by web version). URL: <https://journals.nupp.edu.ua/eir/article/view/3034> (дата звернення: 15.11.2025).

160. Transfi. Ukraine's payment rails & how they work — SEPA links, NBU systems & instant transfers: analytical overview. 01.09.2025. URL: <https://www.transfi.com/blog/ukraines-payment-rails-how-they-work---sepa-links-nbu-systems-instant-transfers> (дата звернення: 15.11.2025).

161. Treiblmaier H. Business Implications and Theoretical Integration of the Markets in Crypto-Assets (MiCA) Regulation // *FinTech*: електрон. наук. журн. 2025. 4(2):11. DOI: <https://doi.org/10.3390/fintech4020011> (дата звернення: 15.11.2025).

162. Tymots M. Analysis of trends and prospects of digital banking in Ukraine // *International Science Journal of Management, Economics & Finance*: electronic

journal. 2025. URL: <https://isg-journal.com/isjmef/article/view/1089>(дата звернення: 15.11.2025).

163. Ukrainian Association of Fintech and Innovation Companies; Ministry of Digital Transformation of Ukraine; National Bank of Ukraine; International Finance Corporation (IFC); State Secretariat for Economic Affairs (SECO); Green for Growth Fund (GGF); Ukrainian Startup Fund (USF). Ukrainian Fintech Catalog 2024: key ecosystem indicators (256 companies; funding structure; internationalization) // UAFIC: electronic resource. 2024. URLs: https://fintechua.org/catalog_2024eng; https://fintechua.org/download_catalog_2024 (дата звернення: 15.11.2025).

164. Ukrainian Association of FinTech and Innovation Companies. Ukrainian Association of FinTech and Innovation Companies: official website // UAFIC: electronic resource. URL: <https://fintechua.org/en> (дата звернення: 15.11.2025).

165. Ukrinform. Торік кількість ідентифікацій у системі BankID НБУ зросла більш ніж удвічі // Ukrinform: news item, electronic resource. 08.02.2025. URL: <https://www.ukrinform.ua/rubric-economy/3957819-torik-kilkist-identifikacij-u-sistemi-bankid-nbu-zrosla-bils-niz-udvici.html> (дата звернення: 16.11.2025).

166. Urikova O., Mysko Y., Karyu O. Fintech Industry of Ukraine: Prospects and Challenges // Scientific Bulletin of Lviv Polytechnic National University. Series “Management and Entrepreneurship in Ukraine”. 2025. Vol. 9, No. 1. P. 96–111. DOI: 10.23939/semi2025.01.096 (дата звернення: 15.11.2025).

167. Urikova O., Mysko Y., Karyu O. Fintech industry of Ukraine: prospects and challenges // Scientific Bulletin of Lviv Polytechnic National University. Series “Management and Entrepreneurship in Ukraine”. 2025. Vol. 9, No. 1. P. 96–111. URL: <https://science.lpnu.ua/semi/all-volumes-and-issues/volume-9-number-1-2025/fintech-industry-ukraine-prospects-and-challenges> (дата звернення: 16.11.2025).

168. Varga S., Brynielsson J., Franke U. Cyber-threat perception and risk management in the Swedish financial sector // Computers & Security: електрон. наук. журн. 2021. Vol. 105. Article 102239. DOI: <https://doi.org/10.1016/j.cose.2021.102239> (дата звернення: 15.11.2025).

169. Verheliuk Y., Hantsiak M., Fomov D. Digital transformation of the banking system: global guidelines for Ukraine // Finance of Ukraine: електрон. наук. журн. 2025. № 3. С. 45–57. DOI: <https://doi.org/10.33763/finukr2025.03.045>(дата звернення: 15.11.2025).
170. Verkhovna Rada of Ukraine. Pro platizhni posluhy (On Payment Services): Law of Ukraine of 30.06.2021 No. 1591-IX // Database “Legislation of Ukraine”: electronic resource. URL: <https://zakon.rada.gov.ua/go/1591-20> (дата звернення: 15.11.2025).
171. Verkhovna Rada of Ukraine. Pro zatverdzhennia Polozhennia pro vidkrytyi banking v Ukraini: Resolution of the Board of the National Bank of Ukraine of 25.07.2025 No. 80 // Database “Legislation of Ukraine”: electronic resource. URL: <https://zakon.rada.gov.ua/go/v0080500-25> (дата звернення: 15.11.2025).
172. Vijayagopal P., Karthikeyan P., Natarajan B., Chitra K. Regulations and Fintech: A Comparative Study of the Global Fintech Regulatory Landscape // Journal of Risk and Financial Management: електрон. наук. журн. 2024. 17(8):324. DOI: <https://doi.org/10.3390/jrfm17080324> (дата звернення: 15.11.2025).
173. Visa. Visa Stay Secure Study 2025: 80% of Ukrainians mostly or completely trust digital payments: press release of 14.05.2025 // Visa: official website, electronic resource. URL: https://www.visa.com.ua/en_UA/about-visa/newsroom/press-releases/prl-14052025.html (дата звернення: 15.11.2025).
174. Wen W., Liang Y. Digital Transformation and Liquidity Creation in Commercial Banks: Evidence from the Chinese Banking Industry // PLOS ONE: електрон. наук. журн. 2025. 20(2):e0318785. DOI: <https://doi.org/10.1371/journal.pone.0318785> (дата звернення: 15.11.2025).
175. World Bank. Global Financial Inclusion (Global Findex) Database 2021 – Ukraine: microdata & documentation // World Bank Microdata Library: електрон. ресурс. 2022. URL: <https://microdata.worldbank.org/index.php/catalog/4721>(дата звернення: 15.11.2025).
176. World Bank. Global Findex Database 2021 // World Bank: official website, electronic resource. URL: <https://globalfindex.worldbank.org/> (дата звернення: 16.11.2025).

177. World Bank. The Global Findex Database 2021 – Chapter 2: Use of Accounts // World Bank: електрон. ресурс. 29.06.2022.
URL: <https://www.worldbank.org/en/publication/globalfindex/brief/the-global-findex-database-2021-chapter-2-use-of-accounts> (дата звернення: 15.11.2025).

178. YouControl. YouControl company – online company verification service: official website // YouControl: electronic resource.
URL: <https://youcontrol.com.ua/en/> (дата звернення: 15.11.2025).

ДОДАТКИ

Додаток А

Ключові технологічні платформи та їх роль у цифровій операційній моделі

Технологічна платформа	Основна роль / функція	Типові кейси у фінансових інститутах	Ключові вимоги / ризики
AI/ML	Аналітичне ядро прийняття рішень	Кредитний і поведінковий скоринг, антифрод, персоналізація, ціноутворення ризику	Якість даних, model risk, explainability, уникнення дискримінації
Big Data	Збір та збагачення даних	Реальний час аналітики, клієнтські 360-профілі, альтернативні дані	Data governance, приватність, DQ-політики
Хмарні обчислення, мікросервіси	Операційна платформа	CI/CD, еластичність під піки, модульна модернізація core	Vendor lock-in, кіберризики, SLA з провайдерами
DLT / смарт-контракти	Альтернативний механізм довіри	Токенізація, швидкий кліринг, параметричне страхування	Вартість інтеграції, регуляторна невизначеність
API / open finance	Інтероперабельність, інтеграції	Open banking, embedded finance, B2B2C-партнерства	Безпека API, моніторинг, управління доступом партнерів
eID / eKYC, біометрія	Дистанційна ідентифікація	Онбординг, підписання договорів, SCA	Точність, недискримінаційність, захист біометричних шаблонів
RPA / low-code	Автоматизація бек-офісу	KYC/AML-перевірки, звітність, супровід кредитів	Управління змінами, контроль «shadow IT»
Zero Trust / кіберстійкість	Безпековий каркас	Постійна верифікація, мікросегментація, DevSecOps	Складність впровадження, потреба в безперервному моніторингу

Джерело: створено автором за матеріалами [44; 66; 88; 95; 98; 140; 168]