Міністерство освіти і науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

Магістерська робота

на тему «Розвиток банківського сектору України в умовах цифровізації: виклики та перспективи»

Виконав: студент 6-го курсу, групи 601-ЕФ
Спеціальності
072 «Фінанси, банківська справа, страхування та фондовий ринок»
за освітньо-професійною програмою «Фінанси, банківська справа та страхування»
другого (магістерського) рівня вищої освіти
Тіхонов І.Г.
Керівник: к.е.н., доц. Скриль В.В.
Рецензент: дир. відділення «Полтавське № 3»
Sense Bank (м.Полтава)
Турченко М.М.

Засвідчую, що в цій роботі немає запозичень із праць інших авторів без відповідних посилань
Тіхонов І.Г.
Підтверджую достовірність даних, використаних у роботі
Тіхонов І.Г.

Полтава, 2026 року

АНОТАЦІЯ

Тіхонов І.В. Розвиток банківського сектору України в умовах цифровізації: виклики та перспективи. Рукопис. Магістерська робота на здобуття другого (магістерського) рівня вищої освіти зі спеціальності 072 «Фінанси, банківська справа, страхування та фондовий ринок» за освітньо-професійною програмою «Фінанси, банківська справа та страхування», Національний університет «Полтавська політехніка імені Юрія Кондратюка»,, Полтава, 2026.

Робота містить 76 сторінок, 15 таблиць, 13 рисунків, список літератури з 92 джерел та 9 додатки.

Ключові слова: цифровізація, цифровая трансформація, банківський сектор України, фінансові технології (FinTech), необанки, дистанційне банківське обслуговування, безготівкові платежі, штучний інтелект (AI), GenAI, кібербезпека, Zero Trust, цифрова зрілість, відкритий банкінг, регуляторна гармонізація, конкурентоспроможність банків.

Тема магістерської роботи є досить актуальною, оскільки розвиток банківського сектору України в умовах цифровізації є критично важливим чинником забезпечення його довгострокової фінансової стійкості та конкурентоспроможності. Цифровізація як складний процес перетворення інформації та операцій у цифрову форму істотно впливає не лише на поточну трансформацію ринку фінансових послуг, а й фактично визначає стратегічні траєкторії його подальшого розвитку.

Метою роботи є визначення ключових викликів та перспектив розвитку банківського сектору України в умовах цифровізації.

Об’єкт дослідження є банківський сектор України як система фінансових інститутів, що функціонує в умовах цифрової трансформації та макроекономічної нестабільності.

Предмет дослідження є сукупність економічних, організаційних та технологічних відносин, що виникають у процесі цифровізації банківської діяльності, а також механізми впливу цифрових технологій на стійкість, безпеку та конкурентоспроможність банків.

У теоретичній частині роботи розкрито теоретико-методичні основи цифровізації банківської діяльності, зокрема економічну сутність цифрової трансформації, методи оцінювання рівня цифрової зрілості (Digital Maturity) та особливості нормативно-правового регулювання цифрового банкінгу.

У розрахунково-аналітичній частині роботи здійснено аналіз сучасного стану та ключових викликів розвитку банківського сектору України в умовах цифровізації, включаючи оцінку динаміки безготівкових платежів, поширення необанківських моделей, а також аналіз бар'єрів цифрової трансформації, зумовлених наявністю застарілих IT-систем (Legacy Systems), зростанням кіберризиків та впливом зовнішніх факторів; окреслено перспективи та напрями розвитку банківського сектору України в умовах цифровізації, визначено стратегічні пріоритети інноваційного розвитку, обґрунтовано підходи до нейтралізації кіберзагроз і запропоновано комплекс заходів, спрямованих на підвищення конкурентоспроможності банківських установ.

Інформаційне забезпечення дослідження включає нормативно-правову базу України та міжнародні стандарти; статистичні та аналітичні дані НБУ; Науково-методичну літературу та експертні звіти; аналітичну інформацію про ринок FinTech та необанків, а також аналітичні матеріали щодо інновацій та зовнішніх ризиків, що формують ключові виклики та перспективи розвитку українського банківського сектору.

SUMMARY

Tikhonov I.V. Development of Ukraine's banking sector in the context of digitalization: challenges and prospects. Master's work on obtaining a second (master's) level of higher education from the specialty 072 "Finance, Banking, Insurance and Stock Market" in the educational and professional program "Finance, Banking and Insurance", National University Yuri Kondratyuk Poltava Polytechnica, Poltava, 2026.

The work comprises 76 pages, 15 tables, 13 figures, a list of references with 92 sources, and 9 appendices.

Keywords: digitalization, digital transformation, banking sector of Ukraine, financial technologies (FinTech), neobanks, remote banking, cashless payments, artificial intelligence (AI), GenAI, cybersecurity, Zero Trust, digital maturity, open banking, regulatory harmonization, competitiveness of banks.

The topic of the master's thesis is quite relevant, since the development of the banking sector of Ukraine in the context of digitalization is a critical factor in ensuring its long-term financial stability and competitiveness. Digitalization as a complex process of converting information and transactions into digital form significantly affects not only the current transformation of the financial services market, but also actually determines the strategic trajectories of its further development.

The purpose of the work is to identify key challenges and prospects for the development of the banking sector of Ukraine in the context of digitalization.

The object of the study is the banking sector of Ukraine as a system of financial institutions functioning in the context of digital transformation and macroeconomic instability.

The subject of the study is a set of economic, organizational and technological relations that arise in the process of digitalization of banking, as well as the

mechanisms of influence of digital technologies on the sustainability, security and competitiveness of banks.

In the theoretical part of the work, the theoretical and methodological foundations of digitalization of banking activities are revealed, in particular, the economic essence of digital transformation, methods for assessing the level of digital maturity (Digital Maturity) and the peculiarities of regulatory regulation of digital banking.

In the calculation and analytical part of the work, an analysis of the current state and key challenges of the development of the banking sector of Ukraine in the context of digitalization is carried out, including an assessment of the dynamics of cashless payments, the spread of neobanking models, as well as an analysis of digital transformation barriers due to the presence of outdated IT systems (Legacy Systems), the growth of cyber risks and the impact of external factors; outlines the prospects and directions of development of the banking sector of Ukraine in the context of digitalization, identifies strategic priorities for innovative development, substantiates approaches to neutralizing cyber threats and proposes a set of measures aimed at increasing the competitiveness of banking institutions.

Information support of the study includes the regulatory framework of Ukraine and international standards; statistical and analytical data of the NBU; Scientific and methodological literature and expert reports; analytical information on the FinTech and neobank market, as well as analytical materials on innovations and external risks that form key challenges and prospects for the development of the Ukrainian banking sector.

ЗМІСТ

ВСТУП ..……..... 5

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ЦИФРОВІЗАЦІЇ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ…….……...……. 7

1.1.Економічна сутність та фактори впливу цифровізації на банківський бізнес…….……..... 7

1.2. Формування методичного інструментарію оцінки рівня цифровізації банків...……. 11

1.3. Нормативно-правове регулювання цифрового банкінгу в Україні та світі……..……..……...…….. 14

Висновки до розділу 1……. 19

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ТА ВИКЛИКІВ РОЗВИТКУ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ В УМОВАХ ЦИФРОВІЗАЦІЇ …… 20

2.1. Оцінка рівня цифровізації банківського сектору України …….. 20

2.2. Виклики та бар'єри на шляху цифрової трансформації українських банків…….……....…… 32

2.3. Вплив зовнішніх факторів на процеси цифровізації банківського сектору..……...…….. 36

Висновки до розділу 2……. 39

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА НАПРЯМИ РОЗВИТКУ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ В УМОВАХ ЦИФРОВІЗАЦІЇ…… 41

3.1. Стратегічні пріоритети інноваційного розвитку банківського сектору …….……. 41

3.2. Шляхи подолання викликів кібербезпеки та вдосконалення регулювання……..……. 45
3.3. Пропозиції щодо підвищення конкурентоспроможності українських банків…….……. 50
Висновки до розділу 3……. 59
ВИСНОВКИ ……..... 61
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ …….. 67
ДОДАТКИ ……... 76

ВСТУП

Актуальність теми полягає в тому, що розвиток банківського сектору України в умовах цифровізації є критично важливим чинником забезпечення його довгострокової фінансової стійкості та конкурентоспроможності. Цифровізація як складний процес перетворення інформації та операцій у цифрову форму істотно впливає не лише на поточну трансформацію ринку фінансових послуг, а й фактично визначає стратегічні траєкторії його подальшого розвитку. В умовах стрімкої глобальної цифрової трансформації та безпрецедентних економічних викликів банківський сектор України перебуває у фазі глибоких структурних змін. Особливої актуальності досліджувана проблематика набула у 2022–9 місяців 2025 роках, коли зовнішні шокові фактори, зумовлені воєнним конфліктом, стали каталізатором прискореної модернізації бізнес-моделей банків, а цифрові технології трансформувалися із джерела конкурентних переваг у базовий інструмент забезпечення операційної стійкості та безперервності діяльності. У цих умовах потреба в упровадженні сучасних цифрових рішень є об’єктивною передумовою підвищення ефективності функціонування банківських установ і зміцнення їх позицій на фінансовому ринку.

Метою роботи є визначення ключових викликів та перспектив розвитку банківського сектору України в умовах цифровізації. Досягнення поставленої мети зумовлює необхідність вирішення комплексу завдань, а саме: дослідження економічної сутності цифровізації та чинників її впливу на банківський бізнес, формування методичного інструментарію оцінювання рівня цифровізації банків; аналізу сучасного стану та оцінки глибини цифрової трансформації банківського сектору України, зокрема щодо масштабу впровадження безготівкових розрахунків і цифрових карткових технологій; ідентифікації ключових викликів, бар’єрів і впливу зовнішніх чинників на процеси цифрової трансформації вітчизняних банків, у тому числі проблем застарілої IT-інфраструктури, зростання кіберризиків та кадрових обмежень; визначення стратегічних пріоритетів інноваційного розвитку банківського сектору з акцентом на

модернізацію ядра банківських систем, впровадження генеративного штучного інтелекту (GenAI) та інструментів гіперперсоналізації клієнтського досвіду; розроблення практичних напрямів протидії кіберзагрозам шляхом впровадження архітектури нульової довіри (Zero Trust) і вдосконалення регуляторного середовища через гармонізацію із європейськими стандартами (GDPR, MiFID II); формування прикладних пропозицій щодо підвищення конкурентоспроможності українських банків, зокрема шляхом розвитку партнерств у форматі Bank–FinTech та системного підвищення рівня цифрової грамотності клієнтів і персоналу.

Об’єкт дослідження є банківський сектор України як система фінансових інститутів, що функціонує в умовах цифрової трансформації та макроекономічної нестабільності.

Предмет дослідження є сукупність економічних, організаційних та технологічних відносин, що виникають у процесі цифровізації банківської діяльності, а також механізми впливу цифрових технологій на стійкість, безпеку та конкурентоспроможність банків.

Структура роботи включає вступ, три розділи, висновки, список використаних джерел і додатки. У першому розділі розкрито теоретико-методичні основи цифровізації банківської діяльності, зокрема економічну сутність цифрової трансформації, методи оцінювання рівня цифрової зрілості (Digital Maturity) та особливості нормативно-правового регулювання цифрового банкінгу. Другий розділ присвячено аналізу сучасного стану та ключових викликів розвитку банківського сектору України в умовах цифровізації, включаючи оцінку динаміки безготівкових платежів, поширення необанківських моделей, а також аналіз бар’єрів цифрової трансформації, зумовлених наявністю застарілих IT-систем (Legacy Systems), зростанням кіберризиків та впливом зовнішніх факторів. У третьому розділі окреслено перспективи та напрями розвитку банківського сектору України в умовах цифровізації, визначено стратегічні пріоритети інноваційного розвитку, обґрунтовано підходи до нейтралізації кіберзагроз і запропоновано комплекс заходів, спрямованих на підвищення конкурентоспроможності банківських установ.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ЦИФРОВІЗАЦІЇ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

1.1. Економічна сутність та фактори впливу цифровізації на банківський бізнес

Цифровізація – це складний процес перетворення інформації, даних у цифрову форму, що підвищує потенціал їх використання для виконання окремих завдань. Важливо розуміти, що сам процес цифровізації не є кінцевою метою, а лише інструментом досягати конкретних цілей, які є складними або неможливими досягати цього шляхом традиційної обробки інформації. Оцифрування додає нові можливості до нецифрових артефактів, роблячи їх програмованими, адресованими, розумними, комунікабельними, запам'ятовуваними, відстежуваними та соціативними [1].

Сьогодні процеси цифровізації набирають обертів і поступово проникають у всі сектори країни економіка та громадське життя. Відповідно, вони також створювати нові можливості, особливо в бізнесі поле. Однак підвищення ефективності економічної діяльності шляхом активного використання цифровізації можливе лише через розуміння природи цього процесу, ознак його впливу на функціонування різних систем, включно з ринком фінансових послуг. Цифровізація впливає не лише на зміни, що відбуваються на цьому ринку, вона фактично визначає його подальший розвиток. Потреба у використанні відповідних нових технологій є об'єктивною передумовою для банків та інших фінансових компаній, щоб підвищити свою конкурентоспроможність на фінансових ринках. Тепер можна виявити вже чітко сформовані трансформації в розвитку цього ринку, які були спричинені впливом інформаційних технологій. До них належать наступні:

- полегшення переказу коштів між особами клієнти;
- доступність швидких способів оплати товарів;

- онлайн-сервіси для обслуговування клієнтів;

- можливість замовляти фінансові послуги онлайн (страхування, кредит, депозитні послуги);

- підвищення прозорості банківських установ та фінансових послуг, можливість відстежувати рух власних фінансових ресурсів за допомогою спеціальних додатків;

- миттєві грошові перекази через смартфон;

- скорочення часу на фінансові послуги;

- можливість отримання консультацій та інших Інформація цілодобово онлайн консультації, чат-форуми;

- збільшується доступність фінансових послуг, фінансова інклюзія активно розвивається;

- активний розвиток нових стартапів, що призвело до створення нової сфери FinTech;

- підвищення рівня конкуренції між фінансами установи;

- зниження витрат на обслуговування клієнтів;

- активний розвиток віртуальних банків та інших фінансові установи.

Для проведення аналізу варто розглянути наукові підходи щодо тлумачення концепції «цифровізації» (табл.Додаток А).

Виходячи з наведених вище визначень, можна зробити висновок, що цифровізація банківського бізнесу пов'язана з оцифрування всіх бізнес-процесів та інформації про діяльність банку. Отже, впровадження цифрових технологій Технології в банківському бізнесі вимагають врахування потреб трьох суб'єктів цього процесу – споживача, інвестора та самого банку.

Під час виконання своєї діяльності банки стають учасниками та джерелами створення великої кількості інформації, яка має різні форми та різні цілі, тому для її використання слід встановити визначений режим. Регулювання роботи банків з інформацією, яка насамперед пов'язана з конфіденційною інформацією, є важливим для всього банківського сектору.

Автори статті [7] віднесли основні чинники, що впливають на процес цифровізації банківського бізнесу: формування концепції цифровізації, формування цифрових компетенцій у персоналі та відмову від застарілих технологій.

Саме тому варто розглянути поняття «цифрової трансформації» в банківській сфері.

Цифрова трансформація в банківській справі інтегрує технології в усі сфери банківської справи для підвищення ефективності, доступності та обслуговування клієнтів.

Цифрова трансформація в банківській справі використовує технології, щоб зробити банківські послуги ефективнішими, доступнішими та орієнтованішими на клієнта. Наприклад, мобільний банкінг та онлайн-транзакції надають клієнтам легший доступ до своїх рахунків та спрощують проведення транзакцій. Перехід до цифрових технологій також звільняє місце для розширеного аналізу даних та штучного інтелекту (ШІ). Разом ці інновації допомагають банкам налаштовувати взаємодію зі своїми клієнтами, виявляти шахрайські дії та прогнозувати фінансові тенденції.

З розвитком банківської галузі цифрова трансформація стає дедалі популярнішою. Клієнти хочуть інтегрованого, персоналізованого, прозорого та безпечного цифрового досвіду. Щоб це сталося, банкам необхідно централізувати свої дані. Це дозволить їм створити безперебійний клієнтський досвід на всіх каналах, включаючи мобільні додатки та вебсайти [8].

Варто зазначити, що існують чотири основні сфери цифрової трансформації в банківській справі (рис.1.1).

Покращення клієнтського досвіду передбачає розробку зручних мобільних банківських додатків та проектування безперебійного омніканального досвіду. Аналітика та аналітика даних використовують машинне навчання та великі дані для виявлення тенденцій, раннього виявлення шахрайства та використання прогнозного моделювання для передбачення потреб та поведінки клієнтів. Операційна ефективність досягається шляхом впровадження хмарної

інфраструктури для масштабованості та економічної ефективності, а також використання роботизованих процесів для автоматизації завдань. Інновації бізнес-моделей включають впровадження блокчейну для безпечних та економічно ефективних транскордонних транзакцій та впровадження інноваційних цифрових продуктів, таких як рішення для однорангових платежів. Разом ці сфери стимулюють розвиток банківської справи відповідно до сучасних вимог.

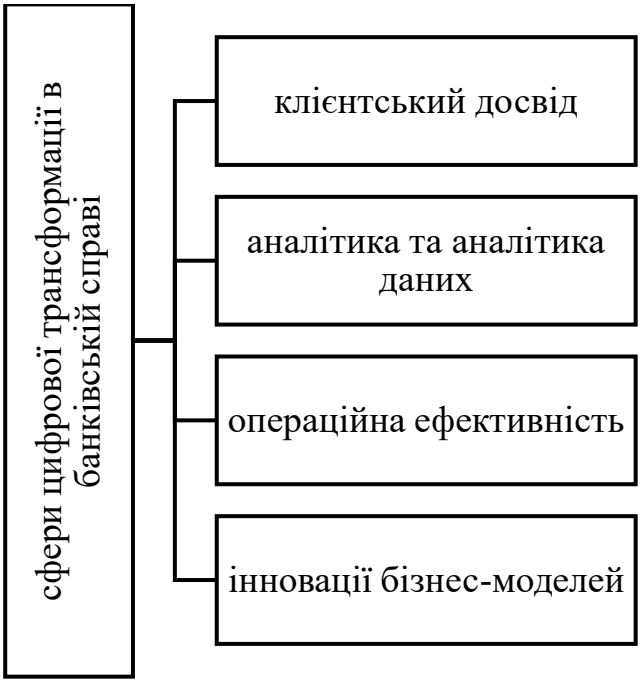

Рис. 1.1. Сфери цифрової трансформації в банківській справі [сформовано астором]

Одним із найважливіших аспектів цифрової трансформації в банківській сфері є адаптація до змін. Банки традиційно обтяжені проблемами безпеки, правилами та суворими практиками, що забезпечують конфіденційність клієнтів та безпеку даних. Для успішної цифровізації банки повинні розвивати свою політику, щоб відповідати змінам попиту клієнтів та ринкових умов. Створення цифрової культури та побудова необхідних платформ і послуг є основоположними кроками. Після того, як ці елементи будуть впроваджені, банки можуть надавати значну цінність своїм клієнтам, використовуючи автоматизацію, штучний інтелект, зрілість даних та технології блокчейн.

Варто відзначити той факт, що банки використовують цифрові технології в кількох напрямках (рис.1.2).

Отже, банки впроваджують цифрові інструменти для пришвидшення запуску нових продуктів і послуг. Ці технології формують клієнтоорієнтований досвід. Вони також спрощують внутрішні бізнес-моделі. Хмарні банківські інтерфейси, такі як Salesforce Financial Services Cloud, є безпечними та надійними. Це дозволяє банкам зосередитися на інноваціях для клієнтів і швидше виводити продукти на ринок.

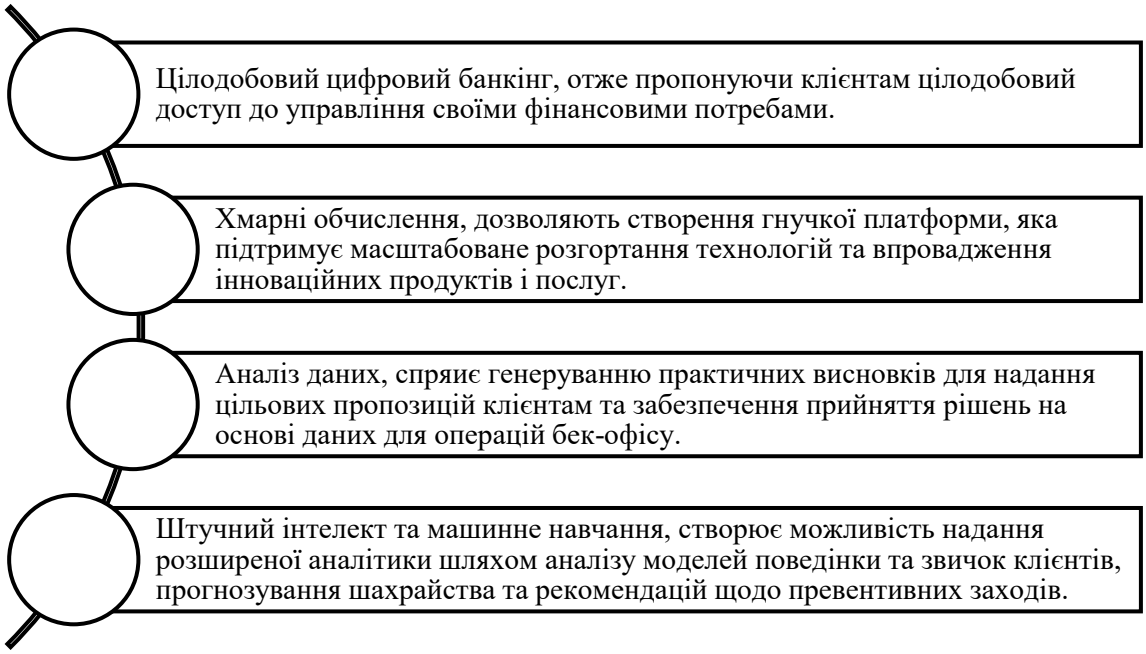

Рис. 1.2. Напрями використання цифрових технологій у банківській сфері [сформовано автором]

1.2. Формування методичного інструментарію оцінки рівня цифровізації банків

Формування методичного інструментарію на основі критеріїв та показників оцінки цифрової зрілості (Digital Maturity) банківської установи. Варто відзначити, що цифрова зрілість (Digital Maturity) є ключовим стратегічним імперативом для світової банківської індустрії, перетворившись із можливого напряму на необхідну умову для збереження

конкурентоспроможності та задоволення постійно зростаючих потреб клієнтів [9,10]. Висока цифрова зрілість безпосередньо корелює зі значним зростанням доходів: найбільш розвинені банки та кредитні спілки звітують про двократне збільшення річного приросту доходу порівняно з менш зрілими конкурентами [11].

Отже, цифрова зрілість – це стан, у якому організація успішно інтегрує три критичні компоненти: стратегію, технології та культуру [12]. Цифрові лідери активно використовують розширену аналітику, щоб персоналізувати взаємодію, ідентифікувати можливості для зростання та диверсифікувати пропозиції.

Так, для об'єктивного вимірювання рівня цифровізації використовують багатовимірні методологічні інструменти, такі як багатовимірна модель цифрової зрілості (Multi-Dimensional Digital Maturity Framework – MDDMF), що ґрунтується на п’яти основних стовпах: стратегія та узгодженість, операційна досконаліть, клієнтський досвід (CX), технології та дані, а також управління, ризик-менеджмент та комплаєнс (GRC).

На сьогодні, Європейський центральний банк (ЄЦБ) у своїй наглядовій діяльності також виділяє ключові критерії оцінки, які включають [13]:

– Формулювання чіткої та добре артикульованої цифрової стратегії.

– Наявність адекватних фінансових та нефінансових виконавчих можливостей для належної реалізації стратегії.

– Розробка всеосяжної системи ключових показників ефективності (KPIs) для моніторингу реалізації стратегії.

Враховуючи результати дослідження, можна зазначити, що цифрова зрілість охоплює чотири різні сегменти, які демонструють різний рівень інтеграції цифрових технологій:

1. Patiently exploring (14% опитаних). Невеликі організації, які лише починають свій цифровий шлях і покладаються на сторонніх постачальників.

2. Innovation-ready (39%). Мають базову цифрову присутність і готові до інвестицій у технології, пріоритетом є користувацький досвід.

3. Digital-forward (38%). Вище середнього рівня, мають сильну цифрову стратегію та активно автоматизують внутрішні процеси.

4. Data-first (9%). Найбільш просунута стадія, характеризується стратегічним, керованим даними мисленням (data-driven mindset) для прийняття рішень та інновацій [14].

Також в роботі для формування методичного інтсрументарію було досліджено критерії та показники оцінки рівня автоматизації (операційна досконаліть).

Так, рівень автоматизації є критичним показником операційної досконалості (Pillar II MDDMF). Організації з високою цифровою зрілістю активно автоматизують бек-енд процеси та використовують сучасні технології.

Автоматизація внутрішніх процесів та модернізація IT-інфраструктури є ключовими цілями цифрової стратегії, оскільки це підвищує операційну ефективність. Технології, як-от роботизована автоматизація процесів (RPA) та штучний інтелект (AI), відіграють важливу роль у оптимізації операцій, зниженні витрат на обробку, підвищенні продуктивності праці співробітників та мінімізації людських помилок [15]. В таблиці Додаток Б сформовано основні показники рівня автоматизації банківської системи.

Наступним кроком було досліджено методичний інструментарій оцінки критерієв та показників оцінки частки цифрових продажів банківської системи.

Оцінка частки цифрових продажів належить до критеріїв стратегії та узгодженості (Pillar I) та клієнтського досвіду (Pillar III), демонструючи комерційний успіх цифрової трансформації.

Банки з високою цифровою зрілістю зосереджуються на редизайні ключових клієнтських епізодів для забезпечення зручності в усіх каналах [16]. В таблиці Додатоку В сгруповано ключові показники (KPI) оцінки цифрових продажів у банківському секторі.

На настпуному етапі варто визначити методичний іструментарій критерієв та показників оцінки залученості клієнтів (клієнтський досвід).

Цифровий банкінг є «платою за вхід» у фінансові відносини, особливо для міленіалів, хоча і для покоління X (86%) та бебі-бумерів (90%) якісний цифровий досвід також є важливим. Оцінка залученості клієнтів є центральною для клієнтського досвіду (Pillar III).

Цифрові лідери (Data-first) використовують розширену аналітику для персоналізації взаємодії з клієнтами [17,18]. В таблиці Додатку Г представлено їх аналіз.

Послідовне відстеження та реагування на ці показники дозволяє банкам покращувати користувацький досвід, культивувати міцні відносини з клієнтами та процвітати в сучасному цифровому середовищі.

Також варто відзначити, що для оцінки рівня цифровізації в банківському секторів використовують традиційні методи бюджетування капіталу, що є необхідною відправною точкою, оскільки вони забезпечують базову фінансову мову щодо ефективності та часової вартості грошей. В таблиця Додатку Д сформовано традиційні методи оцінки ефективності цифрових інвестицій у банківському секторі.

Застосування ROI та NPV для оцінки інвестицій у цифрові технології виявляє значні методологічні обмеження, особливо з огляду на специфіку банківського середовища.

1.3. Нормативно-правове регулювання цифрового банкінгу в Україні та світі

Регуляторний ландшафт цифрових фінансових послуг в Україні характеризується процесом гармонізації національного законодавства з нормами Європейського Союзу (ЄС), зокрема з директивою PSD2 (Revised Payment Services Directive) [35]. Національний банк України (НБУ) виступає центральним регулятором та наглядовим органом, який визначає правила функціонування платіжних систем, фінансового моніторингу та кіберзахисту [36].

Визначальну роль у цифровій трансформації фінансового сектора України відіграє Закон України «Про платіжні послуги» (№ 1591-IX від 30.06.2021), який створює архітектуру для сучасного платіжного ринку [35].

Відкритий банкінг в Україні визначається як безпечний та структурований обмін даними між надавачами платіжних послуг з обслуговування рахунку (ASPSP) та сторонніми надавачами платіжних послуг (TPP, а саме PISP/AISP) через спеціалізовані інтерфейси (API). Цей обмін здійснюється виключно за згодою користувача [37].

Варто відзначити, що ключові нормативні акти НБУ, що регулюють відкритий банкінг:

– Положення про відкритий банкінг в Україні [37].

– Порядок авторизації діяльності надавачів нефінансових платіжних послуг [38].

– Положення про використання електронних довірчих послуг (ЕДП) (Постанова Правління НБУ № 82 від 25.07.2025). Воно є критично важливим для забезпечення безпечної електронної взаємодії та ідентифікації сторонніх надавачів платіжних послуг (PISP, AISP) перед ASPSP, що є аналогом вимоги PSD2 щодо використання кваліфікованих eIDAS-сертифікатів [39].

– Положення про порядок страхування відповідальності PISP/AISP, яке є ключовим механізмом захисту споживачів [40].

– Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку [41].

Організація та здійснення належної перевірки клієнта (Customer Due Diligence, CDD) в Україні регламентується Законом України «Про запобігання та протидію легалізації [42]» та Положенням НБУ № 107 від 28.07.2020 [43].

НБУ дозволяє використовувати повноцінні моделі віддаленої ідентифікації та верифікації, які можуть застосовуватися без лімітів до операцій:

– Відеоверифікація (спілкування з уповноваженим працівником через відеотрансляцію).

– BankID + Кваліфікований електронний підпис (КЕП) клієнта.

– Отримання е-паспорта клієнта (завіреного електронною печаткою «ДІЯ») разом із фотофіксацією особи з використанням методу розпізнавання реальності особи (Liveness detection method).

Також передбачені спрощені моделі верифікації (наприклад, BankID, КЕП, верифікація даних через бюро кредитних історій), які можуть використовуватися, якщо ризик ділових відносин є низьким, але при цьому діють ліміти на видаткові фінансові операції: не більше 40 тис. грн на місяць та 400 тис. грн на рік.

Щодо міжнародних стандартів безпеки та захисту даних варто відзначити, що у своїй роботі вони використовують Директиву PSD2 та посилену автентифікація (SCA). Розглянемо більш детальної ці стандарти.

PSD2 є європейською директивою, що набула чинності в січні 2018 року, і спрямована на посилення безпеки та конкуренції в електронних платежах. Ключовою вимогою є Strong Customer Authentication (SCA) – посилена автентифікація, яка вимагає використання двох або більше незалежних факторів з трьох категорій:

1. Знання (те, що знає лише користувач, наприклад, пароль або PIN-код).

2. Володіння (те, чим володіє користувач, наприклад, токен, мобільний пристрій).

3. Приналежність (те, чим користувач є, наприклад, біометричний ідентифікатор).

Крім того, регуляторні технічні стандарти (RTS) PSD2 вимагають динамічного пов'язування (Dynamic Linking), що гарантує, що код автентифікації є унікальним для конкретної суми платежу та отримувача. Будь-яка зміна суми або отримувача робить початковий код недійсним. Для безпеки та ідентифікації TPP зобов'язані використовувати кваліфіковані eIDAS-сертифікати, видані Кваліфікованим надавачем довірчих послуг (QTSP) [44].

Щодо загального регламенту про захист даних (GDPR), то варто зазначити, що GDPR – це найсуворіший у світі закон про конфіденційність та безпеку даних, який поширюється на організації, що обробляють персональні дані громадян або резидентів ЄС, незалежно від місцезнаходження самої організації [51].

Також варто відзначити, що основні принципи обробки персональних даних згідно зі статтею 5 GDPR включають:

– Законність, справедливість та прозорість обробки.

– Обмеження цілі, тобто дані повинні збиратися для визначених, явних і законних цілей.

– Мінімізація даних, значить дані мають бути адекватними, релевантними та обмеженими до необхідного.

– Обмеження зберігання, тобто дані повинні зберігатися у формі, що дозволяє ідентифікацію, не довше, ніж це необхідно для цілей обробки.

– Цілісність та конфіденційність, тобто обробка має забезпечувати належну безпеку персональних даних.

– Підзвітність (Accountability), це свідчить про те, що контролер несе відповідальність за демонстрацію відповідності цим принципам.

Наступним головним кроком і життєвою необіхдністю сьогодення є кіберзахист та управління технологічними ризиками.

НБУ розробив вимоги до функціонування системи кіберзахисту в банківській системі України, затверджені Постановою Правління НБУ № 178 від 12 серпня 2022 року, які визначають основні засади функціонування системи кіберзахисту та принципи інформаційного обміну з Центром кіберзахисту НБУ [45].

Для небанківських фінансових установ (страховиків, кредитних спілок, фінкомпаній, ломбардів) НБУ розробив проєкт Положення, яке встановлює вимоги до інформаційної безпеки та кіберзахисту з урахуванням Регламенту ЄС про цифрову операційну стійкість фінансового сектору (DORA). Серед ключових вимог:

– Надавач фінансових послуг зобов’язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем.

– Потрібно забезпечити дотримання принципу надання мінімального рівня повноважень.

– Встановлено заборону аутсорсингу юридичним особам та фізичним особам-підприємцям, які є резидентами держави-агресора, або здійснюють обробку/зберігання даних за допомогою хмарних обчислень на території держави-агресора.

Наступним не менш важливим є зниження системних ризиків таких як хмарні обчислення та штучний інтелект [55].

1. Концентраційний ризик (Cloud Risk). Збільшення впровадження хмарних послуг фінансовими установами (FIs) призвело до занепокоєння регуляторів (зокрема, Рада з фінансової стабільності, FSB) щодо потенційного концентраційного ризику – залежності від обмеженої кількості великих постачальників хмарних послуг. Цей ризик виникає як на рівні окремої установи (через численні домовленості з одним провайдером), так і в ширшому фінансовому секторі. Міжнародні органи, такі як Банк міжнародних розрахунків (BIS), розробляють принципи для протидії широкомасштабним збоям.

2. Вразливості, пов'язані з AI. Швидке впровадження Штучного інтелекту (AI), зокрема Генеративного AI (GenAI), може посилювати системні вразливості. FSB визначила, що ці ризики включають: посилення залежностей від третіх сторін, ринкові кореляції, кіберризик та ризик моделі (Model Risk):

– Ризик моделі. Це потенціал несприятливих наслідків, що виникають через рішення, засновані на неправильних або неналежно використаних моделях. Посилений модельний ризик викликаний, зокрема, недостатньою пояснюваністю (opacity) AI-моделей.

– Рекомендації FSB/BIS. Регулятори закликають посилювати моніторинг впровадження AI, оцінювати, чи є чинні політичні рамки достатніми для управління AI-ризиками, та вдосконалювати наглядові можливості. Існує потреба в міжнародній співпраці для вирішення проблеми різноманітності визначень AI та забезпечення більш послідовного нагляду.

– Концентрація AI-провайдерів. Зростаюча концентрація постачальників хмарних послуг та AI-сервісів серед невеликої кількості великих технологічних фірм підсилює аргументи на користь прямого нагляду за цими критичними сторонніми провайдерами.

Висновок до розділу 1

У результаті проведеного дослідження встановлено, що цифровізація банківської діяльності є об’єктивним і незворотним процесом, який суттєво змінює економічну сутність банківських послуг, бізнес-моделі та конкурентне середовище фінансового ринку. Визначено, що цифровізація виступає не самоціллю, а стратегічним інструментом підвищення ефективності, доступності та якості банківського обслуговування, формуючи нові можливості для розвитку фінансових послуг та взаємодії з клієнтами.

Обґрунтовано, що ключовою умовою успішної цифрової трансформації є досягнення високого рівня цифрової зрілості, яка базується на інтеграції стратегії, технологій та організаційної культури. Доведено доцільність використання комплексних моделей оцінювання рівня цифровізації, зокрема багатовимірних підходів, що дозволяють об’єктивно вимірювати операційну ефективність, результативність цифрових продажів та рівень залученості клієнтів, а також оцінювати економічну доцільність інвестицій у цифрові технології.

Встановлено, що нормативно-правове регулювання цифрових процесів у банківській сфері в Україні перебуває в активній фазі гармонізації з європейськими стандартами, що створює передумови для розвитку відкритого банкінгу, підвищення рівня безпеки фінансових операцій та захисту прав споживачів. Водночас доведено, що цифровізація супроводжується зростанням кіберризиків, концентраційних ризиків та ризиків, пов’язаних із використанням штучного інтелекту, що актуалізує необхідність удосконалення систем управління ризиками та посилення регуляторних вимог до інформаційної безпеки.

Узагальнено, що подальший розвиток банківської сфери неможливий без системного впровадження цифрових технологій, формування цифрової культури та забезпечення балансу між інноваційністю, безпечністю й регуляторною відповідністю, що створює методологічну основу для подальших аналітичних досліджень у наступних розділах роботи.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ТА ВИКЛИКІВ РОЗВИТКУ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ В УМОВАХ ЦИФРОВІЗАЦІЇ

2.1. Оцінка рівня цифровізації банківського сектору України

В умовах стрімкої глобальної цифровізації та безпрецедентних економічних викликів, банківський сектор України перебуває у фазі глибокої трансформації. Саме тому здійснимо аналіз сучасного стану фінансових установ, ідентифікації ключових можливостей, що їх відкриває інтеграція FinTech-рішень, а також викликів, пов'язаних із кібербезпекою, регуляторним навантаженням та конкуренцією з боку небанківських гравців.

Розвиток платіжного ринку в Україні демонструє послідовне та стійке домінування безготівкових платежів, яке прискорилося навіть в умовах повномасштабної війни. За п'ять років до 2024 року частка безготівкових операцій зросла більш ніж утричі. Аналіз частики безготівкових розрахунків (ЧБР) проводиться за двома основними метриками: за кількістю операцій (що відображає частоту використання) та за обсягом (що відображає фінансовий потік) [60].

У 2021 році, який розглядається як довоєнний базовий період, частка безготівкових операцій становила 61% за сумою та 90,1% за кількістю. Незважаючи на суттєві інфраструктурні втрати на початку повномасштабної війни, зокрема скорочення кількості активних платіжних терміналів приблизно на третину станом на 01.05.2022, платіжний ринок не лише зберіг стабільність, а й продемонстрував подальше посилення рівня цифровізації [61].

В таблиці 2.1 наведено динаміка частки безготівкових операцій із використанням платіжних карток у 2021–2025 рр.

Наступним варто розглянути структурний розподіл безготівкових операцій за їх типами. Узагальнена інформація щодо аналізу структури безготівкових

операцій (POS, P2P, E-commerce) представлена у таблиці 2.2. і показує, як змінювалися споживчі пріоритети в умовах війни та економічної стабілізації.

Таблиця 2.1

Динаміка частки безготівкових операцій із використанням платіжних карток у 2021–2025 рр. [63]

Період	ЧБР за кількістю (%)	ЧБР за сумою (%)	Різниця (кількість – сума), п.п.
2021 рік	90,1%	61,0%	29,1
Квітень 2022 (адаптація)	90,0%	71,0%	19,0
2023 рік	93,5%	65,0%	28,5
2024 рік	94,6%	64,5%	30,1
I квартал 2025	95,2%	65,2%	30,0
I півріччя 2025	95,3%	65,3%	30,0
9 місяців 2025	95,4%	65,4%	30,0

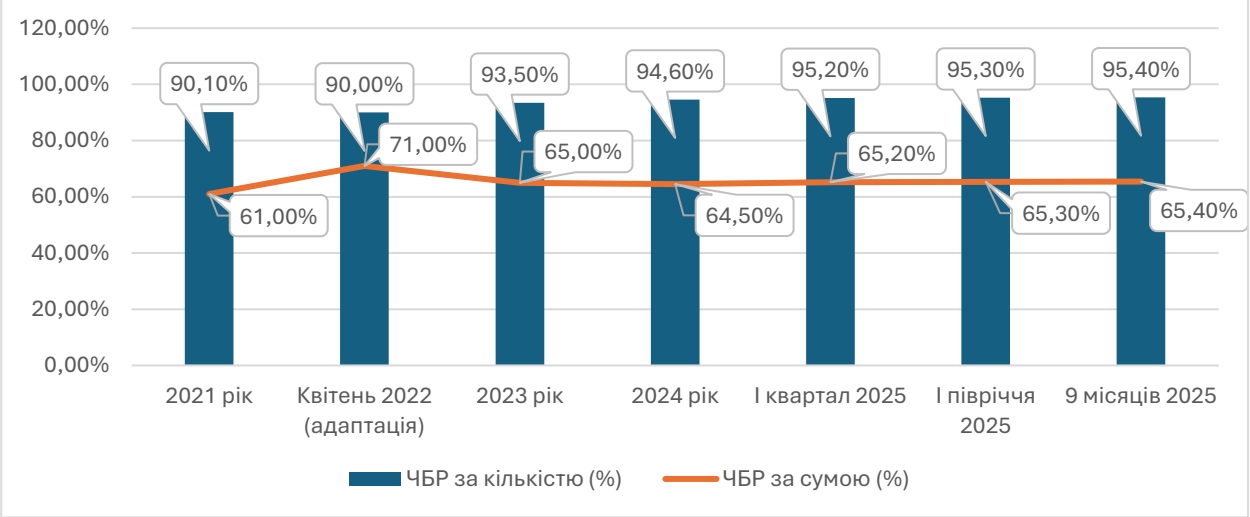

Рис.2.1. Динаміка частки безготівкових операцій із використанням платіжних карток в Україні у період 2021–2025 рр.

Спостерігається зменшення частки P2P-переказів за сумою (з 37,1% у 2023 р. до 26,7% у 9 місяцях 2025 р.) та зростання частки POS-операцій (з 40,4% до 50,7% за той же період). Це свідчить про повернення платіжних потоків до споживчого рітейлу та зменшення питомої ваги нерегулярних (волонтерських, кризових) великих переказів. POS-транзакції домінують за кількістю, перевищуючи 74% у 9 місяцях 2025 року.

Таблиця 2.2

Структура безготівкових операцій за типом (за кількістю та обсягом) у 2023–2025 рр. [63]

Сегмент	2023 рік	2024 рік	9 місяців 2025 року
POS (Торг. мережа), % кількість	~70%	73,4%	74,4%
POS (Торг. мережа), % сума	40,4%	46,8%	50,7%
P2P (Перекази), % кількість	10,1%	8,2%	7,3%
P2P (Перекази), % сума	37,1%	31,1%	26,7%
Online (E-commerce), % кількість	18,0%	13,6%	13,7%
Online (E-commerce), % сума	16,0%	14,7%	16,1%

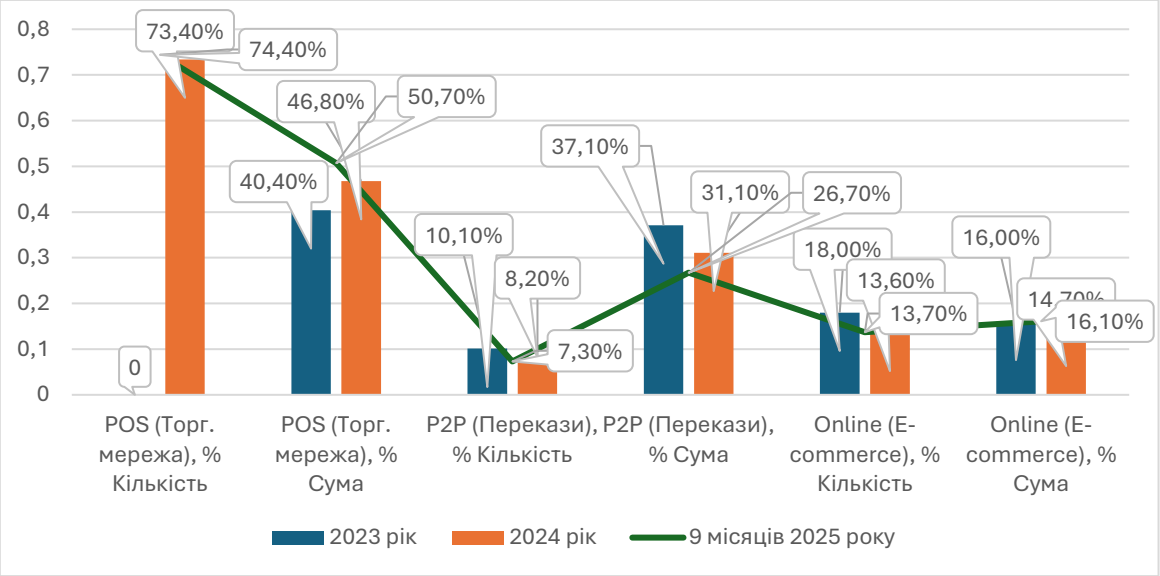

Рис.2.2. Зміни у структурі безготівкових платежів за обсягом у період 2023-9 місяців 2025 рр.

На наступному етапі здійснимо динаміку середнього розміру безготівкової операції (AVT). В таблиці 2.3 сформовано динаміка середньої суми однієї безготівкової операції за 2021-9 місяців 2025 рр.

За результатами рис.2.3 спостерігається істотне зростання AVT у рітейлі та E-commerce (зростання POS з 238 грн у 2021 р. до 345 грн у 9М 2025 р.). Середній чек P2P-переказів продемонстрував зниження на 129 грн у 9 місяцях 2025 року порівняно з аналогічним періодом 2024 року. Це зниження свідчить про глибоке проникнення мобільного банкінгу та використання P2P-сервісів для регулярних, дрібніших розрахунків, а не лише для великих нерегулярних сум.

Таблиця 2.3

Динаміка середньої суми однієї безготівкової операції (AVT), грн у період 2021–2025 рр. [66]

Період	POS (торг. мережа), грн	P2P (перекази), грн	Online (інтернет), грн
2021 рік	238	1 512	395
2023 рік	325	1 972	490
9 місяців 2024	322	1 976	553
2024 рік	330	1 958	561
9 місяців 2025	345	1 847	598
Приріст 9М 2024 до 9М 2025	+23 грн	-129 грн	+45 грн

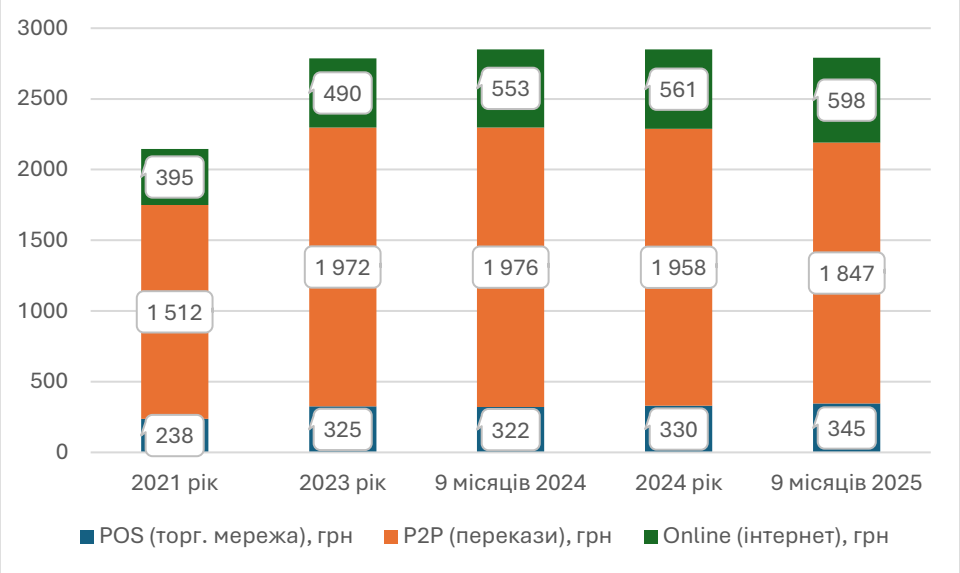

Рис. 2.3. Порівняння середнього чека (AVT) за ключовими сегментами у період 2021- 9 місяців 2025 рр.

Наступним проаналізуємо проникнення Інтернет-банкінгу та мобільних додатків.

Високі показники безготівкових розрахунків неможливі без широкого проникнення цифрових банківських каналів. НБУ активно розвиває інфраструктуру, а споживачі демонструють високу лояльність до мобільних рішень.

Інтернет-банкінг (через ПК) та мобільні додатки є основними каналами управління рахунками. Хоча дані щодо України від Асоціації банків (АУБ) не

надані в джерелах у форматі порівняння каналів, аналіз, представлений Американською асоціацією банкірів (ABA) щодо користувачів, може бути використаний для ілюстрації загальносвітового тренду, який, ймовірно, повторюється і в Україні, зважаючи на високий рівень цифровізації [69].

Щодо до загального проникнення мобільного банкінгу, то у світовому контексті (за даними опитування ABA, 2024 р.) мобільні додатки стали каналом, який використовують найчастіше, для 55% американських споживачів.

Серед покоління Gen X (1965–1980) 55% опитаних використовують мобільні додатки, тоді як онлайн-банкінг через ПК – 24%. Це співвідношення (понад 2:1) підкреслює структурний зсув на користь мобільних рішень як основного інтерфейсу для фінансових послуг.

Також НБУ визначив, що можливість використовувати картки щодня є базовою потребою під час війни. Наявність 132 мільйонів емітованих платіжних карток станом на 1 січня 2025 року та висока частка активних карток (58,8 млн шт. або 44,5% від емітованих) свідчить про високу цифрову інклюзію.

Відзначається і високий рівень проникнення мобільних додатків сприяє зростанню популярності безконтактних платежів, що ініціюються через NFC-технологію або токенізовані картки. В таблиці 2.4 представлено динаміка проникнення цифрових карткових технологій [70,71,72].

Таблиця 2.4

Динаміка проникнення цифрових карткових технологій за 2023-2025 рр.

Показник	грудень 2023 року	грудень 2024 року	9 місяців 2025 року	Зміна (2023–2024)
Активні токенізовані картки (млн шт.)	12,4	16,5	18,6	+33%
Частка токенізованих карток у активних (%)	Приблизно 23,8% (кожна 4-та)	Приблизно 28,1% (майже кожна 4-та)	31,5% (майже кожна 3-тя)	+4,3 в.п.
Активні безконтактні картки (млн шт.)	30,6	35,0	(N/A)	+14%
Частка безконт. операцій у рітейлі (Кількість)	90,0%	95,0%	98,2% (розрах.)	+5,0 в.п.

**за 9 місяцях 2025 року лише 1,8% операцій за кількістю здійснювалися з фізичним зчитуванням даних, відповідно 98,2% були безконтактними/NFC.*

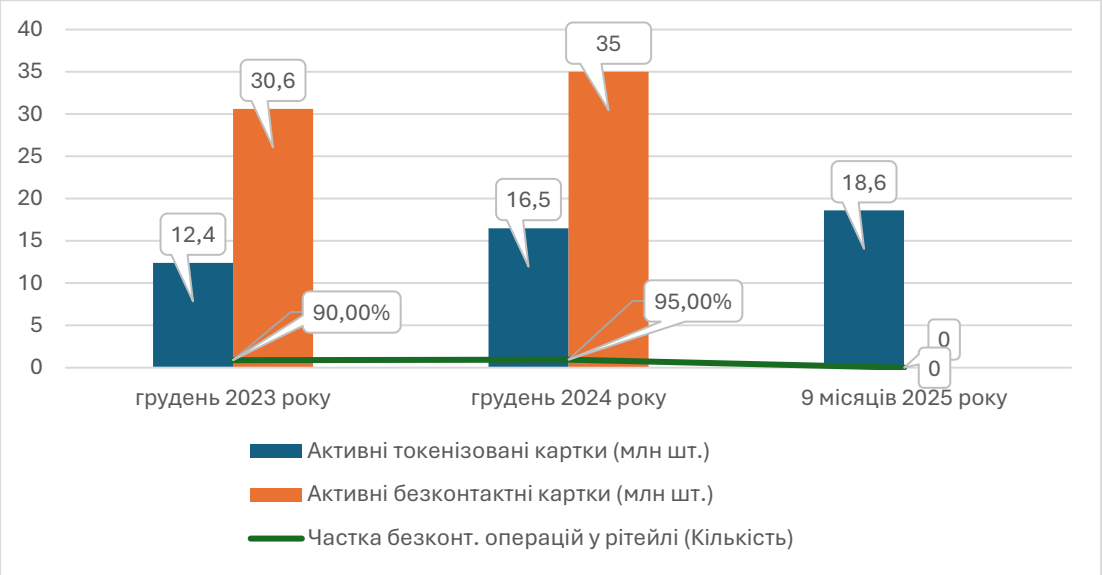

Рис.2.5. Кількість активних токенізованих платіжних карток у період 2023–2025 та їх частка у загальній кількості активних карток

Кількість токенізованих карток (NFC) зросла на 33% у 2024 році, досягнувши 16,5 млн. Станом на 9 місяців 2025 року токенізованою є майже кожна третя активна платіжна картка (31,5%).

Майже всі транзакції в рітейлі є безконтактними: у 2024 році це становило близько 95% за кількістю та сумою, а за 9 місяців 2025 року частка операцій з фізичним зчитуванням даних скоротилася до 1,8% за кількістю.

Ще одним із викликів є низький рівень проникнення віддалених банківських послуг.

Система BankID НБУ, як державний інструмент віддаленої ідентифікації, є критичною для розвитку інтернет- та мобільного банкінгу. Згідно статистичних даних за 2021 рік кількість успішних електронних ідентифікацій через Систему BankID НБУ зросла учетверо порівняно з 2020 роком (понад 30 млн ідентифікацій у 2021 р. порівняно з 7,6 млн у 2020 р.). Так, завдяки системі, понад 99,6% громадян, які мають рахунки в банках України, мають можливість отримувати дистанційні послуги. Саме використання BankID НБУ дозволяє отримувати такі дистанційні послуги, як відкриття рахунків, гаманців з електронними грошима та кредитування [70,71,72].

Але, варто дослідити і розвиток платіжної інфраструктури у 2021-2025 рр. Стійкість і розширення інфраструктури, що керується НБУ та учасниками ринку, є основою для високого проникнення цифрового банкінгу. У таблиці 2.5 показана динаміка розвитку платіжної інфраструктури.

Таблиця 2.5

Динаміка розвитку платіжної інфраструктури (тис. шт., на кінець періоду)

Показник	Кінець 2021 року	Кінець 2023 року	Кінець 2024 року	Вересень 2025 року
Платіжні термінали (POS)	426,0 (розрах.)	449,5	496,6	548,7
Зміна терміналів (рік)	N/A	+25,1% (2023 до 2022)	+10,5% (2024 до 2023)	+10,5% (9М 2025 до 9М 2024)
Банкомати (АТМ)	18,4 тис. (розрах.)	15,8 тис.	15,7 тис.	15,6 тис.
П.П.С., що приймають картки (торг. точки)	371,6	459,7	518,4	592,5

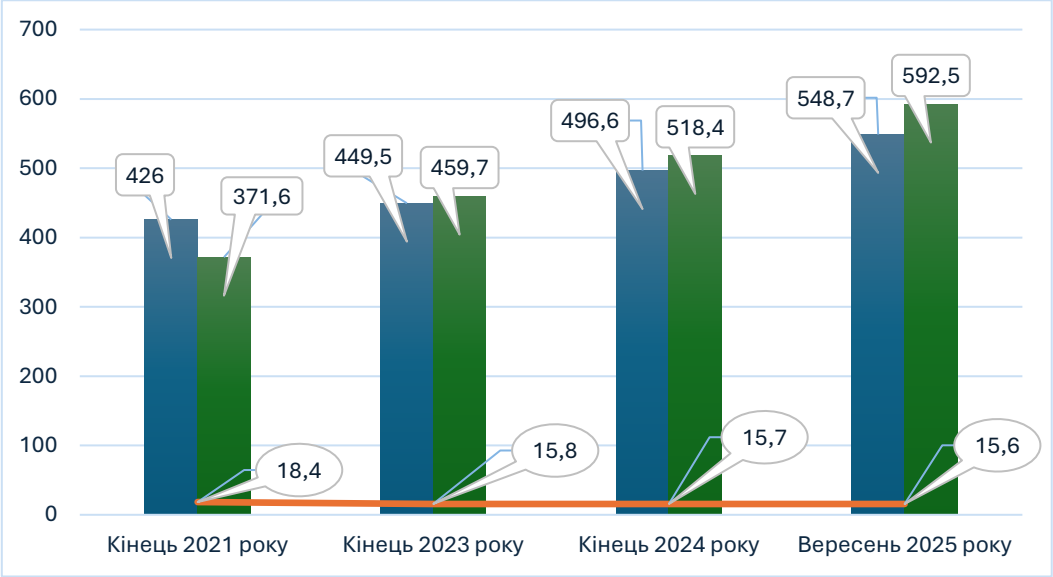

Рис.2.6. Динаміка відновлення та зростання мережі POS-терміналів у 2021–9 місяців 2025 рр.

До кінця 2023 року мережа POS-терміналів повністю відновилася від втрат першого року вторгнення.

Кількість терміналів продовжує зростати: на кінець 2024 року їхня кількість (496,6 тис.) на 16,4% перевищувала показник кінця 2021 року. У вересні 2025 року кількість активних POS-терміналів становила 548,7 тис.

Банкоматна мережа скоротилася порівняно з довоєнним рівнем (через тимчасову окупацію територій), і залишалася майже стабільною у 2024–2025 рр.

Окрему категорію банківського сектору Україна становлять необанки. Стрімкий розвиток технологій, нові потреби клієнтів (орієнтація на мобільний інтернет, хмарні технології) та глобальні виклики, як-от пандемія COVID-19, стимулювали активне впровадження цифрових інновацій та, як наслідок, появу нових учасників на ринку фінансових послуг – необанків. Особливістю українського необанкінгу є те, що, на відміну від багатьох інших країн, необанки в Україні не мають самостійної банківської ліцензії і функціонують на базі ліцензії традиційного банку-партнера, виступаючи у ролі операційного підрозділу.

На початок 2021 року в Україні діяло 7 необанків. Перша хвиля їхнього створення відбулася у 2017 році (Monobank), а друга – у 2019 та 2020 роках. У таблиці Додаток Е наведено харктеристка необанків.

Лідером на українському ринку беззаперечно є Monobank. Станом на грудень 2021 року, лише за чотири роки існування, кількість його клієнтів зросла до 5 млн осіб.

Але, варто відзначити і той факт, що незважаючи на перспективність, кількість необанків в Україні скоротилася внаслідок зовнішніх змін та ліквідації банків-партнерів.

– Todobank (проєкт АТ «МЕГАБАНК») припинив діяльність після віднесення «Мегабанку» до категорії неплатоспроможних у червні 2022 року.

– NEOBANK (проєкт АТ «АКБ «КОНКОРД») був закритий після відкликання ліцензії банку «Конкорд» НБУ у серпні 2023 року.

– Sportbank (працював на базі ліцензій «Таскомбанку» та «ОКСІ БАНК») припинив роботу у квітні 2024 року через необхідність коригування бізнес-

моделі та стратегії «Таскомбанку» в умовах значних змін у зовнішньому середовищі.

Таким чином, із семи необанків, що діяли станом на 2021 рік, до кінця 2024 року залишилося чотири: Monobank, O.Bank, Izibank та Банк «Власний рахунок»

Скорочення кількості необанків не вплинуло негативно на загальний розвиток цифрового банкінгу, оскільки традиційні банки активно впроваджують нові цифрові рішення.

Поява необанків створює нові правила гри для традиційних банків. Необанки стали каталізатором цифрової трансформації всього банківського сектору.

Конкурентні переваги необанків над класичними банками включають:

– Низька вартість продуктів (недорогі, часто без щомісячної плати за обслуговування).

– Прозорість (відсутність прихованих комісій і надмірних штрафів).

– Інноваційні мобільні додатки (можливість оперативно керувати фінансами, прогнозувати активність рахунку).

– Спрощена процедура кредитування завдяки автоматизації оцінки кредитоспроможності.

– Орієнтація на специфічні сегменти ринку (наприклад, Sportbank для фізично активних людей, NEOBANK для бізнесу, «Банк Власний Рахунок» для клієнтів мережі Fozzy).

У конкурентній боротьбі необанки пропонують кращі умови, ніж традиційні банки, зокрема, вищі процентні ставки за вкладами, відсутність комісії за обслуговування та нижчі проценти за кредитами [80].

Monobank, як лідер, складає значну конкуренцію традиційному лідеру ринку – «ПриватБанку». Представники ПриватБанку визнавали, що маркетингова стратегія будь-якого роздрібного банку в Україні – це «відкусити» свій шматок від ПриватБанку, а конкуренти пильно стежать за їхніми кроками.

Окремої звітності необанків, які працюють за ліцензією материнського банку, не існує. Ми здійснили аналіз на основі показників банків-ліцензіатів, що представлений у таблиці 2.6.

Таблиця 2.6

Показники доходів та фінансової діяльності АТ «Універсал Банк» (ліцензіат Monobank), 2020–2022 рр. [70]

Показник, тис. грн	2020	2021	2022	Приріст 2020-2022, %
Процентні доходи	2 798 139	4 967 541	6 973 994	149%
Комісійні доходи	2 211 773	4 107 742	3 689 003	67%
Чистий процентний дохід	1 592 679	3 608 843	5 743 727	261%
Чистий прибуток	409 226	2 461 549	877 849	115%

Протягом 2020–2022 рр. спостерігалося суттєве зростання основних фінансових показників АТ «Універсал Банк», зокрема чистого процентного доходу, який збільшився на 261%, що свідчить про успішну діяльність.

Монобанк залишається незаперечним лідером на ринку необанків, маючи суттєвий відрив за показниками доходу материнської компанії та чистими активами станом на 2023 рік. Усі необанки за результатами 2023 року отримали суттєво вищий дохід, ніж у 2021 році, що говорить про їхній розвиток, незважаючи на складну ситуацію в країні.

Подальший розвиток необанкінгу в Україні тісно пов'язаний із процесами цифрової трансформації банківського сектору та впровадженням нового регуляторного поля.

Розвиток необанкінгу та фінтеху є частиною Стратегії розвитку фінансового сектору України до 2025 року та Стратегії розвитку фінтеху в Україні до 2025 року.

Ключові напрями, спрямовані на створення сприятливої фінтех-екосистеми та стимулювання розвитку цифрового банкінгу, включають:

1. Запровадження стандартів відкритого банкінгу (Open Banking) та імплементація директив ЄС (зокрема, PSD2) через прийняття Закону України

«Про платіжні послуги». Цільове значення на 01.01.2025: Не менше 80% суб'єктів ринку працюють за стандартами відкритого банкінгу.

2. Розвиток інструментів віддаленої ідентифікації та верифікації. Цільове значення використання системи BankID НБУ (за загальними активами) до 01.01.2025: Не нижче 70%.

3. Створення повноцінної регуляторної «пісочниці» (sandbox) на базі НБУ для апробації інноваційних фінансових послуг. Цільове значення на 01.01.2025: 16–20 оброблених заявок на рік. НБУ також має на меті стати членом Глобальної мережі фінансових інновацій (GFIN).

Популярність цифрового банкінгу постійно зростає, що створює сприятливе середовище для необанків. На рис. 2.7 наведено динаміку проникнення цифрового банкінгу в Україні.

Очікується, що до 2025 року цифровий банкінг охоплюватиме 22% населення України, що є високим показником і підтверджує постійний попит на цифрові фінансові послуги.

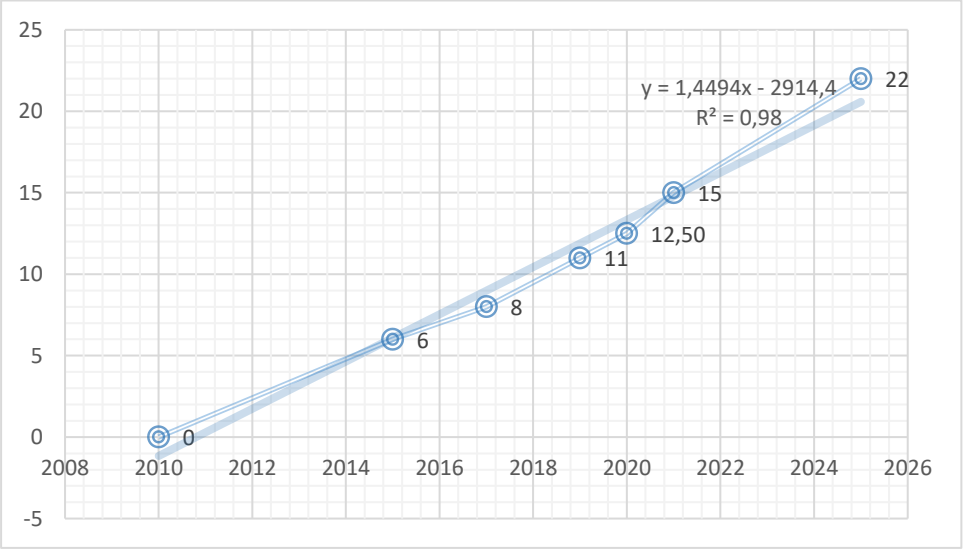

Рис.2.7. Проникнення цифрового банкінгу в Україні, % населення (2010–2025 рр.)

Отже, можемо зазначити, що Політика Національного банку України (НБУ) у сфері цифровізації протягом 2022–2025 років була ключовим елементом

загальнодержавної стратегії, спрямованої на економічне відновлення та інтеграцію у міжнародний фінансовий простір. Цифрова трансформація фінансового сектору закріплена у Стратегії НБУ до 2025 року як критичний драйвер економічного зростання [78].

Стратегія НБУ 2025 структурована навколо трьох ключових напрямків, серед яких Другий напрям, «Цифрові Фінанси як Драйвер Цифровізації Економіки», безпосередньо стосується зовнішньої цифрової трансформації та включає такі стратегічні цілі, як розвиток безготівкової економіки, підвищення рівня фінансової інклюзії, розвиток FinTech-інновацій та кіберзахист фінансового сектору. Третій напрям передбачає внутрішню цифрову трансформацію НБУ, включаючи вдосконалення системи управління даними та IT-інфраструктури, необхідну для ефективного нагляду (SupTech).

Ключовими сферами регуляторної діяльності НБУ у період 2022–2025 років, які безпосередньо стосувалися цифровізації, були електронні гроші, BankID та фінансовий моніторинг (FinMon). Архітектурною основою для більшості цифрових платіжних ініціатив став Закон України «Про платіжні послуги» (№ 1591-IX від 30.06.2021), який заклав фундамент для гармонізації з європейським законодавством (PSD2).

Звичайно політика НБУ у період 2022-2025 років також направлена на цифровізацію. В таблиці Додаток Е представлено основні вектори цифровізації НБУ у період 2022-2025 рр.

Аналіз політики НБУ в період 2022–2025 рр. виявляє низку викликів, пов’язаних насамперед із безпековим контекстом та нерівномірністю впровадження цифрових стандартів. Їх аналіз наведено у таблиці Додаток Є.

Отже, можна зазначити, що політика цифровізації НБУ в період 2022–2025 років являє собою балансування між активним впровадженням інновацій (BankID, CBDC) та забезпеченням абсолютної кіберстійкості та фінансової цілісності, що особливо критично в умовах військових ризиків.

2.2. Виклики та бар'єри на шляху цифрової трансформації українських банків

Цифрова трансформація в українському банківському секторі в період 2022–2025 років відбувалася в умовах безпрецедентних викликів, спричинених повномасштабною війною. Ключовим пріоритетом для фінансових установ стало забезпечення операційної стійкості та безперервності бізнесу (BCP). Аналіз показує, що три основні категорії бар'єрів – операційний, ризиковий та кадровий – функціонують не ізольовано, а в тісному взаємозв'язку, створюючи синергетичний ефект, що ускладнює стратегічну трансформацію. Головна перешкода полягає у дилемі «Стійкість vs. Інновації», коли значні фінансові ресурси, які могли б бути спрямовані на модернізацію ядра (CapEx), змушені витрачатися на підтримку безпеки, персоналу та життєдіяльності старих систем (OpEx та BCP CapEx).

По перше, проблема застарілої IT-інфраструктури (Legacy Systems) є одним із найпотужніших стримуючих факторів цифрової трансформації, оскільки ці системи часто були розроблені 30 і більше років тому. Узагальнення цих проблем наведено на рис.2.8.

Отже, можна зазначити, що модернізація є економічним імперативом. Впровадження сучасних платформ, крім зниження TCO, може забезпечити на 62% швидший час виходу на ринок (Time-to-Market) для нових банківських продуктів. В таблиці Додаток Є наведено фінансова оцінка справжньої вартості володіння.

По друге, зростання кіберризиків є одним із найбільш критичних викликів для фінансового сектору України, який є об'єктом критичної інфраструктури та постійною мішенню ворожих атак [84].

Ключові фактори зростання кіберризиків у банківському секторі України пов’язані передусім з ескалацією кіберзагроз у воєнний час. Так, у 2024 році кількість кібератак зросла приблизно на 70%, причому значна їх частина була спрямована не лише на фінансове збагачення зловмисників, а й на дестабілізацію

фінансової системи та підрив довіри до неї. Атаки включали розповсюдження шкідливого ПЗ, фішингові кампанії та компрометацію облікових записів.

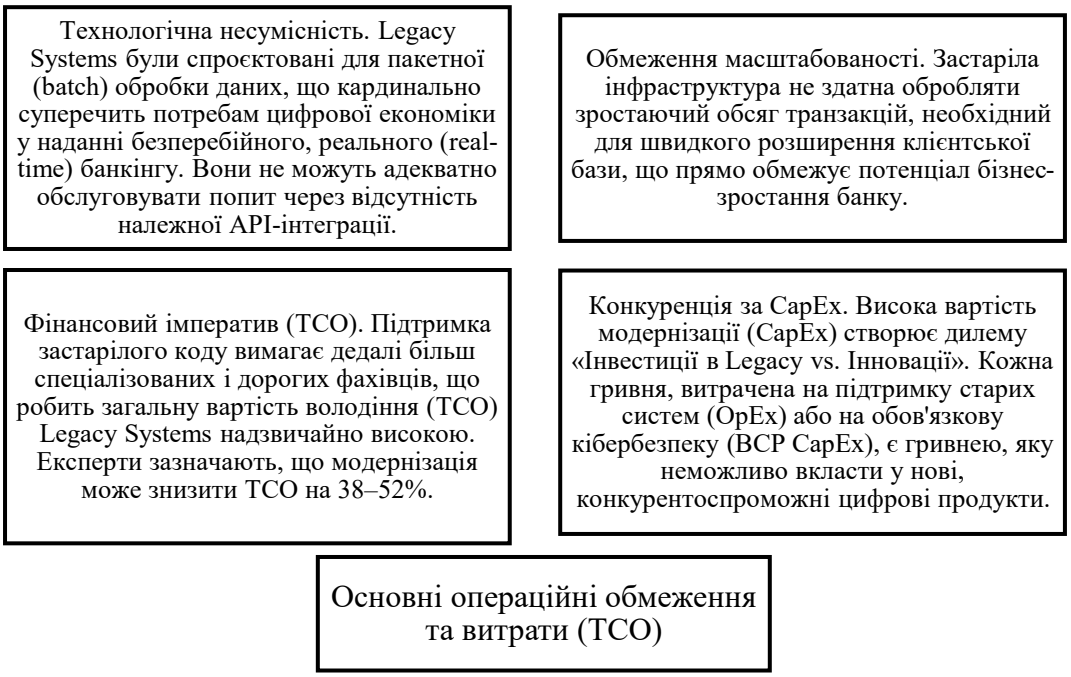

Рис.2.8. Основні операційні обмеження та витрати (TCO) в банківському секторі України [82]

У відповідь на посилення загроз Національний банк України посилив регуляторні вимоги щодо кіберстійкості. Важливим кроком стало ухвалення Постанови Правління НБУ № 178 від 12.08.2022 р. (у чинній редакції від 08.07.2025 р.), якою затверджено Положення про організацію кіберзахисту в банківській системі та оновлено критерії визначення об’єктів критичної інфраструктури. Це зумовило необхідність системних інвестицій з боку банків у забезпечення кібербезпеки [45].

Разом із тим посилення вимог НБУ призвело до зростання витрат на ІТ-інфраструктуру. Значна частина бюджетів спрямовується на обов’язковий CapEx, необхідний для захисту критично важливих систем. Відповідно, ці кошти не можуть бути використані на інноваційний розвиток, модернізацію банківських продуктів чи вдосконалення ІТ-ядра, що створює додатковий фінансовий тиск на трансформаційні проєкти.

Ще одним фактором, що ускладнює цифрову трансформацію, є зростання комплаєнс-навантаження. Протягом дії воєнного стану НБУ регулярно оновлював вимоги у сфері фінансового моніторингу та санкційної політики. Це потребує високої гнучкості ІТ-систем для оперативної інтеграції нових санкційних списків і регуляторних правил. Для банків, які використовують застарілі Legacy Systems, така адаптація є значним технологічним викликом, що додатково підсилює ризики та знижує ефективність операційної діяльності.

Банки, які ефективно інвестували в планування безперервності бізнесу (BCP) та відновлення після катастроф (DRP), змогли зберегти високий рівень операційної стабільності, що є необхідним фундаментом для подальших інновацій. У таблиці Додаток Ж узагальнено регуляторна база НБУ щодо кіберстійкості в період 2022-2025 рр.

Третім, нестача кваліфікованих ІТ-фахівців є критичним бар’єром, значно посиленим макрофакторами, спричиненими війною. На рис.2.9 згруповано основні кадрові та культурні виклики банківського сектору України.

Також, успіх цифрової трансформації визначається здатністю банку здійснити глибокий культурний зсув. Це зсув має ґрунтуватися на:

1. Клієнтоорієнтованості (Customer-Centricity), тобто сучасні банки повинні прагнути не просто надавати послуги, а й передбачати потреби користувачів, адаптуючись до їхнього стилю життя та уподобань. Банки, такі як Креді Агріколь Банк, дотримуються клієнтоорієнтованої моделі, зосередженої на побудові довготривалих відносин з клієнтами.

2. Перехід до Agile. Для досягнення цієї гнучкості необхідний перехід на продуктовий (Agile) підхід. Це вимагає зміни внутрішньої логіки функціонування банку, принципів прийняття рішень, комунікації та моделі управління даними.

3. Роль лідерства. Саме цей фундаментальний культурний бар'єр часто знаходиться у вищому керівництві (C-Level). Воно має очолити культурний зсув, подолавши опір середнього менеджменту та інерцію ієрархії, оскільки справжня трансформація починається зі зміни принципів прийняття рішень.

Рис.2.9. Основні кадрові та культурні виклики банківського сектору України [85]

Для успішного впровадження цих змін банки повинні дотримуватися системного і послідовного підходу, що включає діагностику, стратегічне планування та ітеративну реалізацію.

Організаційна зміна (культурна трансформація) є системним процесом і повинна відбуватися за чіткими етапами. Дана етапність представлена у таблиці Додаток Ж.

Отже, цифрова трансформація українських банків у період 2022–2025 років визначалася не стільки прагненням до інновацій, скільки необхідністю забезпечення стійкості (операційної та кібер-). Вимушені інвестиції в кіберзахист (НБУ № 178) та підтримку персоналу в умовах війни конкурували з CapEx, потрібним для модернізації Legacy Systems. Подолання цих синергетичних бар'єрів вимагає від банків не лише фінансової стійкості, але й здійснення глибокого культурного зсуву тобто переходу до клієнтоорієнтованих, гнучких (Agile) моделей, щоб залучити та утримати критично необхідний кваліфікований ІТ-персонал.

2.3. Вплив зовнішніх факторів на процеси цифровізації банківського сектору

Період 2022–2025 років став для українського банківського сектору часом кардинальної трансформації, внаслідок чого цифровізація перетворилася з джерела конкурентних переваг на критичний інструмент операційної стійкості та базовий стандарт ведення діяльності. Ключові зовнішні фактори, спричинені військовим конфліктом, форсували структурну модернізацію фінансової системи.

Розглянемо ключові зовнішні фактори та їх вплив на цифровізацію. Так, варто відзначити наступні:

1. Військовий конфлікт та макроекономічна нестабільність. Воєнний конфлікт виступає ключовим бар’єром для подальшого екстенсивного зростання, суттєво звужуючи український фінтех-сектор. Він спричинив зміну парадигми: основний інвестиційний фокус змістився з розширення функціоналу на забезпечення технологічної стійкості та оптимізацію вартості утримання критичної IT-інфраструктури. Економічна криза значно обмежує обсяги інвестицій у IT, змушуючи банки відкладати масштабні проєкти з невизначеною дохідністю.

2. Енергетична криза (блекаути). Тривалі відключення електроенергії стали однією з найбільш відчутних фізичних загроз, що прямо вплинули на цифрову стратегію сектору. Згідно з опитуванням, 76% компаній підтвердили вплив тривалих відключень електроенергії на їхню роботу, при цьому IT-функції увійшли до трійки найбільш постраждалих сфер (27% компаній). Це призвело до значних додаткових фінансових витрат (CAPEX та OPEX) на придбання та обслуговування резервного обладнання (генераторів, палива).

3. Кадрові виклики. Нестабільність призвела до відтоку кваліфікованих IT-кадрів за кордон, що є істотним бар’єром для розвитку фінтеху. Цей дефіцит ресурсів стимулює банки максимально покладатися на автоматизацію та впровадження штучного інтелекту (AI). Експерти прогнозують, що до 2025 року технічні знання стануть обов'язковими для банківських менеджерів [86].

У таблиці 2.7 наведено систематизований аналіз впливу ключових зовнішніх факторів на цифровізацію банківського сектору України у період 2022–2025 рр.

Таблиця 2.7

Зовнішні фактори впливу на банківський сектор України у 2022–2025 рр.

Категорія фактору	Основний вплив на цифровізацію	Операційні наслідки	Стратегічна відповідь сектору
Військовий конфлікт	Зміна парадигми від конкуренції до стійкості (базовий стандарт)	Зниження рентабельності, необхідність релокації, посилення кіберзахисту	Фокус на OPEX/CAPEX для стійкості, посилення KYC/AML
Енергетична криза (блекаути)	Стимулювання фізичного та логістичного резервування IT-інфраструктури	Зростання OPEX на паливо/обслуговування, критичний вплив на IT (27% компаній)	Power Banking, інвестиції у генерацію, 7-денна автономія ЦОД
Кадрові та інфраструктурні	Відтік кваліфікованих IT-фахівців, регіональні інфраструктурні прогалини	Підвищення вартості IT-послуг, нижче проникнення онлайн-банкінгу порівняно з ЄС	Обов'язкові технічні знання для менеджерів (TechMind) до 2025 р., інвестиції в автоматизацію

Високий рівень цифрової зрілості українського фінансового сектору, який був накопичений до 2022 року, виявився критичним неявним військовим активом. Завдяки значній частці операцій через цифрові канали (понад 94% банківських операцій прогнозується через цифрові канали до 2025 року), фінансова система мінімізувала свою залежність від фізичних відділень, що забезпечило безперебійність критичних платіжних функцій навіть за умов бойових дій.

Саме тому в роботі сформовано ключові механізми забезпечення безперервності [86]:

1. Гібридна стійкість та Power Banking. Для протидії фізичним загрозам, зокрема наслідкам блекаутів, банківський сектор впровадив концепцію гібридної стійкості, що поєднує цифрову доступність із фізичною інфраструктурою резервування.

Цифрова доступність дозволяє здійснювати більшість послуг від відкриття рахунків до управління інвестиціями через мобільні застосунки. Наприклад, у ПриватБанку понад 80% транзакцій здійснюється через Приват24.

Фізична інфраструктура (Power Banking) сприяла тому, що системно важливі банки об'єдналися для створення спільної мережі Power Banking. Ці відділення здатні надавати базові банківські послуги навіть під час блекауту, маючи резервні джерела енергії та зарезервовані канали зв'язку від кількох операторів. НБУ встановив вимогу, що не менше третини банківських відділень мають бути опорними. У рамках цієї мережі запроваджено банкоматний національний роумінг.

2. Технологічна стійкість (хмарні обчислення та кібербезпека). Саме цифровізація забезпечила життєздатність систем шляхом впровадження рішень, які гарантують швидке відновлення роботи та збереження даних.

Хмарні обчислення (Cloud Adoption). НБУ унормував процес використання банками хмарних сервісів, завдяки чому банки мають можливість швидко відновити штатне функціонування та зберегти всю необхідну інформацію в разі руйнування фізичної інфраструктури. Хмара забезпечує географічну диверсифікацію та резервування, що є критичним. НБУ вимагає, щоб банки гарантували функціонування своїх дата-центрів (ЦОД) протягом семи днів відсутності основного електропостачання. Положення НБУ про застосування технології хмарних обчислень набирає чинності з 01 листопада 2025 року.

Кібербезпека. Посилена стійкість банківської системи до кібератак була ключовим завданням НБУ у 2022 році. Глобально, збитки від кібератак до 2025 року зростуть до $10,5 трлн щорічно, що робить кібербезпеку однією з найбільших загроз для цифрового банкінгу. Банки активно інвестують у технології ШІ для захисту даних клієнтів і стримування витоків даних швидше (на 27% швидше завдяки ШІ).

3. Регуляторна уніфікація безперервності (НБУ BCP-Комплаєнс).

Кризовий досвід 2022–2024 років був інституціоналізований Національним банком, який систематизував близько 200 нормативно-правових та

розпорядчих актів у єдиний алгоритм регулювання безперебійного функціонування учасників ринку в особливий період.

Ця система визначає три основні режими функціонування: режим підвищеної готовності, обмежений режим та критичний режим. Метою є забезпечення синхронності та скоординованості режимів роботи усіх учасників ринку.

Учасники ринку фінансових послуг зобов’язані розробити та затвердити внутрішні документи щодо забезпечення безперебійного функціонування до 02 лютого 2025 року.

4. Цифрова трансформація НБУ. Стратегічні ініціативи (2022-2025).

Національний банк України відіграє ключову роль у стимулюванні розвитку фінтеху та забезпеченні стабільності, впроваджуючи регуляторні ініціативи та стратегії. Це особливо помітно у контексті адаптації до вимог часу та забезпечення інтеграції України до світових економічних процесів.

В таблиці Додаток З сформовано заходи Національного банку України, спрямовані на сприяння розвитку ринку FinTech та забезпечення стабільності фінансової системи в умовах війни, які охоплюють період 2022–2025 рр.

Таким чином, цифрова трансформація у 2022–2025 рр. була каталізована зовнішніми викликами та набула стратегічного значення як механізм виживання та підтримки макрофінансової стабільності. Інвестиції в цифрові технології (Cloud, AI) тепер тісно пов'язані з фізичним резервуванням інфраструктури, що є ключем до операційної безперервності.

Висновок до розділу 2

У ході аналізу встановлено, що розвиток банківського сектору України в умовах цифровізації у 2022–2025 роках відбувався під визначальним впливом безпрецедентних зовнішніх викликів, передусім повномасштабної війни, що трансформувало саму природу цифрових інновацій. Цифровізація перестала бути інструментом досягнення конкурентних переваг і набула статусу базової

умови виживання та забезпечення операційної й кібернетичної стійкості банківських установ.

Доведено, що український платіжний ринок характеризується високим рівнем цифрової зрілості, що проявляється у стійкому домінуванні безготівкових операцій, глибокій інтеграції мобільного банкінгу у повсякденні фінансові практики населення та високому рівні технологічного проникнення безконтактних і токенізованих платіжних інструментів. Відновлення та розвиток платіжної інфраструктури, а також удосконалення регуляторного середовища створили умови для збереження доступності фінансових послуг навіть в умовах воєнного стану.

Водночас ідентифіковано системні бар'єри цифрової трансформації, серед яких ключовими є конфлікт між необхідністю інвестувати у стійкість і обмеженими ресурсами для інновацій, наявність застарілих IT-систем, зростання кіберризиків та посилення регуляторного тиску, а також дефіцит кваліфікованих кадрів і потреба у трансформації організаційної культури банків. Обґрунтовано, що без модернізації технологічної архітектури та впровадження гнучких клієнтоорієнтованих моделей управління подальший цифровий розвиток сектору буде суттєво обмежений.

Узагальнено, що зовнішні кризи стали не лише деструктивним, а й трансформаційним чинником, який прискорив впровадження моделі гібридної стійкості, поєднання фізичної надійності інфраструктури з розвитком хмарних технологій та посиленням кібербезпеки. Подальший розвиток банківського сектору України потребує стратегічного балансу між інноваційністю та стійкістю, системного оновлення технологічних платформ і формування нової цифрової культури управління як передумови підвищення конкурентоспроможності та довгострокової стабільності.

РОЗДІЛ 3
ПЕРСПЕКТИВИ ТА НАПРЯМИ РОЗВИТКУ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ В УМОВАХ ЦИФРОВІЗАЦІЇ

3.1. Стратегічні пріоритети інноваційного розвитку банківського сектору

Стратегічні пріоритети інноваційного розвитку сучасного банківського сектору формуються на перетині технологічної модернізації, трансформації клієнтського досвіду та посилення вимог до операційної та фінансової стійкості. Для забезпечення довгострокового зростання та конкурентоспроможності, банки повинні балансувати інвестиції між розширенням зростання (через гіперперсоналізацію та нові бізнес-моделі) та підвищенням стійкості (через інтелектуальне управління ризиками та модернізацію інфраструктури) [82].

Аналіз світових тенденцій та експертних опитувань (зокрема, KPMG та Deloitte) визначає шість основних напрямків інвестиційних пріоритетів банківського сектору, що наведені на рис.3.1.

Ці пріоритети можна згрупувати у три основні стратегічні вектори, як представлено у таблиці Додаток З.

Отже, ключовим елементом стратегічної трансформації є GenAI, який виступає не лише як інструмент клієнтського обслуговування, але й як засіб для вирішення проблеми технічного боргу.

Банки переходять до рішень, керованих штучним інтелектом, які здатні перекладати та переписувати успадкований код на сучасні мови програмування. Цей підхід є критично важливим, оскільки застарілі монолітні системи, побудовані десятиліття тому, є найбільшим бар'єром для гнучкості, інновацій та інтеграції з API-Driven екосистемами [90].

Згідно прогнозних даних очікується, що всі банки використовуватимуть GenAI для розробки додатків, а значна частина зможе мігрувати зі своїх старих основних платформ, використовуючи GenAI для безпечного рефакторингу коду.

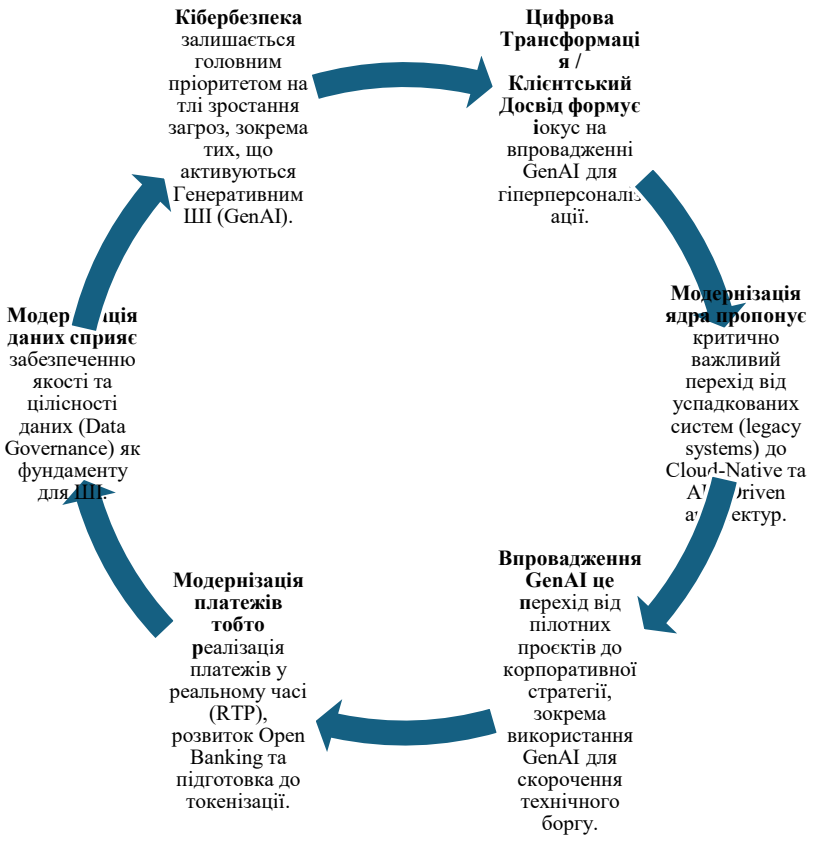

Рис.3.1. Основні напрямки інвестиційних пріоритетів інноваційного розвитку сучасного банківського сектору

Для забезпечення масштабування рішень на базі GenAI та прискорення виведення продуктів на ринок необхідною умовою є архітектурна еволюція банківських систем. Ключову роль у цьому відіграватиме використання технологій з відкритим програмним кодом. Зокрема, open-source рішення, такі як Linux, стануть основою інфраструктури банків до 2030 року, оскільки забезпечують високу гнучкість, ефективність та можливість глибокого налаштування операційних процесів під потреби бізнесу [56].

Важливим стратегічним напрямом також є впровадження cloud-native та API-орієнтованих архітектур. Перехід до хмарних технологій та API-керованих систем дозволяє банкам створювати масштабовані та динамічні IT-рішення, забезпечувати сумісність між різними платформами та ефективно інтегруватися з FinTech-компаніями та партнерськими екосистемами. Це формує технічну

основу для швидкого інноваційного розвитку, підвищення продуктивності та розширення можливостей цифрової трансформації.

Стратегія клієнтського досвіду (CX) зазнає суттєвих змін, переходячи від традиційної реактивної моделі, що базувалася на широкій сегментації, до проактивної гіперперсоналізації. Такий підхід спрямований на відновлення «людського дотику», який був значною мірою втрачений під час першої хвилі цифровізації фінансових послуг [75].

Одним із ключових елементів цієї трансформації є прогнозована взаємодія (Predictive Engagement). Завдяки можливостям GenAI банки можуть відмовитися від статичного групування клієнтів на сегменти та перейти до динамічної мікроперсоналізації. Штучний інтелект аналізує транзакційну активність, поведінкові дані та життєві події клієнтів у режимі реального часу, що дозволяє проактивно пропонувати відповідні продукти або попереджати про потенційні ризики. У результаті рівень залученості клієнтів може зрости приблизно на 20%.

Окремим напрямом розвитку є омніканальність, у якій GenAI відіграє ключову роль. Сучасні клієнти очікують цілісної та послідовної взаємодії у всіх каналах обслуговування від мобільного застосунка до фізичного відділення. GenAI забезпечує таку безшовність завдяки ряду інструментів. Зокрема, автоматизоване резюмування дозволяє ШІ-ботам відстежувати всі точки контакту та формувати миттєве резюме попередньої комунікації, що знімає з клієнта потребу повторювати свій запит. Крім того, інтегроване планування зустрічей, яке синхронізує історію взаємодії та індивідуальні дані клієнта, підвищує якість обслуговування у відділеннях та може збільшити конверсію продажів на 24% порівняно з неплановими візитами [86].

На рисунку 3.2 представлено фонд трансформації банку.

Також наступим кроком є інновації у сфері грошей та платежів (зокрема, DLT, токенізовані депозити та стейблкоїни) вимагають від банків інфраструктурної готовності, щоб зберегти «єдність грошей» [88].

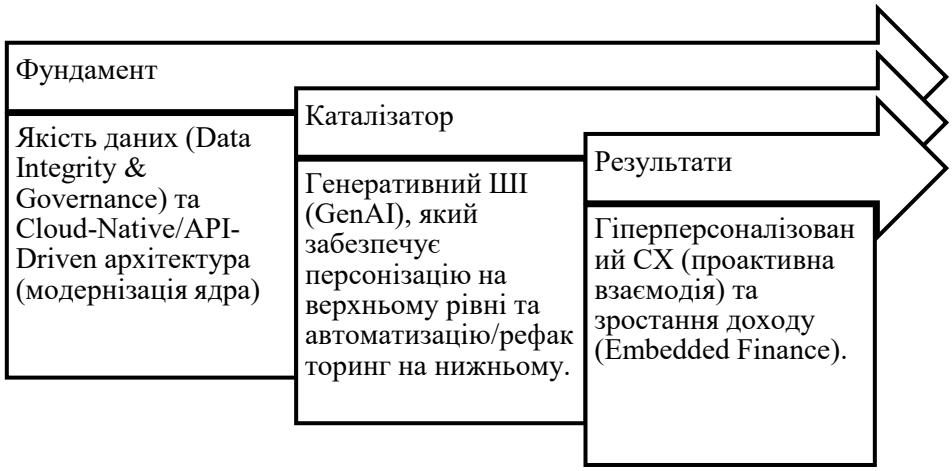

Рис.3.2. Фонд інноваційної трансформації банку

Технологія розподіленого реєстру (DLT) відкриває можливості для створення спільних, синхронізованих реєстрів, які оновлюються одночасно для всіх учасників транзакції. Це значно зменшує потребу у ручному звірянні даних, скорочує операційні ризики та підвищує загальну ефективність фінансових процесів. Для комерційних банків стратегічною передумовою є адаптація внутрішніх інформаційних систем до майбутньої токенізації активів та появи нових форм цифрових грошей.

Позиція регуляторів також відіграє важливу роль у цьому процесі. Зокрема, Банк Англії (BoE) наголошує на низькому апетиті до ризику щодо відходу від розрахунків у центральних грошах на користь приватних цифрових платіжних активів, оскільки такі зміни можуть створити загрози фінансовій стабільності. У відповідь на це центральні банки активізували модернізацію своїх інфраструктурних систем [78].

Одним із ключових напрямів такої модернізації є RTGS Renewal Programme, який передбачає впровадження нових функціональних можливостей, зокрема синхронізаційного інтерфейсу (synchronisation interface). Це забезпечує підключення системи валових розрахунків у реальному часі (RTGS) до зовнішніх платформ на основі DLT з метою здійснення атомарних розрахунків токенізованих активів за моделями DvP та PvP.

Паралельно Банк Англії проводить експерименти з оптовою цифровою валютою центрального банку (wCBDC). Запровадження wCBDC створює умови для здійснення операцій з токенізованими активами та грошима в межах єдиного DLT-середовища, забезпечуючи повну синхронізацію та атомарність розрахунків.

За таких умов комерційні банки мають забезпечити технічну та операційну сумісність своїх внутрішніх систем з новими інфраструктурними рішеннями, що стане ключовою умовою успішної інтеграції у майбутню цифрову фінансову екосистему [79].

І останні це RegTech є необхідним елементом стійкості, оскільки він допомагає фінансовим установам швидко адаптуватися до нових регуляторних вимог. Використання технологій, таких як машинне навчання, для проактивного управління комплаєнсом дозволяє мінімізувати ризики, автоматизувати аудит та уникнути штрафів, звільняючи ресурси для інновацій, орієнтованих на зростання.

3.2. Шляхи подолання викликів кібербезпеки та вдосконалення регулювання

Зростаюча складність кіберзагроз, особливо цільових атак на хмарні інфраструктури, вимагає від банківського сектопу фундаментального архітектурного зсуву та активної гармонізації національної регуляторної бази з європейськими стандартами, такими як DORA та NIS2. Для подолання викликів, пов’язаних із компрометацією ідентичності та системними ризиками третіх сторін, необхідне комплексне впровадження передових архітектур, інтеграція штучного інтелекту та посилення проактивного регуляторного нагляду [91].

Відхід від застарілих моделей захисту, заснованих на периметрі («замок та рів»), є стратегічною необхідністю. Традиційні підходи, які неявно довіряють суб'єктам всередині мережі, виявилися неспроможними в умовах віддаленої

роботи та хмарних середовищ, де атакуючі, наприклад, група SCATTERED SPIDER, можуть зловживати легальними функціями хмарних платформ.

Так, банківський сектор використовує архітектуру нульової довіри базується на принципі «Ніколи не довіряй, завжди перевіряй», що передбачає явну верифікацію кожного запиту на доступ, незалежно від його походження. Ключовим для архітектури нульової довіри є аксіома «Припусти, що тебе зламали».

Таблиця 3.1

Основні принципи та реалізаційні вимоги архітектури нульової довіри [85]

Принцип нульової довіри	Опис та цільове призначення	Ключові технології реалізації
Жодної неявної довіри	Усунення довіри до будь-якого користувача чи пристрою, незалежно від розташування (всередині/зовні мережі),.	Сильне управління ідентифікацією та Доступом (IAM): MFA, біометрична верифікація,.
Найменші привілеї (Least Privilege Access)	Надання суворо мінімального рівня авторизації, необхідного для виконання поточної функції,.	Динамічний, контекстуальний доступ (на основі ролі, репутації пристрою, поведінки),.
Мікро-сегментація (Micro-Segmentation)	Розподіл мережі та ресурсів на малі ізольовані частини (мікро-периметри),.	Обмеження бічного руху (lateral movement) зловмисників у разі компрометації одного сегменту,,.
Постійна верифікація	Безперервна оцінка ризику та автентифікація навіть після надання початкового доступу.	Шифрування (наприклад, TLS) та системи Secure Access Service Edge (SASE) для віддаленого доступу

Так, на сьогодні інтеграція штучного інтелекту (ШІ) та машинного навчання (МН) ШІ та МН є критично важливими для виявлення та запобігання фінансовому шахрайству, оскільки вони здатні аналізувати масивні обсяги даних і розпізнавати складні патерни, які людські аналітики можуть пропустити. Ці моделі використовуються для моніторингу транзакцій у реальному часі та прогностичного аналізу аномальної поведінки.

Технологічна модернізація повинна супроводжуватися посиленням організаційної стійкості, включно з управлінням ризиками третіх сторін (TPRM) та постійним моделюванням загроз.

Отже, однією з найкращих сучасних практик у банківському секторі є перехід до посилених механізмів багатофакторної аутентифікації (MFA), які

поєднують біометричні та адаптивні методи і забезпечують значно вищий рівень захисту порівняно з традиційними паролями.

Таблиця 3.2

Методи машинного навчання для виявлення фінансового шахрайства [87]

Метод навчання	Принцип роботи	Результат для кібербезпеки
Кероване навчання (Supervised Learning)	Моделі тренуються на великих обсягах даних, вже позначених як відомі приклади шахрайства.	Автоматичне розпізнавання та блокування шахрайських транзакцій, що відповідають відомим патернам,.
Некероване навчання (Unsupervised Learning)	Моделі самостійно роблять висновки з немаркованих даних для виявлення нових, непередбачуваних патернів поведінки (anomaly detection).	Виявлення нових, еволюціонуючих тактик шахрайства до того, як про них дізнаються людські агенти,.
Прогностична аналітика	Використання ШІ для оцінки типової поведінки користувача.	Розпізнавання незвичної частоти, місця розташування, або типу транзакції, що вказує на компрометацію,.

Першим ключовим напрямом є впровадження багатофакторної та адаптивної аутентифікації. Банки поступово відмовляються від простих статичних паролів, замінюючи їх динамічними багаторівневими системами. Обов’язкове застосування MFA передбачає використання щонайменше двох незалежних факторів аутентифікації наприклад, комбінації знань (пароль або PIN), володіння (смартфон, токен) та біометрії (відбиток пальця або обличчя). Адаптивна аутентифікація додатково аналізує ризики в режимі реального часу, оцінюючи контекстні параметри: геолокацію користувача, поведінкову біометрію, час доби, історію дій та інші фактори. У разі виявлення аномалій система автоматично активує додатковий фактор перевірки для зниження ризику шахрайства [91].

Другим напрямом є широке застосування біометричних методів, які забезпечують одночасно високий рівень безпеки та зручності. Серед найбільш поширених рішень аутентифікація за відбитком пальця, розпізнавання обличчя на основі 3D-технологій та сканування райдужної оболонки ока, яке забезпечує особливо високу точність. Важливим компонентом є захист конфіденційності:

банки повинні зберігати не самі біометричні дані, а їх криптографічні шаблони, що мінімізує ризик компрометації у разі кібератаки.

Третім напрямом цифрової трансформації систем захисту є впровадження безпарольних технологій (Passwordless). Використання стандартів FIDO2/WebAuthn дозволяє повністю усунути потребу у паролях і здійснювати аутентифікацію за допомогою біометрії чи фізичних ключів безпеки (наприклад, YubiKey). Такі рішення є стійкими до фішингових атак та забезпечують високий рівень захисту. Додатковою технологією є прив'язка пристрою (Device Binding), яка забезпечує доступ до облікового запису лише з авторизованого фізичного пристрою, що значно знижує ймовірність несанкціонованого доступу.

Упровадження цих підходів дозволяє банківським установам суттєво підвищити рівень кіберстійкості, мінімізувати ризики шахрайства та сформувати більш безпечний і зручний клієнтський досвід [75].

Також, для подолання викликів кібербезпеки та вдосконалення регулювання має бути врегульовано українське законодавство. Основна мета гармонізації полягає у підвищенні прозорості, посиленні захисту прав споживачів та інвесторів, а також інтеграції українського фінансового ринку в європейський простір. Досягнення поставленої мети можливо за рахунок:

1. Впровадження стандартів MiFID II (Markets in Financial Instruments Directive II).

MiFID II регулює надання інвестиційних послуг та діяльність фінансових ринків. Його імплементація вимагає значних змін у законодавстві про цінні папери та банківську діяльність.

Таблиця 3.3

Впровадження стандартів MiFID II для вдосконалення врегулювання банківського сектору [90]

Напрям гармонізації	Рекомендовані заходи
1	2
Захист інвесторів	Впровадити вимоги щодо оцінки придатності (suitability) та відповідності (appropriateness) фінансових інструментів. Банки повинні перевіряти, чи відповідає запропонований інвестиційний продукт знанням, досвіду та фінансовому становищу клієнта.

Продовження табл.3.3

1	2
Прозорість (Pre- & Post-trade)	Запровадити норми щодо прозорості ціноутворення до і після здійснення операцій з фінансовими інструментами. Це включає обов'язкове розкриття інформації про витрати, комісії та можливі конфлікти інтересів.
Корпоративне управління	Посилити вимоги до внутрішнього контролю, управління ризиками та відповідальності керівництва банків за надання інвестиційних послуг.
Звітність (Reporting)	Встановити жорсткі правила щодо звітності про транзакції до регулятора (НБУ/НКЦПФР) в уніфікованому форматі та у стислі терміни.
Визначення Фінансових Інструментів	Розширити перелік фінансових інструментів, що підпадають під регулювання, відповідно до MiFID II (включно з деривативами та інструментами, що торгуються поза біржею - OTC).

2. Впровадження стандартів GDPR (General Data Protection Regulation).

GDPR є найсуворішим у світі регламентом щодо захисту персональних даних. Його впровадження критично важливе для банків, які працюють із даними громадян ЄС або планують вихід на європейські ринки.

Таблиця 3.4

Впровадження стандартів GDPR для вдосконалення врегулювання банківського сектору [92]

Напрям гармонізації	Рекомендовані заходи
Правова основа	Внести зміни до Закону України «Про захист персональних даних», чітко визначивши поняття згоди суб'єкта даних (має бути вільною, конкретною, інформованою та однозначною) та законні підстави для обробки.
Права суб'єктів даних	Забезпечити реалізацію ключових прав, передбачених GDPR:
	* Право на доступ. Клієнт має право отримати підтвердження, чи обробляються його дані, та їх копію.
	* Право на виправлення. Право вимагати виправлення неточних даних.
	* Право на забуття (стирання). Право вимагати видалення персональних даних, якщо вони більше не потрібні.
Відповідальність та управління	Запровадити вимогу про призначення Спеціаліста із захисту даних (Data Protection Officer – DPO) у великих банках та фінансових установах, які здійснюють масштабну обробку даних.
Приватність за замовчуванням (Privacy by Design)	На законодавчому рівні закріпити необхідність інтеграції принципів захисту даних на етапі проєктування систем і продуктів.
Повідомлення про витоки	Встановити жорсткі терміни (до 72 годин) для повідомлення регулятора та суб'єктів даних про витік персональних даних.

Для ефективної гармонізації необхідно уніфікувати підходи до фінансового нагляду та корпоративного управління. Важливим кроком є посилення функцій НБУ та НКЦПФР шляхом надання регуляторам додаткових повноважень для контролю за дотриманням нових норм, особливо у сфері захисту прав інвесторів відповідно до вимог MiFID II та забезпечення інформаційної безпеки згідно з принципами GDPR. Наступним елементом є прийняття вторинного законодавства, що передбачає швидку розробку НБУ та іншими регуляторами підзаконних актів, методичних рекомендацій і стандартів звітності, які деталізують практичну імплементацію вимог MiFID II та GDPR у діяльності банківських установ. Додатково необхідно впровадити обов'язкові програми навчання та сертифікації для співробітників банків, які працюють з інвестиційними послугами та персональними даними, аби забезпечити високий рівень професійної компетентності та відповідність новим регуляторним вимогам.

3.3. Пропозиції щодо підвищення конкурентоспроможності українських банків

Для підвищення конкурентоспроможності українських банків дуже важливим є співпраця між традиційними фінансовими установами (банками) та FinTech-стартапами, та є критично важливою стратегією для забезпечення конкурентоспроможності та довгострокової релевантності в умовах глибокої трансформації світового фінансового ландшафту. Партнерства дозволяють банкам інтегрувати передові технології (наприклад, AI) без необхідності повної заміни основної застарілої інфраструктури (Legacy Systems).

Варто відзначити той факт, що партнерства Bank-FinTech не є просто технологічним аутсорсингом; вони є інструментом для досягнення вимірних стратегічних цілей, які зміцнюють основну діяльність банку. Найважливішими цілями партнерства є обсяг кредитування, продуктивність кредитування та отримання нового доходу.

Найбільш вимірний вплив FinTech-партнерства мають на підвищення операційної ефективності та зниження ризиків. Це підтверджує, що банки використовують FinTech для зміцнення свого існуючого операційного ядра, а не лише для створення абсолютно нових, високоризикованих продуктів. В таблиці 3.5 сформовано пріоритетні цілі співпраці банків та FinTech

Таблиця 3.5

Пріоритетні цілі співпраці банків та FinTech [91]

Категорія цілей	Ключові показники (KPI)	Середнє покращення (%)	Ключові домени
Підвищення операційної ефективності	Продуктивність кредитування (loan productivity)	37%	Платежі, рух коштів, кредитування
Зростання доходів та обсягів	Обсяг кредитування (loan volume), обсяг депозитів	28% / 27%	Мобільні гаманці, нові продукти
Управління ризиками	Зниження шахрайських втрат (fraud losses)	24%	Управління ризиками та шахрайством

Вибір моделі співпраці визначається необхідним рівнем контролю, швидкістю впровадження та готовністю банку брати на себе регуляторний ризик. Однією з найпоширеніших моделей є пряме партнерство (Direct Contract), яке передбачає традиційний формат взаємодії та забезпечує високий рівень контролю банку над питаннями комплаєнсу та інтеграції. У цьому випадку критично важливо ретельно оцінити FinTech-партнера з точки зору його масштабованості, технічної надійності та досвіду в релевантній сфері. Інша модель – Banking-as-a-Service (BaaS) – дає змогу фінтех-компаніям використовувати банківський чартер через посередника. Проте через збільшену дистанцію між банком і кінцевим клієнтом контроль над процесами ускладнюється. Сектор BaaS перебуває під сильним регуляторним тиском з боку OCC та FDIC, що змушує банки бути максимально обережними та вимагати повного контролю над комплаєнсом. Третьою моделлю є стратегічні угоди M&A або створення спільних підприємств (JV), що дозволяє банку отримати повний контроль над технологіями, експертизою та командою

партнера. Хоча інтеграція може бути складною, такий підхід мінімізує зовнішні комплаєнс-ризики та забезпечує довгострокову стабільність співпраці.

Таблиця 3.6

Порівняння ключових моделей партнерства Bank-FinTech [92]

Параметр оцінки	Пряме партнерство (direct contract)	Banking-as-a-Service (BaaS)	Стратегічне M&A/JV
Контроль банку	Високий (прямий контроль комплаєнсу та операцій)	Обмежений (залежність від baas-посередника)	Повний (у випадку m&a)
Регуляторний ризик	Середній (легше забезпечити прямий комплаєнс)	Дуже високий (під пильною увагою регуляторів)	Низький (повна інтеграція під чартер)
Швидкість імплементації	Середня	Висока (доступ до готової інфраструктури)	Низька (високі вимоги до інтеграції)
Критичний фактор успіху	Технічна спроможність fintech інтегруватися з core banking system	Надійність та комплаєнс-контроль baas-провайдера	Успіх культурної та технологічної інтеграції

Регулятори розглядають банк як кінцево відповідальну сторону за діяльність FinTech-партнерів, тому програма належної перевірки має бути не разовою процедурою, а постійним елементом комплексної системи управління ризиками третіх сторін. У межах рекомендацій для банку важливо формувати крос-дисциплінарну команду, до складу якої входять юристи, фахівці з комплаєнсу та IT-експерти, що дозволяє всебічно ідентифікувати та управляти ризиками співпраці. Особливу увагу слід приділяти регуляторному комплаєнсу: ретельний Due Diligence повинен зосереджуватися на відповідності вимогам Bank Secrecy Act (BSA), Anti-Money Laundering (AML), а також програмам ідентифікації клієнтів (CIP/CDD). Важливим аспектом є мінімізація UDAP-ризиків шляхом забезпечення повної прозорості щодо продуктів, тарифів і комісій, а також гарантування того, що FinTech-партнер надає коректні та зрозумілі розкриття інформації, що унеможливлює недобросовісні або оманливі практики. Крім того, банк повинен мати чіткі плани непередбачених ситуацій,

які включають механізми швидкого переходу клієнтів або поглинання критичних функцій у разі різкого припинення партнерства.

FinTech-компаніям також рекомендовано проводити реципроктний Due Diligence банку-партнера, щоб оцінити рівень його стабільності, підхід до комплаєнсу та регуляторний ризик. Зокрема, під час переговорів FinTech має отримати інформацію про попередні або чинні регуляторні дії щодо банку, які можуть вплинути на запуск або стабільність партнерської програми. Також важливо з'ясувати вимоги банку щодо щорічних сторонніх аудитів, потенційні зобов'язання щодо найму окремого комплаєнс-офіцера та оцінити історію індемніфікаційних претензій, які банк висував своїм попереднім партнерам. Такий підхід забезпечує обопільну прозорість, зміцнює довіру між сторонами та мінімізує ризики вже на етапі укладання партнерства [78].

Успішна співпраця між банками та FinTech-компаніями значною мірою залежить від здатності подолати культурні, операційні та технологічні відмінності, адже корпоративна культура відіграє важливішу роль у розвитку інновацій, ніж розмір організації чи обсяг інвестицій. Одним із ключових напрямів інтеграції є модернізація технологічної бази через API-first підхід: банки мають інвестувати у створення гнучкої, модульної та гібридної архітектури, оскільки застарілі системи обмежують швидкість інновацій та ускладнюють ефективну взаємодію з партнерами. Важливим є й формування культури експериментів керівництво повинно демонструвати відкритість до нових підходів, підтримувати командні ініціативи та створювати атмосферу психологічної безпеки, в якій працівники можуть пропонувати ідеї без страху помилок. Крім того, спільні продукти мають базуватися на принципах користувацько орієнтованого дизайну, що забезпечує інтуїтивний, безперебійний та прозорий досвід для клієнтів, які очікують високої якості цифрових сервісів [79].

Для максимізації цінності партнерств і забезпечення надійності з точки зору регуляторних вимог банкам і FinTech-компаніям варто дотримуватися низки стратегічних підходів. Перш за все, доцільно створити «Шлюз інновацій»

спеціалізовану крос-функціональну команду, яка виступатиме єдиною точкою взаємодії та відповідатиме за підготовку повного регуляторно готового пакета документів, зокрема для проведення Due Diligence. Такі команди також повинні захищати FinTech-проєкти від повільних внутрішніх процесів банку, забезпечуючи необхідну швидкість інтеграції та зберігаючи Agility партнерів. Значну увагу потрібно приділити інвестуванню в AI-рішення для підсилення комплаєнсу, автоматизації виявлення шахрайства, транзакційного моніторингу та підвищення ефективності операцій, зокрема кредитування [86].

Крім цього, усі партнерські угоди мають передбачати юридичні зобов'язання щодо нерозривності нагляду та доступу до даних: FinTech повинен забезпечити банку повний доступ до API, даних і технічної документації, що дасть змогу безперервно обслуговувати клієнтів у разі регуляторного втручання або завершення співпраці. У довгостроковій перспективі банки повинні переорієнтовуватися з ролі постачальників окремих продуктів на статус довірених радників, підсилюючи взаємодію з клієнтами персоналізованими та емпатичними цифровими рішеннями, розвиток яких стає можливим завдяки FinTech-партнерствам.

Наступним кроком підвищення рівня конкурентоспроможності банків є підвищення цифрової грамотності клієнтів та співробітників банку. Досягнення поставленої мети можливо за рахунок інвестиції в цифрову грамотність клієнтів і співробітників банку є стратегічним інструментом для подолання цього «розриву між можливостями та компетентністю» та забезпечення довгострокової стійкості [19].

Інвестиції в підвищення цифрової грамотності клієнтів необхідно розглядати як механізм прямого впливу на ключові фінансові показники: зростання доходу, підвищення лояльності та скорочення операційних витрат.

Дослідження підтверджують чітку кількісну кореляцію між цифровою залученістю клієнта та його цінністю для банку. Клієнти, які активно використовують цифровий банкінг, демонструють суттєво вищу прибутковість, лояльність та глибину відносин із банком порівняно з традиційними

користувачами. Передусім, цифрові клієнти забезпечують значно більший приріст доходу 10,7%, що на 6,2 процентних пункти перевищує показник серед нецифрових клієнтів, у яких приріст становить лише 4,5%. Крім того, вони виявляють більшу схильність до розширення взаємодії з банком: у середньому цифрові користувачі додають 1,1 нового продукту за аналізований період, тоді як клієнти, які не користуються цифровими каналами, не додають жодного. Це свідчить про їхню більшу залученість та довіру до банківських сервісів [27].

Цифрові клієнти також демонструють значно нижчий рівень відтоку. Показник attrition rate серед них становить лише 8,9%, що помітно менше, ніж 13,8% серед нецифрових клієнтів. Завдяки цьому банки суттєво знижують ризик втрати довгострокової цінності клієнта (Customer Lifetime Value) приблизно на 35%. У сукупності ці дані доводять, що інвестиції в розвиток цифрових каналів та адаптацію клієнтів до них підвищують не тільки ефективність взаємодії, але й забезпечують стійке зростання доходів і зміцнення конкурентних позицій банку.

Легкий доступ до інформації про рахунки та баланси, забезпечений завдяки навченості клієнта, усуває когнітивний бар'єр і дозволяє приймати частіші та швидші платіжні рішення.

Таблиця 3.7

Фінансовий аналіз клієнтської цінності на базі цифрової залученості [90]

Показник	Цифрові клієнти	Нецифрові клієнти	Фінансова перевага (ключ до roi)
Приріст інкрементального доходу	10,7%	4,5%	+6,2 п.п. (вищий дохід)
Середня кількість додаткових продуктів	1,1	0,0	зростання share-of-wallet
Річний рівень відтоку (attrition rate)	8,9%	13,8%	зниження ризику втрати clv на 35%
Вартість обслуговування (cost-to-serve)	низька (через самообслуговування)	висока (через відділення/кол-центр)	значне зниження операційних витрат

Отже, цифрова грамотність клієнтів є потужним важелем для скорочення операційних витрат банку. Клієнти, які впевнено почуваються в цифровому

середовищі, обирають канали самообслуговування, що є значно менш витратними для банку, ніж особисте обслуговування у відділеннях чи допомога кол-центрів. Освічені клієнти мігрують на нижчі за вартістю канали транзакцій, що призводить до значного зниження потреби у дороговартісних взаємодіях через фізичні відділення. Клієнти, які розуміють функціонал цифрових інструментів (наприклад, онлайн bill pay), ініціюють менше дзвінків до служби підтримки, прямо знижуючи витрати на утримання кол-центрів.

Інвестиції в безпекову грамотність клієнтів є критично важливим заходом ризик-менеджменту з огляду на зростання фінансового ризику, що походить від людського фактора, який експлуатується через соціальну інженерію.

Дані Національного банку України (НБУ) підтверджують ескалацію шахрайства через людський фактор. Соціальна інженерія є найбільш розповсюдженим методом шахрайства в Україні, відповідаючи за 80% від загальної суми фінансових втрат, що свідчить про те, що основні втрати виникають через розголошення клієнтами чутливих особистих даних. Майже все шахрайство відбувається в Інтернеті (83% від загальної кількості), тоді як фізичні пристрої становлять лише 17% втрат. Кількість незаконних дій за платіжними картками зросла на чверть, а збитки виросли на 73%. Середня сума однієї незаконної операції через Інтернет зросла на 30% протягом року, перевищивши 3100 грн. Особливо небезпечним є тренд "Self Fraud", коли жертва мотивується шахраями самостійно ініціювати платіж через власний банкінг; у цьому випадку освіта є єдиним ефективним захисним рубіжем, оскільки традиційні технічні засоби банку безсилі [55].

Дослідження підтверджує, що вищий рівень цифрової фінансової грамотності підвищує обізнаність споживачів про ризики (фішинг, хакерські атаки, крадіжка даних). Для боротьби з комплексними шахрайськими тактиками необхідні глибокі фінансові знання, а не просто обачна фінансова поведінка (наприклад, ведення бюджету), яка має лише незначні ефекти для виявлення шахрайства.

Таблиця 3.8

Динаміка ризику шахрайства та роль освіти (сформовнао за даними України, 2023 р.) [73]

Метрика ризику	Показник	Обґрунтування інвестицій у навчання
частка втрат через соціальну інженерію	80% від загальної суми втрат	освіта є єдиним ефективним бар'єром проти шахрайства, яке використовує людський фактор.
зростання середньої суми втрати (інтернет)	+30% за рік (понад 3100 грн)	демонструє ескалацію фінансової відповідальності та збільшення потенційних збитків.
вимога до запобігання	просунуті фінансові знання	необхідність навчання складним концепціям шахрайства та кібергігієни, що виходять за рамки базових порад.

Вартість інвестицій у превентивну освіту клієнтів є меншою, ніж сукупні потенційні втрати від шахрайства та репутаційна шкода. Активні програми навчання щодо кібербезпеки також створюють для банку регуляторний щит. НБУ здійснює нагляд за дотриманням законодавства про захист прав споживачів фінансових послуг та реклами. Банк, який може продемонструвати всебічне інформування клієнтів про ризики, мінімізує ймовірність застосування до нього заходів впливу та штрафів за порушення.

Щодо підвищення цифрової компетентності співробітників, то варто зазанчити, що інвестиції у внутрішню грамотність персоналу є необхідною передумовою для досягнення зовнішнього ROI та забезпечення операційної стійкості [88].

Існує прямий причинно-наслідковий зв'язок між внутрішньою компетентністю та зовнішньою залученістю клієнтів. Компетентні співробітники фронт-офісу є першою точкою контакту для цифрової міграції. Їхня здатність кваліфіковано пояснити клієнтам, як використовувати новий функціонал мобільного банкінгу, безпосередньо впливає на показник Adoption Rate та глибину використання клієнтом цифрових продуктів. Недостатня підготовка персоналу створює «вузьке місце», яке унеможливлює отримання вигоди від капітальних інвестицій в IT, зменшуючи ROI технологічних інвестицій.

Таким чином, інвестиції в персонал є забезпечувальною інвестицією для всієї цифрової стратегії.

Внутрішня грамотність є критичною для зниження ризику, що походить від самого банку. Навчання співробітників, зокрема у відділах інформаційної безпеки, є життєво необхідним для посилення внутрішніх захисних механізмів та протидії злочинцям в умовах зростання шахрайства. Крім того, НБУ запроваджує чіткі вимоги до корпоративного управління, внутрішнього контролю та розкриття інформації, особливо для значимих фінансових компаній. Належна професійна компетентність персоналу у сфері комплаєнсу та захисту прав споживачів, зокрема знання положень НБУ про нагляд за нефінансовими платіжними послугами, є прямою інвестицією у мінімізацію ризиків регуляторних порушень та потенційних штрафів.

Таблиця 3.9

Оцінка потреби в компетентності співробітників та внутрішній ROI [92]

Сфера компетенції	Ключові ролі	Внутрішні вимоги	Пряма фінансова вигода
Адаптація та залучення (digital adoption)	Фронт-офіс, менеджери з продажів	Глибоке знання функціоналу мобільного банкінгу та сценаріїв навчання клієнтів	Зростання показників залучення клієнтів (adoption rate) та продуктової диверсифікації.
Кібергігієна та запобігання шахрайству	Всі співробітники, іб-відділ	Здатність ідентифікувати загрози соціальної інженерії та внутрішні ризики; протоколи реагування	Зменшення внутрішніх операційних ризиків та запобігання фінансовим втратам.
Регуляторна компетентність	Комплаєнс, юридичний відділ, керівники	Знання нових положень нбу про корпоративне управління та захист прав споживачів	Мінімізація ризику регуляторних штрафів та застосування заходів впливу.

Отже, успішна інвестиційна стратегія повинна бути узгоджена з державними пріоритетами, що надає стратегічні переваги.

Програми банку мають бути позиціоновані як підтримка Національної стратегії розвитку фінансової грамотності до 2030 року, ініційованої НБУ. Інвестиції банку повністю відповідають одній із п’яти ключових цілей Стратегії 2030 «Просунута цифрова фінансова грамотність». Стратегія вимагає розширення уваги на доросле населення, особливо на такі групи, як підприємці, ветерани, внутрішньо переміщені особи та люди старшого віку. Ці групи часто мають нижчий рівень цифрової обізнаності: лише 35% дорослого населення у віці 65+ користується банківськими рахунками, порівняно з 70% молоді до 35 років; 57% жінок мають доступ до рахунків, порівняно з 67% чоловіків. Тому цільові програми банку можуть відкрити для них доступ до фінансових послуг та розширити клієнтську базу. Співпраця з державними інституціями, такими як Мінцифри, яке презентує освітні серіали для підприємців, та НБУ, дозволяє отримати значний іміджевий виграш, використати апробовані методології та знизити витрати на розробку контенту. Отже, інвестиції у підвищення цифрової грамотності є не просто бажаними операційними витратами, а критично важливими капітальними інвестиціями для забезпечення конкурентоспроможності, операційної ефективності та захисту капіталу в умовах домінування соціальної інженерії та стрімкої цифровізації.

Висновки до розділу 3

У результаті дослідження встановлено, що стратегічний розвиток банківського сектору України в умовах цифровізації повинен ґрунтуватися на поєднанні технологічних інновацій, підвищенні операційної стійкості та формуванні клієнтоорієнтованих бізнес-моделей. Доведено, що сучасні технології, зокрема генеративний штучний інтелект, відіграють роль ключового каталізатора трансформації банківських процесів, забезпечуючи можливості гіперперсоналізації послуг, оптимізації внутрішніх операцій і подолання проблеми технічного боргу через модернізацію застарілих IT-рішень.

Обґрунтовано, що зростання складності кіберзагроз вимагає переходу банків до нових підходів у сфері інформаційної безпеки, насамперед до

архітектури «нульової довіри» та впровадження інтелектуальних систем моніторингу транзакцій у реальному часі. Встановлено, що відмова від традиційних статичних механізмів захисту на користь адаптивної багатофакторної та безпарольної аутентифікації є критично важливою умовою забезпечення стабільності та довіри клієнтів у цифровому середовищі.

Доведено необхідність подальшої гармонізації національного регуляторного поля з європейськими стандартами, що сприятиме підвищенню прозорості фінансових ринків, посиленню захисту прав споживачів і інтеграції української банківської системи до єдиного європейського фінансового простору. Виявлено, що стратегічні партнерства з фінтех-компаніями є ефективним інструментом підвищення конкурентоспроможності банків, дозволяючи прискорити інноваційні процеси, оптимізувати операційну діяльність та розширити спектр цифрових послуг.

Особливу увагу приділено ролі цифрової грамотності як фактору фінансової стабільності та збереження капіталу. Встановлено, що інвестиції в підвищення цифрової культури клієнтів і персоналу мають безпосередній економічний ефект, проявляючись у зростанні доходів, підвищенні лояльності клієнтів та зниженні втрат від шахрайства. Узагальнено, що саме освіта у сфері цифрових фінансів є найефективнішим бар’єром проти соціальної інженерії та внутрішніх операційних ризиків.

Таким чином, обґрунтовано, що успішна стратегія розвитку банківського сектору України в умовах цифровізації має базуватися на комплексній архітектурній модернізації, проактивному управлінні кіберризиками, гармонізації регуляторного середовища та системних інвестиціях у цифрову грамотність як ключовому чиннику стійкого розвитку і довгострокової конкурентоспроможності.

ВИСНОВКИ

В результаті проведеного дослідження щодо розвитку банківського сектору України в умовах цифровізації: виклики та перспективи було сформовано наступні висновки.

В теоретичний розділ роботи було присвячено дослідженню теоретико-методичних основ цифровізації банківської діяльності, її економічної сутності, чинників впливу, а також методологічного інструментарію оцінки та нормативно-правового регулювання. У розділі обґрунтовано, що цифровізація є складним процесом трансформації інформації та даних у цифрову форму, який підвищує потенціал їх використання для вирішення завдань, що є складними або недоступними для традиційних методів обробки. Доведено, що цифровізація виступає не самоціллю, а інструментом підвищення ефективності, надаючи нецифровим об’єктам нові властивості, зокрема програмованість, комунікабельність і відстежуваність, та об’єктивно визначає подальший розвиток ринку фінансових послуг. Її вплив зумовив глибокі трансформації у банківському бізнесі, проявом яких є спрощення грошових переказів, поява швидких платіжних інструментів, розширення доступу до онлайн-сервісів (кредитування, страхування), зниження витрат на обслуговування клієнтів, а також активний розвиток сфери фінансових технологій і віртуальних банків. Встановлено, що цифрова трансформація у банківській діяльності полягає в інтеграції технологій у всі ключові процеси з метою підвищення ефективності, доступності фінансових послуг і якості клієнтського сервісу, а її основними напрямами є покращення клієнтського досвіду, розвиток аналітики даних, зростання операційної ефективності та впровадження інноваційних бізнес-моделей, що вимагає формування відповідної цифрової культури та гнучкої стратегічної політики банків.

У розділі доведено, що цифрова зрілість (Digital Maturity) є ключовим стратегічним чинником конкурентоспроможності банку, який прямо корелює зі зростанням фінансових результатів і передбачає інтеграцію трьох базових

компонентів: стратегії, технологій та організаційної культури. Для вимірювання рівня цифровізації розглянуто багатовимірну модель MDDMF, що базується на п’яти ключових вимірах, зокрема операційній досконалості та орієнтації на клієнта. Систематизовано основні індикатори оцінювання цифрової трансформації, серед яких показники операційної ефективності (час виконання операцій, співвідношення витрат до доходів), рівень цифрових продажів (частка операцій у цифрових каналах), а також показники залученості клієнтів (кількість щомісячно активних користувачів, індекс лояльності NPS). Обґрунтовано, що банки з високим рівнем цифрової зрілості активно використовують роботизовану автоматизацію процесів (RPA) та інструменти штучного інтелекту для оптимізації операційної діяльності. Встановлено, що для оцінки ефективності інвестицій у цифрові технології застосовуються показники рентабельності інвестицій (ROI) та чистої приведеної вартості (NPV), тоді як показник загальної вартості володіння (TCO) виступає базовою умовою коректного визначення обсягів інвестицій та запобігання заниженню витрат.

Блок нормативно-правового регулювання охоплює аналіз процесів гармонізації українського регуляторного середовища з правом Європейського Союзу, зокрема з положеннями директиви PSD2. Визначено провідну роль Закону України «Про платіжні послуги» у формуванні архітектури відкритого банкінгу, що забезпечує безпечний обмін фінансовими даними між учасниками ринку за згодою користувачів. Охарактеризовано регуляторні вимоги Національного банку України щодо віддаленої ідентифікації клієнтів, які передбачають використання відеоверифікації, технологій BankID, кваліфікованого електронного підпису та цифрових документів через застосунок «Дія». Проаналізовано міжнародні стандарти посиленої клієнтської автентифікації (SCA), що передбачають застосування щонайменше двох незалежних факторів підтвердження, а також положення регламенту GDPR щодо захисту персональних даних, які ґрунтуються на принципах законності, мінімізації даних та підзвітності. Особливу увагу приділено питанням кібербезпеки та управління ризиками, включно з вимогами до багатофакторної автентифікації та обмеженнями щодо аутсорсингу критичних функцій

резидентам держави-агресора. Також визначено системні ризики цифровізації, зокрема концентраційний ризик, пов’язаний із залежністю від обмеженого кола постачальників хмарних сервісів, та ризики застосування штучного інтелекту, що виникають через недостатню прозорість і пояснюваність алгоритмічних моделей.

В аналітичному розділ роботи зосереджено на аналізі сучасного стану та ключових викликів розвитку банківського сектору України в умовах цифровізації, яка відбувається на тлі глобальної трансформації фінансових ринків та безпрецедентних економічних потрясінь, насамперед унаслідок повномасштабної війни. У дослідженні доведено, що цифровізація перестала бути лише джерелом конкурентних переваг і перетворилася на базовий стандарт функціонування банків та критичний інструмент забезпечення їх операційної стійкості.

Встановлено, що платіжний ринок України характеризується стійкою тенденцією до домінування безготівкових операцій, яка зберігалася і навіть посилилася в умовах воєнного стану. Очікується, що до дев’яти місяців 2025 року частка безготівкових операцій за кількістю досягне понад 95%, а за обсягом – понад 65%. Одночасно відбуваються структурні зрушення у платіжних потоках, зокрема скорочення частки P2P-переказів та зростання частки розрахунків у торговельній мережі через POS-термінали, що свідчить про повернення платіжної активності до споживчого сектору та глибоке проникнення мобільного банкінгу в повсякденні фінансові практики населення.

Дослідження показало високий рівень цифрової інклюзії та технологічного проникнення у банківській системі. Значна частка платіжних карток є токенізованими, а безконтактні технології стали домінуючим стандартом у роздрібних платежах. Відновлення та розширення платіжної інфраструктури після перших руйнувань війни, а також розвиток системи віддаленої ідентифікації клієнтів на базі BankID забезпечили збереження доступності фінансових послуг для більшості населення. Регуляторна політика Національного банку України у 2022–2025 роках закріпила цифрову трансформацію як один із ключових драйверів економічного відновлення, а

прийняття Закону України «Про платіжні послуги» створило правові передумови для впровадження відкритого банкінгу відповідно до європейських стандартів.

Окрему увагу приділено ролі необанків, які стали потужним каталізатором цифрових змін у секторі. Зокрема, приклад Monobank засвідчує, що повністю цифрові бізнес-моделі здатні формувати нові стандарти клієнтського сервісу та змушувати традиційні банки прискорювати впровадження інноваційних рішень.

Водночас ідентифіковано комплекс системних бар'єрів цифрової трансформації. Ключовою проблемою виступає дилема між необхідністю забезпечення стійкості та впровадженням інновацій, коли значні фінансові ресурси спрямовуються на підтримку безперервності діяльності та кіберзахист замість інвестицій у модернізацію. Застарілі IT-системи суттєво ускладнюють інтеграцію з сучасними цифровими рішеннями, знижують швидкість виведення нових продуктів на ринок і підвищують сукупну вартість володіння технологіями. Посилення кіберзагроз та зростання регуляторного тиску з боку Національного банку України зумовлюють необхідність обов'язкових інвестицій у системи кібербезпеки, що додатково обмежує інноваційний потенціал банків. Значним стримувальним фактором є дефіцит кваліфікованих IT-кадрів та потреба у трансформації організаційної культури в напрямі гнучких, клієнтоорієнтованих моделей управління.

Доведено, що зовнішні шоки, зокрема військові дії та енергетичні ризики, не лише ускладнили функціонування банківської системи, але й виступили каталізатором технологічних змін. Відповіддю сектору стало формування моделі гібридної стійкості, що поєднує фізичну надійність інфраструктури через розбудову мережі опорних відділень та впровадження резервних джерел живлення, а також технологічну стійкість завдяки використанню хмарних рішень і посиленню кіберзахисту. Інституціоналізація кризового досвіду через вимоги до планів безперервності діяльності (BCP) закріпила нові стандарти управління операційними ризиками.

Загалом встановлено, що цифрова трансформація банківського сектору України у 2022–2025 роках визначалася насамперед необхідністю забезпечення операційної та кібернетичної стійкості, а не лише прагненням до інноваційного

розвитку. Подальший прогрес у цій сфері потребує подолання структурних бар'єрів, модернізації технологічної бази та глибоких змін організаційної культури, що формує основу для стратегічного розвитку банків в умовах високої невизначеності.

Практичний розділ роботи був присвячений аналізу стратегічних пріоритетів та напрямів розвитку банківського сектору України в умовах цифровізації, визначенню шляхів мінімізації цифрових ризиків, а також формуванню практичних пропозицій щодо підвищення конкурентоспроможності банківських установ. У ході дослідження встановлено, що стратегічні орієнтири інноваційного розвитку банків формуються на перетині технологічної модернізації, трансформації клієнтського досвіду та підвищення операційної стійкості, при цьому ключовим каталізатором цих процесів виступає генеративний штучний інтелект (GenAI), який забезпечує можливості гіперперсоналізації фінансових продуктів і сервісів, а також сприяє подоланню проблеми «технічного боргу» шляхом автоматизованого перекладу та безпечного рефакторингу застарілого програмного коду. Для масштабування таких рішень обґрунтовано необхідність переходу банків до Cloud-Native, Open Source та API-орієнтованих архітектур.

Доведено, що зростання складності сучасних кіберзагроз, у тому числі загроз, посилених застосуванням GenAI, зумовлює потребу у фундаментальній трансформації підходів до безпеки, насамперед через впровадження архітектури нульової довіри (Zero Trust), яка базується на принципі «ніколи не довіряй, завжди перевіряй». Обґрунтовано важливість використання інструментів штучного інтелекту та машинного навчання для моніторингу транзакцій у режимі реального часу, проведення прогностичної аналітики та виявлення нових патернів шахрайства, а також переходу від статичних паролів до адаптивної багатофакторної та безпарольної автентифікації як елемента підвищення кіберстійкості банківських систем.

У межах розділу встановлено, що підвищення прозорості функціонування банківського сектору та його інтеграція до європейського фінансового простору потребують активної гармонізації національного законодавства з нормативними

стандартами ЄС, зокрема положеннями MiFID II щодо захисту прав інвесторів та забезпечення прозорості фінансових ринків, а також вимогами GDPR у частині захисту персональних даних і реалізації принципу «приватність за замовчуванням». Окремо обґрунтовано, що зростання конкурентоспроможності українських банків в умовах цифрової трансформації значною мірою забезпечується через розвиток стратегічних партнерств із FinTech-компаніями, що дозволяє суттєво підвищити операційну ефективність, зокрема збільшити продуктивність кредитних процесів. При цьому доведено, що вибір моделі взаємодії (пряме партнерство, модель Bank-as-a-Service або угоди злиття та поглинання) має визначатися рівнем допустимого регуляторного ризику та потребою банку у збереженні контролю над ключовими процесами, оскільки регулятори розглядають саме банк як кінцево відповідальну сторону.

Особливу увагу приділено ролі цифрової грамотності як інструменту захисту та нарощування капіталу банків. Установлено, що інвестиції у підвищення цифрових компетенцій клієнтів і працівників мають характер довгострокових капітальних вкладень, які прямо впливають на фінансові результати, адже цифрово активні клієнти демонструють вищі темпи зростання доходів і нижчий рівень відтоку. З урахуванням того, що значна частка фінансових втрат зумовлена соціальною інженерією, освітні програми для клієнтів та персоналу визначено як один із найбільш ефективних інструментів протидії шахрайству та зниження операційних ризиків.

Таким чином, у розділі обґрунтовано, що ефективна стратегія розвитку банківського сектору України в умовах цифровізації має базуватися на комплексній архітектурній модернізації із застосуванням GenAI, проактивному впровадженні сучасних моделей кіберзахисту на основі принципів Zero Trust, прискореній гармонізації регуляторного середовища з європейськими стандартами та стратегічних інвестиціях у цифрову грамотність як ключовий чинник зростання, підвищення операційної ефективності та зниження ризиків.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Yoo, Y., Lyytinen, K., Thummadi, B. V., & Weiss, A.(2010). Unbounded innovation with digitalizaiton: Acase of digital camera. Annual Meeting of the Academyof Management, 1-41.

2. Кльоба Л. Г. Цифровізація – інноваційний напрям розвитку банків. *Ефективна економіка*. 2018. № 12. – URL: http://www.economy.nayka.com.ua/?op=1&z=6741 (дата звернення: 02.12.2025). DOI: 10.32702/2307-2105-2018.12.84.

3. Anderton, R., Jarvis, V., & Labhard, V. (2020). The digital economy and the euro area. ECB Economic Bulletin, 8. URL: https://www.ecb.europa.eu/pub/ economic-bulletin/articles/2021/html/ecb.

4. De Clerck, J.-P. (n.d.). Digitization, digitalization and digital transformation: the differences. URL:https://cutt.ly/VL49Dz9.

5. Reis, J., Amorim, M., Melão, N., Cohen, Y., & Rodrigues, M. (2020). Digitalization: A Literature Review and Research Agenda. In Proceedings on 25th International Joint Conference on Industrial Engineering and Operations Management. Springer International Publishing. URL: https://doi.org/10.1007/978-3-030-43616-2_47.

6. Borysyuk, O., Datsyuk-Tomchuk, M., & Lipovska-Makovetska, N. (2020). Imperatyvy rozvytku finansovoho rynku Ukrayiny v umovakh tsyfrovizatsiyi. Ekonomichnyy chasopys Skhidnoyevropeys′koho natsional′noho universytetu imeni Lesi Ukrayinky, 2, 168-176. URL:https://doi.org/10.29038/2411-4014-2020-02-168-176.

7. Владика, Ю., & ТуроваЛ. (2021). РОЛЬ СУЧАСНИХ DIGITAL-ТЕХНОЛОГІЙ У ФУНКЦІОНУВАННІ БАНКІВСЬКОЇ СИСТЕМИ. *Економіка та суспільство*, (25). https://doi.org/10.32782/2524-0072/2021-25-21.

8. Що таке цифрова трансформація в банківській справі? URL:https://www.salesforce.com/financial-services/digital-transformation-banking/.

9. Basel Committee on Banking Supervision (BCBS). (2021). Principles for operational resilience. Bank for International Settlements (BIS). 31 March 2021. URL: URL:https://bank.gov.ua/admin_uploads/article/.

10. Basel Committee on Banking Supervision (BCBS). (2024). Digitalisation of finance. Bank for International Settlements (BIS). May 2024. URL:https://www.fsb.org/uploads/P221024-2.pdf.

11. Çelik, K. (2025). How to Conduct a Digital Maturity Assessment: Tools and Resources. Digitopia. 21 March 2025. URL:https://digitopia.co/blog/digital-maturity-assessment/.

12. European Central Bank (ECB). (2023). Banks' digital transformation: where do we stand? ECB Banking Supervision. 15 February 2023. URL:https://www.bankingsupervision.europa.eu/press/supervisory.

13. European Central Bank (ECB). (2024). Digitalisation: key assessment criteria and collection of sound practices. ECB Banking Supervision. URL:https://www.ethoca.com/ethoca-consumer.

14. Strategies: Excelling at Basics & Striving for Digital Maturity - The Financial Brand. URL:https://thefinancialbrand.com/news/digital-banking/2025-strategies-excelling-at-the-basics-striving-for-digital-maturity-182401.

15. Formation of Methodological Tools for Assessing the Level of Digitalization of Banks/. URL: https://www.researchgate.net/publication/390135698.

16. How digital banks can build an integrated data management system. Wolters Kluwer / Regnology Group GmbH. URL: https://www.google.com/aclk?sa=.

17. How to Begin a Digital Banking Evaluation. Alkami Technology. 22 August 2025. URL:https://www.alkami.com/blog/how-to-begin-a-digital-banking-evaluation-project/.

18. Hunt, A. The Importance Of Digital Risk KRIs For Mid-Sized And Community Banks. 360Factors Blog. URL: https://www.360factors.com/blog/the-importance-of-kris-in-risk-management/.

19. KPMG. (2020). Proposed Principles of Operational Resilience and Operational Risk. Regulatory Alert. August 2020. URL: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2020/10/proposed.

20. Papusha, D. A. (2024). Methods for assessing digital maturity in banking during digital transformation. *Journal of Regional and International Competitiveness*, 5(4), 15-24.

21. Pieton, M. (2024). 2025 Strategies: Excelling at the Basics & Striving for Digital Maturity. The Financial Brand. 23 October 2024. URL: https://thefinancialbrand.com/news/digital-banking/2025-strategies-excelling-at-the.

22. Slivka, O. (2024). 7 Digital Banking KPIs Every Bank Should Focus On. Tapix. 08 April 2024.

23. Vater, D., Engelhardt, J., & Blaser, P. How Digital Done Right Pays Off for Retail Banks. Bain & Company. URL: https://www.bain.com/insights/how-digital-done-right-pays-off-for-retail-banks/.

24. Your roadmap to digital maturity starts here. Alkami Technology. URL:https://www.alkami.com/digital-maturity/.

25. Addo, T. B. A., Chow, C. W., & Haddad, K. M. (2004). Development of an IT Balanced Scorecard. *Journal of International Technology and Information Management*, *13*(4). URL:https://www.researchgate.net/publication/367416698.

26. BairesDev Editorial Team. (2025). Technology ROI: Maximizing Returns on Your Technology Investments. URL: https://www.bairesdev.com/blog/investment-in-technology/.

27. Chen, J. (2025). Economic Value Added (EVA): Boosting Shareholder Value Explained. *Investopedia.* URL:https://www.investopedia.com/terms/e/eva.asp.

28. Danyliv, M. M., Vasilenko, O. A., & Ozherel`eva, O. N. (2020). Evaluation of Investment Attractiveness of the Project “Meat Processing Complex”. URL:https://www.researchgate.net/publication/356766850_Evaluation_of_distributi.

29. Gartner. (2024). Gartner forecasts worldwide IT spending to grow 6.8% in 2024. URL:https://www.gartner.com/en/newsroom/press-releases/01-17-2024-gartner-forecasts-worldwide-it-spending-to-grow-six-point-eight-percent-in-2024.

30. Koi-Akrofi, G. Y. (2017). Justification for IT Investments: Evaluation Methods, Frameworks, and Models. *Texila International Journal of Management*, *3*(2), 410–423.

31. Kraus, P., Kappl, J., & Schlegel, D. (2024). To invest or not to invest in digital initiatives? An exploratory examination of procedures, evaluation criteria and barriers. *Digital Transformation and Society*, *3*(4), 410–423.

32. Pather, S. (2012). ICT Evaluation: Are We Asking the Right Questions? *Electronic Journal on Information Systems in Developing Countries*, *50*(5), 1–14.

33. Sanghvi, P. (2024). Real Options Analysis: Incorporating Flexibility and Optionality into Valuation. *Financial Modeling Prep.* URL:https://site.financialmodelingprep.com/education/financial-analysis/Real.

34. The Value Management Office: Aligning strategy with sustainable value creation. (2025). *Consultancy-me.com.* URL: https://www.consultancy-me.com/news/11699/the-value-management-office-aligning-strategy-with.

35. Закон України «Про платіжні послуги» від 30.06.2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20/stru.

36. Національний банк України. URL: https://bank.gov.ua/ua/legislation/Resolution_27032024_36.

37. Положення про відкритий банкінг в Україні. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/proekt_2025-05-01.pdf .

38. Порядок авторизації діяльності надавачів нефінансових платіжних послуг. URL: https://zakon.rada.gov.ua/laws/show/v0081500-25#Text.

39. Положення про використання електронних довірчих послуг (ЕДП). URL: https://bank.gov.ua/ua/legislation/Resolution_25072025_82.

40. Положення про порядок страхування відповідальності PISP/AISP. URL: https://zakon.rada.gov.ua/laws/show/v0071500-25#Text

41. Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку. URL: https://zakon.rada.gov.ua/laws/show/v0058500-23#Text

42. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text

43. Положенням НБУ № 107 від 28.07.2020 «Про затвердження Положення про здійснення установами фінансового моніторингу». URL: https://zakon.rada.gov.ua/laws/show/v0107500-20#Text.

44. ПОСТАНОВА НБУ 28.09.2017 № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України». URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text.

45. Постанова Правління Національного банку України від 12 серпня 2022 року № 178 "Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об’єктів критичної інфраструктури в банківській системі України". URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text

46. Постанова Правління Національного банку України від 25.07.2025 № 81 "Про затвердження Положення про порядок здійснення авторизації діяльності надавачів нефінансових платіжних послуг". URL: https://zakon.rada.gov.ua/laws/show/v0081500-25#Text

47. Положення про здійснення установами фінансового моніторингу, затверджене постановою Правління Національного банку України від 28.07.2020 № 107. URL:https://bank.gov.ua/ua/news/all/postanovi-pravlinnya-natsionalnogo.

48. Дистанційна ідентифікація та верифікація клієнта (Презентація). URL: https://bank.gov.ua/admin_uploads/article/Vymogy_u_sferi_PVK_FT_pr_work.

49. Вимоги в сфері ПВК/ФТ до суб'єктів первинного фінансового моніторингу. URL: https://bank.gov.ua/admin_uploads/law/28072020_107.pdf.

50. II. Міжнародні та Європейські Нормативні Акти (ЄС). URL: https://www.kmu.gov.ua/storage/app/sites/1/%.

51. General Data Protection Regulation (GDPR) (Art. 5) – Principles relating to processing of personal data. URL: https://gdpr-info.eu/art-5-gdpr/.

52. PSD2 General FAQs. MUFG EMEA. URL: https://www.mufgemea.com/governance/psd2-general-faqs/.

53. Strong Customer Authentication & Compliance Under PSD2. Ping Identity. URL: https://www.pingidentity.com/en/resources/blog/post/the-scoop-on-strong.

54. III. Звіти міжнародних фінансових регуляторів та експертний аналіз. URL:https://documents1.worldbank.org/curated/en/516101484648225381/txt/11211.

55. Cloud Adoption in the Financial Sector and Concentration Risk. Program on International Financial Systems (PIFS). April 2023. URL:https://www.fsb.org/uploads/PIFS.pdf.

56. Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector. Financial Stability Board (FSB). URL:https://www.fsb.org/2025/10/monitoring-adoption-of-artificial-intelligence.

57. The Financial Stability Implications of Artificial Intelligence – Press Release. Financial Stability Board (FSB). 14 November 2024. URL: https://www.fsb.org/uploads/P14112024.pdf.

58. Regulating AI in the financial sector: recent developments and main challenges. Financial Stability Institute (FSI) / Bank for International Settlements (BIS). December 2024. URL: https://www.bis.org/fsi/publ/insights63.htm.

59. Financial stability implications of artificial intelligence - Executive Summary. FSI Executive Summaries / Bank for International Settlements (BIS). 26 June 2025. URL:https://www.bis.org/fsi/fsisummaries/exsum_23904.htm

60. Cashless Payments Dominated Card Transactions in 2024. URL:https://bank.gov.ua/en/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo.

61. Другий рік повномасштабної війни: обсяги безготівкових розрахунків зростають. URL: https://bank.gov.ua/ua/news/all/drugiy-rik-povnomasshtabnoyi.

62. Барабаш Ю. Українські необанки: ключові гравці і потенційні ніші для розвитку. НВ Бізнес. 29 січня 2021. URL: https://biz.nv.ua/ukr/experts/monobank-izibank-abo-sportbank-u-kogo-keshbek-bilshe-novini-ukrajini-50138385.html.

63. Верховодов А. Кейс RBS: як традиційний банк вривається на ринг цифрових фінтехів. URL: https://center42.tech/blog/case-rbs-neobank.

64. Губа М., Лінник А., Колесник Д. Розвиток необанків в Україні та світі. Регіональна економіка та менеджмент, 2019. № 2 (24). С. 71-74. URL: http://biblio.umsf.dp.ua/jspui/bitstream/123456789/3830/1/71-74.pdf.

65. Деркач М. Премія PSM Awards 2023: найкращий цифровий банк. URL: https://psm7.com/uk/news/premiya-psm-awards-2023-luchshij-cifrovoj-bank.html.

66. Деркач М. Які необанки працюють в Україні: огляд. PaySpace Magazine. 01.05.2024. URL: https://psm7.com/uk/fintech/yaki-neobanki-praczyuyut-v-ukrayini-oglyad.html.

67. Еркес О. Є., Калита О. В., Гордієнко Т. М. Потенціал цифрового розвитку банків України. Науковий вісник Ужгородського національного університету. 2019. № 28. С. 108-114.

68. Іршак О. С., Творидло О. І. Розвиток необанків в Україні. Економіка та суспільство. 2022. № 36. URL: https://doi.org/10.32782/2524-0072/2022-36-10.

69. Маркевич К. Необанки vs традиційні банки: як необанки змінюють фінансову систему. Разумков Центр. 17.02.2022. URL: https://razumkov.org.ua/statti/neobanky-vs-tradytsiini-banky-iak-neo-banky-zminiuiut-finansovu-systemy#a4.

70. Річний звіт Національного банку України за 2022 рік. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2022.pdf?v=4.

71. Річний звіт Національного банку України за 2023 рік. URL:https://bank.gov.ua/admin_uploads/article/annual_report_2023.pdf.

72. Річний звіт Національного банку України за 2024 рік. URL:https://bank.gov.ua/ua/news/all/richniy-zvit-natsionalnogo-banku-ukrayini-za-2024-rik.

73. Чуб П. М., Охрименко І. Б., Білошапка В. С. Стан та перспективи розвитку необанків України. Наукові перспективи. 2023. № 1. С. 405–421. DOI: URL:https://doi.org/10.52058/2708-7530-2023-1(31)-405-421.

74. Постанова Правління Національного банку України від 24 лютого 2022 року № 18 «Про роботу банківської системи в період запровадження воєнного стану». URL:https://zakon.rada.gov.ua/laws/show/v0018500-22#Text.

75. Постанова Правління Національного банку України від 29 вересня 2022 року № 210 «Про затвердження Положення про випуск електронних грошей та здійснення платіжних операцій з ними». URL:https://zakon.rada.gov.ua/laws/show/v0210500-22.

76. Постанова Правління Національного банку від 12 січня 2021 року № 2 «Про внесення змін до деяких нормативно-правових актів Національного банку України» (Щодо відтермінування строків автоматизації FinMon). URL:https://zakon.rada.gov.ua/laws/show/v0002500-21.

77. Положення про Систему BankID Національного банку України (Затверджено Правлінням НБУ). URL:https://zakon.rada.gov.ua/laws/show/v0032500-20.

78. Стратегія Національного банку України до 2025 року. URL:https://bank.gov.ua/ua/about/strategy/strategy2022.

79. Зелена книга з розвитку регуляторних технологій на фінансовому ринку України. Національний банк України. URL:https://bank.gov.ua/ua/news/all/zelena-kniga-z-rozvitku-regulyatornih.

80. Про е-гривню – цифрові гроші Національного банку. URL:https://bank.gov.ua/ua/payments/e-hryvnia.

81. Оновлено порядок здійснення установами фінансового моніторингу стосовно PEP / Офіційне Інтернет-представництво Національного банку України. URL:https://bank.gov.ua/ua/news/all/onovleno-poryadok-zdiysnennya-ustanovami-.

82. Бабенко А. С., Вовк Є. О., Марченко Б. В. Фактори та виклики розвитку FinTech-індустрії. *Економіка та суспільство*. 2024. Вип. 61. DOI: URL:https://doi.org/10.32782/2524-0072/2024-61-128.

83. Банки України посилюють підготовку до можливих перебоїв у електропостачанні. *Асоціація українських банків (АУБ)*. 14 листопада 2023 р. URL: https://aub.org.ua.

84. Капралов О. М. Фінтех в Україні: виклики та перспективи в умовах війни та цифрової трансформації. *International Financial Club "BANKIR"*. 09 жовтня 2025 р. URL: https://bankir.kiev.ua.

85. Коваленко А. 2025 рік у банківській сфері: чому менеджерам необхідно володіти технічними знаннями. *IAMPM.* 23 грудня 2024 р. URL: https://iampm.club/ua/blog/2025-rik-u.

86. Тимоць М. В. Аналіз трендів та перспектив цифрового банкінгу в Україні. *International Science Journal of Management Economics & Finance*. 2025. Vol. 4(5). С. 23–32. DOI: 10.46299/j.isjmef.20250405.03.

87. Тривалі відключення електроенергії мають вплив на роботу 76% компаній – нове опитування Deloitte Ukraine та Американської торговельної палат. URL:https://www.deloitte.com/ua/uk/about/press-room/deloitte-acc-winter-resilience-strategy.html.

88. Бугель Ю., Очеретко Б. Цифрова трансформація банківської системи: інновації та вплив на фінансові послуги. *Економічний аналіз*. 2024. Том 34. № 3. С. 257-273. DOI: https://doi.org/10.35774/econa2024.03.257.

89. Цифровий банкінг: ризики фінансової дигіталізації / В. О. Корнівська // Проблеми економіки. - 2017. - № 3. - С. 254-261. - Режим доступу: URL:http://nbuv.gov.ua/UJRN/Pekon_2017_3_34.

90. Національна стратегія розвитку фінансової грамотності до 2030 року. URL:https://bank.gov.ua/ua/about/strategy-fin-literacy.

91. Фінансова грамотність для підприємців. URL:https://business.diia.gov.ua/education/finansova_gramotnist_dla_pidpriemciv.

92. Engels C., Kumar K., Philip D. Financial Literacy and Fraud Detection. *Durham University Business School*. January 2019. URL:https://gflec.org/wp-content/uploads/2019/04/Philip_Dennis.pdf?x37611.

ДОДАТКИ

Додаток А

Таблиця

Підходи до інтерпретації концепції «цифровізації»

Автор	Інтерпретація
Кляба Л.Г.	Оцифрування в банківській справі – це сукупність інновацій в економічній, інституційної, організаційній та управлінській сферах природа в будь-якій сфері функціонування банку, пов'язана з впровадженням цифрових технологій [2].
Андретон Р., Джарвіс В., Лабхард В., Петролакіс Ф., Рубен І.	Цифровізація – це поширення цифрових технологій, що веде до цифрової економіки, що призводить до змін у моделях споживання та виробництва, бізнес-моделях, уподобаннях і відносних цінах, а отже й у всій економіці [3].
De Clerck J.-P.	Цифровізація – це використання цифрових даних і технологій для отримання доходу, покращення бізнесу шляхом трансформації бізнес-процесів та створення цифрового бізнес-середовища, в якому цифрова інформація є основою [4].
Reiss J., Amorim M., Melao N., Cohen I.	Оцифрування – це оцифрування аналогових даних, що, у свою чергу, може покращити взаємовідносини між клієнтом та компанія, що приносила додану цінність всій економіці та суспільству [5].
Борисюк О., Дацюк-Томчук М., Ліповська-Маковецька Н.	Перетворення інформації у цифровий формат, що часто призводить до зниження витрат і створення нових можливостей, серед інших результатів, є ширшою тенденцією в ефективності глобального розвитку. Однак, щоб цифрова трансформація інформації суттєво сприяла цій тенденції, вона має відповідати певним критеріям: охоплюючи такі сфери, як виробництво, бізнес, наука, соціальна сфера та повсякденне життя громадян. Крім того, її ефективність залежить від ефективного використання результатів, забезпечуючи користувачам трансформованої інформації доступ до та необхідні навички для ефективної роботи з цифровою інформацією [6].

Додаток Б

Таблиця

Основні показники оцінки рівня автоматизації банківської системи [15]

Показник	Формула або визначення	Значення для оцінки
Час виконання операції (Turnaround Time, TAT)	(Загальний час, витрачений на виконання конкретного бізнес-процесу / Кількість завершених процесів)	Вимірює ефективність критично важливих бізнес-процесів (наприклад, платежів, затвердження кредитів). Коротший час означає кращу операційну ефективність.
Коефіцієнт витрат до доходу (Cost-to-Income Ratio Improvement)	Поліпшення коефіцієнта C/I	Цифровізація дозволяє автоматизувати ручні процеси та оптимізувати операції, що призводить до економії коштів та зниження C/I.
Ефективність внутрішніх процесів	Частка цифрових транзакцій та середній час виконання операцій (депозитів/вилучень)	Використовується для вимірювання ефективності внутрішніх процесів; оптимізація знижує витрати та покращує якість обслуговування.
Показники командної продуктивності	Швидкість виконання завдань (Lead Time), відсоток виконання запланованих завдань у періоді (спринті), середній час розгортання коду у робоче середовище.	Використовується для оцінки зрілості IT та DevOps процесів

Додаток В

Таблиця

Ключові показники оцінки цифрових продажів у банківському секторі [16]

№	Назва показника (KPI)	Мета використання / опис	Приклади комерційних результатів
1.	Частка продажів через цифрові канали (Digital Sales Share)	Оцінка ефективності оцифрування процесів. Показує, яка частина загального обсягу продажів проходить через мобільні додатки, інтернет-банкінг та інші автоматизовані канали.	Банки з високою оцифровкою (≥80% епізодів), мають 73% продажів через цифрові канали. Банки з низькою оцифровкою (40–60% епізодів), мають лише 41% продажів через цифрові канали. Лідери цифрової зрілості (Digital-first), демонструють у 5 разів більше зростання річного доходу, ніж конкуренти.
2.	Цифровий чистий банківський дохід (Digital Net Banking Income Tracker)	Відокремлення фінансового внеску цифрових ініціатив від загального доходу. Допомагає керівництву оцінити, наскільки інвестиції у цифровізацію окупаються та генерують нову вартість.	Дохід, отриманий виключно від комісій за цифрові транзакції, продажів у додатку або обслуговування цифрових продуктів.
3.	Комерційні результати (Commercial Results)	Деталізована оцінка ефективності на рівні окремих продуктів та клієнтів. Ці показники необхідні для тонкого налаштування маркетингу та операційних процесів.	а) Операційна прибутковість на продукт (визначення найбільш маржинальних цифрових продуктів). б) Вартість залучення клієнта на продукт (CAC) (оцінка ефективності цифрових маркетингових каналів). в) Кількість банківських продуктів у портфелі клієнта (оцінка крос-продажів та лояльності клієнтів).

Додаток Г

Таблиця

Основні показники залученості клієнтів до банківського сектору

Показник	Формула або визначення	Значення для оцінки
Коефіцієнт залучення функцій (Feature Adoption Depth)	(Кількість функцій, використаних клієнтом на місяць / Загальна кількість доступних функцій) * 100	Вимірює, наскільки глибоко клієнти використовують різні можливості додатку. Вищий показник свідчить про цінність функцій для користувачів.
Щомісячні активні користувачі (Monthly Active Users, MAUs)	(Кількість унікальних користувачів, які відкрили додаток хоча б раз за 30 днів / Загальна кількість користувачів) * 100	Надає чітке уявлення про залученість користувачів з часом, є провідним індикатором лояльності та актуальності додатку.
Коефіцієнт цифрового залучення (Digital Adoption Rate, DAR)	Відсоток загальної клієнтської бази, що зареєструвалася та успішно мігрувала на цифрову платформу.	Ключовий показник для підтвердження ефективності стратегії переходу на цифровий канал.
Середній час до першої транзакції (Average Time to First Transaction, ATFT)	(Загальний час, витрачений усіма користувачами на першу транзакцію / Кількість користувачів)	Вимірює, як швидко нові користувачі завершують першу транзакцію. Коротший час свідчить про ефективну та інтуїтивно зрозумілу процедуру онбордингу.
Рівень відмов (Abandonment Rate)	((Кількість користувачів, які відмовилися від процесу / Загальна кількість користувачів, які розпочали процес) * 100)	Надає інформацію про перешкоди на шляху користувача під час транзакцій або процесів. Високий показник вказує на проблеми зі зручністю або складністю.
Індекс чистої підтримки (Net Promoter Score, NPS)	(Відсоток промоутерів – Відсоток детракторів)	Вимірює загальну задоволеність клієнтів та їхню лояльність. Цифрові лідери перевершують конкурентів за NPS на 11 балів.
Коефіцієнт утримання (Retention Rate)	((Кількість унікальних користувачів, що повертаються / Загальна кількість унікальних користувачів за певний період) * 100)	Один із найважливіших KPI для вимірювання лояльності. Вищий коефіцієнт вказує на те, що користувачі знаходять постійну цінність у додатку

Додаток Д

Таблиця

Традиційні методи оцінки ефективності цифрових інвестицій у банківському секторі [25-33]

№	Показник / Метод	Формула / Економічна Сутність	Переваги та застосування	Роль ТСО
1.	Рентабельність інвестицій (Return on Investment, ROI)	$ROI = \left[\frac{\text{Фінансова цінність} - \text{Вартість проєкту}}{\text{Вартість проєкту}}\right]$	Перевага це простота та універсальність, дозволяє порівнювати різні за масштабом проєкти (наприклад, впровадження нового ПЗ чи інструментів ШІ). Застосування це оцінка, чи генерує технологія позитивну вартість. Корисно усереднювати вигоди за перші роки.	Прямий вплив. Необхідний для точного визначення знаменника «Вартість Проєкту» (початкові витрати). Недооцінка ТСО призводить до штучного завищення ROI.
2.	Чиста теперішня вартість (Net Present Value, NPV)	$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} IC$ де: CF_t – чистий грошовий потік у період t, r – ставка дисконтування, IC – початкові інвестиції.	Сутність методу дисконтованих грошових потоків (DCF) полягає в тому, що він враховує часову вартість грошей. Прийняття рішення, якщо NPV > 0 (проєкт створює цінність і приймається); NPV < 0 (проєкт знищує цінність). Критично, що чутливий до вибору ставки дисконтування (r).	Критичний вплив. ТСО забезпечує точну оцінку початкових інвестицій (IC) та впливає на прогноз майбутніх відтоків (CF_t) через операційні витрати, підтримку та міграцію.
3.	Загальна вартість володіння (Total Cost of Ownership, TCO)	Сума всіх прямих та непрямих витрат, пов’язаних з цифровим активом протягом усього його життєвого циклу.	Ціль це забезпечення точної основи для розрахунків ROI та NPV. Складові це початкове придбання, налаштування, кастомізація, міграція даних, інтеграція з *legacy*-системами, поточна підтримка та експлуатація.	Базова умова це ТСО виступає як корегуючий фактор, який запобігає заниженню інвестиційних відтоків, гарантуючи точність фінансових рішень.

Додаток Е

Таблиця

Процес становлення та розвитку необанків в Україні, 2017–2021 рр. та їх характеристики [83]

Найменування необанку	Рік заснування	Банківська ліцензія	Кількість клієнтів (станом на 01.07.2021)	Споживчий сегмент
Monobank	2017	АТ «УНІВЕРСАЛ БАНК»	3,1 млн	Фізичні особи, ФОП
Sportbank	2019	АТ «ТАСКОМБАНК», АТ «ОКСІ БАНК»	240 тис.	Фізичні особи (активний спосіб життя)
todobank	2019	АТ «МЕГАБАНК»	-	Фізичні особи (фокус на Харків)
Izibank	2020	АТ «ТАСКОМБАНК»	100 тис.	Фізичні особи
O.Bank	2020	АТ «Ідея Банк»	120 тис.	Фізичні особи
NEOBANK	2020	АТ «АКБ «КОНКОРД»	-	ФОП, юридичні та фізичні особи (орієнтація на бізнес)
Банк власний рахунок	2021	ПАТ «БАНК ВОСТОК»	-	Фізичні особи (клієнти мережі Fozzy)

Таблиця

Вектори цифровізації НБУ у 2022–2025 рр. [70,71,72]

Напрямок	Технологія	Ключовий суб'єкт	Регуляторний статус автоматизації FinMon
Внутрішній нагляд	SupTech (Наглядові технології)	НБУ	Активний розвиток та впровадження (Концепція 2021)
Зовнішній комплаєнс	RegTech (Регуляторні технології)	Банки та платіжні системи	Обов’язковий (з 2021 р., після відтермінування)
Зовнішній комплаєнс	RegTech (Регуляторні технології)	Небанківські фінустанови	Рекомендаційний

Додаток Є

Таблиця

Виклики щодо впровадження цифрових стандартів у банківський сектор України [82]

Виклик (2022–2025)	Опис згідно з аналізом НБУ	Стратегічний ризик
Системна залежність BankID	Перетворення BankID на єдиний метод автентифікації для критичних державних сервісів, таких як «Резерв+».	Високий ризик кібербезпеки та безперервності діяльності, що має наслідки для національної безпеки, а не лише для фінансової стабільності.
Регуляторний розрив RegTech/FinMon	Існування диспаритету, де автоматизація FinMon є лише рекомендованою для більшості небанківських фінансових установ.	Уповільнення використання повного потенціалу SupTech-систем НБУ та підвищення ризиків легалізації коштів у менш регульованому секторі.
Обмеження обігу Е-грошей	Тимчасове призупинення операцій з випуску та розповсюдження електронних грошей через воєнний стан (Постанова № 18).	Відтермінування реалізації інноваційного потенціалу, закладеного у Законі «Про платіжні послуги».
Невизначеність CBDC	Необхідність точного моделювання макро-фінансових ризиків, зокрема ризиків дезінтермедіації (перетікання депозитів) та впливу на інфляцію у разі досягнення великих обсягів обігу е-гривні.	Макроекономічні ризики, якщо впровадження CBDC не буде зваженим та керованим.

Таблиця

Фінансова оцінка справжньої вартості володіння Legacy Systems (TCO)

Показник	Legacy Systems (старий підхід)	Модернізовані платформи (новий підхід)	Стратегічна вигода (за даними експертів)
Загальна вартість володіння (TCO)	Висока, посилена OpEx на унікальних фахівців та комплаєнс	Нижча	Потенційне зниження TCO на 38-52%
Time-to-Market (нові продукти)	Місяці або роки (через складність зміни коду)	Дні або тижні (завдяки API-економіці)	Прискорення випуску нових продуктів до 62%
Комплаєнс (регуляторний тягар)	Ускладнений, повільна обробка даних	Полегшений (завдяки гнучкій архітектурі)	Зниження операційного ризику та штрафів
Масштабованість	Обмежена	Висока (наприклад, хмарна архітектура)	Сприяння необмеженому зростанню клієнтської бази

Додаток Ж

Таблиця

Регуляторна база НБУ щодо кіберстійкості в період 2022-2025 рр. [70,71,72]

Регуляторний акт	Дата / Редакція	Основний фокус	Вплив на цифрову трансформацію (виклик)
Постанова № 178 НБУ	12.08.2022 (чинна ред. 08.07.2025)	Організація Кіберзахисту та визначення критичної інфраструктури	Вимагає негайних капітальних інвестицій у захищену IT-інфраструктуру, створюючи конкуренцію інноваційним CapEx.
Оновлення порядку (фінмоніторинг, Санкції)	Протягом дії воєнного стану	Виконання вимог фінмоніторингу, валютного нагляду, санкційної політики	Потреба у швидких та адаптивних IT-системах для комплаєнсу, що є складним для Legacy Systems.
Оцінка якості активів та стрес-тестування	Заплановано на 2025 рік	Оцінка стійкості банківської системи та забезпечення рівня капіталу	Стимулює банки до оптимізації TCO через модернізацію та забезпечення операційної стійкості

Таблиця

Етапи культурної трансформації банківського сектору України [85]

Етап	Опис
1. Діагностика поточного стану	Комплексний аналіз існуючої інформаційної інфраструктури, визначення рівня цифрової зрілості та ідентифікація технологічних обмежень.
2. Формування стратегії	Розробка деталізованої моделі майбутнього стану, включаючи визначення цілей, пріоритетів та ключових показників ефективності (KPI).
3. Розробка організаційної моделі трансформації	Створення послідовного плану дій (дорожньої карти), що деталізує етапи переходу, вибір оптимальних технологічних рішень, розподіл ресурсів та визначення відповідальних осіб.
4. Пілотні проєкти та ітеративна реалізація	Впровадження експериментальних проєктів (Agile/Scrum) для перевірки ефективності обраних технологій та підходів.
5. Моніторинг та адаптація	Збір та аналіз даних для оцінки ефективності реалізації стратегії, виявлення відхилень та внесення коректив (постійне вдосконалення)

Додаток З

Таблиця

Заходи НБУ щодо сприяння розвитку ринку FinTech та забезпечення стабільності фінансової системи України в умовах війни у 2022–2025 рр. [70,71,72]

Заходи та нормативні зміни	Якісне покращення	Період запровадження
Закон України «Про платіжні послуги» та імплементація PSD2	Комплексне оновлення платіжного ландшафту й поява нових учасників, розширення їхніх можливостей.	2022
Регуляторна платформа «пісочниці»	Створення умов для оперативного розвитку інноваційних продуктів і послуг та їх швидкого виходу на ринок.	2023
Міжнародний стандарт ISO 20022	Нове покоління СЕП НБУ на базі міжнародного стандарту ISO 20022 в цілодобовому режимі.	2023
SEPA та запуск миттєвих платежів	Приєднання до ключових світових розрахункових систем.	2024
Відкритий банкінг	Сприятиме появі нових платіжних стартапів та забезпечить здорову конкуренцію на платіжному ринку.	2025

Таблиця

Комплексні стратегічні пріоритети інноваційного розвитку сучасного банківського сектору на 2025–2030 рр. [70,71,72]

Стратегічний вектор	Пріоритет (напрямок)	Ключова інноваційна мета
I. Технологічна фундація	Модернізація ядра та даних	Перехід до Cloud-Native/Open Source архітектур; використання GenAI для усунення технічного боргу.
	Впровадження GenAI	Масштабування ШІ (від пілотів до корпоративної стратегії) та забезпечення якості даних (AI-Ready Data).
II. Зростання та CX	Гіперперсоналізація	Проактивна, GenAI-керована мікро-персоналізація досвіду та продуктів (Shift from Selling to Solving).
	Омніканальність та Embedded Finance	Безшовна інтеграція цифрових та фізичних каналів; використання API для Embedded Finance.
III. Стійкість та ризики	Cybersecurity та RegTech	Проактивне управління комплаєнсом (RegTech); протидія GenAI-загрозам (Black Hat GenAI); архітектура Zero Trust.
	ESG-Інтеграція	Вбудовування ESG-критеріїв у ризик-менеджмент та розробка інноваційних продуктів сталого фінансування.
	DLT/Токенізація	Забезпечення сумісності систем з майбутньою інфраструктурою центробанків (wCBDC, оновлений RTGS) для wholesale-розрахунків