

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»**

Кваліфікаційна наукова праця
на правах рукопису

ВОЛОШИН ДМИТРО МИКОЛАЙОВИЧ

УДК 336.71:005.21:004.8:005.334:336.76


ДИСЕРТАЦІЯ

**ФОРМУВАННЯ СТРАТЕГІЇ РОЗВИТКУ ФІНАНСОВИХ
ПОСЕРЕДНИКІВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ**

Галузь знань: 07 «Управління та адміністрування»
Спеціальність: 072 «Фінанси, банківська справа та страхування»

Подається на здобуття ступеня доктора філософії.

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


_____ Д. М. Волошин

Науковий керівник:
Шишкіна Олена Вікторівна,
доктор економічних наук, професор,
професор кафедри фінансів,
банківської справи та страхування
Національного університету
«Чернігівська політехніка»

Чернігів – 2026

АНОТАЦІЯ

Волошин Д. М. Формування стратегії розвитку фінансових посередників в умовах цифровізації економіки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 072 «Фінанси, банківська справа та страхування» (07 «Управління та адміністрування»). – Національний університет «Чернігівська політехніка». – Чернігів, 2026.

Дисертаційну роботу присвячено поглибленню теоретико-методичних засад та розробці практичних механізмів формування стратегії розвитку фінансових посередників в умовах цифровізації економіки. Актуальність теми зумовлена глибокими інституційними змінами, яких зазнає фінансовий сектор під впливом цифрових технологій, а також необхідністю адаптації фінансових установ до викликів воєнного часу та завдань повоєнної відбудови України, інтеграції вітчизняного фінансового ринку до єдиного цифрового простору Європейського Союзу.

У першому розділі роботи досліджено еволюцію ролі та функцій фінансових посередників у цифровій економіці. Доведено, що сучасний фінансовий посередник поступово перетворюється з традиційного інституту акумуляції та перерозподілу ресурсів на цифрову платформу, координатора екосистеми та постачальника даних-центричних сервісів.

Запропоновано авторську класифікацію фінансових посередників за критеріями ступеня цифровізації технологічної основи, функціонального призначення та рівня регуляторної інтеграції. Виокремлено шість взаємодоповнюючих механізмів впливу фінансових посередників на розвиток цифрових фінансових сервісів – інституційний, технологічний, платформний, регуляторно-інноваційний, освітньо-комунікаційний та інвестиційно-фінансовий – та доведено, що їх системна взаємодія створює синергетичний ефект, який підсилює інноваційний потенціал цифрового фінансового ринку.

Досліджено трансформацію ключових функцій фінансових посередників – управління ризиками (перехід від реактивного до проактивного підходу на основі Big Data та AI), формування довіри (перехід від інституційної до технологічної та алгоритмічної довіри), інфраструктурної, інноваційної, фінансової інклюзії та стратегічного розвитку. Визначено чотири рівні участі фінансових інновацій у формуванні стратегічної моделі розвитку: технологічна база, інноваційні рішення, стратегічні імперативи та стратегічні результати. Обґрунтовано імперативи платформізації, екосистемності, алгоритмічної довіри та кіберстійкості як основи нової стратегічної архітектури фінансового посередництва. У межах теоретичного аналізу також досліджено феномен кіберзагроз, систематизовано їхні види та обґрунтовано багаторівневу архітектуру кіберзагроз фінансових посередників (клієнтський, технологічний, організаційний та інституційний рівні).

У другому розділі розроблено методологічний інструментарій оцінювання цифрової зрілості фінансових посередників. Проведений аналіз міжнародних підходів засвідчив відсутність універсальної методики, адаптованої до умов функціонування фінансових посередників у країнах з ринками, що розвиваються, особливо в умовах воєнних викликів. На основі гібридного підходу запропоновано авторську модель оцінювання цифрової зрілості (Digital Capability Maturity Index, DCMI), яка інтегрує шість ключових вимірів: технологічну інфраструктуру, процесну зрілість, клієнтську цифрову взаємодію, інноваційну спроможність, кіберстійкість та регуляторно-інституційну відповідність.

Розроблено методику розрахунку інтегрального показника, що включає процедури нормування, визначення вагових коефіцієнтів та агрегування. Проведено аналіз глобальних трендів цифрової трансформації фінансового посередництва, виокремлено три провідні моделі – європейську (регуляторно-орієнтовану, з високими стандартами операційної стійкості), американську (ринково-інноваційну, з домінуванням BigTech) та азійську (платформно-екосистемну, з максимальною фінансовою інклюзією) – та обґрунтовано

доцільність формування гібридної моделі для України, яка інтегрує європейські стандарти кіберстійкості, американську інноваційну гнучкість та азійську масштабованість. Здійснено пілотне оцінювання цифрової зрілості двох системно важливих банків України. Визначено пріоритетні напрями подальших інвестицій для кожної установи.

У третьому розділі запропоновано практичні механізми формування та реалізації стратегії розвитку фінансових посередників в Україні в умовах повоєнного відновлення. Розроблено триетапну дорожню карту імплементації Регламенту ЄС про цифрову операційну стійкість (DORA) на період 2026–2030 років, яка охоплює оцінювально-нормативний (2026–2027), пілотний (2027–2028) та масштабний (2028–2030) етапи. Визначено основні розриви між чинним регулюванням Національного банку України та вимогами DORA за п'ятьма сферами: управління ІКТ-ризиками, звітування про інциденти, тестування операційної стійкості, управління ризиками від третіх ІКТ-провайдерів та обмін інформацією про кіберзагрози. Обґрунтовано архітектуру запровадженого з серпня 2025 року відкритого банкінгу в Україні у вигляді трирівневої моделі, яка забезпечує баланс між стимулюванням інновацій через безоплатний доступ до базових API та захистом прав споживачів.

Запропоновано організаційно-економічний механізм інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку, який складається з трьох блоків: координаційного (Координаційний центр інтеграції на базі НБУ за участі профільних асоціацій), ресурсного (державне фінансування, міжнародна технічна допомога, приватні інвестиції) та моніторингового (система кількісних і якісних показників зі зворотними зв'язками). Для кожного блоку визначено інструменти стимулювання, диференційовані за трьома групами (фінансові, регуляторні, організаційні) та цільовими аудиторіями (кредитні спілки, страхові компанії, фінтех-стартапи, банки).

Розроблено типову структуру стратегії кіберстійкості фінансового посередника, яка складається з семи взаємопов'язаних розділів (політики та організаційна структура, ідентифікація активів, управління ризиками, захисні заходи, виявлення та моніторинг, реагування на інциденти, відновлення після інцидентів) та шестикроковий циклічний алгоритм її впровадження (самооцінка → усунення розривів → технічне впровадження → навчання персоналу → сертифікація → постійний моніторинг). Ключовою особливістю алгоритму є наявність зворотних зв'язків, що забезпечують адаптивність до змін середовища загроз.

Запропоновано систему показників ефективності впровадження цифрових рішень, що охоплює чотири групи КРІ (фінансові, операційні, ризикові, клієнтські) з бенчмарками та цільовими значеннями. Сформульовано диференційовані рекомендації для фінансових посередників з високим, середнім і базовим рівнем цифрової зрілості.

Ключові слова: фінансові посередники, цифрова трансформація, стратегія розвитку, цифрова зрілість, кіберстійкість, кіберзагрози, відкритий банкінг, цифрова ідентифікація, інноваційна інфраструктура, екосистемна взаємодія.

ABSTRACT

Voloshyn D. M. Formation of a development strategy for financial intermediaries in the context of economic digitalisation. – A qualifying academic paper in manuscript form.

Thesis for the degree of Doctor of Philosophy in the specialisation 072 “Finance, Banking and Insurance” (07 “Management and Administration”). – Chernihiv Polytechnic National University. – Chernihiv, 2026.

This thesis is devoted to the further development of the theoretical and methodological foundations and the design of practical mechanisms for formulating a development strategy for financial intermediaries in the context of the economy digitalisation. The relevance of this topic stems from the profound institutional changes the financial sector is undergoing as a result of digital technologies, as well as the need for financial institutions to adapt to the challenges of wartime and the tasks of Ukraine’s post-war reconstruction, and to integrate the domestic financial market into the European Union’s single digital space.

Chapter 1 of this study examines the evolution of the role and functions of financial intermediaries in the digital economy. It demonstrates that the modern financial intermediary is gradually transforming from a traditional institution for the accumulation and redistribution of resources into a digital platform, an ecosystem coordinator and a provider of data-centric services.

The following is a proposed classification of financial intermediaries based on the degree of digitalisation of their technological infrastructure, their functional purpose and the level of regulatory integration. Six complementary mechanisms through which financial intermediaries influence the development of digital financial services have been identified: institutional, technological, platform-based, regulatory and innovation-related, educational and communication-related, and investment and financial – and it has been demonstrated that their systematic interaction creates a synergistic effect that enhances the innovative potential of the digital financial market.

The study examined the transformation of key functions performed by financial intermediaries: risk management (the shift from a reactive to a proactive approach based on Big Data and AI), trust-building (the shift from institutional to technological and algorithmic trust), infrastructure, innovation, financial inclusion and strategic development. Four levels of financial innovation's involvement in shaping a strategic development model have been identified: technological infrastructure, innovative solutions, strategic imperatives and strategic outcomes. The imperatives of platformisation, ecosystem-based approaches, algorithmic trust and cyber resilience are substantiated as the foundations of a new strategic architecture for financial intermediation. As part of the theoretical analysis, the phenomenon of cyber threats is also examined, their types are systematised, and a multi-level architecture of cyber threats to financial intermediaries (client, technological, organisational and institutional levels) is substantiated.

Section 2 sets out a methodological framework for assessing the digital maturity of financial intermediaries. The analysis of international approaches has revealed that there is no universal methodology adapted to the operating conditions of financial intermediaries in emerging markets, particularly in the context of military challenges. Based on a hybrid approach, the authors propose a model for assessing digital maturity (Digital Capability Maturity Index, DCMI), which integrates six key dimensions: technological infrastructure, process maturity, customer digital interaction, innovation capability, cyber resilience and regulatory and institutional compliance. A methodology has been developed for calculating a composite indicator, which includes standardisation procedures, the determination of weighting coefficients, and aggregation. An analysis of global trends in the digital transformation of financial intermediation has been carried out, identifying three leading models – the European model (regulation-oriented, with high standards of operational resilience), the American model (market-driven and innovation-focused, dominated by Big Tech) and the Asian (platform-ecosystem-based, with maximum financial inclusion) – and the feasibility of developing a hybrid model for Ukraine has been demonstrated, one that integrates European cyber resilience standards,

American innovative flexibility and Asian scalability. A pilot assessment of the digital maturity of two systemically important banks in Ukraine has been carried out. Priority areas for further investment have been identified for each institution.

Section 3 proposes practical mechanisms for formulating and implementing a development strategy for financial intermediaries in Ukraine in the context of post-war reconstruction. A three-stage roadmap has been drawn up for the implementation of the EU Digital Operational Resilience Act (DORA) for the period 2026–2030, covering the assessment and regulatory phase (2026–2027), pilot (2027–2028) and full-scale (2028–2030) phases. The key gaps between the current regulations of the National Bank of Ukraine and the DORA requirements have been identified across five areas: ICT risk management, incident reporting, operational resilience testing, management of risks from third-party ICT providers, and the exchange of information on cyber threats. The architecture of open banking in Ukraine, to be introduced in August 2025, has been justified as a three-tier model that strikes a balance between encouraging innovation through free access to basic APIs and protecting consumer rights.

An organisational and economic mechanism has been proposed for integrating financial intermediaries into the innovative infrastructure of the digital financial market, comprising three components: a coordination component (a Coordination Centre for Integration based at the NBU, with the participation of relevant associations), a resource block (state funding, international technical assistance, private investment) and a monitoring block (a system of quantitative and qualitative indicators with feedback mechanisms). For each sector, incentive measures have been identified, categorised into three groups (financial, regulatory and organisational) and targeted at specific audiences (credit unions, insurance companies, fintech start-ups and banks).

A standard framework for a financial intermediary's cyber resilience strategy has been developed, comprising seven interrelated sections (policies and organisational structure, asset identification, risk management, protective measures, detection and monitoring, incident response, and incident recovery) and a six-step

cyclical algorithm for its implementation (self-assessment → gap resolution → technical implementation → staff training → certification → continuous monitoring). A key feature of the algorithm is the presence of feedback loops, which ensure adaptability to changes in the threat environment.

A system of performance indicators for the implementation of digital solutions has been proposed, covering four groups of KPIs (financial, operational, risk-related and customer-related) with benchmarks and target values. Tailored recommendations have been formulated for financial intermediaries with high, medium and basic levels of digital maturity.

Key words: financial intermediaries, digital transformation, development strategy, digital maturity, cyber resilience, cyber threats, open banking, digital identification, innovative infrastructure, ecosystem interaction.

ЗМІСТ

ВСТУП.....	15
Розділ 1. Теоретичні засади формування стратегії розвитку	
фінансових посередників в умовах цифровізації економіки.....	24
1.1. Еволюція ролі та функцій фінансових посередників у цифровій економіці: стратегічні орієнтири трансформації	24
1.2. Вплив цифрових технологій та фінансових інновацій на архітектуру стратегічного управління розвитком фінансових посередників.....	54
1.3. Імперативи довіри та кібербезпеки в системі стратегічних викликів цифровізації фінансового сектору	87
Висновки до розділу 1	114
Розділ 2. Методичні підходи до оцінювання та аналізу стратегічного розвитку фінансових посередників в умовах цифровізації.....	117
2.1. Методологічний інструментарій дослідження цифрової трансформації фінансових посередників.....	117
2.2. Аналіз впливу цифрових технологій на ефективність стратегічного управління фінансовими посередниками в Україні	239
2.3. Інтегральне оцінювання рівня цифрової зрілості фінансових посередників як детермінанти їх конкурентоспроможності	175
Висновки до розділу 2	190
Розділ 3. Практичні механізми формування та реалізації стратегії розвитку фінансових посередників в Україні	193
3.1. Імплементация міжнародного досвіду цифрової трансформації фінансового посередництва в умовах повоєнного відновлення України	193
3.2. Організаційно-економічний механізм інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку України	208

3.3. Науково-практичні рекомендації щодо реалізації стратегії кіберстійкості та оцінка ефективності впровадження цифрових рішень у діяльність фінансових посередників.....	230
Висновки до розділу 3	248
ВИСНОВКИ	251
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	255
ДОДАТКИ	283

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті в іноземних наукових виданнях: SCOPUS

1. Basiurkina N., Krylov D., Karpinska H., Pchela A., **Voloshyn D.** The Impact of Digitalization on Financial Mechanisms for Managing the Strategic Development of Enterprises in The Face of Modern Challenges. *Pacific Business Review (International)*. 2026. Vol. 18, Issue 9, March. P. 123–136. URL: https://www.pbr.co.in/2026/2025_month/March/11.pdf (1,9 ум. друк. арк.).
Особистий внесок автора: досліджено вплив цифровізації на фінансові механізми стратегічного управління підприємствами в умовах сучасних викликів (0,38 ум. друк. арк.).

Статті у фахових виданнях України

2. Шишкіна О., **Волошин Д.**, Ринжук Д. Вплив цифрових технологій на стратегії розвитку фінансових посередників в Україні. *Проблеми і перспективи економіки та управління*. 2024. № 2(38). С. 177–189. [https://doi.org/10.25140/2411-5215-2024-2\(38\)-177-189](https://doi.org/10.25140/2411-5215-2024-2(38)-177-189) (1,5 ум. друк. арк.).
Особистий внесок автора: здійснено аналіз сучасних цифрових технологій та їх впливу на стратегічний розвиток фінансових посередників в Україні; сформульовано висновки щодо перспектив впровадження цифрових інструментів у діяльність фінансових установ (0,5 ум. друк. арк.).

3. Малихін А., **Волошин Д.** Аналіз ролі фінансових посередників у процесі формування інноваційної інфраструктури ринку цифрових фінансових послуг України. *Науковий вісник Полісся*, 2025. №1 (30), 284–299. [https://doi.org/10.25140/2410-9576-2025-1\(30\)-284-299](https://doi.org/10.25140/2410-9576-2025-1(30)-284-299) (1,9 ум. друк. арк.).
Особистий внесок автора: визначено чинники, що обумовлюють розвиток цифрового фінансового середовища в Україні; запропоновано підходи до оцінювання інноваційного потенціалу фінансових посередників (0,95 ум. друк. арк.).

4. Шишкіна О. В., **Волошин Д. М.**, Малихін А. Г. Стратегічні підходи до інтеграції цифрових рішень у діяльність фінансових посередників на ринку України. *Проблеми і перспективи економіки та управління*. 2025. № 3(43). С.

310-325. DOI: [https://doi.org/10.25140/2411-5215-2025-3\(43\)-310-325](https://doi.org/10.25140/2411-5215-2025-3(43)-310-325) (1,9 ум. друк. арк.). Особистий внесок автора: обґрунтовано методичні засади оцінювання ефективності цифровізації; сформовано практичні рекомендації щодо впровадження інноваційних технологій (0,65 ум. друк. арк.).

5. Волошин Д. М. Теоретико-методичні аспекти оцінювання цифрової зрілості фінансових посередників. *Успіхи і досягнення у науці*”. 2026. № 4(26) 2026. С. 1119-1132. DOI: [https://doi.org/10.52058/3041-1254-2026-4\(26\)](https://doi.org/10.52058/3041-1254-2026-4(26)) (1,6 ум. друк. арк.).

Публікації, що засвідчують апробацію матеріалів дисертації

6. Шишкіна О. В., **Волошин Д. М.** Роль нових технологій у формуванні стратегії розвитку фінансових посередників. *Юніст ь науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених* (м. Чернігів, 26-27 квітня 2023 р.). Чернігів : НУ «Чернігівська політехніка», 2023. С. 90-91 (0,1 ум. друк. арк.). Особистий внесок автора: обґрунтовано перспективні напрями технологічного оновлення фінансових установ (0,05 ум. друк. арк.).

7. Шишкіна О. В., **Волошин Д. М.** Актуальні типи кіберзагроз функціонування і розвитку фінансових установ. *Економіко-правові та управлінсько-технологічні виміри сьогодення: молодіжний погляд : матеріали міжнародної науково-практичної конференції* (м. Дніпро, 03 листопада 2023 р.): у 3 т. Том 1. Дніпро : Університет митної справи та фінансів, 2023. С. 258-260 (0,2 ум. друк. арк.). Особистий внесок автора: систематизовано актуальні типи кіберзагроз для фінансових установ та проаналізовано їх вплив на функціонування і розвиток фінансового сектору (0,1 ум. друк. арк.).

8. **Волошин Д.**, Шишкіна О., Киселиця С. Етичні виклики цифровізації: філософський аналіз довіри як основи фінансового посередництва. *Соціальне підприємництво як інструмент відновлення України: Форум стейкхолдерів розвитку соціального підприємництва* (м. Чернігів, 16 вересня 2024 р.) : тези доповідей. Чернігів : НУ «Чернігівська політехніка», 2024. С. 90-92. URL:

<https://stu.cn.ua/wp-content/uploads/2024/09/zbirnyk.pdf> (0,1 ум. друк. арк.).

Особистий внесок автора: здійснено аналіз етичних викликів, пов'язаних із цифровізацією фінансового посередництва (0,03 ум. друк. арк.).

9. Шишкіна О., **Волошин Д.**, Ринжук Д. Роль цифрових технологій у формуванні стратегій розвитку фінансових посередників. *Соціальне підприємництво як інструмент відновлення України: Форум стейкхолдерів розвитку соціального підприємництва* (м. Чернігів, 16 вересня 2024 р.) : тези доповідей. – Чернігів : НУ «Чернігівська політехніка», 2024, С. 183-185. URL: <https://stu.cn.ua/wp-content/uploads/2024/09/zbirnyk.pdf> (0,2 ум. друк. арк.).
Особистий внесок автора: обґрунтовано взаємозв'язок між рівнем цифровізації та конкурентоспроможністю фінансових установ (0,06 ум. друк. арк.).

10. Шишкіна О. В., **Волошин Д. М.**, Малихін А. Г., Цифровізація економіки як фактор конкурентоспроможності фінансових посередників в Україні. *Юність науки – 2025* : збірник тез доповідей XV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 23-25 квітня 2025 р.). Чернігів : НУ «Чернігівська політехніка», 2025. С. 107-108 <https://ir.stu.cn.ua/items/7024c8b0-86f3-4ff4-baa0-3548f8c61574> (0,1 ум. друк. арк.).
Особистий внесок автора: визначено ключові цифрові фактори підвищення ринкових позицій фінансових установ (0,03 ум. друк. арк.).

11. Шишкіна О. В., **Волошин Д. М.**, Малихін А. Г. Роль фінансових посередників у створенні та впровадженні інноваційних фінансових продуктів в умовах цифровізації. *Збірник наукових праць IV міжнародної науково-практичної конференції (Запоріжжя-Мелітополь, 20 травня 2025 р., МДПУ імені Богдана Хмельницького)*. Запоріжжя : Видавництво МДПУ ім. Б. Хмельницького, 2025. С. Випуск 14. С. 249-253 (0,3 ум. друк. арк.).
Особистий внесок автора: проаналізовано роль фінансових посередників у розробці та впровадженні інноваційних фінансових продуктів в умовах цифрової трансформації (0,1 ум. друк. арк.).

ВСТУП

Актуальність теми дослідження. Цифрова трансформація економічних процесів змінює інституційне середовище, форми конкурентної взаємодії та механізми створення вартості у фінансовому секторі. Фінансові посередники – банки, небанківські фінансові установи, фінтех-компанії – опиняються в центрі цих змін. Вони не лише адаптуються до нових умов, а й дедалі частіше виступають драйверами впровадження інновацій, забезпечують цифровий доступ до капіталу та формують інфраструктуру сучасного фінансового ринку. Однак цифровізація одночасно породжує нові ризики – кіберзагрози, операційну нестабільність, алгоритмічну вразливість. Це актуалізує потребу в перегляді стратегічних орієнтирів розвитку фінансових посередників.

Для України зазначена проблематика набуває особливого звучання. Умови повномасштабної військової агресії та необхідність повоєнної відбудови створили безпрецедентний виклик для фінансової системи. Цифрові фінансові інструменти в цих екстремальних умовах продемонстрували відносну стійкість, забезпечивши безперебійність платежів. Водночас постало завдання не лише зберегти досягнутий рівень, а й сформувати нову архітектуру фінансового посередництва, здатну відповідати викликам цифрової економіки та євроінтеграційним вимогам. Інтеграція до єдиного цифрового простору Європейського Союзу, імплементація стандартів відкритого банкінгу та регуляторних рамок кіберстійкості стають не просто бажаними, а обов'язковими напрямками розвитку. Це зумовлює необхідність системного дослідження стратегічних механізмів розвитку фінансових посередників в умовах цифровізації.

Проблематика цифрової трансформації фінансових посередників перебуває у фокусі уваги багатьох вітчизняних і зарубіжних науковців. Зарубіжна наукова думка представлена кількома напрямками. З огляду на значну кількість публікацій, присвячених різним аспектам цифрової трансформації фінансового сектору, у межах цього дослідження неможливо охопити всі

напрацювання вітчизняних та зарубіжних учених. Саме тому аналіз наукової літератури нами був зосереджено на тих працях, які безпосередньо стосуються обраної теми та мають найбільший вплив на формування концептуальних засад дослідження. Зокрема, Еволюцію FinTech, регуляторні виклики та концепцію RegTech досліджують Д. Арнер, Дж. Барберіс та Р. Баклі. П. Гомбер, Я. Кох та М. Зірінг у свої роботах аналізують трансформацію бізнес-моделей банків, процеси «анбандлінгу» та «ребандлінгу» фінансових послуг, відкритий банкінг. Компоненти фінтех-екосистем, роль уряду, фінансових інститутів, венчурного капіталу та споживачів розглядають І. Лі та Й. Дж. Шін. Роль венчурних інвесторів та краудфандингових платформ у фінансуванні ранніх інновацій на ринках, що розвиваються висвітлено в працях Т. Залан та Е. Туфайлі.

Питання кіберстійкості та управління ризиками у фінансовому секторі досліджують Є. Копп, Л. Каффенбергер, К. Вілсон (IMF), а також автори робіт у рамках Базельського комітету з банківського нагляду та ENISA. Вплив FinTech на прибутковість банків аналізують С. Бен Насер, Б. Канделон, С. Елекдаг, Д. Емруллаху (IMF). Розвиток цифрових платежів, відкритого банкінгу та API-економіки досліджується в роботах OECD, BIS, Світового банку, Європейського центрального банку, а також у звітах провідних консалтингових і аналітичних компаній - McKinsey & Company, Accenture, Capgemini, Deloitte, Gartner. Стандартизацію та регуляторні рамки цифрової операційної стійкості (DORA) висвітлено в документах Європейського Союзу та аналітичних матеріалах DLA Piper, Bernitsas Law.

Практику впровадження цифрових технологій у фінансовий сектор на прикладі різних країн досліджують Фейен Е., Фрост Дж., Гамбасорта Л., Натараджан Х., Саал М. (BIS), а також автори звітів Світового банку щодо цифрової фінансової інклюзії та глобальних трендів FinTech. Розвиток систем миттєвих платежів та цифрових валют центральних банків аналізується в публікаціях BIS, Європейського центрального банку та Світового банку. Питання кібербезпеки цифрового банкінгу розглядають Азура Й. Т. Й.,

Азад М. А., Ахмед Й., а також Алікхдур Т., АльВаді Б. М., Альравад М. та інші. Довіру та FinTech досліджують Девлін Дж. Ф., Рой С. К., Сехон Х., Моїн С. М. А., Сахінер М.

Вітчизняна наукова школа охоплює кілька напрямів. Теоретико-методологічні засади функціонування фінансових посередників та їх ролі у розвитку фінансового ринку досліджували О. Вовчак, І. Школьник, М. Дубина, М. Швець. Сутність FinTech та особливості його функціонування в умовах цифровізації висвітлено в роботах М. Дубини, С. Шкарлета, О. Жука, Ю. Вергелюк та ін. Ризики та перспективи цифровізації фінансових установ, зокрема використання штучного інтелекту, хмарних технологій та блокчейну, розглянуто в публікаціях О. Шишкіної, О. Шевченко, Л. Рудич, Р. Щура, О. Парубець, А. Тарасенка, М. Федішин, Н. Приказюк та ін.

Динаміку розвитку фінтех-компаній в Україні аналізують О. Тоцька, В. Шевчук, Ю. Вергелюк, М. Ганцяк, Д. Фомов. Трансформацію платіжних систем та кредитного менеджменту досліджують І. Ситник, В. Фоміна, О. Лобко, М. Дубина, О. Заєць. Питання цифрової інфраструктури, кастомізації кредитних послуг та стратегічного розвитку кредитних установ висвітлено в працях І. Садчикової, А. Волок, Н. Іванової, О. Попело, М. Дубини, Ю. Федоріва, Н. Версаль, Н. Приказюк, М. Балицької, В. Ерастова. Регулювання банківської діяльності в кризових умовах та забезпечення фінансової стійкості розглядають Н. Приказюк, А. Мирончук, І. Поліщук та ін.

Дослідження цих авторів створили теоретичне підґрунтя для розуміння процесів цифровізації. Водночас поза увагою залишилася низка аспектів. По-перше, недостатньо розробленими є питання системного оцінювання цифрової зрілості фінансових посередників, що ускладнює порівняльний аналіз та прийняття управлінських рішень. По-друге, потребують дослідження механізми інтеграції вимог кіберстійкості (зокрема, європейського регламенту DORA) в стратегічне планування діяльності фінансових установ. По-третє, малодослідженими є адаптивні моделі взаємодії між банками, небанківськими установами та фінтех-компаніями в умовах воєнних викликів та повоєнного

відновлення. По-четверте, поза межами системного аналізу залишається трансформація ринку кредитних послуг, зокрема процеси кастомізації кредитних продуктів та розвиток альтернативних форм кредитування.

Окреслене коло проблем обумовлює вибір теми дисертаційної роботи, її мету, завдання та логіку дослідження.

Зв'язок роботи з науковими програмами, планами та темами.

Дисертаційну роботу виконано відповідно до планів науково-дослідних робіт Національного університету «Чернігівська політехніка» в межах таких тем: «Розвиток фінансової системи в умовах турбулентності та становлення цифрової економіки» (номер державної реєстрації 0125U000298), де автором обґрунтовано концептуальні засади цифрової трансформації фінансових посередників; «Стратегічні детермінанти розвитку ринку фінансових послуг в умовах цифровізації національної економіки» (номер державної реєстрації 0123U104317), у межах якої здобувачем розроблено методичний підхід до оцінювання цифрової зрілості фінансових установ; «Розробка механізму фінансування інноваційного відновлення стратегічно важливих секторів економіки у післявоєнний період» (номер державної реєстрації 0123U104318), де автором визначено імперативи кіберстійкості та операційної надійності фінансових посередників.

Мета та завдання дослідження. Метою дисертаційної роботи є поглиблення теоретико-методичних засад та розробка практичних механізмів формування й реалізації стратегії розвитку фінансових посередників в умовах цифровізації економіки.

Для досягнення поставленої мети в роботі вирішено такі завдання:

- розкрити сутність та змістовні ознаки трансформації ролі фінансових посередників у цифровій економіці;
- визначити ключові механізми впливу фінансових посередників на розвиток цифрових фінансових сервісів;
- запропонувати класифікацію фінансових посередників з урахуванням рівня цифровізації та технологічної основи діяльності;

- дослідити вплив цифрових технологій та фінансових інновацій на архітектоніку стратегічного управління розвитком фінансових посередників;
- обґрунтувати методологічний інструментарій оцінювання цифрової зрілості фінансових посередників;
- провести інтегральне оцінювання рівня цифрової зрілості фінансових посередників України (на прикладі системно важливих банків);
- розробити практичні механізми імплементації міжнародного досвіду цифрової трансформації в умовах повоєнного відновлення;
- запропонувати організаційно-економічний механізм інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку;
- сформулювати науково-практичні рекомендації щодо реалізації стратегії кіберстійкості та оцінювання ефективності впровадження цифрових рішень.

Об'єктом дослідження є процес стратегічного розвитку фінансових посередників в умовах цифровізації економіки.

Предметом дослідження виступає сукупність теоретичних, методичних та прикладних положень щодо формування й реалізації стратегії розвитку фінансових посередників у цифровому середовищі.

Методи дослідження. У роботі застосовано комплекс загальнонаукових та спеціальних методів дослідження. Метод контент-аналізу та систематизації використано для узагальнення наукових підходів до визначення сутності фінансових посередників, цифрової зрілості, кіберзагроз, фінансової стабільності. Системний підхід застосовано для дослідження інноваційної інфраструктури цифрового фінансового ринку як цілісного утворення. Методи абстрагування та узагальнення – для характеристики особливостей функціонування фінансових посередників в умовах фінансової нестабільності та воєнних викликів. Статистичні методи аналізу, зокрема порівняльний аналіз та індексний метод – для оцінювання сучасного стану ринку цифрових фінансових послуг в Україні. Методи економетричного моделювання – для

обґрунтування впливу макроекономічних чинників на діяльність кредитних установ. Методи аналізу та синтезу – при конкретизації перешкод розвитку ринку кредитних послуг та обґрунтуванні заходів їх подолання. Графоаналітичний і табличний методи використано для наочного представлення результатів.

Інформаційну базу дослідження становлять законодавчі та нормативно-правові акти України, звітні дані Національного банку України, Державної служби статистики України, аналітичні матеріали міжнародних організацій (OECD, BIS, IMF, World Bank), наукові праці вітчизняних та зарубіжних дослідників, дані офіційних веб-сайтів фінансових установ та міжнародних рейтингових агенцій.

Наукова новизна одержаних результатів полягає в поглибленні теоретико-методичних засад та розробці науково-практичних рекомендацій щодо формування й реалізації стратегії розвитку фінансових посередників в умовах цифровізації економіки. Найбільш суттєві результати, що визначають наукову новизну роботи, є такими:

вперше:

– запропоновано модель оцінювання цифрової зрілості фінансових посередників (Digital Capability Maturity Index, DCMI), яка інтегрує шість ключових вимірів: технологічну інфраструктуру, процесну зрілість, клієнтську цифрову взаємодію, інноваційну спроможність, кіберстійкість та регуляторно-інституційну відповідність; на відміну від існуючих підходів, розроблена модель враховує галузеву специфіку фінансових посередників та умови функціонування в періоди макроекономічної нестабільності, що є критичним для України;

удосконалено:

– класифікацію фінансових посередників, яку розширено за рахунок таких критеріїв, як ступінь цифровізації, технологічна основа (API, AI, блокчейн), функціональне призначення та рівень регуляторної інтеграції; така деталізація дозволяє не лише ідентифікувати окремі групи установ у межах єдиної цифрової екосистеми, а й оцінювати їхню здатність до взаємодії;

— систематизацію механізмів впливу фінансових посередників на розвиток цифрових фінансових сервісів, що реалізовано через виділення шести взаємодоповнюючих механізмів: інституційного, технологічного, платформного, регуляторно-інноваційного, освітньо-комунікаційного та інвестиційно-фінансового; така структуризація дозволяє врахувати багатовимірний характер впливу, що важливо для розробки комплексних стратегій розвитку;

— наукові положення щодо трансформації функцій фінансових посередників в умовах цифровізації, зокрема функцій управління ризиками, формування довіри, інфраструктурної, інноваційної, фінансової інклюзії та стратегічного розвитку; визначення напрямів та механізмів їх взаємозв'язку в цифровому середовищі дає змогу подолати фрагментарність досліджень, яка була властива попереднім працям, та сформувати цілісне уявлення про діяльність посередників в умовах цифрової трансформації;

набули подальшого розвитку:

— понятійно-категоріальний апарат дослідження через уточнення сутності дефініцій «цифрова зрілість фінансових посередників», «цифрова трансформація фінансового посередництва», «фінансові інновації в цифровій економіці», «операційна стійкість фінансових установ». Уточнення цих понять створює концептуальну основу для подальших емпіричних досліджень та уніфікації наукового дискурсу;

— теоретичні положення щодо архітектоніки стратегічного управління розвитком фінансових посередників під впливом цифрових технологій, які доповнено імперативами платформізації, екосистемності, алгоритмічної довіри та кіберстійкості. Це дозволяє врахувати сучасні реалії, де конкурентоспроможність установи дедалі більше залежить не від її розміру, а від здатності інтегруватися в цифрові екосистеми;

— науково-практичні рекомендації щодо імплементації міжнародного досвіду цифрової трансформації (адаптація регламенту DORA, стандартів відкритого банкінгу PSD2, рамки eIDAS 2.0) в умовах повоєнного відновлення

України; на відміну від існуючих узагальнених порад, запропонований підхід передбачає пропорційність вимог до різних груп фінансових посередників (системно важливі банки, кредитні спілки, страхові компанії) та поетапне впровадження, що враховує обмеженість ресурсів та необхідність забезпечення безперервності базових фінансових послуг у воєнний та постконфліктний періоди.

Практичне значення отриманих результатів полягає в тому, що основні положення дисертації доведено до рівня методичних розробок та практичних рекомендацій. Результати дослідження можуть бути використані Національним банком України при вдосконаленні вимог до управління ІКТ-ризиками та кіберстійкості фінансових установ, Міністерством цифрової трансформації України при розробці стратегії розвитку цифрових фінансових сервісів, фінансовими установами при формуванні власних стратегій цифрової трансформації та кіберстійкості.

Окремі результати дисертаційної роботи впроваджено в діяльність: Публічного АТ «Райффайзен Банк» – пропозиції щодо запровадженні інформаційних кампаній для клієнтів щодо безпечного користування цифровими кредитними продуктами; підвищення обізнаності клієнтів щодо ризиків шахрайства при дистанційному отриманні кредитів; методики оцінювання цифрової зрілості фінансових посередників (довідка №5 від 01.05.2026); страхової компанії «ПЗУ Україна» при вдосконаленні підходів до цифровізації страхових послуг та управління операційною стійкістю (довідка № 152 від 13.05.2026 р.); Національного університету «Чернігівська політехніка» – у навчальний процес при викладанні дисциплін «Банківські операції», «Страховий менеджмент», «Банкострахування» (довідка №202/08-838 від 12.05.2026 р.).

Особистий внесок здобувача. Дисертація є самостійним науковим дослідженням. Усі наукові результати, висновки та рекомендації, що виносяться на захист, отримано автором особисто. Внесок автора в працях, опублікованих у співавторстві, конкретизовано в списку публікацій.

Апробація результатів дослідження. Основні положення та результати дисертації доповідалися й обговорювалися на міжнародних та всеукраїнських науково-практичних конференціях, зокрема: XIII Міжнародній науково-практичній конференції «Юність науки – 2023» (м. Чернігів, 26-27 квітня 2023 р.), Міжнародній науково-практичній конференції «Економіко-правові та управлінсько-технологічні виміри сьогодення: молодіжний погляд» (м. Дніпро, 03 листопада 2023 р.), Форумі стейкхолдерів розвитку соціального підприємництва (м. Чернігів, 16 вересня 2024 р.), XV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених «Юність науки – 2025» (м. Чернігів, 23-25 квітня 2025 р.), IV Міжнародній науково-практичній конференції (Запоріжжя-Мелітополь, 20 травня 2025 р.).

Публікації. Основні результати дисертаційної роботи опубліковано у 11 наукових працях, з них: 1 стаття в іноземному науковому виданні, що індексується в наукометричній базі Scopus; 4 статті у наукових фахових виданнях України, включених до міжнародних наукометричних баз; 6 робіт апробаційного характеру (тези доповідей). Загальний обсяг публікацій становить 9,8 друк. арк., з яких особисто автору належить 4,45 друк. арк.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 290 сторінок, з яких основний текст – 240 сторінок. Робота містить 37 таблиць, 29 рисунків. Список використаних джерел налічує 236 найменувань.

Розділ 1

ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ СТРАТЕГІЇ РОЗВИТКУ ФІНАНСОВИХ ПОСЕРЕДНИКІВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

1.1. Еволюція ролі та функцій фінансових посередників у цифровій економіці: стратегічні орієнтири трансформації

У контексті глобальної цифровізації фінансовий сектор України зазнає суттєвих трансформацій. Інтенсивний розвиток цифрових технологій сприяє виникненню нових фінансових продуктів, послуг і бізнес-моделей, що, своєю чергою, зумовлює необхідність формування адекватної інноваційної інфраструктури. Ключову роль у цьому процесі відіграють фінансові посередники – банки, небанківські фінансові установи, фінтех-компанії та інші інститути, які виступають каталізаторами впровадження інновацій, забезпечують доступ до капіталу для інноваційних проєктів і сприяють підвищенню рівня фінансової грамотності населення.

Особливої актуальності це питання набуває в умовах повномасштабної збройної агресії та в контексті повоєнної відбудови. У цих екстремальних умовах цифрові фінансові інструменти продемонстрували стійкість, забезпечивши безперебійність платежів і фінансових операцій. Отже, подальший розвиток зазначеної інфраструктури є критично важливим для залучення інвестицій, прозорого розподілу коштів, спрямованих на відновлення, а також для інтеграції українського фінансового ринку до єдиного цифрового простору Європейського Союзу.

Актуальність дослідження посилюється в контексті визначення перспектив післявоєнного відновлення економіки України, де цифровізація фінансових послуг може стати одним із драйверів економічного зростання. З огляду на це, дослідження ролі та місця фінансових посередників у формуванні інноваційної інфраструктури, комплексний аналіз їхніх функцій,

моделей взаємодії та визначенні бар'єрів, що стримують формування ефективної інноваційної інфраструктури, набуває особливої актуальності і є критично важливим для розробки ефективної державної політики, спрямованої на стимулювання інноваційного розвитку ринку цифрових фінансових послуг.

Аналіз наукових публікацій останніх десятиліть свідчить про значний інтерес вітчизняних та закордонних учених до проблеми розвитку ринку цифрових фінансових послуг. Систематизація результатів опублікованих наукових доробок вітчизняних та іноземних дослідників дозволяє виокремити декілька ключових напрямів досліджень у зазначеній сфері.

Іноземні науковці приділяють значну увагу феномену FinTech. Значний спектр їхніх інтересів лежить у полі зору дослідження його впливу на традиційну фінансову систему; вони розглядають проблематику формування фінтех-екосистем, вивчають роль венчурного капіталу і досліджують нові форми фінансування.

У контексті виявлених напрямів вважаємо доцільним відзначити наукові доробки П. Гомбера, Я. А. Коха та М. Зірінга, які, на наш погляд, є фундаментальними для розуміння того, як цифровізація змінює бізнес-моделі банків. Автори аналізують процеси анбандлінгу (розпакування) та ребандлінгу (перезбирання) фінансових послуг [81]. А запропонована ними ідея відкритого банкінгу, яка передбачає надання доступу третім сторонам до банківських даних через програмні інтерфейси (API), розглядається як ключовий механізм взаємодії банків та фінтех-компаній. У межах зазначених наукових напрямів варто відзначити здобутки Д. В. Арнера, Дж. Н. Барберіса та Р. П. Баклі. Досліджуючи еволюцію FinTech і пов'язані з ним регуляторні виклики, вони наголосили на необхідності створення регуляторами «пісочниць» для безпечного тестування інновацій [14; 15].

Ще один напрям досліджень — аналіз факторів, що сприяють розвитку національних фінтех-екосистем. І. Лі та Й. Дж. Шін розглядають компоненти такої екосистеми й детально описують роль уряду, фінансових інститутів,

технологічних стартапів, венчурного капіталу та споживачів [97]. Вони доводять: успіх екосистеми залежить переважно від зв'язків між її елементами, а не від самих елементів. Дослідження І. Лі (у співавторстві) зосереджені на досвіді провідних фінтех-хабів — Лондона, Сінгапуру, Кремнієвої долини. Це, на нашу думку, дає змогу обрати кращі практики для інших країн, зокрема для України.

Ролі венчурних інвесторів та краудфандингових платформ як ключових посередників у фінансуванні ранніх інновацій присвячено роботу Т. Залан та Е. Туфайлі «The promise of fintech in emerging markets: Not so disruptive?» [144]. Автори показують, що нові посередники є гнучкішими й більш схильними до ризику, ніж традиційні банки. Завдяки цьому вони стають каталізаторами проривних технологій у фінансовому секторі.

Іноземні дослідження надають міцну теоретичну та методологічну базу для аналізу ролі посередників і пропонуючи моделі екосистем та деталізований аналіз глобальних трендів. Водночас вони рідко враховують специфіку країн, які розвиваються і особливо тих, які перебувають в умовах військових конфліктів, що ускладнює можливість адаптації світового досвіду у практиці вітчизняних фінансових посередників.

Українські науковці активно вивчають проблему цифрових фінансів, однак здебільшого зосереджуються на окремих її аспектах. Зокрема, на ролі фінансових посередників у розвитку фінансового ринку, розвитку цифрового банкінгу та платіжних систем, перспективах фінтех-ринку України, а також на фінансовій інклюзії та цифровізації. Наприклад, Вовчак О. визначає типи фінансових посередників [153], Школьник І. О. досліджує їхню роль у перерозподілі ресурсів та стимулюванні інвестицій на фінансовому ринку України [234].

Проблема сутнісного визначення FinTech, а також особливостей функціонування цього явища в сучасних умовах активного становлення інформаційного суспільства висвітлюється в роботах М. В. Дубини, С. М. Шкарлета, О. С. Жука [233]. Крім того, М. В. Дубиною проаналізовано світовий і вітчизняний досвід еволюції електронного банкінгу [160].

Дослідження динаміки розвитку фінтех-компаній в Україні, а також їхньої ролі у впровадженні інноваційних рішень і цифрових сервісів здійснюють О. Тоцька та В. Шевчук [132]. Дещо відмінний дослідницький підхід простежується в публікації О. М. Шевченко та Л. В. Рудич. Зазначені автори розглядають фінансові технології через призму цифровізації національної економіки, акцентуючи увагу на змістовій природі фінтеху, його сильних і слабких сторонах, пов'язаних із ним ризиках, а також на поточному стані вітчизняного ринку [217].

Ключова роль фінансових посередників у створенні інноваційно-сприятливого середовища для надання цифрових фінансових послуг обґрунтовується в працях О. В. Шишкіної [220; 221; 229]. Водночас авторка наголошує на необхідності адаптації регуляторних механізмів для підтримки розвитку фінтеху в Україні. Своєю чергою, І. П. Ситник та В. С. Фоміна зосереджують науковий інтерес на аналізі сучасних тенденцій та оцінюванні ефективності застосування фінансових технологій у платіжних системах, а також на вивченні специфіки українського сегмента FinTech [204].

У сучасних умовах цифрової трансформації економіки сутність фінансових посередників зазнає глибоких концептуальних та функціональних змін. Традиційно фінансові посередники визначаються як інституції, що забезпечують акумуляцію тимчасово вільних коштів, їх трансформацію та перерозподіл у формі кредитів, інвестицій та інших фінансових інструментів. Це «інститути, що акумулюють тимчасово вільні кошти одних економічних агентів і надають їх іншим у формі кредитів, інвестицій чи інших фінансових інструментів» [174]. Вони виконують ключові функції: трансформацію строків, обсягів та ризиків; зниження інформаційної асиметрії; забезпечення платіжного обігу; підтримання фінансової стабільності.

Однак цифровізація економічних процесів зумовлює переосмислення класичного розуміння фінансового посередництва. Цифрові технології змінюють не лише форми, а й сутнісні характеристики фінансового посередництва, оскільки «способи реалізації ключових функцій посередників суттєво трансформуються під впливом FinTech, Big Data, автоматизації та блокчейн-технологій» [226].

У цифровій економіці фінансові посередники стають не лише каналами перерозподілу ресурсів, а й платформами інновацій, що забезпечують доступ до фінансових послуг через цифрові канали, автоматизовані сервіси, штучний інтелект, блокчейн тощо.

Проведені теоретико-прикладні дослідження функціонування і розвитку фінансових посередників в умовах цифровізації, дозволяють стверджувати, що цифрова трансформація змінює традиційну архітектуру фінансового посередництва, перетворюючи його на багатофункціональну, технологічно орієнтовану систему, що проявляється в таких напрямках:

- *бізнес-моделі* зазнають зсуву від класичних (депозитно-кредитних) до платформних, у межах яких фінансові посередники виступають не лише провайдерами послуг, а й координаторами екосистем (наприклад, банківсько-фінтехові альянси або необанки без фізичних відділень);

- змінюються *канали взаємодії з клієнтами*, у тому числі замість традиційного офлайн-спілкування з'являються мобільні застосунки, чатботи, вебплатформи, які забезпечують персоналізований досвід, цілодобовий доступ та знижують операційні витрати;

- набуває цифрової форми *продуктова лінійка*: поширюються онлайн-кредити, цифрові гаманці, смартконтракти, які автоматизують фінансові операції та створюють умови для появи нових типів послуг (наприклад, мікроінвестування).

- адаптується *регуляторне поле*, у тому числі з'являються RegTech-рішення, які допомагають посередникам дотримуватися нормативів у режимі реального часу, впроваджується супервізія на основі даних і т. ін. [174].

Таким чином, цифрова трансформація не просто змінює інструменти – вона перебудовує роль фінансових посередників, вимагаючи нових підходів до їх ідентифікації та класифікації [174]. У цифровій економіці посередники виступають не лише інституціями, що оперують фінансовими ресурсами, а і платформами, технологічними інфраструктурами, постачальниками цифрових сервісів, учасниками дата-центричних (data-centric) процесів, агентами інноваційних екосистем.

Саме з метою систематизації нових форм фінансового посередництва пропонується класифікація фінансових посередників, що враховує не лише інституційну природу, а й рівень цифровізації, функціональну спеціалізацію, технологічну базу, регуляторний статус та географічний масштаб їхньої діяльності (табл. 1.1) [174].

Таблиця 1.1

Класифікація фінансових посередників у контексті цифровізації

Критерій	Класифікаційні групи	Приклади	Характеристика
1	2	3	4
1. За інституційною природою	Банківські	ПриватБанк, Ощадбанк	Ліцензовані установи, що здійснюють депозитно-кредитні операції, регулюються НБУ, мають доступ до міжбанківських розрахунків
	Небанківські	Кредитні спілки, страхові компанії, фінансові компанії	Не мають банківської ліцензії, але можуть надавати окремі фінансові послуги (страхування, мікрокредитування, факторинг тощо)
2. За ступенем цифровізації	Традиційні	Райффайзен Банк	Основна діяльність офлайн, обмежене використання цифрових каналів
	Гібридні	monobank (через партнерство з банком)	Поєднують фізичну присутність із цифровими сервісами
	Цифрові	Revolut, izibank	Повністю онлайн, мобільні додатки, автоматизовані сервіси, відсутність фізичних відділень
3. За функціональним призначенням	Кредитні	Upstart, кредитні спілки	Надають позики фізичним та юридичним особам, оцінюють ризики, формують кредитні портфелі
	Інвестиційні	Robinhood, інвестфонди	Акумулюють кошти інвесторів, розміщують у цінні папери, управляють активами
	Платіжні	Payoneer, Wise	Забезпечують перекази коштів, обмін валют, електронні гаманці
	Страхові	Lemonade	Пропонують страхові продукти, використовують AI для оцінки ризиків
	Інформаційно-аналітичні	Bloomberg, Refinitiv	Надають фінансову аналітику, ринкові дані, API для трейдингу
4. За технологічною основою	API-платформи	Plaid	Забезпечують інтеграцію між банками та фінтехами через відкриті інтерфейси
	AI-посередники	Upstart, Theoriq AI	Використовують штучний інтелект для оцінки ризиків, персоналізації послуг

Закінчення таблиці 1.1

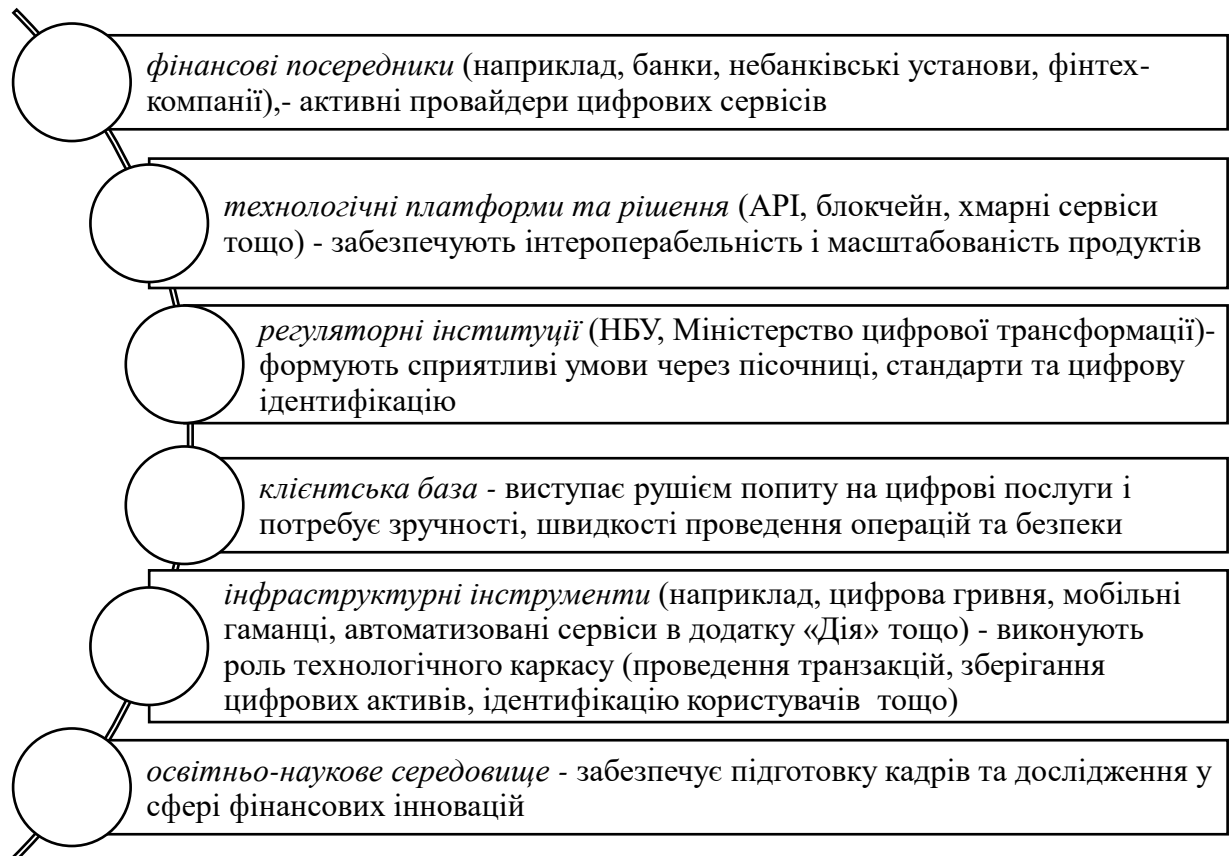
1	2	3	4
	Blockchain-посередники	Aave, Compound	Децентралізовані фінансові сервіси (DeFi), смартконтракти, прозорість транзакцій
5. За рівнем регуляторної інтеграції	Ліцензовані	Банки, страхові компанії	Підлягають нагляду НБУ, мають дозвіл на надання фінансових послуг
	Регуляторні пісочниці	Fintech Sandbox (НБУ)	Тестують інноваційні продукти в контрольованому середовищі
	Нерегульовані	DeFi-платформи	Працюють без централізованого регулятора, високий ризик, але і гнучкість
6. За географічним охопленням	Локальні	izibank, Sportbank	Орієнтовані на внутрішній ринок, адаптовані до національного законодавства
	Глобальні	PayPal, Revolut	Працюють у багатьох країнах, мають мультивалютну підтримку, дотримуються міжнародних стандартів

Джерело: розроблено на основі [14-16; 97; 152; 176; 190; 233; 234] й опубліковано автором у [226].

Запропонована класифікація дозволяє не лише описувати окремі групи посередників (наприклад, банки, небанківські фінансові установи, фінтех-компанії, платформи P2P-кредитування, криптовалютні біржі тощо), а й оцінювати ступінь їхньої цифрової зрілості, інтеграції в цифрову інфраструктуру та здатність до участі у формуванні цифрових фінансових екосистем, у тому числі завдяки розвитку API, AI та блокчейн-рішень.

Така систематизація дозволяє не тільки детально проаналізувати сучасний стан інноваційної інфраструктури ринку цифрових фінансових послуг в Україні, а й оцінити готовність фінансових посередників до реалізації інноваційного потенціалу вітчизняної фінансової системи.

Інноваційна інфраструктура цифрового фінансового ринку України складається із сукупності взаємопов'язаних елементів, основними з яких є: фінансові посередники, технологічні платформи та рішення, регуляторні інституції, клієнтська база, інфраструктурні інструменти, а також освітньо-наукове середовище (рис. 1.1).



**Рис. 1.1 – Елементи інноваційної інфраструктури
цифрового фінансового ринку**

Джерело: розроблено й опубліковано автором у [226].

Взаємодія компонентів, представлених на рис. 1.1, сприяє формуванню нового середовища, яке набуває здатності адаптуватися до трансформаційних зрушень, що виникають у процесі цифровізації діяльності фінансових посередників. В українському контексті описана динаміка суттєво прискорилося. Ключовими чинниками, які зумовили зазначену тенденцію, стали пандемія COVID-19 та воєнні дії. Пандемічний період стимулював банківські установи та фінтех-компанії до інтенсивної розбудови дистанційних каналів обслуговування. Водночас воєнний стан об'єктивно актуалізував необхідність забезпечення віддаленого доступу споживачів до фінансових сервісів у цифровій формі.

Інноваційна інфраструктура України останніми роками формується завдяки поєднанню зусиль держави, бізнесу та міжнародних донорів. У Каталозі фінтех-компаній України станом на 2025 налічується близько 260

активних фінтех-гравців, які впроваджують мобільні застосунки, блокчейн-технології та AI-рішення [209]. До того ж, за даними аналітичного дослідження Української асоціації фінтех та інноваційних компаній, 94 % фінтех-компаній назвали штучний інтелект перспективною технологією, а використання блокчейну зросло упродовж 2023-2024 років з 4 до 12 % [208]. Без перебільшення, ключовим елементом цифрової взаємодії держави і громадян є платформа «Дія». Вона інтегрує фінансові послуги, наприклад, такі як податкові сервіси і забезпечує банківські верифікації [180].

Окремо варто відзначити особливості інноваційної інфраструктури, які були сформовані за підтримки національного регулятора. Це впровадження Національним банком України у квітні 2023 року регулятивної платформи – «пісочниці» для тестування інноваційних продуктів та розробка концепції цифрової валюти – е-гривні [183; 184; 186; 216]. Не менш важливою новацією також стало впровадження нових законодавчих ініціатив щодо персональних даних [177].

Процес формування та розвитку інноваційної інфраструктури супроводжується сукупністю об'єктивних викликів та проблемних аспектів. Серед ключових перешкод виокремлюється регуляторна невизначеність, яка виявляється у відсутності усталених норм і правил щодо обігу нових цифрових продуктів, що, своєю чергою, ускладнює їхнє масштабування. Іншим суттєвим обмеженням виступає дефіцит фінансових ресурсів, необхідних для проведення досліджень, розробки та подальшого впровадження новацій. Окрім того, спостерігається недостатня забезпеченість кваліфікованими кадрами у сфері фінансових технологій та кібербезпеки. Зазначений кадровий дисбаланс набуває особливої вагомості в умовах зростання кількості кібератак на цифрові платформи та загального посилення загроз кібербезпеці [52; 211].

Розуміння особливостей структури та функціональних параметрів сучасних фінансових посередників у цифровому середовищі дозволяє глибше оцінити не лише їхню типологію, а й способи взаємодії з ринком. Однак класифікація - це лише основа для подальшого аналізу. Наступним логічним кроком є визначення ключових механізмів, за допомогою яких фінансові посередники впливають на розвиток цифрових фінансових сервісів (табл. 1.2).

Таблиця 1.2

Основні механізми впливу фінансових посередників на цифрові фінансові сервіси

Механізм	Сутність	Характерні особливості	Переваги	Недоліки і обмеження використання	Приклади застосування
1	2	3	4	5	6
Інституційний механізм	участь фінансових посередників у формуванні цифрової фінансової екосистеми через створення нових організаційних структур (фінтех-компанії, цифрові банки, платіжні системи).	швидкість виходу на ринок	сприяння оперативності транзакцій; зменшення витрат	регуляторні обмеження для новачків	запуск цифрових банків (monobank, izibank), які діють на базі партнерства з традиційними банками.
Технологічний механізм	впровадження інноваційних технологій (API, блокчейн, AI, Big Data) у фінансові продукти та сервіси	адаптація технологій до фінпослуг	зручність використання; утримання клієнтів	Високий технічний бар'єр входження на ринок	використання штучного інтелекту для скорингу позичальників або блокчейн для смартконтрактів у страхуванні.
Платформний механізм	створення цифрових платформ, які об'єднують різні фінансові сервіси у єдиному середовищі (банкінг, страхування, інвестиції).	Інтеграція цифрових сервісів у єдине цифрове середовище; можливість дії через цифрові застосунки та підключення сторонніх сервісів	Гнучкість і масштабованість; інноваційний потенціал; підвищена конкурентоспроможність	Висока вартість розробки та технічної підтримки; ризики кібербезпеки й витоку даних	інтеграція фінансових сервісів у мобільні додатки (наприклад, monobank або «Дія»).
Регуляторно-інноваційний механізм	участь у формуванні регуляторного середовища через пілотні проєкти, «пісочниці», стандарти відкритого банкінгу.	Пілотування продуктів у контрольованих умовах	Зниження регуляторних бар'єрів; безпека	Складність реалізації	участь банків у Fintech Sandbox від НБУ для тестування нових цифрових продуктів.

Закінчення таблиці 1.2

1	2	3	4	5	6
Освітньо-комунікаційний механізм	підвищення фінансової та цифрової грамотності клієнтів, просування нових сервісів через цифрові канали.	Високий потенціал для реалізації	Нові джерела фінансування, швидка масштабованість	Повільне залучення капіталу на початкових стадіях	запуск освітніх платформ банками (наприклад, «ПриватБанк.Університет») або чат-ботів для консультацій.
Інвестиційно-фінансовий механізм	фінансування стартапів, інвестування у цифрову інфраструктуру, венчурні проекти.	фокус на фінансування інновацій; можливість формування фондів спільного інвестування; участь у розбудові цифрової інфраструктури; інституційна роль у підтримці стартапів	мультиплікативний ефект розвитку через розширення капіталізації ринку; гнучкість моделей фінансування; інтеграційна здатність	обмеженість венчурного капіталу; високі ризики окупності; низький рівень інвестиційної культури та взаємної довіри; нерозвинутість регуляторних стимулів	участь банків у фінансуванні фінтех-компаній або створення власних венчурних підрозділів.

Джерело: розроблено автором на основі [180; 112; 215; 219] і опубліковано у [174].

Ці механізми формуються на перетині інституційних, технологічних, регуляторних та комунікаційних змін і дозволяють оцінити, яким чином посередники не лише адаптуються до цифрового середовища, а й активно трансформують фінансову інфраструктуру, створюючи нову якість взаємодії з клієнтами, державою та технологічними партнерами.

Таблиця 1.2 демонструє, що фінансові посередники впливають на розвиток цифрових фінансових сервісів через шість взаємодоповнюючих механізмів: інституційний, технологічний, платформний, регуляторно-інноваційний, освітньо-комунікаційний та інвестиційно-фінансовий. Кожен із них має власну функціональну спеціалізацію: від трансформації бізнес-моделей до поширення цифрової грамотності та підтримки інновацій.

Переваги механізмів полягають у масштабованості, гнучкості та швидкому впровадженні інновацій, проте їхню ефективність стримують такі обмеження, як недостатня регуляторна визначеність, обмежений доступ до ресурсів і потреба в розвитку цифрових компетенцій користувачів.

У системній взаємодії ці механізми формують синергетичний ефект, що підсилює інноваційний потенціал цифрового фінансового ринку та відкриває нові напрями для розвитку інфраструктури в Україні.

Проведений аналіз механізмів впливу фінансових посередників засвідчив, що їхня участь у цифровій трансформації ринку не обмежується лише впровадженням окремих технологічних рішень. Йдеться про комплексну трансформацію ролі посередників – від провайдерів фінансових ресурсів до інтеграторів інноваційної інфраструктури, учасників регуляторних експериментів, освітніх ініціатив та стратегічних партнерств із державними й технологічними структурами [174].

Однак глибше усвідомлення потенціалу й обмежень таких механізмів можливе лише в контексті порівняння з міжнародними практиками, де фінансові посередники вже стали каталізаторами змін. Тому доцільним з наукового погляду є огляд закордонного досвіду взаємодії фінансових

посередників з інноваційною інфраструктурою, що дозволить виявити ефективні моделі, механізми державної підтримки та підходи до побудови цифрових екосистем.

Для цього дослідження було опрацьовано іноземний досвід взаємодії фінансових посередників з інноваційною інфраструктурою, у тому числі практику США у сфері венчурного капіталу і фінансових платформ як драйверів інновацій, Великої Британії щодо створення регуляторних «пісочниць» і відкритого банкінгу, а також Сінгапуру в контексті державної підтримки й цифрового ліцензування. Крім того, вивчено особливості розвитку фінансових посередників Європейського Союзу через програми Horizon Europe, InvestEU та практики інтегрування у єдину цифрову інфраструктуру з урахуванням стандартів PSD2, eIDAS та Південної Кореї, де фінансові посередники є вагомим елементом національної інноваційної стратегії (табл. 1.3).

Таблиця 1.3

**Порівняння міжнародного досвіду взаємодії фінансових посередників
з інноваційною інфраструктурою**

Країна / Регіон	Форми участі фінансових посередників	Інструменти інноваційної інфраструктури	Особливості
США	Венчурні фонди, інвестбанки, краудфандинг	Акселератори, стартап- хаби, платформи AngelList	Сильний приватний капітал, гнучке регулювання
Велика Британія	Банки, платіжні провайдери	Regulatory Sandbox FCA, Open Banking, API	Активна роль регулятора, відкриті стандарти
Сінгапур	Банки, цифрові посередники з ліцензією MAS	APIX, FinLab, цифрові ліцензії	Держава – інвестор та координатор
ЄС	Банки, фонди, фінтехи	Horizon Europe, PSD2, eIDAS	Транснаціональна інтеграція інфраструктури
Південна Корея	Банки, інституційні інвестори	Національні інноваційні парки, держгарантії	Частина національної інноваційної стратегії держави

Джерело: розроблено автором на основі [74; 77; 143; 148; 214; 133] і опубліковано у [174].

Проведене дослідження іноземного досвіду дозволяє стверджувати:

- фінансові посередники у провідних країнах не лише адаптуються до цифрових змін, а й активно формують інноваційну інфраструктуру;
- ключовими інструментами є регуляторні «пісочниці», відкриті API, цифрові ліцензії, венчурне фінансування та державно-приватні партнерства;
- Україна може адаптувати ці практики, зокрема через розвиток «пісочниць», стимулювання відкритого банкінгу та підтримку фінтех-екосистеми [174].

Цифрова економіка, таким чином, не просто розширює функції фінансового посередника – вона змінює саму природу цього поняття. Якщо класична теорія зводила посередника до ролі трансформатора заощаджень в інвестиціях, то сьогодні він стає системним учасником цифрової фінансової екосистеми: формує інфраструктуру доступу до ресурсів, керує специфічними цифровими ризиками та виробляє нові механізми довіри між суб'єктами, які ніколи не можуть взаємодіяти офлайн. Власне, саме через ці функції – а не через організаційно-правову форму чи розмір балансу – і доцільно досліджувати місце фінансових посередників у новому середовищі.

Цифровізація економіки зумовлює глибоку трансформацію функцій фінансових посередників, змінюючи не лише технологічні форми їх реалізації, а і зміст, обсяг і стратегічну значущість цих функцій. У наших роботах неодноразово наголошується на думці, що цифрові технології змінюють способи виконання класичних функцій фінансових посередників, формуючи нові механізми створення фінансової цінності та нові канали взаємодії з клієнтами [174].

Розглянемо трансформацію ключових функцій фінансових посередників у цифровому середовищі, акцентуючи увагу на управлінні фінансовими ризиками, формуванні довіри, інноваційній та інфраструктурній функції, а також функції стратегічного розвитку.

У традиційній фінансовій системі *функція управління ризиками* полягає в диверсифікації, оцінці кредитоспроможності, моніторингу платоспроможності та застосуванні регуляторних норм. Однак цифрова економіка значно розширює спектр ризиків і додає нові виміри – технологічні, інформаційні, алгоритмічні.

Досліджуючи це питання в роботі «Актуальні типи кіберзагроз функціонування і розвитку фінансових установ» нами було детально класифіковано сучасні загрози й ризики, до основних з яких було віднесено такі, як:

- фішинг та соціальна інженерія;
- атаки на платіжні системи;
- втручання в роботу API та цифрових платформ;
- зловмисні DDoS-атаки;
- витоки персональних та фінансових даних;
- внутрішні цифрові загрози [224].

Вважаємо, що ці ризики здатні «повністю паралізувати діяльність фінансової установи та підірвати довіру клієнтів» [224].

З метою систематизації співвідношення між технологічними можливостями й ризиками нами виділено такі спільні переваги і недоліки інноваційних технологій, які фінансовим посередникам варто враховувати у процесі розробці та прийнятті стратегічних планів розвитку (таблиця 1.4).

Узагальнення переваг і недоліків представлених у таблиці 1.4 дозволяє стверджувати, що цифрові технології, водночас підвищуючи ефективність і швидкість операцій, створюють новий рівень стратегічної вразливості, який посередники мають враховувати при формуванні бізнес-моделей.

**Переваги і недоліки використання нових технологій
у формуванні стратегії розвитку фінансових посередників**

Переваги	Недоліки
Підвищення ефективності процесів	Висока вартість впровадження технології в практику діяльності фінансових посередників
Зменшення витрат на здійснення операцій	Необхідність оновлення інфраструктури та перепідготовки персоналу
Підвищення швидкості та точності обробки інформації	Потреба в забезпеченні безпеки та конфіденційності даних
Забезпечення доступності фінансових послуг для широкого кола користувачів	Ризик відмови від традиційних методів та несприйняття клієнтами нових технологій
Підвищення рівня конкурентоспроможності фінансових посередників на фінансовому, фондовому, валютному, страховому та інших ринку	Ризик технічних помилок та вразливості системи перед кібератаками
Можливість підвищення рівня персоналізації фінансових послуг	Неповний ефект охоплення щодо деяких груп населення (наприклад, покоління старшої вікової групи; осіб, які не є користувачами смартфонів і мобільних застосунків тощо)

Джерело: розроблено автором на основі [6; 60; 125; 130; 196; 221] і опубліковано у [225].

Щодо трансформації *функції формування довіри* зазначимо, що у класичному фінансовому посередництві довіра ґрунтується на регуляторному статусі, фінансовій стійкості, репутації та історії діяльності інституції. Однак цифрова економіка переносить основу довіри в іншу площину – на етичні, технологічні та поведінкові фактори.

У процесі філософського аналізу довіри як основи фінансового посередництва ми дійшли висновку, що цифрова довіра є «етико-технологічним ресурсом», який включає прозорість алгоритмів, коректність обробки даних, відповідальність за алгоритмічні рішення, цифрову ідентифікацію клієнтів, кіберстійкість [154]. Це, по суті, пояснює, чому довіра стає не просто функцією, а елементом цифрового соціального капіталу фінансових посередників.

Зі змінами зазначеної функції тісно взаємопов'язана *трансформація інфраструктурної функції*, яка, на нашу думку, зумовлюється здатністю фінансових посередників забезпечувати створення, підтримку та розвиток

фінансово-технологічних платформ, сервісів, технологічних модулів та механізмів, які є основою для здійснення фінансових операцій у цифровій економіці.

У авторській статті «Аналіз ролі фінансових посередників у процесі формування інноваційної інфраструктури...» обґрунтовано, що фінансові посередники стають ключовими вузловими елементами цифрової інфраструктури [174]. Це відбувається за рахунок того, що фінансові посередники підтримують інфраструктуру миттєвих платежів, реалізують технології відкритого банкінгу, інтегруються в регуляторні пісочниці НБУ, забезпечують цифрову ідентифікацію клієнтів, виступають провайдерами API-рішень, беруть участь у запуску цифрових валют центральних банків на рівні пілотних проєктів.

Зазначені положення системно узагальнені у вищенаведених таблицях 1.1–1.3, які, на нашу думку, є необхідними для висвітлення інституційної еволюції функцій фінансових посередників.

Трансформація інфраструктурною функції є основою для змін інноваційної, оскільки без цифрової інфраструктури неможливо розробляти й запускати нові фінансові продукти, впроваджувати цифрові сервіси, використовувати Великі дані, Штучний інтелект і Машинне навчання, а також створювати моделі відкритої взаємодії та масштабувати інновації.

Виходячи з вищенаведеного, *інноваційна функція фінансових посередників* також зазнає суттєвих змін в умовах цифровізації економіки. Проведені авторські дослідження, результати яких опубліковані у співавторстві в роботі «Роль цифрових технологій у формуванні стратегій розвитку фінансових посередників» доводять, що фінансові посередники виконують не лише трансформаційні, а й інноваційно-платформні функції [231].

У тому числі було виявлено, що цифровізація сприяє: появі цифрових платформ кредитування і страхування; алгоритмічному управлінню активами; розвитку поширених цифрових продуктів; формуванню цифрових каналів взаємодії з клієнтами; зростанню ролі Великих даних (Big Data), машинного навчання (ML) і клієнтської аналітики; впровадженню смартконтрактів.

Набула нового змісту в умовах цифрової економіки і *функція фінансової інклюзії*. Зокрема, якщо раніше доступ до фінансових послуг залежав від того, чи є поблизу відділення банку, наскільки широка його географічна мережа і чи відповідає клієнт певним соціально-економічним критеріям, то сьогодні на перший план виходять інші речі: мобільні технології, цифрова ідентифікація, низька вартість доступу, зручність користування, можливість налаштувати продукт під себе та безперервність сервісу. І контексті трансформації цієї функції зауважимо, що не йдеться про те, щоб «охопити» якомога більше людей. Йдеться про те, як залучити малий та середній бізнес до фінансування через онлайн-інструменти, цифрові системи аналізу грошових потоків та спрощену перевірку. Про те, як надати доступ до базових фінансових послуг вразливим групам – пенсіонерам, внутрішньо переміщеним особам, молоді, людям без стабільного доходу, причому без необхідності бути присутніми у фізичних установах фінансових посередників.

Це також передбачає розробку інноваційних продуктів соціального характеру – мікрокредитування, цифрових соціальних карток, мобільних ощадних програм. Водночас цифровізація забезпечила цілодобову доступність фінансових послуг незалежно від географічного розташування клієнта. Мобільні пристрої фактично замінили традиційні відділення банків, що призвело до фундаментальної трансформації самої концепції фінансової інклюзії. Отже, фінансова інклюзія перестала бути просто послугою таких фінансових посередників, як банки. Сьогодні вона стала питанням цифрової рівності та соціальної стабільності.

Процес цифровізації фінансового сектору спричинив фундаментальні зміни в реалізації *функції формування стратегій розвитку фінансових посередників*. Детермінантами цієї трансформації виступають кілька взаємопов'язаних чинників.

По-перше, прискорення технологічних циклів інновацій призвело до скорочення життєвого циклу фінансових продуктів і послуг, що унеможливило застосування традиційних моделей довгострокового планування з

фіксованими горизонтами. По-друге, масиви структурованих і неструктурованих даних перетворилися на критичний стратегічний актив, використання якого вимагає нових компетенцій та аналітичних можливостей. По-третє, трансформація поведінкових патернів споживачів фінансових послуг, їхні очікування щодо персоналізації, швидкості обслуговування та омніканальності взаємодії формують нові вимоги до стратегічного позиціонування. По-четверте, платформізація фінансового ринку та поява екосистемних бізнес-моделей змінюють конкурентне середовище та вимагають переосмислення меж і можливостей фінансового посередництва. По-п'яте, ескалація кіберризиків та посилення регуляторних вимог щодо захисту даних і операційної стійкості зумовлюють необхідність інтеграції ризик-менеджменту в стратегічне планування.

Унаслідок дії цих факторів функція формування стратегій зазнає комплексної трансформації, характеризуючись переходом від традиційної моделі довгострокового планування до динамічної, даних-орієнтованої та технологічно інтегрованої моделі стратегічного управління, що базується на принципах адаптивності, аналітичності та екосистемної взаємодії.

Названі функції не охоплюють увесь спектр діяльності фінансових посередників, проте вважаємо, що саме вони зазнали найбільш суттєвих змін в умовах цифровізації та є визначальними в контексті стратегічного розвитку. Однак не варто розглядати ці функції окремо оду від одної, оскільки це, на нашу думку, призводить до фрагментарного розуміння діяльності фінансових посередників та неповної оцінки наслідків управлінських рішень. Зокрема, якщо функції розглядаються автономно, то втрачається розуміння того, як зміни в одній сфері впливають на результативність інших. Наприклад, інвестиції в інфраструктурний розвиток без урахування їхнього впливу на інноваційний потенціал або рівень ризиків можуть не дати очікуваного ефекту або навіть спричинити негативні наслідки.

Системний підхід дозволяє виявити синергетичні ефекти та мультиплікатори розвитку. Взаємопідсилення функцій створює ефект, що перевищує суму індивідуальних внесків кожної функції. Так, поєднання розвиненої інфраструктури, активних інновацій та ефективного ризик-менеджменту створює якісно новий рівень конкурентоспроможності, недосяжний при фокусуванні лише на одному напрямку. Водночас розуміння взаємозв'язків дозволяє ідентифікувати вузькі місця та системні обмеження розвитку – часто саме слабка ланка у функціональному ланцюгу обмежує ефективність усієї системи.

Особливо важливим є розуміння циклічних та зворотних ефектів між функціями. Вони не лише впливають одна на одну лінійно, а й створюють петлі зворотного зв'язку. Наприклад, успішні інновації підсилюють довіру, що стимулює інвестиції в інфраструктуру, які знову створюють можливості для нових інновацій. Або навпаки, реалізований кіберризик руйнує довіру, що знижує попит на цифрові послуги, зменшує інвестиції та гальмує інноваційний розвиток. На нашу думку, ця взаємозалежність посилюється через технологічну інтеграцію та платформізацію, коли сучасні технології одночасно впливають на інфраструктуру, інновації, ризики та довіру.

Основу для обґрунтованого стратегічного планування та розподілу ресурсів забезпечує системне бачення функціонального взаємозв'язку. Розуміючи механізми взаємовпливу, керівництво компанією може визначати оптимальну послідовність інвестицій, пріоритетність проєктів та очікувані каскадні ефекти від конкретних ініціатив, уникаючи марнотратства ресурсів на розвиток функцій, результативність яких обмежена станом інших елементів системи.

Нарешті, системний аналіз критично важливий для оцінки соціально-економічних результатів діяльності фінансових посередників, і у тому числі фінансової інклюдії. Інклюзія є емерджентним результатом, що виникає не з окремої функції, а з ефективної взаємодії всієї системи функцій. Спроби досягти інклюдії без комплексного розвитку інфраструктури, інновацій, довіри

та ризик-менеджменту приречені на обмежений успіх. Це, у свою чергу, підтверджує необхідність системного підходу до аналізу функціонування фінансових посередників у цифровій економіці.

Вищенаведені аргументи дозволили нам узагальнити основні аспекти трансформації основних функції фінансових посередників та їх взаємозв'язку в таблиці 1.5.

Таблиця 1.5

**Взаємозв'язок і трансформація функцій фінансових посередників
в умовах цифровізації**

Функція фінансових посередників	Традиційна сутність	Трансформація в умовах цифровізації	Напрями та механізми взаємозв'язку з іншими функціями
1	2	3	4
1. Функція управління фінансовими ризиками	Контроль і моніторинг ризиків вручну; регулятивна звітність; реактивне управління	– Big Data–аналіз, машинне навчання для прогнозування ризиків; – програмні рішення (RegTech); автоматизоване AML/KYC; – кіберризик як частина ризик-апетиту	Інфраструктурна функція забезпечує регуляторні та технічні умови; інноваційна – формує нові інструменти ризик-менеджменту; стратегічна – визначає ризик-апетит для розвитку
2. Функція формування довіри	Довіра базувалася на фізичній присутності, репутації, нагляді держави	– Довіра, яка формується через кіберстійкість, прозорість алгоритмів, етичну обробку даних, якість цифрових сервісів; – цифрова ідентичність	Інфраструктурна функція дає технічну безпеку; інноваційна – створює нові продукти, які вимагають довіри; стратегічна – визначає політику прозорості та етичного управління даними
3. Інноваційна функція	Інновації впроваджувалися повільно, здебільшого продуктово	– Постійне створення цифрових продуктів: API-сервіси, токенизація, robo-advisory, AI-скоринг, smart contracts	Інфраструктура → передумова інновацій; управління ризиками → оцінка безпеки інновацій; стратегічний розвиток → визначає напрям інновацій
4. Інфраструктурна функція	Банківська мережа, внутрішні IT-системи, власні канали	– Платформи миттєвих платежів, відкрита архітектура (API), хмара, цифрова ідентифікація, RegTech, Open Banking	Інфраструктура забезпечує реалізацію всіх інших функцій; створює умови для інновацій, інклюзії, довіри, ризик-менеджменту

1	2	3	4
5. Функція фінансової інклюзії	Залежала від географії, доступності відділень, соціально-економічного статусу	<ul style="list-style-type: none"> – Цифровий доступ до фінансових послуг незалежно від місця проживання; – мобільні сервіси; – мікрокредити; – онлайн-ідентифікація; – кастомізовані продукти 	Інфраструктурна функція відкриває канали доступу; інноваційна – створює продукти для різних груп; стратегічна – визначає пріоритети інклюзії
6. Функція стратегічного розвитку	Планування розширення мережі; продуктова стратегія; операційна ефективність	<ul style="list-style-type: none"> – Стратегія переходить до цифрових платформ, екосистем, даних, партнерських моделей, інноваційних продуктів; – управління цифровими ризиками та довірою 	Стратегічна функція об'єднує інші функції: від інфраструктури – до інновацій; формує довгострокову модель розвитку

Джерело: розроблено автором на основі [57; 146; 152; 162; 167; 163; 170; 171; 192; 199; 213; 235].

Зважаючи на характеристики зазначених функцій, наведених у табл. 1.5, можна сформулювати такі особливості їх взаємопов'язаності.

Як було вище зазначено, діяльність фінансових посередників у цифровому середовищі характеризується складною системою взаємопов'язаних функцій, які не існують ізольовано одна від одної. Кожна функція впливає на інші, створюючи ефект взаємопідсилення або, навпаки, обмежуючи можливості розвитку всієї інституції. Це системна взаємодія має циклічний характер, що вимагає комплексного розуміння логіки функціонування фінансових посередників.

Інфраструктурна функція є фундаментом, на якому будується вся діяльність фінансових посередників у цифрову епоху. Вона охоплює технологічні, регуляторні та організаційні передумови роботи: системи цифрової ідентифікації клієнтів, інфраструктуру миттєвих платежів, можливості API-інтеграції для співпраці з партнерами в екосистемі, хмарні обчислювальні потужності та RegTech-інструменти для автоматизації дотримання регуляторних вимог.

Однак, технологічна досконалість сама по собі не гарантує ефективності. Не менш важливими є готовність персоналу працювати з новими інструментами, здатність організаційної культури адаптуватися до змін та вміння керівництва узгоджувати технологічні нововведення з реальними можливостями людей. Без розвиненої інфраструктури та компетентних співробітників неможливо впроваджувати інновації, досягати фінансової інклюзії чи забезпечувати прозорість управління ризиками.

Інноваційна діяльність фінансових посередників проявляється через створення нових продуктів і технологічних рішень: платформ автоматизованого інвестиційного консультування, токенизації активів, систем оцінки кредитоспроможності на основі штучного інтелекту, смартконтрактів на блокчейні. Ці інновації прямо залежать від рівня розвитку інфраструктури – емпіричні дослідження підтверджують пряму залежність між якістю інфраструктури та інноваційним потенціалом організації.

Однак технологічні можливості не є єдиним чинником успіху. Результативність інновацій значною мірою залежить від креативності фахівців, їхньої здатності виявляти реальні потреби клієнтів, готовності до експериментів і спроможності долати опір змінам. Протидія інноваціям може виникати як усередині організації (з боку колег), так і зовні – з боку клієнтів, прихильних до традиційних способів ведення справ.

Цифровізація фінансів суттєво трансформує структуру *ризиків*. Особливої актуальності набувають кіберризики, загрози витоку та неправомірного використання даних, а також модельні ризики, зумовлені помилками алгоритмів і упередженістю систем штучного інтелекту. Рівень інноваційної активності фінансового посередника безпосередньо визначає ефективність управління цими ризиками.

Водночас ключовим залишається людський фактор. Помилки співробітників, недостатня обізнаність щодо кіберзагроз, недбале дотримання протоколів безпеки або неетична поведінка здатні нівелювати ефективність навіть найнадійніших технологічних систем захисту. Таким чином, сучасне управління ризиками має поєднувати технологічні рішення з управлінням поведінковими аспектами безпеки.

Довіра об'єднує результати роботи інфраструктурної, інноваційної функцій та функції управління ризиками. Стейкхолдери довіряють фінансовому посереднику тоді, коли бачать безпечну інфраструктуру, передбачувані та надійні інновації, прозорі процеси прийняття рішень у ризикових ситуаціях.

У цифрових фінансах довіра формується не лише завдяки якісним технологіям, а й через людську взаємодію: професіоналізм консультантів, етичну поведінку менеджменту, відповідальність організації перед клієнтами та суспільством. Репутація, яку формували роками, може бути зруйнована миттєво через неетичні дії окремих працівників або сумнівні управлінські рішення.

Стратегічна функція координує роботу всієї системи. Саме на рівні стратегії визначаються пріоритети інноваційної активності, напрями інфраструктурних інвестицій, прийнятний рівень ризиків, способи побудови довіри та цільові сегменти клієнтів. Ця функція інтегрує та балансує всі інші елементи відповідно до стратегічних цілей організації.

Успіх стратегічного розвитку залежить від компетентності топменеджменту, його бачення майбутнього, здатності залучати талановитих фахівців і утримувати їх, формувати культуру інновацій та відповідальності в організації. Навіть бездоганна на папері стратегія залишиться лише декларацією, якщо немає команди, здатної її реалізувати.

Фінансова інклюзія є підсумковим соціально-економічним результатом ефективної взаємодії всіх функцій. Щоб фінансове посередництво стало справді інклюзивним, необхідне одночасне виконання низки умов: доступність цифрової інфраструктури для всіх, масштабованість інноваційних рішень, наявність довіри з боку споживачів, контрольованість ризиків та стратегічна орієнтація на залучення маргіналізованих груп населення, тобто тих, яких суспільство «відсунуло» на другий план і які мають обмежений доступ до економічних ресурсів, політичної влади, соціальних благ і культурного визнання.

Водночас фінансова інклюзія – це не лише питання технологій. Вона вимагає змін у свідомості працівників фінансових установ, подолання упереджень щодо певних соціальних груп, розвитку емпатії та розуміння специфічних потреб вразливих категорій клієнтів. Необхідна також готовність інвестувати у фінансову освіту населення, розуміючи, що це довгострокова інвестиція в розширення ринку та соціальну стабільність.

Розвиток фінансових посередників традиційно визначався стратегічними орієнтирами, що ґрунтувалися на забезпеченні стабільності, розширенні ринку, підвищенні ефективності операцій та формуванні конкурентних переваг у межах фінансової системи. У класичному підході стратегія розглядалася як довгостроковий план розвитку інституції, що враховує регуляторні обмеження, структуру ринку, рівень ризиків та необхідність підтримання фінансової стійкості.

У цифровій економіці концептуальні засади стратегічних орієнтирів зазнають сутнісного переосмислення, проте загальний зміст стратегічної функції зберігається: вона залишається інструментом формування траєкторії розвитку фінансового посередника, визначення його місії, цілей та довгострокових пріоритетів. Водночас цифровізація змінює характер стратегічного планування, роблячи його більш:

- адаптивним;
- інтенсивним у використанні даних;
- клієнтоцентричним;
- інноваційним на концептуальному рівні;
- системно інтегрованим із технологічними змінами.

У науковій літературі стратегічні орієнтири фінансових посередників у цифровій економіці описуються через низку базових категорій: клієнтська цінність, ефективність, довіра, корпоративна стійкість, підвищення якості управління ризиками, цифрова готовність, інноваційна здатність, інституційна гнучкість [26; 40; 107; 146; 152; 162; 167; 163; 165; 170; 171; 199; 213; 235;]. У теоретичному вимірі ці орієнтири формують цілісну рамку, у межах якої фінансові посередники визначають пріоритети розвитку в умовах швидких технологічних і ринкових змін.

Цифровізація поглиблює роль стратегічного бачення, оскільки цифрові процеси посилюють конкуренцію, знижують бар'єри входу на ринок та змінюють характер взаємодії фінансових посередників із клієнтами, регуляторами та партнерами. У цьому контексті стратегічні орієнтири охоплюють:

- формування клієнтської цінності на основі цифрових каналів;
- розвиток інноваційних моделей фінансової послуги як елемента загальної ринкової екосистеми;
- забезпечення прозорості діяльності та підвищення довіри;
- підвищення стійкості бізнес-моделі в умовах цифрових ризиків.

Таким чином, стратегічна функція зберігає фундаментальний характер, але її зміст у цифровій економіці набуває нових теоретичних акцентів: від домінування операційної ефективності – до домінування цінності, інноваційності та стійкого розвитку. Ці орієнтири стають основою для подальшого аналізу механізмів формування стратегій (підрозділ 1.2).

Сформульовані вище теоретичні стратегічні орієнтири свідчать, що фінансові посередники в умовах цифрової економіки функціонують у середовищі, де пріоритети розвитку визначаються не лише класичними економічними чинниками, а й глибинними технологічними зрушеннями. Останні не обмежуються впровадженням окремих технологічних рішень, а формують нову логіку функціонування фінансових інституцій.

Звідси впливає необхідність теоретичного осмислення цифрової трансформації як наукової категорії, визначення її ключових елементів та впливу на сучасну модель фінансового посередництва.

У науковій літературі цифрова трансформація фінансових посередників трактується як складний соціально-економічний та інституційний процес, що змінює сутність, функції та ринкову роль фінансового посередництва. У теоретичному плані цифровізація є не стільки технологічним явищем, скільки зміною парадигми функціонування фінансових інституцій.

Цифрова трансформація фінансових посередників становить собою багатовимірне явище, яке потребує аналізу крізь призму різних теоретичних підходів. Кожен із них розкриває окремі аспекти цього процесу, а їхній синтез дає змогу сформувати цілісне уявлення про сутність трансформаційних змін.

Інформаційно-технологічний підхід розглядає цифрову трансформацію як перехід до моделей, що працюють на основі даних. Акцент змінюється. Замість обробки паперів і транзакцій – робота з цифровими даними. Їх аналіз відбувається в реальному часі. Результати аналізу використовують для управлінських рішень. Дані більше не є побічним продуктом. Вони стають стратегічним активом, який визначає, чи має економічний суб'єкт конкурентні переваги.

У центрі уваги *інституціонального підходу* зміни в поведінці, ролях і взаємодії учасників ринку. Цифровізація ламає старі інституційні межі між фінансовими посередниками. З'являються нові форми взаємодії між тими, хто надає послуги, і тими, хто їх отримує. Регуляторні механізми теж змінюються. Виникають нові гравці – фінтех-компанії, великі технологічні корпорації. Вони або конкурують із традиційними установами, або співпрацюють із ними. Так чи інакше, правила гри переформатовуються.

Екосистемний підхід вивчає цифрові платформи як основу сучасних фінансів. У традиційній моделі фінансовий посередник надавав послуги через власні канали. Тепер платформи створюють середовище. У цьому середовищі багато провайдерів і багато споживачів взаємодіють разом. У межах однієї екосистеми. Логіка створення вартості змінюється. Вартість тепер формується на основі взаємодії учасників, а не тільки через діяльність одного посередника.

Поведінковий підхід враховує вплив цифрових сервісів на поведінку споживачів фінансових послуг. Цифровізація змінює не лише технічні аспекти надання послуг, а і психологію прийняття фінансових рішень. Доступність інформації, персоналізація пропозицій, гейміфікація, соціальні функції – усе це формує нові поведінкові патерни, які фінансові посередники мають враховувати у своїй діяльності. Водночас виникають нові ризики, пов'язані з імпульсивністю цифрових рішень, надмірним споживанням фінансових продуктів або, навпаки, з цифровим відчуженням окремих груп населення.

Функціональний підхід фокусується на трансформації традиційних функцій фінансових посередників. Базові функції – акумуляція ресурсів, їх розміщення, управління ризиками, забезпечення платежів – не зникають, але радикально

змінюється спосіб їх реалізації. З'являються нові функції, пов'язані з управлінням даними, забезпеченням цифрової ідентичності, інтеграцією екосистемних партнерів. Функціональні межі між різними типами посередників розмиваються, оскільки технології дозволяють одному актору виконувати функції, які раніше були розподілені між кількома спеціалізованими інституціями.

У теоретичній перспективі цифрова трансформація є наслідком трьох взаємопов'язаних фундаментальних зрушень, які разом формують нову реальність фінансового посередництва.

Перше зрушення полягає в *переході від фізичної інфраструктури до цифрової*. Традиційні відділення банків, паперові документи, фізичні картки поступово замінюються або доповнюються цифровими платформами, електронною ідентифікацією, хмарними інформаційними системами. Це не просто технічна заміна одних інструментів іншими. По суті, це трансформація самої логіки організації взаємодії. Цифрова інфраструктура дозволяє масштабувати послуги без пропорційного зростання витрат, персоналізувати пропозиції для мільйонів клієнтів одночасно, надавати послуги цілодобово та без географічних обмежень.

Друге – пов'язане зі *зростанням ролі даних як економічного ресурсу*. Якщо раніше фінансові посередники оперували переважно з фінансовими активами та зобов'язаннями, то тепер дані про поведінку клієнтів, їхні транзакції, переваги стають не менш цінним активом. Це змінює логіку прийняття рішень. Відбувається перехід від використання агрегованої статистики та експертних суджень до предиктивної аналітики на основі машинного навчання. Одночасно трансформується роль фінансового посередника. Він з простого посередника в русі капіталу перетворюється на інформаційного інтегратора, який створює цінність через синтез даних з різних джерел та надання інсайтів клієнтам.

Третє зрушення характеризується *формуванням нових моделей взаємодії на фінансовому ринку*. Традиційна модель, за якої банки та інші регульовані фінансові установи виконували функції посередництва, доповнюється та/або

витісняється новими моделями. Водночас альтернативні способи виконання посередницьких функцій пропонують великі технологічні компанії, фінтех-стартапи, цифрові платформи, децентралізовані фінансові системи (DeFi). Це створює як конкуренцію, так і можливості для співпраці, формує гібридні моделі, у яких традиційні та нові учасники об'єднують свої компетенції.

Базуючись на розглянутих теоретичних підходах та фундаментальних зрушеннях, цифрову трансформацію фінансового посередництва можна визначити як комплексний процес структурних змін у діяльності фінансових посередників (рис. 1.2).



Рис. 1.2. Структурні зміни в діяльності фінансових посередників у процесі цифрової трансформації

Джерело: розроблено автором на основі [14; 81; 97; 174; 226].

Узагальнюючи різні теоретичні перспективи, можна сформулювати узагальнене визначення: **цифрова трансформація фінансового посередництва** – це якісна зміна способу виконання посередницьких функцій на фінансовому ринку, що відбувається під впливом цифровізації інфраструктури, датафікації процесів прийняття рішень та платформізації бізнес-моделей, і призводить до переформатування інституціональної структури ринку, трансформації ролей традиційних учасників та появи нових форм фінансової взаємодії.

Ці концептуальні зміни визначають нову роль фінансового посередника в цифровій економіці. Сучасний фінансовий посередник функціонує не просто як організація, що надає послуги, а як інтегратор цифрової екосистеми. Він поєднує традиційні функції акумуляції та розміщення ресурсів із новими функціями управління даними, забезпечення цифрової ідентичності, координації взаємодії учасників платформи.

Довіра, яка традиційно будувалася на репутації, капіталі та регуляторному нагляді, тепер формується також через технологічну прозорість – здатність клієнта бачити, як використовуються його дані, як приймаються рішення, як забезпечується безпека. Інфраструктурна роль посередника трансформується: від володіння фізичними активами (будівлями, банкоматами) до управління цифровими платформами, API, алгоритмами.

Водночас посилюється соціальна відповідальність фінансових посередників. У цифровому середовищі, де технології можуть як включати, так і виключати людей з фінансової системи, де алгоритми можуть відтворювати або посилювати нерівність, роль посередника полягає не лише в максимізації прибутку, а й у забезпеченні справедливому доступу, захисті вразливих груп, сприянні фінансовій грамотності та інклюзії.

Розгляд цифрової трансформації як теоретичної категорії дає змогу сформувати цілісне уявлення про те, які чинники та інституційні зміни визначають нову природу фінансового посередництва. Однак концептуальний аналіз потребує подальшої конкретизації щодо того, яким чином відбувається формування цифрових фінансових посередників, які технологічні, організаційні та інституційні механізми забезпечують трансформацію їхньої діяльності, та які функції зазнають найбільш суттєвих змін.

Ці питання утворюють зміст підрозділу 1.2, у якому увага зосереджується на процесах формування цифрових фінансових посередників, трансформації їх функцій, появі нових моделей взаємодії та адаптації стратегічних підходів до умов цифрової економіки.

1.2. Вплив цифрових технологій та фінансових інновацій на архітектуру стратегічного управління розвитком фінансових посередників

Цифрові технології та фінансові інновації кардинально трансформують діяльність фінансових посередників у XXI ст. Класичні стратегічні орієнтири (експансія мережі, капіталізація, продуктове урізноманітнення) поступаються моделям створення вартості на основі даних, алгоритмів, платформ та екосистемної взаємодії. Цифровізація стає не технологічним, а стратегічним чинником, що визначає конкурентоспроможність, стійкість та інноваційний потенціал установ.

Зазначені зміни впливають на архітектуру стратегічного управління: вони вимагають переходу від клієнто- та ризик-центричних моделей до платформно-інфраструктурних, дата- та технологічно-орієнтованих. Зростає роль кіберстійкості, відкритих API, хмарних рішень та алгоритмічної довіри. У такому середовищі стратегія набуває рис динамічної системи адаптації, партнерства й екосистемної координації.

Мета підрозділу – визначити, які саме технології та інновації формують сучасні стратегічні орієнтири фінансових посередників, як вони видозмінюють традиційні підходи до розвитку та як ці зміни мають відображатися в стратегії.

Особливого значення набуває переосмислення базових функцій, насамперед управління фінансовими ризиками (кредитними, ринковими, ліквідності, операційними, правовими). Ця функція безпосередньо впливає на довіру, стабільність бізнес-моделі та здатність до впровадження інновацій. У класичному фінансовому посередництві вона реалізувалася через експертні процедури, стандартизовані методики оцінювання, внутрішній контроль і звітність.

Розвиток цифрової економіки суттєво видозмінює ризиковий профіль фінансових установ. Якщо раніше домінували кредитні та ринкові ризики, то цифровізація висуває на перший план операційні та технологічні загрози, які не піддаються ефективному контролю традиційними методами.

Масове поширення дистанційних каналів (мобільні додатки, вебінтерфейси, чатботи) робить кожен із них критичною інфраструктурою. Відмова цифрового каналу, на відміну від локального збою у фізичному відділенні, паралізує обслуговування всіх клієнтів одночасно. Використання відкритих API та концепції відкритого банкінгу, створюючи можливості для інновацій, водночас породжує додаткові канали проникнення для зловмисників, оскільки безпека установи частково залежить від рівня захищеності систем її партнерів.

Мобільні пристрої клієнтів стають точками доступу до фінансових систем поза контрольованим середовищем. Ризики втрати, крадіжки, інфікування пристроїв, використання незахищених мереж або фішингу змушують установу забезпечувати безпеку за умов, коли значна частина ланцюга взаємодії перебуває поза її контролем, що підвищує вартість послуг.

Масштабні потоки електронних платежів (мільйони транзакцій на день) вимагають автоматизованого моніторингу, але створюють ризики, пов'язані з виявленням шахрайства та витримуванням пікових навантажень. Миттєві операції, які стали стандартом, скорочують час реагування до кількох секунд. Це породжує асиметрію: клієнти очікують миттєвості, однак шахраї використовують її для виведення коштів до спрацювання систем захисту, а технічні збої або помилки алгоритмів можуть завдати збитків за лічені секунди.

Поєднання дистанційності, відкритості систем, мобільності доступу, електронної форми операцій та миттєвості формує середовище, де операційні й технологічні ризики стають головними загрозами. Це вимагає переосмислення пріоритетів ризик-менеджменту, перерозподілу ресурсів, нових компетенцій та організаційних структур. Застосування традиційних підходів до управління ризиками в цифровому середовищі робить фінансові установи вразливими та послаблює їхні конкурентні позиції.

У процесі цифрової трансформації суттєво зростає залежність фінансових установ від цифрової інфраструктури, якості даних, кібербезпеки, стійкості інформаційних систем та поведінкових моделей клієнтів. Розглянемо ці аспекти.

Залежність від цифрової інфраструктури. Якщо традиційні установи могли функціонувати за обмеженого технологічного забезпечення, то сучасні критично залежать від безперебійної роботи хмарних сервісів, API-інтеграцій з партнерами та цифрових каналів обслуговування. Збій інфраструктури паралізує діяльність усієї установи, а не окремого відділення. Централізація інфраструктури створює новий рівень системного ризику.

Залежність від якості даних. Алгоритми прийняття рішень (скоринг, автоматизоване консультування) повністю залежать від вхідних даних. Неповнота, неточність, застарілість або упередженість даних призводять до систематичних помилок: відмова кредитоспроможним клієнтам, ризиковане кредитування, неадекватне ціноутворення. Використання зовнішніх джерел даних створює додаткову залежність, а рішення в реальному часі унеможливають людську верифікацію.

Залежність від кібербезпеки. Кібератаки стають глобальними, автоматизованими, здійснюються організованими групами. Фінансові установи — приваблива ціль через концентрацію активів та даних. Спостерігається фундаментальна асиметрія: установа мусить захищати всі точки входу цілодобово, атакувальнику достатньо однієї вразливості разово. Наслідки атаки – не лише прямі фінансові втрати, а й репутаційні збитки, регуляторні санкції, операційні витрати на відновлення.

Залежність від стійкості інформаційних систем. Децентралізація традиційної моделі, яка використовувала значну кількість автономних відділень, змінюється централізованими системами, де один збій паралізує всю установу. Складність програмного забезпечення створює численні можливості для помилок. Ключові аспекти стійкості: технічна надійність, здатність витримувати пікові навантаження, стійкість до каскадних збоїв, швидкість відновлення. Особливу проблему становить взаємодія застарілих систем із новими додатками («технологічний борг»).

Залежність від поведінкових моделей клієнтів. У цифровому середовищі клієнти стають більш мобільними, у тому числі через низькі бар'єри переходу, їхні очікування формуються досвідом інших цифрових

платформ, рішення приймаються імпульсивніше під впливом дизайну інтерфейсу. Соціальні мережі створюють механізми швидкого формування репутації. Установи залежать від точності прогнозування поведінки клієнтів, оскільки помилки в цій сфері стають дедалі дорожчими.

Перелічені типи залежностей не існують ізольовано, а взаємопідсилюють одна одну. Проблеми з кібербезпекою руйнують довіру клієнтів, низька якість даних знижує ефективність персоналізації, збої в інфраструктурі створюють операційні та репутаційні ризики. Отже, зростання цих залежностей є системною характеристикою цифрової трансформації, що вимагає нових підходів до управління операційними ризиками, стратегічного планування та організації діяльності фінансових посередників. Управління ризиками не може ґрунтуватися лише на регулятивних вимогах та історичних даних – необхідним є динамічне, прогнозне та технологічно забезпечене моделювання ризикових сценаріїв.

У цифровій економіці ризики класифікуються не лише за джерелом (внутрішні/зовнішні), але й за їхньою технологічною природою, що відображено й у попередніх авторських дослідженнях [224; 226]. Зокрема, у роботі «Актуальні типи кіберзагроз функціонування і розвитку фінансових установ» розглядаються ризики, пов'язаних із цифровою грамотністю клієнтів, захистом персональних даних, зростанням кількості дистанційних операцій та ширшим використанням мобільних застосунків для доступу до фінансових сервісів [224].

Зазначені чинники підсилюють потребу в нових підходах до ризик-менеджменту, у тому числі у прогнозній аналітиці, машинному навчанні, поведінковій біометрії (технологія ідентифікації людини на основі унікальних особливостей її поведінки при взаємодії з цифровими пристроями), моніторингу аномалій у реальному часі, автоматизованому інцидент-менеджменті (за допомогою якого цифрова система автоматично виявляє, реагує та вирішує проблеми (інциденти) в роботі інформаційних систем без участі або з мінімальною участю людини).

Отже, цифровізація не просто збільшує кількість ризиків – вона змінює їхню природу, роблячи тим самим управління ризиками технологічно залежною, високодинамічною та постійно розширюваною функцією.

Однією з найбільш значущих тенденцій є суттєве зростання кіберризиків, кількісні та якісні характеристики яких суттєво відрізняються від традиційних операційних ризиків. Незважаючи на різноманіття видів фінансових установ та притаманність їм специфічних особливостей, є актуальні типи кіберзагроз, які властиві всім видам фінансових посередників (рис. 1.3).

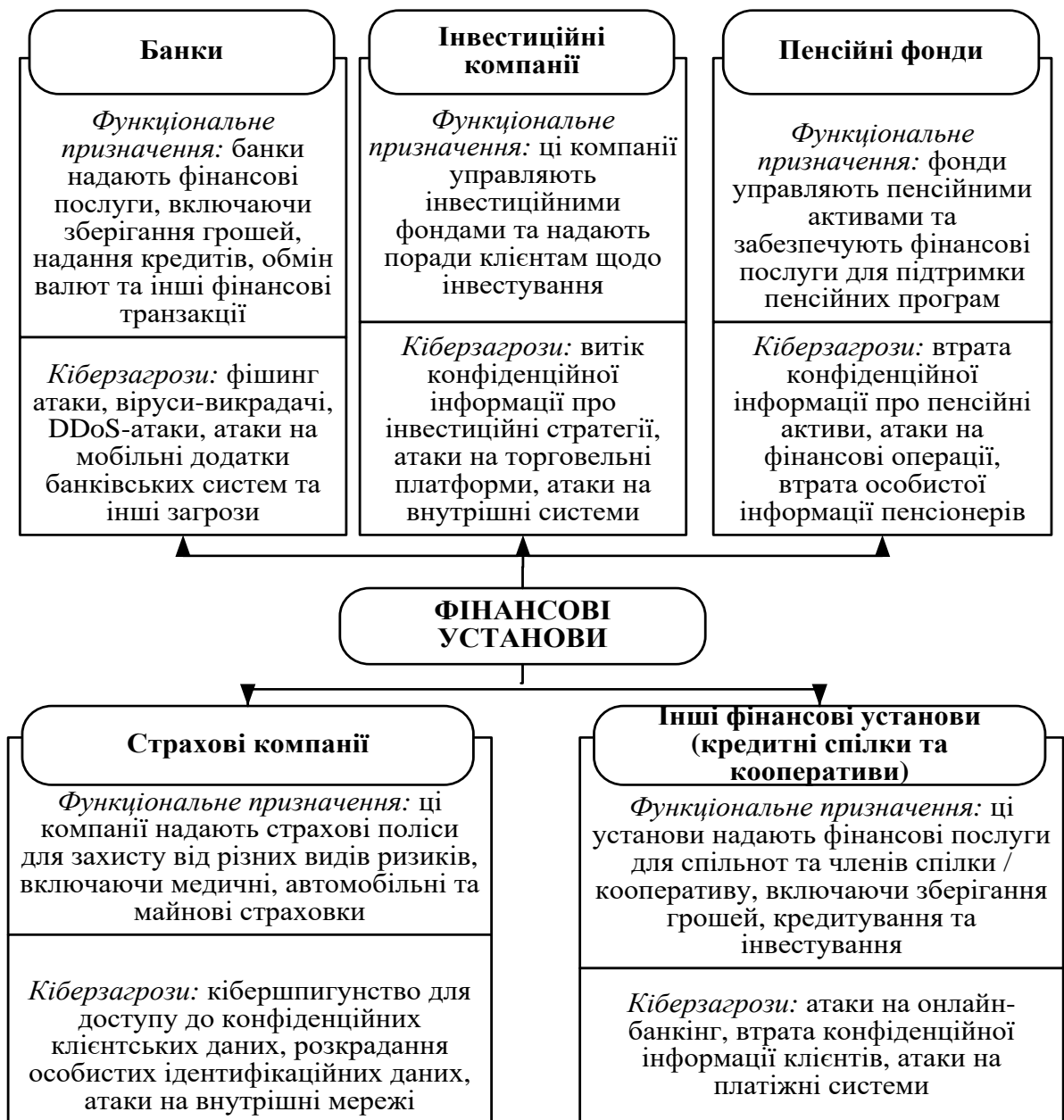


Рис. 1.3 – Функціональне призначення різних видів фінансових установ та властиві їм типи кіберзагроз

Джерело: розроблено автором на основі [18; 93] та опубліковано у [224].

До основних актуальних типів кіберзагроз фінансових установ вважаємо доцільним віднести фішинг, рансомвер, *DDoS-атаки*, кібершпигунство, бізнес-експлуатація, злам внутрішньої безпеки фінансової установи та атаки на мобільні пристрої та електронну пошту [224].

До переліку найбільш актуальних різновидів кіберзагроз для діяльності фінансових установ доцільно зарахувати такі: фішинг, рансомвер (викрадачі-шифрувальники), *DDoS-атаки*, кібершпигунство, бізнес-експлуатацію, злам внутрішніх механізмів безпеки фінансової установи, а також атаки на мобільні пристрої та електронну пошту [224].

Фішинг являє собою різновид кібератаки, орієнтованої на вилучення конфіденційної інформації, зокрема паролів або номерів банківських карток, які надалі можуть бути реалізовані чи використані з протиправною метою, наприклад для розкрадання коштів або привласнення персональних даних. Такі атаки здійснюються шляхом перенаправлення користувачів на фальшиві веб-ресурси або через надсилання електронних листів, що візуально та змістовно імітують легітимні повідомлення від банків чи інших фінансових структур.

Рансомвер належить до категорії програм-вимагачів, які виконують шифрування файлів, розміщених на комп'ютері або мережевому пристрої, із подальшим висуненням вимоги про викуп за їхнє розшифрування у формі криптовалюти. Використання криптовалют робить такі транзакції практично анонімними й ускладнює їх відстеження.

Застосування *DDoS-атак* передбачає цілеспрямоване створення надмірного навантаження на серверне або мережеве обладнання фінансових інституцій, у результаті чого блокується здатність системи обслуговувати правомірні запити користувачів.

Несанкціонований доступ до відомостей обмеженого поширення, зокрема до стратегічних планів розвитку, клієнтських баз даних та інформації про фінансові операції, кваліфікується як *кібершпигунство* щодо діяльності фінансових установ.

Виявлення вразливих місць у бізнес-процесах фінансових установ (зокрема, у торговельних майданчиках чи системах інтернет-банкінгу) з наступним використанням таких вразливостей для отримання несанкціонованого доступу до ресурсів, даних або конкурентних переваг становить сутність *бізнес-експлуатації*.

Атаки, що ініціюються всередині організації, коли діючі працівники або інші внутрішні суб'єкти намагаються заволодіти конфіденційною інформацією та використати її з протиправною метою, визначаються як *злам внутрішньої безпеки фінансової установи*.

Використання мобільних банків та платіжних додатків породжує атаки на мобільні пристрої (віруси, фішинг, атаки на додатки), а також через електронну пошту. Різноманіття кіберзагроз вимагає від фінансових установ постійного моніторингу та вдосконалення заходів кібербезпеки, оскільки зростання масштабів цифровізації ускладнює кіберризикове середовище та підвищує його непередбачуваність.

Важливим наслідком цифровізації є те, що джерелом ризиків стають не лише технічні фактори, а й дані (їхня якість, доступність, критичність, викривлення, втрата). Сучасні фінансові посередники дедалі більше функціонують як дата-орієнтовані організації, що створюють цінність шляхом:

- *обробки великих масивів даних (Big Data)* – збирання та аналіз величезних обсягів інформації (фінансові дані, поведінка в цифрових каналах, транзакції, геолокація, активність у соцмережах). Традиційні методи обробки не справляються, цінність полягає у виявленні закономірностей, трендів, ризиків та можливостей;

- *використання алгоритмів машинного навчання* – замість виключно експертних суджень алгоритми самостійно «навчаються» на даних, виявляючи складні нелінійні залежності (наприклад, розпізнавання шахрайських транзакцій, прогнозування дефолту) та постійно вдосконалюються;

– *автоматизованих рішень на основі ризикових моделей* – рішення про кредитування, інвестиції, встановлення лімітів, виявлення шахрайства приймаються автоматично за мілісекунди, що забезпечує швидкість та консистентність. Виклики: точність, справедливість, зрозумілість моделей для регуляторів;

– *поведінкової цифрової аналітики* – вивчення поведінки клієнта в цифровому середовищі (частота входу, використовувані функції, час прийняття рішень). Це дозволяє розуміти потреби, передбачати дії, виявляти ризики (наприклад, закриття рахунку) та виявляти шахрайство за поведінковими патернами;

– *інтелектуальної сегментації* – замість широких категорій (вік, дохід) створюються деталізовані сегменти на основі множини характеристик (фінансова поведінка, життєві ситуації, психологічні особливості). Це дозволяє персоналізувати пропозиції, прогнозувати потреби (наприклад, іпотека) та динамічно змінювати належність клієнта до сегментів.

У результаті цих змін управління ризиками стає автоматизованим процесом. Прогнозування загроз, виявлення відхилень та реагування на проблеми здійснюють алгоритмічні системи. Роль людини змінюється: фахівці більше не приймають кожне рішення вручну, а контролюють роботу систем, перевіряють їхні висновки та коригують налаштування. Різноманітність, взаємопов'язаність та динамічність цифрових загроз вимагають структурованого аналізу. Систематизація основних типів ризиків, їхніх джерел та впливу на практику управління дає змогу сформулювати цілісне розуміння викликів, з якими стикаються сучасні фінансові посередники. З огляду на це в таблиці 1.6 нами узагальнено ключові характеристики цифрових загроз у їхній діяльності.

Таблиця 1.6

Цифрові загрози фінансових посередників, їхні джерела та вплив на ризик-менеджмент

Категорія ризику / загроза	Тип фінансових посередників, для яких загроза найбільш критична	Обґрунтування вразливості фінансових посередників	Вплив на функцію управління ризиками
1	2	3	4
Фішингові атаки	Мобільні банки (neobank), цифрові платіжні сервіси (PSP), банки з дистанційним обслуговуванням.	ці установи мають найвищу частку клієнтських взаємодій онлайн; використовують мобільні застосунки; мають підвищений ризик підроблених сайтів і застосунків; обробляють значні обсяги дрібних транзакцій.	Потреба в системах поведінкової аналітики; впровадження MFA; використання антифішингових фільтрів; підвищення цифрової грамотності клієнтів; посилення моніторингу операцій у реальному часі.
Рансомвер (шифрувальники)	Банки з великою ІТ-інфраструктурою; страхові компанії; депозитарні установи; кредитні спілки.	працюють із великими архівами даних; володіють критичними серверними вузлами; потребують безперервної роботи; через це є бажаною ціллю для шифрувального ПЗ.	Підсилення потреби у кіберстійкій ІТ-архітектурі, обов'язкове резервування даних; сегментація мережевої інфраструктури та контроль доступу
DDoS-атаки	Платіжні системи (наприклад, СЕП / аналог), інтернет-банкінг банків, торговельні еквайрингові платформи, фінтех-маркетплейси.	їхні сервіси працюють у режимі реального часу; атаки спрямовані на блокування доступності каналів; критичні для виконання транзакцій.	Підсилення безперервності бізнесу; застосування DDoS-митигаторів; резервні канали; автоматизація реагування на інциденти; стрес-тестування пікових навантажень.
Кібершпиунство	Банки; інвестиційні компанії; приватні пенсійні фонди; страхові компанії.	оперують конфіденційною комерційною інформацією, фінансовими профілями та корпоративними даними, що робить їх ціллю для шпигунського ПЗ.	Впровадження DLP-систем; посилена система моніторингу доступів; криптографічний захист; аудит внутрішніх привілейованих доступів.
Атаки через електронну пошту	Банки з великою розгалуженою мережею філій; страхові компанії; інвестиційні брокери; МФО.	великий штат → велика ймовірність соціальної інженерії та компрометації через листування; фішингові кампанії легко масштабуються.	Потреба в антифішингових протоколах, тренінгах, внутрішній політиці безпеки

Закінчення таблиці 1.6

1	2	3	4
Вразливості мобільних застосунків	необанки, мобільні банки, цифрові ощадні платформи, P2P-платформи, застосунки небанківських фінпослуг.	бізнес-модель базується на мобільному каналі; високий ризик атаки через API; уразливість ОС користувачів; інтеграція з іншими сервісами.	Потреба у мобільній кібергігієні, перевірці коду, сертифікації застосунків
Внутрішні загрози (інсайдери)	Банки; депозитарії; страхові компанії; інвестиційні фонди.	персонал має прямий доступ до даних, реєстрів, баз клієнтів; можливість маніпулювання або витоку інформації.	Перегляд політики доступів, контроль дій персоналу, аудит подій, сегментація прав; HR-ризик-менеджмент.
Масові кібератаки та системні збої	Системно важливі банки, оператори платіжних систем, клірингові центри, процесингові компанії.	зупинка однієї установи може створити “ефект доміно” та паралізувати фінансову систему країни.	Інтеграція кіберризиків у макропруденційну політику; створення центрів кіберстійкості; сценарне моделювання; координація з регулятором.
Ризики цифрових платформ (API, хмарні сервіси, дані)	Банки-учасники Open Banking; фінтех-платформи; маркетплейси; оператори цифрових гарантій; кредитні онлайн-платформи.	висока інтеграція з третіми сторонами; залежність від API; можливість зловмисного доступу через партнерські потоки.	Потреба в платформених стандартах безпеки, аудит API, сегментація даних, моделювання загроз; контроль доступу третіх сторін.
Ризики низької цифрової грамотності клієнтів	Банки з мобільними послугами; МФО; страхові онлайн-сервіси; P2P-платформи; оператори онлайн-переказів.	клієнт стає “слабкою ланкою”; атакувальники використовують соціальну інженерію і незнання процедур безпеки.	Антифрод-моніторинг; поведінковий скоринг; освітні програми; UX-дизайн, що знижує ризики неправильних дій.
Загрози конфіденційності даних та витоків	Банки, страхові компанії, платіжні платформи, кредитні бюро, фінансові суперагрегатори.	працюють з великими обсягами персональних і фінансових даних; несуть високу репутаційну відповідальність.	Шифрування; сегментація баз даних; SOC-центри; хмарний аудит; контроль привілейованих доступів.
Технічні ризики цифрової інфраструктури	Процесингові центри; платіжні шлюзи; венчурні фінтех-платформи; банки з високим навантаженням на ІТ.	критична залежність від стабільності серверів, SDK (набір інструментів для розробників), модулів API; високі витрати на підтримку.	Стрес-тестування; масштабування; DevSecOps (швидкість + якість + кіберстійкість); резервні дата-центри; планування відмовостійкості.

Джерело: розроблено автором на основі [7; 56; 224; 18; 83; 72; 147; 157; 175; 207; 221; 222].

Наведена систематизація демонструє, що різні типи фінансових посередників мають неоднакові профілі ризиків залежно від специфіки діяльності. Так, необанки та платіжні сервіси найбільш вразливі до фішингу та атак на мобільні додатки через масову цифрову взаємодію з клієнтами. Системно важливі банки та процесингові центри зазнають найбільших загроз від DDoS-атак і масових збоїв, оскільки їхня зупинка може паралізувати всю фінансову систему. Установи з великими обсягами конфіденційної інформації (банки, страхові компанії, інвестиційні фонди) є привабливою ціллю для кібершпиунства та програм-вимагачів.

Важливо, що кожна загроза потребує специфічних інструментів протидії: від поведінкової аналітики та багатофакторної аутентифікації (проти фішингу) до систем запобігання витоку даних (DLP) для захисту від кібершпиунства, від резервування інфраструктури (проти рансомверу) до аудиту API для безпечної роботи в екосистемах. Водночас людський фактор залишається критичною вразливістю – як через внутрішні загрози з боку персоналу, так і через низьку цифрову грамотність клієнтів, які стають об'єктами соціальної інженерії.

Аналіз наведеного спектра цифрових загроз свідчить, що традиційна модель управління ризиками (періодична оцінка, експертні судження, реактивне реагування на інциденти) втрачає ефективність. Швидкість матеріалізації загроз, їхня складність, взаємопов'язаність та масштаб наслідків вимагають фундаментальної трансформації філософії управління ризиками. У цифровій економіці воно стає:

- *проактивним* – фокус зміщується від реагування до запобігання загрозам через постійний моніторинг, виявлення ранніх сигналів, сценарне моделювання атак та превентивне зміцнення вразливих елементів;

- *прогнозним* – використання предиктивної аналітики, машинного навчання та ШІ дозволяє передбачати ймовірність реалізації ризиків, ідентифікувати нові патерни загроз та адаптувати захист;

– *аналітичним* – рішення ґрунтуються на обробці великих масивів даних про інциденти, вразливості, поведінкові аномалії, що дає змогу виявляти приховані залежності між ризиками та оцінювати їхній кумулятивний ефект;

– *автоматизованим* – необхідність реагування в реальному часі вимагає делегування значної частини рішень алгоритмам, які можуть виявити аномалію, заблокувати підозрілу операцію, ізолювати скомпрометовану систему за секунди;

– *інфраструктурно залежним* – ефективність управління ризиками визначається не лише політиками та процедурами, а й технологічною архітектурою (резервування систем, сегментація мереж, якість API, стійкість хмарної інфраструктури), що робить технологічні рішення невід'ємною частиною ризик-стратегії.

Усе це вимагає зміни політик, систем внутрішнього контролю, корпоративних стратегій, культурних підходів до управління ризиками.

З урахуванням вищенаведеного, ризик-менеджмент у цифровому середовищі перетворюється на ключовий чинник забезпечення інституційної стійкості фінансових посередників. Це серед іншого пояснюється специфікою цифрових ризиків, які якісно відрізняються від традиційних. По-перше, вони є більш масштабними – одна кібератака може одночасно вплинути на мільйони клієнтів. По-друге, вони мають системний характер – проблема в одній установі може швидко поширитися на інші через екосистемні зв'язки. По-третє, цифрові ризики здатні створювати ланцюгові ефекти, коли збій в одному елементі системи спричиняє численні проблеми в інших. По-четверте, вони можуть матеріалізуватися миттєво, не даючи часу на обдумане реагування.

У зазначеному контексті ризик-менеджмент трансформується з допоміжної технічної функції на невід'ємну складову стратегічного управління. Така трансформація зумовлена тим, що якість управління ризиками справляє прямий вплив на всі ключові напрями діяльності фінансової установи. Саме від ефективності ризик-менеджменту залежить здатність організації до активної імплементації інновацій. Слабкий контроль ризиків обмежує діяльність установи

рамками надмірної обережності, тоді як належний рівень контролю, навпаки, створює умови для безпечного проведення експериментів і впровадження змін. Крім того, якість управління ризиками формує рівень довіри з боку клієнтів. Успішна кібератака або витік даних здатні миттєво зруйнувати репутацію, що напружувалася впродовж тривалого часу. Нарешті, ризик-менеджмент впливає на стійкість бізнес-моделі: установа, яка не здійснює належного контролю цифрових ризиків, ризикує втратити операційну спроможність. Отже, з огляду на викладене, ризик-менеджмент набуває критичного значення для забезпечення відповідності регуляторним вимогам, які в цифрову епоху стають дедалі жорсткішими.

Зростання цифрових ризиків вимагає не лише технологічних рішень. Крім них необхідна трансформація культурних та поведінкових моделей взаємодії з ризиками. Це означає підвищення цифрової грамотності клієнтів, які повинні розуміти базові принципи безпеки, що передбачає систематичне навчання співробітників, які, з одного боку, виступають захисниками, а з іншого – основними порушниками системи. Це вимагає посиленої уваги до внутрішніх загроз – від неумисних помилок до свідомих зловживань. У зв'язку з цим виникає потреба у впровадженні систем моніторингу, які фіксують всі події, та аналітики в реальному часі, здатної виявляти аномальні трансакції в мільйонних потоках.

Відповіддю фінансових посередників на нові виклики стає формування комплексної цифрової архітектури управління ризиками. Сучасні системи ризик-менеджменту будуються на основі хмарних технологій, які забезпечують масштабованість та гнучкість. Розподілені системи моніторингу дозволяють відстежувати події одночасно в різних точках інфраструктури. Кіберстійкі архітектури проєктуються так, щоб витримувати атаки та швидко відновлюватися після збоїв.

Регуляторні технології (RegTech) автоматизують дотримання вимог та формування звітності, зменшуючи як операційні витрати, так і ризики помилок. Поведінкова аналітика вивчає патерни дій користувачів, виявляючи

аномалії, які можуть свідчити про шахрайство або компрометацію облікового запису. Біометричні системи ідентифікації роблять доступ до систем більш безпечним та зручним одночасно. Багатофакторна автентифікація створює додаткові рубежі захисту навіть у разі компрометації паролів.

Принципово важливим є те, що в умовах цифровізації ризик-менеджмент перестає бути ізольованою функцією окремого підрозділу. Він інтегрується у всі процеси фінансової установи, стаючи крос-функціональним, платформним та вбудованим механізмом. Це означає фундаментальну зміну в логіці організації.

Ризики тепер враховуються вже на етапі проєктування нових продуктів – не після їх створення, а як невід'ємна частина процесу розробки. Вони оцінюються на рівні архітектури інформаційних систем – безпека закладається в саму основу технологічних рішень, а не додається пізніше як надбудова. Ризики аналізуються в режимі реального часу – системи постійно моніторять потоки даних, транзакцій, подій, виявляючи відхилення від норми. Інноваційні технології автоматизують реагування на загрози – критичні рішення приймаються алгоритмами за секунди, без очікування людського втручання. Регуляторна звітність формується за допомогою RegTech – автоматично, точно, своєчасно, звільняючи ресурси для аналітичної роботи.

Цифрові ризики охоплюють усі напрями діяльності фінансових посередників, унаслідок чого управління ними закономірно інтегрується з іншими ключовими функціями організації. Зазначений системний зв'язок виявляється в кількох аспектах.

Взаємодія з інноваційною функцією має двосторонній характер. З одного боку, ризики здатні стримувати інноваційну активність: високий рівень невизначеності або потенційних загроз спричиняє відмову від перспективних, однак ризикоемних проєктів. З іншого боку, ефективне управління ризиками виступає каталізатором інноваційних процесів. Іншими словами, коли фінансова установа володіє достатньою впевненістю у власній спроможності контролювати нові види загроз, вона отримує змогу активніше експериментувати з передовими технологіями та бізнес-моделями.

Зв'язок ризик-менеджменту з інфраструктурною функцією має фундаментальне значення. Це зумовлено насамперед тим, що рівень ризиків перебуває у прямій залежності від якості цифрової архітектури установи. Надійна, резервована та сегментована інфраструктура забезпечує зниження вразливості до технологічних збоїв і кібератак. Натомість застарілі системи, слабка інтеграція між компонентами та відсутність резервування створюють середовище з підвищеним рівнем ризику.

Взаємозв'язок між ризик-менеджментом та функцією формування довіри набуває критичної ваги. Недостатньо ефективне управління ризиками, наслідком якого стають витoki конфіденційних даних, реалізація кібератак або тривалі порушення в роботі систем, призводить до втрати довіри з боку стейкхолдерів. Навіть одиничний серйозний інцидент може повністю нівелювати репутаційні здобутки, напрацьовані впродовж багатьох років. І навпаки, публічна презентація високих стандартів безпеки, транспарентності в ризик-орієнтованому управлінні та здатності до швидкого реагування на інциденти виступає чинником зміцнення довіри до фінансової інституції.

Фінансова інклюзія також перебуває у тісному зв'язку з ризик-менеджментом, який реалізується через ризики дискримінаційного характеру та виключення певних категорій споживачів. Застосування надміру жорстких процедур клієнтської ідентифікації або використання алгоритмів оцінювання з упередженими налаштуваннями здатне спричинити відмову у доступі до фінансових послуг для вразливих верств населення. З іншого боку, низький рівень контролю за ризиками шахрайських дій може робити економічно не вигідним обслуговування окремих споживчих сегментів. Тому досягнення збалансованості між інклюзивністю та безпековими вимогами позиціонується як одне з актуальних завдань сучасного ризик-менеджменту.

Інтеграція зі стратегічною функцією проявляється через концепцію ризик-апетиту — готовності організації приймати певний рівень ризику заради досягнення стратегічних цілей. Ризик-апетит формує напрям розвитку: консервативний підхід веде до фокусу на стабільності та традиційних продуктах,

агресивний – до експансії в нові сегменти та експериментів з технологіями. Стратегічні рішення про цифрову трансформацію, вихід на нові ринки, запуск інноваційних продуктів неможливі без оцінки пов'язаних з ними ризиків.

Таким чином, у цифровій економіці ризик-менеджмент перетворюється на системоутворювальний елемент фінансового посередництва – він не просто контролює загрози, а інтегрується в стратегію, операції, культуру організації, визначаючи її спроможність функціонувати, розвиватися та залишатися конкурентоспроможною в умовах високої невизначеності та динамічних змін.

Поглиблена трансформація функції управління фінансовими ризиками демонструє, що цифрова економіка впливає не лише на окремі операційні процеси, але й на фундаментальні засади стратегічного розвитку фінансових посередників. Зміщення акценту в бік прогностичної аналітики, кіберстійкості, управління даними та алгоритмічної довіри формує новий контекст, у якому стратегія перестає бути статичним документом і перетворюється на динамічну систему адаптації до технологічних змін.

У цих умовах цифрові технології виступають не просто інструментами модернізації, а ключовими драйверами стратегічної трансформації, що визначають нову логіку конкуренції, джерела створення цінності, бізнес-моделі та формати взаємодії з клієнтами й партнерами. Саме тому виникає необхідність дослідити, які саме технології формують новий стратегічний ландшафт діяльності фінансових посередників, як вони змінюють їхні довгострокові орієнтири та яким чином переорієнтовують інституційний дизайн фінансового сектору.

Стратегічний розвиток фінансових посередників у цифровій економіці визначається здатністю інституцій своєчасно адаптуватися до змін зовнішнього середовища, інтегрувати інновації, формувати нові бізнес-моделі та забезпечувати відповідність сучасним вимогам кіберстійкості, даних, регуляторики та поведінкових очікувань клієнтів. Вище було доведено, що трансформація функції управління ризиками формує нові вимоги до стратегічного планування та операційної моделі фінансових посередників.

Проте вплив цифровізації значно ширший: цифрові технології стають не лише технологічною основою, а ключовим драйвером формування стратегічних орієнтирів розвитку, визначаючи ландшафт конкуренції, регуляторну рамку, клієнтські очікування та архітектуру фінансових екосистем.

У сучасному середовищі спостерігається перехід від традиційної логіки стратегічного управління, побудованої переважно на фінансових, продуктово-ринкових та інституційних факторах, до цифрової логіки, яка ґрунтується на архітектурі даних, алгоритмах, відкритих API, хмарній інфраструктурі, кіберстійкості та партнерських екосистемах. Саме це зумовлює потребу системно проаналізувати, які цифрові технології змінюють стратегічні орієнтири фінансових посередників та як відбувається трансформація стратегічних цілей.

Вплив цифрових технологій на стратегічні орієнтири фінансових посередників. Цифрові технології формують нові канали створення цінності, нові моделі ризик-менеджменту, нові типи клієнтського досвіду та принципово нову інституційну логіку взаємодії між фінансовими установами, платформами, постачальниками технологічних сервісів і регулятором. Провідні міжнародні дослідження OECD, BIS, World Bank, 2022-2024 років підтверджують, що штучний інтелект, великі дані, блокчейн, хмарні сервіси, API-платформізація та RegTech стають основними детермінантами стратегічного розвитку глобальних фінансових систем [22; 85; 113].

Цифрова трансформація фінансового посередництва не є однорідним процесом. Вона реалізується через впровадження конкретних технологій, і кожна з них по-своєму впливає на стратегічні орієнтири організацій. Технології не варто розглядати як нейтральні інструменти. Вони формують нові можливості, а водночас і певні обмеження. Змінюють конкурентні переваги. Визначають вектори подальшого розвитку. Саме тому розуміння специфіки впливу кожної технології є необхідною передумовою вибору обґрунтованої стратегії.

Різні технології впливають на різні аспекти стратегії. Одні посилюють здатність управляти ризиками та персоналізувати пропозиції, інші трансформують інфраструктуру та механізми формування довіри, треті відкривають нові бізнес-моделі та можливості масштабування. При цьому ефект від технологій не є адитивним – їхнє поєднання створює синергію, коли можливості однієї технології підсилюються можливостями іншої.

Для системного розуміння того, як саме технології визначають стратегічні пріоритети сучасних фінансових посередників, доцільно проаналізувати ключові цифрові технології з погляду їхнього впливу на стратегічні орієнтири. Таблиця 1.7 узагальнює цей взаємозв'язок, демонструючи, за рахунок яких технологій відбувається формування різних видів стратегічних напрямів та як це відбувається на практиці.

Таблиця 1.7

**Вплив ключових цифрових технологій
на стратегічні орієнтири фінансових посередників**

Цифрова технологія	Стратегічний орієнтир, на який впливає	Характер впливу	Приклади застосування у фінансових посередників
1	2	3	4
Штучний інтелект (AI/ML)	Ризик-менеджмент; персоналізація	Прогнозні моделі, поведінковий скоринг, автоматизація процесів	ML-скоринг, автоматичний фрод-моніторинг, рекомендаційні системи
Big Data та аналітика	Клієнтоцентричність; формування цінності	Глибока сегментація, аналіз поведінки, шаблонів та ризиковості	KPI-аналітика, аналітика клієнтського шляху, персоналізовані пропозиції
Blockchain / DLT	Довіра; інфраструктура	Незмінність записів, прозорість, зниження ризиків шахрайства	Смарт-контракти, токенизація активів, кліринг/розрахунки
Open Banking / API	Інноваційність; масштабованість	Платформізація, інтеграція з FinTech, розвиток екосистем	API-магазини банків, мультибанкінг, агрегація рахунків
Хмарні технології (Cloud)	Ефективність; операційна стійкість	Масштабування, зниження витрат, модульність сервісів	Хмарні процесингові центри, хмарні CRM/ERP
Біометрія та цифрова ідентифікація	Довіра; фінансова інклюзія	Підвищення безпеки доступу, спрощення підтвердження особи клієнта (KYC)	FaceID/TouchID, BankID, біометричний KYC

Закінчення таблиці 1.7

1	2	3	4
RegTech / SupTech	Регуляторна відповідність; стійкість	Автоматизація моніторингу транзакцій (AML/CTF), контроль операцій	AML-модулі, моніторинг транзакцій у режимі реального часу
DevSecOps / кіберзахист	Кіберстійкість; довгострокова стратегія	Інтегрована безпека, постійний моніторинг, захист активів	Центри операційної безпеки (SOC-центри), Zero Trust (жоден користувач, пристрій чи система не вважається довіреним за замовчування), автоматичне тестування вразливостей

Джерело: розроблено автором на основі [224; 22; 82; 85; 113; 174; 126].

Аналіз впливу ключових цифрових технологій на стратегічні орієнтири фінансових посередників дає змогу зробити кілька важливих висновків.

По-перше, кожна технологія має власний стратегічний фокус. Штучний інтелект та машинне навчання найбільше впливають на управління ризиками та персоналізацію послуг (прогнозні моделі, автоматизація рішень, розпізнавання патернів). Великі дані та аналітика посилюють клієнтоцентричність – глибоке розуміння потреб, сегментацію, оптимізацію клієнтського шляху. Блокчейн і розподілені реєстри трансформують механізми довіри через прозорість та незмінність записів. Відкритий банкінг та API відкривають можливості для інновацій завдяки платформізації та екосистемній інтеграції.

По-друге, деякі технології мають інфраструктурний характер, створюючи основу для інших інновацій. Хмарні технології забезпечують масштабованість та гнучкість. Біометрія та цифрова ідентифікація спрощують безпечний доступ до послуг. RegTech автоматизує регуляторну відповідність, звільняючи ресурси для стратегічних ініціатив. Розробка та впровадження програмного забезпечення, які ґрунтуються на поєднанні трьох базових понять «розробка програмного забезпечення – безпека – експлуатація» (DevSecOps), а також кіберзахист забезпечують стійкість усієї цифрової екосистеми.

По-третє, технології не діють ізольовано – їхня цінність проявляється у взаємодії. Штучний інтелект потребує Big Data для навчання, а відкритий банкінг створює потоки даних для аналітики. Блокчейн може використовувати

біометрію для ідентифікації. Хмарні технології забезпечують інфраструктуру для RegTech. А кіберзахист охороняє всю технологічну екосистему.

Технологічні пріоритети безпосередньо визначають стратегічну траєкторію фінансового посередника. Фінансовий посередник, який інвестує в штучний інтелект та аналітику, закономірно обирає розвиток у напрямку персоналізації та автоматизації рішень (останнє передбачає, зокрема, алгоритмічне прийняття ризикових рішень). Установа, що робить ставку на відкритий банкінг та API, рухається до платформної моделі та екосистемної інтеграції — без цього сьогодні неможливо уявити сучасну конкурентну стратегію. Окремий випадок — блокчейн. Фокусування на технологіях розподіленого реєстру спрямовує стратегію в бік прозорості та децентралізації, відкриваючи передусім можливості для смартконтрактів, міжнародних платежів і токенизації активів. І, нарешті, цілеспрямоване інвестування в кіберзахист і RegTech слід розглядати не як суто захисну дію, а як свідомий вибір стратегії операційної стійкості та регуляторної надійності. Саме такий вибір, до речі, дедалі частіше стає вирішальним фактором довгострокової конкурентоспроможності.

Нарешті, технологічний вибір не є суто технічним рішенням — він має глибокі стратегічні наслідки. Технології формують організаційні можливості, які визначають конкурентні переваги. У цифровій економіці стратегія фінансового посередника дедалі більше залежить не стільки від традиційних факторів (розмір капіталу, мережа відділень), скільки від технологічних компетенцій і здатності ефективно використовувати цифрові інструменти для створення цінності.

Еволюція стратегічних орієнтирів у традиційній та цифровій моделях. Зміна логіки стратегічного управління є закономірним результатом переходу від індустріальної до цифрової економіки. Цей перехід не зводиться до простого додавання нових технологій до існуючої моделі — він передбачає фундаментальне переосмислення самих стратегічних орієнтирів, їхнього змісту та способів реалізації. Для розуміння глибини цих змін необхідно порівняти трансформацію ключових стратегічних орієнтирів при переході до цифрової

моделі та визначити технології, що забезпечують цю трансформацію. Таблиця 1.8 систематизує цю еволюцію, демонструючи не просто зміну інструментів, а зміщення самої стратегічної логіки функціонування фінансових посередників.

Таблиця 1.8

**Еволюція стратегічних орієнтирів фінансових посередників
у традиційній та цифровій моделях**

Стратегічний орієнтир	Традиційна модель (до цифровізації)	Цифрова модель (в умовах цифрової економіки)	Цифрові технології, що забезпечують перехід
Управління ризиками	Реактивне, постфактум, статистичні моделі	Прогнозне, пов'язане з даними, real-time	AI/ML, DevSecOps, хмарні SOC, кіберзахист
Клієнтська цінність	Стандартизовані продукти, масовий підхід	Персоналізація, поведінкова аналітика, UX	Big Data, ML, Біометричний онбординг (biometric onboarding)
Інфраструктура	Закриті внутрішні системи	Платформи, API, модульність, хмара	Open Banking, Cloud (хмарні обчислення), мікросервіси
Інноваційність	Окремі нові продукти	Безперервний інноваційний цикл	FinTech-партнерства, RegTech
Масштабованість	Географічне розширення	Миттєве масштабування через хмару	Cloud, API
Довіра	Репутація, регуляторний контроль	Технологічна довіра, прозорі алгоритми	Біометрія, Blockchain, кіберстійкість
Фінансова інклюзія	Обмежена каналами обслуговування	Mobile-first (концепція цифрового дизайну), цифровий доступ, e-KYC	Цифрові платформи, мобільні сервіси

Джерело: розроблено на основі [46; 48; 49; 224; 22; 85; 113; 173; 184].

Аналіз трансформації стратегічних орієнтирів виявляє кілька фундаментальних зрушень у логіці управління фінансовими посередниками.

Управління ризиками зазнає радикальної трансформації від реактивного до проактивного підходу. Традиційна модель спиралася на статистичний аналіз минулих подій та постфактумне реагування на вже реалізовані ризики. Рішення ухвалювали на основі історичних даних, часто з значним запізненням. Цифрова модель принципово інша – вона базується на прогнозній аналітиці, обробці потоків даних у реальному часі, автоматизованому виявленні аномалій

до того, як вони переростуть у проблеми. Штучний інтелект та машинне навчання дозволяють виявляти приховані патерни ризиків, хмарні центри операційної безпеки забезпечують цілодобовий моніторинг, DevSecOps інтегрує безпеку в усі процеси розробки та експлуатації систем.

У площині *клієнтської цінності* спостерігається перехід від масового підходу до глибокої персоналізації. Раніше, як відомо, фінансові посередники пропонували стандартизовані продукти широким сегментам, виходячи з гіпотези про однорідність потреб. Однак цифрова економіка не лише робить можливим індивідуальний підхід, а й перетворює його на необхідну умову. Технології великих даних дають змогу накопичувати й аналізувати значні обсяги інформації про поведінку, уподобання та життєві обставини клієнтів. Алгоритми машинного навчання виявляють індивідуальні патерни та прогнозують запити. Біометрична ідентифікація суттєво спрощує онбординг — початок співпраці стає швидким і зручним. Увага до користувацького досвіду (UX) перетворюється з технічного питання дизайну на стратегічну конкурентну перевагу.

Що ж до *інфраструктурного орієнтира*, то тут відбувається радикальна трансформація: від закритих внутрішніх систем — до відкритих платформ. У традиційній моделі фінансовий посередник самотійно розробляв і контролював усі свої системи, які функціонували ізольовано. Цифрова модель натомість базується на відкритості. API забезпечують інтеграцію з партнерами, Відкритий банкінг (за згодою клієнта) відкриває доступ до даних стороннім провайдерам, хмарні технології дають гнучкість і масштабованість, а мікросервісна архітектура дозволяє змінювати окремі компоненти без перебудови всієї системи. Така конфігурація змінює саму логіку: фокус зміщується від внутрішньої самодостатності до екосистемної співпраці, тобто від конкуренції окремих установ до конкуренції цілих екосистем.

Характер інноваційної діяльності також зазнає змін. *Інноваційність* трансформується з епізодичної активності на безперервний процес. У традиційній моделі інновації являли собою окремі проекти — час від часу установа розробляла новий продукт або впроваджувала чергову технологію.

Цифрова реальність, однак, вимагає постійного інноваційного оновлення. Швидкість ринкових змін, поява нових технологій, еволюція клієнтських очікувань, конкуренція з боку фінтех-компаній — усе це перетворює інноваційність не на разову ініціативу, а на сталий режим повсякденної роботи. Партнерства з FinTech-компаніями дозволяють швидко інтегрувати нові рішення, а RegTech автоматизує дотримання регуляторних вимог, звільняючи ресурси власне для інновацій.

Не менш суттєво трансформується і саме поняття *масштабованості*. Раніше зростання фінансового посередника означало насамперед географічну експансію – відкриття нових відділень, вихід в інші регіони чи країни. Це був повільний і капіталомісткий процес. Цифрові технології, особливо хмарні платформи та API, дозволяють масштабуватися практично миттєво. Додатковий мільйон користувачів може бути обслужений без пропорційного зростання фізичної інфраструктури – потрібні лише обчислювальні потужності, які можна оперативно нарощувати. І це принципово змінює економіку зростання.

Окремо слід розглянути *довіру*, яка набуває нових форм і механізмів формування. Традиційно довіра будувалася на репутації установи, тривалості її присутності на ринку, розмірі капіталу, регуляторному нагляді. Ці фактори, безумовно, залишаються важливими, однак стають недостатніми. У цифровому середовищі виникає поняття технологічної (або алгоритмічної) довіри. Клієнти довіряють тоді, коли розуміють, як приймаються рішення про їхні фінанси, коли впевнені в захисті своїх даних, коли бачать стійкість систем до атак і збоїв. Біометрія робить аутентифікацію безпечною та зручною. Блокчейн забезпечує прозорість і незмінність записів. Кіберстійкість демонструє здатність протистояти загрозам. Прозорість алгоритмів, своєю чергою, дає змогу пояснити клієнту, чому система прийняла те чи інше рішення.

Ще один важливий зсув стосується *фінансової інклюзії*. Вона перетворюється із соціальної декларації на стратегічний пріоритет розширення ринків. У традиційній моделі обслуговування клієнтів обмежувалося наявністю фізичних каналів – відділень, банкоматів. Це

природно виключало з доступу населення віддалених регіонів, людей з обмеженою мобільністю, тих, для кого вартість відвідування відділення була надто високою. Цифрові платформи усувають ці бар'єри. Мобільні сервіси (mobile-first підхід) дозволяють отримувати послуги будь-де й будь-коли. Електронна ідентифікація (e-KYC) спрощує процес верифікації, роблячи його можливим дистанційно. У підсумку фінансова інклюзія стає не лише соціально відповідальною практикою, а й бізнес-можливістю — доступом до раніше неохоплених сегментів ринку.

Слід наголосити, що зазначені зміни не відбуваються ізольовано. Вони взаємопов'язані та взаємопідсилюють одна одну, що є принциповим для розуміння їхньої системної природи. Технологічна довіра підтримує інклюзію — люди готові користуватися цифровими послугами саме тоді, коли впевнені в їхній безпеці. Персоналізація, своєю чергою, підвищує клієнтську цінність, що додатково зміцнює довіру. Платформна інфраструктура створює можливості для безперервних інновацій, а ефективне управління ризиками в реальному часі дозволяє сміливіше експериментувати з новими моделями. Масштабованість через хмарні технології, до речі, робить інклюзію економічно доцільною.

Таким чином, стратегічний розвиток фінансових посередників у цифровій економіці відбувається не лінійно, а екосистемно. Технології визначають не лише операційну ефективність, а й самі стратегічні драйвери створення цінності. Установи, які розуміють цю логіку та здатні трансформувати свої стратегічні орієнтири відповідно до нових реалій, отримують конкурентні переваги. Ті ж, хто продовжує мислити категоріями індустріальної епохи, ризикують втратити релевантність у цифровому середовищі.

З огляду на вищенаведене, пропонуємо розглядати цифрові технології як цілісну систему, що формує нову стратегічну архітектуру фінансового посередництва. Узагальнене відображення цієї архітектури наведено на рисунку 1.4.

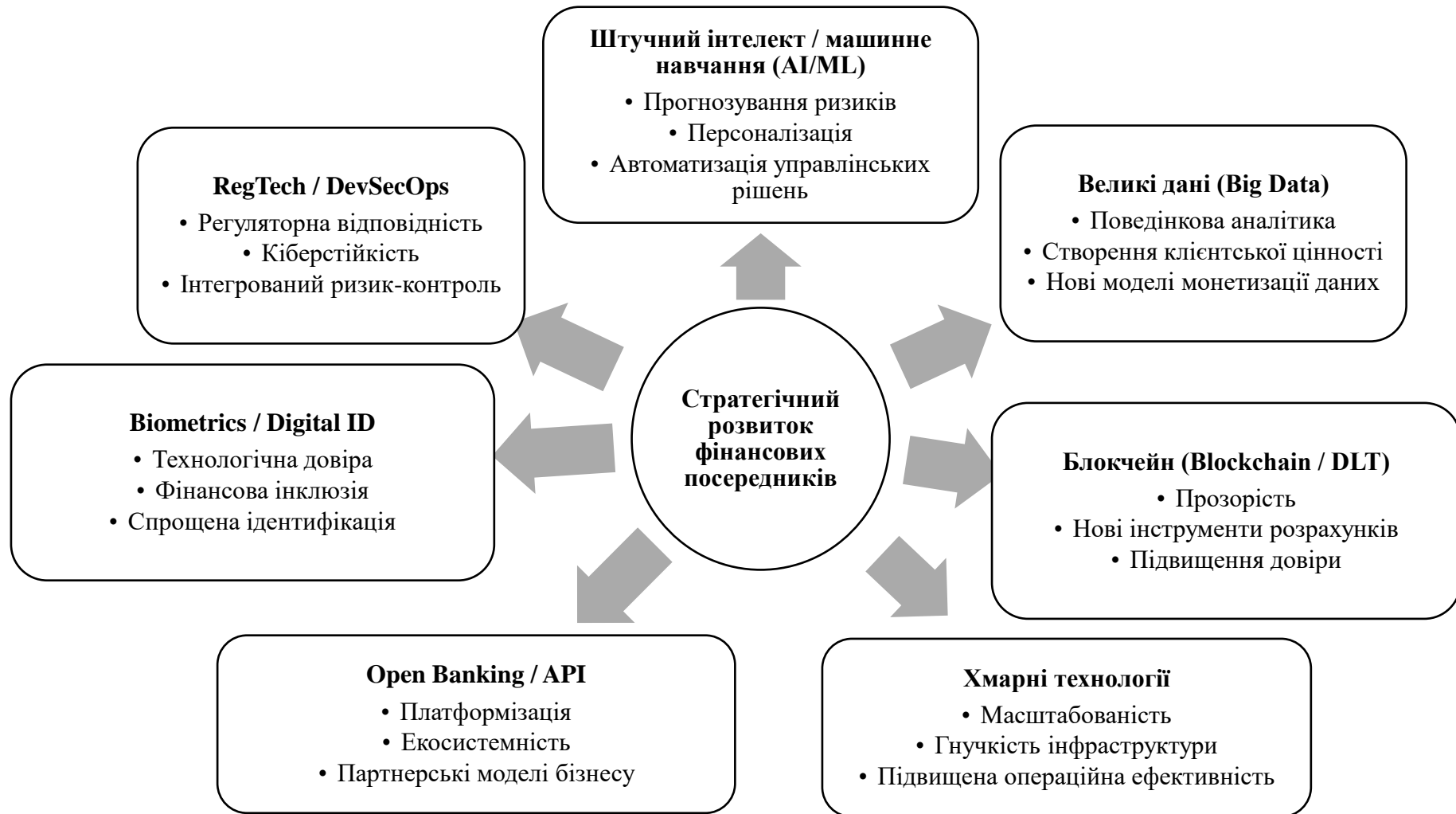


Рисунок 1.4 - Нова стратегічна архітектура фінансового посередництва: технологічні драйвери стратегічного розвитку фінансових посередників

Джерело: розроблено автором на основі [46; 48; 49; 224; 22; 85; 113; 184].

Із досліджених технологічних драйверів стратегічного розвитку фінансових посередників та рис. 1.4 можна зробити висновок, що вплив цифрових технологій на стратегічні орієнтири фінансових посередників має системний характер і проявляється в імперативах платформізації, екосистемності, алгоритмічної довіри, кіберстійкості, масштабованості через технології, операційної стійкості (рис. 1.5).

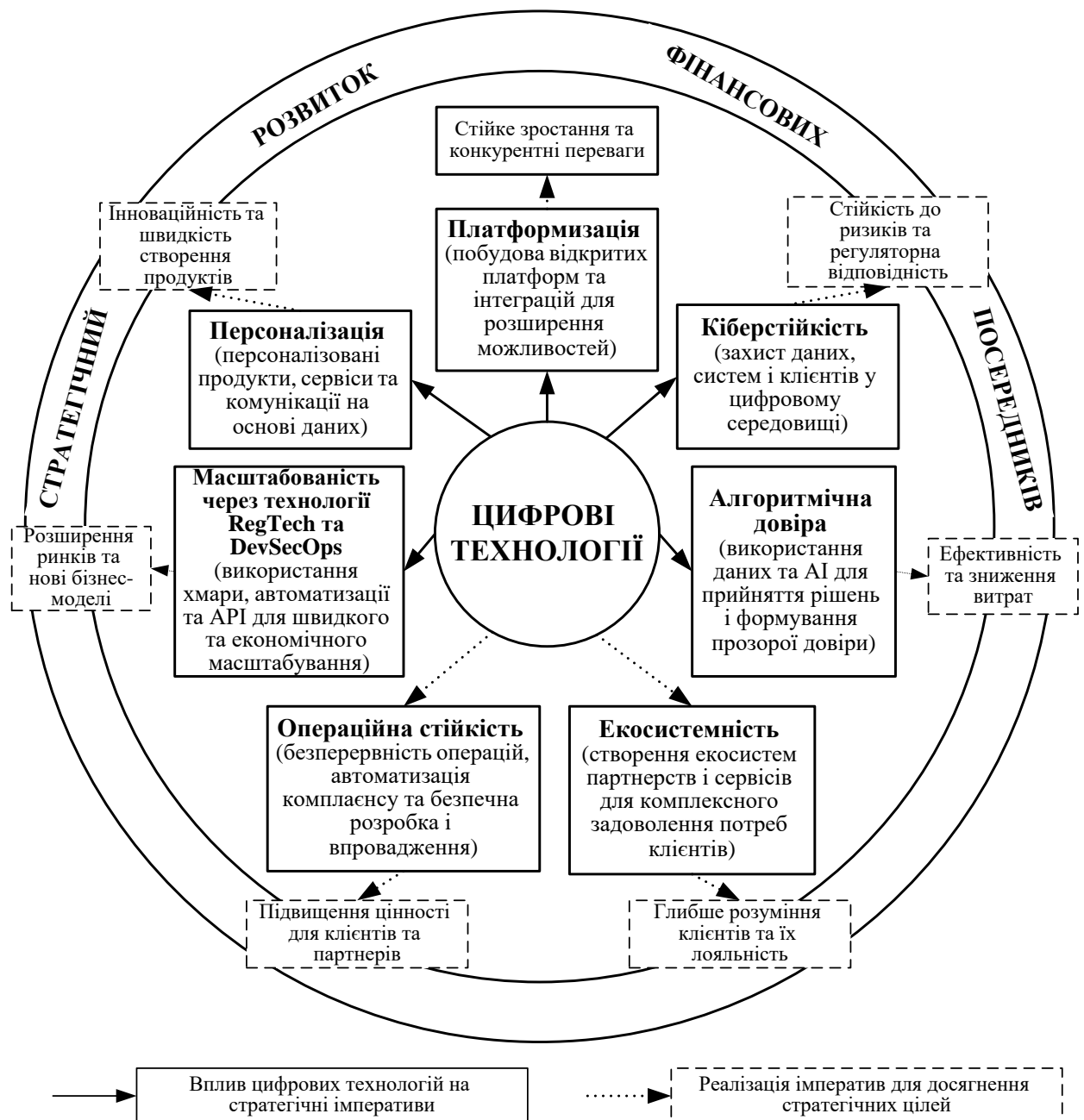


Рис. 1.5 – Системний вплив цифрових технологій на стратегічні орієнтири фінансових посередників

Джерело: розроблено автором на основі [161; 230].

Перелічені імперативи визначають траєкторію стратегічних рішень фінансових посередників і створюють підґрунтя для поглибленого аналізу та моделювання стратегічної архітектури цифрової трансформації.

Стрімкий розвиток цифрових технологій формує нову конкурентну динаміку фінансового сектору й зумовлює необхідність перегляду стратегічних орієнтирів фінансових посередників. Як показують дослідження, цифровізація впливає одночасно на бізнес-моделі, внутрішні процеси, клієнтську взаємодію та інноваційну спроможність фінансових установ. У раніше опублікованій статті «Аналіз ролі фінансових посередників у процесі формування інноваційної інфраструктури ринку цифрових фінансових послуг» ми наголошували, що фінансові посередники «стають не лише каналами перерозподілу ресурсів, а й платформами інновацій, що забезпечують доступ до фінансових послуг через цифрові канали, автоматизовані сервіси, штучний інтелект, блокчейн» [174]. На наш погляд, сутність фінансових інновацій у цифровій економіці найповніше описують нові або вдосконалені продукти, процеси, механізми, моделі взаємодії та інфраструктурні рішення, що створюються на основі цифрових технологій і змінюють способи здійснення фінансових операцій, управління ризиками та створення доданої вартості.

Запропоноване авторське визначення фінансових інновацій ґрунтується на двох основних характеристиках: технологічній залежності та результаті синергії. Перша з них, тобто технологічна залежність, уже докладно описана у вищенаведених дослідженнях. Що ж до синергії, то тут варто пояснити детальніше.

Сучасні інновації, на відміну від інновацій минулих десятиліть, є результатом синергії одразу кількох технологічних складових: штучного інтелекту, великих даних, хмарної інфраструктури, API-економіки, розподілених реєстрів, біометричної ідентифікації та автоматизованого комплаєнсу (RegTech). Такі інновації не просто змінюють продуктову лінійку. Вони визначають стратегічні напрями розвитку фінансової установи, ставлячи

її перед принциповими виборами: платформа чи традиційний банк? екосистема чи вертикально інтегрована модель? клієнтська цінність чи операційна ефективність? прогнозний ризик-менеджмент чи реактивний контроль? Саме тому, на наше переконання, інновації в умовах цифрової економіки варто розглядати як архітектурний чинник, що перебудовує інституційну роль фінансових посередників.

Опираючись на сучасні підходи (OECD, BIS, World Bank), а також на авторські публікації, вважаємо за доцільне виділити п'ять ключових груп фінансових інновацій, які визначають стратегічні можливості фінансових посередників. Їх систематизовано в таблиці 1.9.

Таблиця 1.9

**Класифікація фінансових інновацій та їх стратегічний вплив
на розвиток фінансових посередників**

Група фінансових інновацій	Зміст / приклади інновацій	Стратегічний ефект для фінансових посередників
1	2	3
1. Продуктові інновації	<ul style="list-style-type: none"> – цифрові гаманці; – миттєві перекази; – інноваційні кредитні продукти; – цифрові інвестиційні платформи; – страхові продукти; – токенизовані активи. 	<ul style="list-style-type: none"> – вихід на нові ринкові сегменти; – підвищення клієнтської залученості; – зміцнення конкурентних позицій; – створення нової продуктової цінності.
2. Процесні інновації	<ul style="list-style-type: none"> – роботизована автоматизація процесів (RPA); – машинне навчання для прийняття рішень; – цифровий KYC/AML; – біометричний онбординг; – архітектури DevSecOps та Zero Trust. 	<ul style="list-style-type: none"> – зниження операційних витрат; – прискорення обробки операцій; – підвищення точності та прозорості внутрішніх процесів; – зменшення операційних та кіберризиків; – підвищення операційної стійкості.
3. Інновації бізнес-моделей	<ul style="list-style-type: none"> – модель bank-as-a-platform (BaaP); – модель bank-as-a-service (BaaS); – відкритий банкінг (Open Banking) та API-монетизація; – фінансові екосистеми; – цифрові суперагрегатори. 	<ul style="list-style-type: none"> – перехід від конкуренції між установами до конкуренції між екосистемами; – формування партнерських моделей; – отримання нових джерел доходу через API та сервісні моделі; – масштабування без фізичної інфраструктури.

Закінчення таблиці 1.9

1	2	3
4. Інфраструктурні інновації	<ul style="list-style-type: none"> – системи миттєвих платежів; – хмарні процесингові центри; – технології розподілених реєстрів (DLT); – цифрові платформи ідентифікації; – інноваційні рішення у клірингу та розрахунках. 	<ul style="list-style-type: none"> – збільшення масштабованості та гнучкості; – формування нової цифрової фінансової інфраструктури; – підвищення стійкості та швидкості операцій; – зміцнення інституційної взаємодії на ринку.
5. Інновації довіри	<ul style="list-style-type: none"> – біометрична ідентифікація; – поведінкові моделі безпеки; – прозорість на основі DLT; – алгоритмічна довіра; – системи управління даними 	<ul style="list-style-type: none"> – формування технологічної довіри клієнтів; – посилення кіберстійкості; – зниження ризику шахрайства; – підвищення репутаційної надійності; – підтримка цифрових каналів обслуговування.

Джерело: розроблено автором на основі [55; 224; 147; 157; 22; 85; 113; 174; 221; 222].

Аналіз фінансових інновацій, систематизований у таблиці 1.9, дає змогу виокремити їхню системну роль у формуванні сучасних стратегічних моделей розвитку фінансових посередників.

Розгляньмо спочатку **продуктові інновації**. Вони забезпечують переорієнтацію діяльності фінансових установ на створення нової клієнтської цінності та вихід на раніше недоступні сегменти ринку. Поширення токенизованих активів, страхових технологічних рішень (InsurTech), цифрових гаманців і миттєвих переказів демонструє зростання попиту на швидкі, персоналізовані та технологічно зручні продукти. І це стає ключовим чинником конкурентної боротьби в цифровому середовищі.

Процесні інновації суттєво трансформують внутрішню логіку функціонування фінансових посередників. Роботизована автоматизація процесів, машинне навчання, цифрові модулі KYC/AML, біометричний онбординг і сучасні підходи до кіберзахисту (DevSecOps, Zero Trust) формують новий стандарт операційної ефективності. У підсумку це забезпечує скорочення витрат, автоматизацію рутинних операцій, підвищення точності управлінських рішень і зниження операційних ризиків.

Стратегічний зсув від вертикально інтегрованих установ до платформних структур демонструють *інновації бізнес-моделей* (ВааР, ВааS, відкритий банкінг, фінансові екосистеми та суперагрегатори). У такій конфігурації ключовим ресурсом стають дані, партнерські взаємодії та мережеві ефекти. Конкуренція між окремими установами, до речі, замінюється конкуренцією між екосистемами. Це у свою чергу вимагає від фінансових посередників розвитку інтеграційних компетентностей та API-інфраструктури.

Інфраструктурні інновації створюють основу для масштабування цифрових фінансових послуг. Яку саме основу? Технології миттєвих платежів, хмарні процесингові центри, розподілені реєстри, цифрові ідентифікаційні платформи — усі вони забезпечують новий рівень швидкості, стійкості, взаємодії між суб'єктами ринку. Так формується оновлена цифрова інфраструктура. Інфраструктура, яка дозволяє фінансовим посередникам інтегрувати інновації не в дискретні моменти, а в режимі реального часу. Щоправда, на практиці цей процес часто гальмується через інерційність наявних систем — але саме тут і виникає поле для подальших досліджень.

Окремої уваги потребують інновації довіри. Їхня роль зростає. Причина — цифрова трансформація суттєво підвищує вимоги до безпеки та прозорості. Біометрична ідентифікація, поведінкові моделі безпеки, прозорість даних на основі DLT, алгоритмічна довіра, системи управління даними — ці елементи разом формують нову архітектуру технологічної довіри. Без цієї архітектури, як свідчить аналіз, стає функціонування цифрових фінансових посередників видається неможливим. Принаймні так впливає з наявних емпіричних спостережень, хоча остаточних підтверджень бракує.

Узагальнюючи, можна стверджувати, що фінансові інновації не є ізольованими явищами. Вони формують цілісну інноваційну екосистему, у межах якої цифрові технології, бізнес-моделі, інфраструктурні рішення та механізми забезпечення довіри взаємодіють між собою. Саме ця системність, на наш погляд, визначає стратегічні орієнтири розвитку фінансових посередників у цифровій економіці, забезпечуючи їхню здатність адаптуватися до технологічних змін і підвищувати конкурентоспроможність на глобалізованому ринку.

Фінансові інновації суттєво змінюють стратегічні моделі розвитку, формуючи нову логіку ринкової поведінки та організаційної побудови. Одним із найважливіших наслідків цифрової трансформації є перехід від традиційних лінійних бізнес-моделей до *екосистемного підходу*. У межах цього підходу фінансові установи перетворюються на інтеграторів сервісів, провайдерів даних і вузлові хаби взаємодії між клієнтами, партнерами та сторонніми постачальниками фінансових і нефінансових послуг. Така зміна архітектури зумовлюється розвитком відкритого банкінгу, API-інтеграцій, цифрової ідентифікації та стандартизованих протоколів обміну даними. І це, своєю чергою, потребує від фінансових посередників нових компетентностей – управління платформами, мережевими взаємодіями та партнерськими моделями.

У межах цифрової конкурентної боротьби інноваційні рішення визначають не тільки змістовне наповнення пропозиції фінансових інституцій, але й динаміку їхнього стратегічного поступу. Використання хмарних обчислювальних архітектур, мікросервісних моделей, підходів DevSecOps, а також автоматизованих засобів тестування уможлиблює для фінансових установ безперервне вдосконалення продуктів і бізнес-процесів. На сучасному етапі конкурентні переваги фінансових посередників формуються передусім під впливом їхньої спроможності до швидкої адаптації, інтенсивного впровадження новацій та оперативного реагування на зміни ринкового середовища. При цьому такі чинники, як розмір організації або її усталена історично інфраструктура, втрачають колишнє значення. Отже, параметрами, що визначають конкурентоспроможність у цифровому просторі, стають передусім швидкість операційних змін та гнучкість управлінських рішень. Зазначений результат цифрової трансформації належить до категорії найбільш очевидних, проте водночас найбільш складних для практичної реалізації.

Цифровізація докорінно трансформує й *клієнтоцентричний вимір стратегії*. Великі дані, аналітика поведінкових моделей, мобільні платформи, інклюзивні цифрові сервіси – їхнє використання забезпечує можливість

точного прогнозування потреб клієнтів. А також персоналізації продуктів, покращення користувацького досвіду, формування довгострокової лояльності. Біометричний онбординг спрощує та прискорює доступ до послуг. Поведінкова аналітика дозволяє зменшувати відтік клієнтів і підвищувати їхню залученість. Підсумуємо: стратегічний акцент зміщується на побудову довготривалої цінності відносин із клієнтом, управління його життєвим циклом, формування довіри через прозорі й безпечні цифрові механізми. *Щоправда, на практиці реалізація цього підходу часто наштовхується на внутрішньоорганізаційні бар'єри – але це вже питання окремого дослідження.*

Важливою складовою стратегічного розвитку стає **інноваційне переосмислення ризик-менеджменту**. Технологічні рішення – автоматизовані системи AML/CTF, прогнозні моделі машинного навчання, поведінкова аналітика для виявлення шахрайства, центри моніторингу безпеки (SOC), а також концепція Zero Trust – формують нову архітектуру управління ризиками. У цій архітектурі ризик-менеджмент виходить за межі традиційного контролю. Він стає динамічним, технологічно керованим процесом, який інтегрується в усі етапи функціонування фінансового посередника.

Окремого значення набувають інновації, спрямовані на фінансову **інклюзію та розширення доступу** до послуг. Простота мобільних платежів, доступність цифрових гаманців, спрощені процедури верифікації клієнтів, розвиток мікрострахування та мікрокредитування – усі ці чинники поступово змінюють статус інклюзії. Вона перетворюється із соціального завдання на важливий інструмент стратегічного зростання. У цифровій економіці розширення доступу сприяє масштабуванню бізнесу, збільшенню клієнтської бази та формуванню сталих потоків доходів.

Узагальнюючи вплив фінансових інновацій, доцільно виділити чотири взаємопов'язані рівні їх участі у формуванні стратегічної моделі розвитку (рис. 1.6).

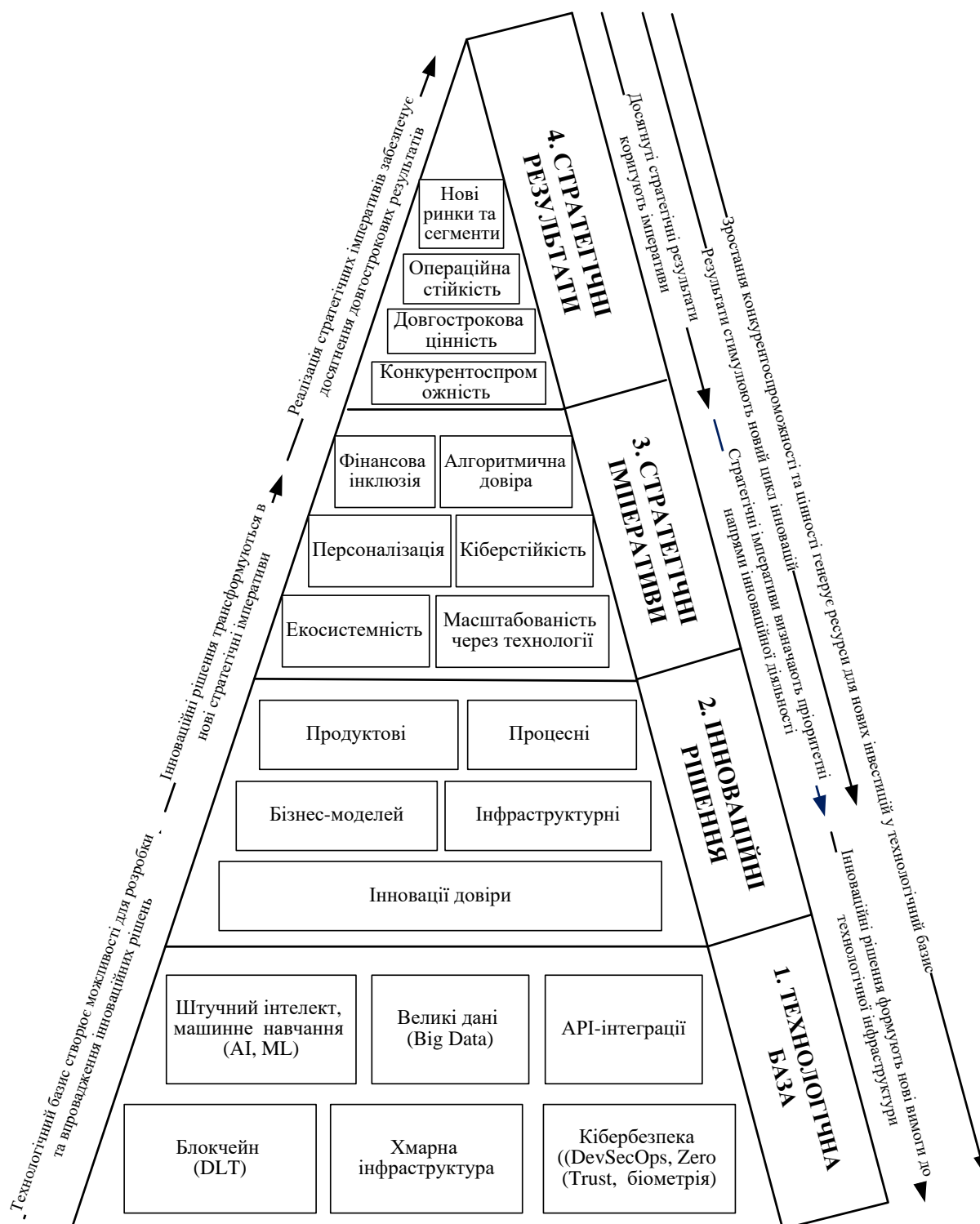


Рис 1.6. Архітектура стратегічного управління розвитком фінансових посередників під впливом цифрових технологій та фінансових інновацій

Джерело: розроблено автором.

Перший рівень – технологічна база: штучний інтелект, великі дані, API-інтеграції, технології розподілених реєстрів, хмарна інфраструктура та сучасні методи безпеки. *Другий* – охоплює інноваційні рішення – продуктові, процесні, бізнес-моделі та інфраструктурні зміни, які виникають на основі цих технологій. *Третій* – формують стратегічні імперативи – екосистемність, довіра, інклюзія, персоналізація та кіберстійкість, що визначають нову логіку діяльності. *Четвертий* – складають стратегічні результати: зростання конкурентоспроможності, підвищення операційної стійкості, освоєння нових ринків та створення довгострокової цінності.

Таким чином, фінансові інновації в умовах цифрової економіки трансформують фінансове посередництво на всіх рівнях – від технологічної основи й продуктового наповнення до організації бізнес-моделей та стратегічної логіки розвитку. Стратегія фінансових посередників у новому середовищі має спиратися на дані, цифрові платформи, кіберстійкість, довіру та здатність до партнерської взаємодії. Саме це, на наше переконання, забезпечує їхню адаптивність і динамічність у глобально конкурентному фінансовому просторі.

1.3. Імперативи довіри та кібербезпеки в системі стратегічних викликів цифровізації фінансового сектору

У контексті цифрової трансформації фінансові посередники стають центральними суб'єктами, на яких фокусується суттєва зміна структури ризиків. У межах цієї структури кіберзагрози набувають статусу не лише технічного, але й стратегічного чинника, що визначає подальший розвиток цих інституцій. Інтенсивне впровадження цифрових сервісів, дистанційних каналів обслуговування, мобільних платформ, API-інтеграцій та хмарних архітектур істотно збільшує технологічну поверхню для потенційних атак, унаслідок чого фінансові установи стають одними з найбільш привабливих

цілей для кіберзлочинців. У попередніх авторських роботах, присвячених аналізу сучасних типів кіберзагроз, зазначається, що рівень складності та частота таких атак зростають відповідно до ступеня цифровізації, а діапазон використовуваних методів – від методів соціальної інженерії до складних технологічних вторгнень – систематично розширюється [224].

Сучасні фінансові установи зазнають впливу сукупності взаємопов'язаних ризиків, серед яких особливу значущість мають фішингові кампанії, DDoS-атаки, шкідливе програмне забезпечення, атаки на мобільні додатки, внутрішні загрози та спроби несанкціонованого доступу до ІТ-інфраструктури. На поточному етапі фішинг зберігає позицію одного з найпоширеніших інструментів первинного проникнення, оскільки поєднує технічні методи із впливом на поведінку клієнтів та персоналу [224]. Для організацій, які активно розвивають мобільні фінансові сервіси, найбільш небезпечними є атаки на мобільні API, а також використання підроблених застосунків, здатних забезпечувати викрадення автентифікаційних даних та перехоплення фінансових транзакцій.

Особливо небезпечними є DDoS-атаки, що здатні паралізувати платіжні сервіси та порушити доступність критичних функцій фінансової інфраструктури. У авторській статті, яка присвячена інноваційній інфраструктурі ринку цифрових фінансових послуг, відзначено, що безперервність функціонування процесингових центрів і платіжних шлюзів є ключовою умовою стабільності фінансової системи, а масовані атаки можуть спричинити системні збої та репутаційні втрати [174].

Цифрова трансформація водночас підвищує рівень внутрішніх ризиків. У попередніх наукових роботах зазначається, що навмисні дії персоналу або необережність при обробці чутливих даних можуть призводити до наслідків, співставних із впливом зовнішніх кібератак. Наявність доступу до конфіденційної інформації, потенціал несанкціонованого втручання в бази

даних або використання службових привілеїв формують складний спектр операційних і репутаційних загроз.

Характерною ознакою цифрової економіки виступає перетворення кіберзагроз на системний ризик, що поширюється не лише на окремі установи, але й на взаємопов'язані складові фінансової інфраструктури. Дане твердження набуває особливої актуальності в контексті відкритого банкінгу та екосистемних бізнес-моделей: кожна нова API-інтеграція підвищує залежність від сторонніх технологічних провайдерів і одночасно збільшує ймовірність компрометації даних.

Це підтверджує положення, викладені у проведених авторських дослідженнях щодо цифровізації як чинника конкурентоспроможності. Доведено, що конкурентні переваги фінансових посередників дедалі більше визначаються їхньою спроможністю забезпечувати стійкість і безпеку власних цифрових платформ.

Водночас кіберзагрози впливають на стратегічну поведінку фінансових посередників, змінюючи підхід до управління ризиками. Ризик-менеджмент більше не може залишатися реактивною системою контролю; він перетворюється на інноваційну функцію, інтегровану в архітектуру цифрового бізнесу. Вимоги до захисту даних, поведінкового моніторингу, прогнозування шахрайства та автоматизації процесів AML/CTF стають новими стандартами ринку. В авторській публікації про етичні виклики цифровізації було доведено, що питання довіри безпосередньо пов'язане з ефективністю кіберзахисту: порушення цілісності або конфіденційності даних не лише знижує операційну стійкість, а й підриває фундаментальний соціальний капітал фінансових посередників.

У цілому кіберзагрози формують новий стратегічний контекст діяльності фінансових посередників. Вони впливають на структуру бізнес-моделей, визначають потребу в інвестиціях у технологічну інфраструктуру, зумовлюють модернізацію управлінських процесів і сприяють переосмисленню ролі

фінансових установ у цифровій економіці. Водночас зростає відповідальність самих посередників за формування безпечного цифрового середовища, що вимагає від них не лише технічних рішень, а й розвитку інституційної культури кіберстійкості та прозорого управління довірою.

З метою впорядкування зазначених явищ необхідно побудувати системну класифікацію кіберзагроз, оскільки цифрове середовище діяльності фінансових посередників вирізняється значною динамікою, неоднорідністю та багатовимірністю притаманних йому ризиків. Відсутність чіткої структуризації перешкоджає своєчасному виявленню загроз, їхньому прогнозуванню та вбудовуванню в наявні моделі ризик-менеджменту. Належним чином розроблена класифікація дає змогу не тільки ідентифікувати основні категорії загроз, але й досягнути їхню сутність, канали проникнення, уразливі елементи інфраструктури та можливі стратегічні наслідки. Отже, узагальнення й типологізація кіберзагроз набувають першочергового значення для створення дієвої системи кіберстійкості, планування захисних заходів і розробки адаптивних стратегій розвитку фінансових посередників.

З огляду на це, запропоновано систематизований підхід до класифікації найбільш поширених кіберзагроз, що є характерними для цифрової діяльності фінансового сектору (таблиця 1.10).

Кожна із зазначених загроз справляє багатоаспектний вплив на діяльність фінансових посередників, видозмінюючи їхню поведінку у сфері ризику, операційну логіку та систему стратегічних пріоритетів. Під дією цифровізації ризик-менеджмент зазнає переходу від реактивної до проактивної парадигми, у межах якої вирішальну роль виконують прогностичні технології, засоби поведінкової аналітики та автоматизовані системи моніторингу.

Класифікація кіберзагроз фінансових посередників та їх характеристика

Тип кіберзагрози	Стисло про сутність загрози	Особливості прояву у фінансових установах	Найбільш вразливі фінансові посередники	Стратегічні наслідки
Фішингові атаки	Маніпуляція користувачем	Отримання доступу до рахунків, підміна застосунків	Мобільні банки, платіжні сервіси	Втрата довіри, шахрайство
DDoS-атаки	Перевантаження сервісів	Недоступність онлайн-банкінгу, процесингу	Банки, еквайринг, процесингові центри	Порушення безперервності
Рансомвер	Блокування даних	Параліч операцій, шифрування баз	Банки, страхові, депозитарії	Зупинка діяльності
Вразливості API	Недостатній захист інтеграцій	Виток даних, фальсифікація транзакцій	Учасники Open Banking	Системні ризики
Інсайдери	Несанкціоновані дії персоналу	Витоки, маніпуляції	Банки, інвесткомпанії	Репутаційні втрати
Мобільні загрози	Підроблені застосунки	Перехоплення транзакцій	Neobank, фінтехи	Зростання фроду
Кібершпигунство	Викрадення чутливих даних	Доступ до стратегічної інформації	Інвесткомпанії, банки	Стратегічні збитки
Витоки даних	Компрометація баз	Масові порушення конфіденційності	Кредитні бюро, банки	Санкції, падіння довіри

Джерело: розроблено автором на основі [122].

Кіберзагрози доцільно інтерпретувати не тільки як технічні або операційні явища, а як чинники, що задають стратегічні рамки функціонування фінансових посередників в умовах цифрової економіки. Їхня дія охоплює фундаментальні функції фінансового посередництва, а саме: управління ризиками, підтримання довіри з боку контрагентів, забезпечення безперервності надання сервісів та збереження конкурентних позицій на ринку. Зростання рівня складності, варіабельності та непередбачуваності кіберінцидентів суттєво ускладнює процедури моніторингу, раннього виявлення та блокування загроз. Підвищеної уваги вимагають ті загрози, які здатні еволюціонувати у системні ризики та порушувати стабільність критичної фінансової інфраструктури.

У зазначеному контексті класифікація кіберзагроз набуває визначального значення, оскільки забезпечує структурований опис різновидів небезпек, конфігурації їхнього поширення, рівнів реалізації атак, імовірності настання та потенційного масштабу втрат. Подібна систематизація є необхідною як для теоретичного осмислення феномену цифрових загроз, так і для вирішення практичних завдань, зокрема розробки комплексних моделей ризик-менеджменту, адаптації систем кіберзахисту, оптимізації процедур реагування на інциденти, визначення пріоритетних напрямів інвестування у безпекові технології та формування регуляторних стандартів.

Систематизація кіберзагроз дає змогу виокремити ті з них, які становлять критичну значущість для фінансових посередників, провести ранжування загроз за ступенем впливу, а також ідентифікувати найбільш уразливі елементи цифрової інфраструктури — від API-інтеграцій і мобільних платформ до внутрішніх процедур управління доступом. Це створює підґрунтя для формування цілісної моделі кіберстійкості, яка інтегрує технологічні, організаційні, кадрові та інституційні складові.

Узагальнення викладених положень дозволяє представити ключові групи кіберзагроз, їхні характеристики та стратегічні наслідки в систематизованому вигляді, що наведено в таблиці 1.11.

Кіберзагрози у фінансовому секторі не можна трактувати виключно як набір окремих технічних інцидентів — вони утворюють багаторівневу та взаємозалежну систему ризиків, що виникає на перетині поведінкових, технологічних, організаційних та інституційних чинників. Така багатовимірність зумовлена тим, що цифровізація фінансових послуг базується на тісній інтеграції клієнтських інтерфейсів, внутрішніх бізнес-процесів та інфраструктурних компонентів із зовнішніми технологічними платформами, а також регуляторними вимогами. Внаслідок цього будь-яка вразливість, що виникає на одному рівні, здатна поширюватися і продукувати ефект ланцюгової реакції, впливаючи на інші елементи фінансової екосистеми.

**Взаємозв'язок між кіберзагрозами
та ключовими функціями фінансових посередників**

Кіберзагроза	Вплив на управління ризиками	Вплив на довіру та репутацію	Вплив на операційну стійкість	Стратегічні відповіді
Фішинг	Ускладнює детекцію фроду.	Зниження довіри	Низький прямий вплив	MFA, цифрова освіта
DDoS	Підвищує значення моніторингу	Негативне сприйняття сервісу	Високий вплив	Митигатори, резервні канали
Ransomware	Порушує цілісність даних	Негативний імідж	Зупинка операцій	Zero Trust, резервування
Інсайдери	Непередбачувані дії	Репутаційні ризики	Середній вплив	Контроль доступів
API-загрози	Формують нові ризики	Сумніви щодо open banking	Системні наслідки	Тестування API
Мобільні загрози	Зростання фроду	Низька довіра до мобільних сервісів	Обмежений вплив	Mobile DevSecOps

Джерело: розроблено автором на основі [39; 224; 27; 45; 111; 156; 205; 207; 236].

На *рівні клієнтської взаємодії* загрози зумовлені поширенням мобільних каналів, цифрових гарантів та дистанційних сервісів, що робить атаки, засновані на поведінкових паттернах і методах соціальної інженерії, надзвичайно результативними. Недостатній рівень цифрової грамотності окремих груп користувачів, а також збільшення кількості підроблених застосунків і фішингових кампаній створюють вразливості, які активно використовуються кіберзлочинцями. Відповідно, клієнтський рівень нерідко виступає точкою первинного проникнення для атак, які згодом трансформуються у технологічні та організаційні ризики.

На *технологічному рівні* загрози виникають внаслідок складності цифрових архітектур, які охоплюють мобільні платформи, хмарні сервіси, API-інтеграції, модулі штучного інтелекту та системи обробки великих масивів даних. Уразливість будь-якого з цих компонентів здатна спричинити витік інформації, порушення доступності сервісів або компрометацію транзакцій. Особливе місце посідає відкритий банкінг (open banking), де розширення

зовнішніх інтеграцій підвищує ймовірність атаки через API або через третіх постачальників технологій. Отже, технологічний рівень загроз є найбільш технічно складним і часто найнебезпечнішим з огляду на системні наслідки.

На *організаційному рівні* кіберзагрози реалізуються у формі інсайдерських ризиків, недосконалості внутрішніх регламентів доступу до даних, помилкового налаштування політик безпеки або внаслідок дії людського чинника. В умовах цифровізації внутрішні загрози здатні бути не менш небезпечними, ніж зовнішні, оскільки персонал володіє прямим доступом до критичних систем. Будь-які вади у процесах контролю доступу, аутентифікації, аудиту дій користувачів або сегментації даних істотно підвищують ймовірність реалізації внутрішніх кібератак, а також випадкових порушень.

На *інституційному рівні* ризики формуються внаслідок нерівномірності розвитку нормативно-правової бази, технологічної фрагментарності інфраструктури та відсутності уніфікованих стандартів щодо безпеки API, хмарних сервісів і нових фінансових платформ. Фінансові ринки різних країн можуть демонструвати неоднаковий рівень готовності до цифрових загроз, що створює передумови для транскордонних інцидентів або системних проблем у межах транзакційної інфраструктури. Інституційні прогалини підсилюють масштаб наслідків кіберінцидентів та ускладнюють координацію дій між фінансовими установами, регуляторними органами й технологічними провайдерами.

Таким чином, кіберзагрози постають як *багаторівнева система взаємозалежних ризиків*, що формується під впливом як технічних, так і поведінкових та організаційних факторів. Усвідомлення цієї багатовимірності є ключовим для побудови ефективної моделі кіберстійкості фінансових посередників, яка має охоплювати всі рівні – від клієнтського до інституційного (рис. 1.7).

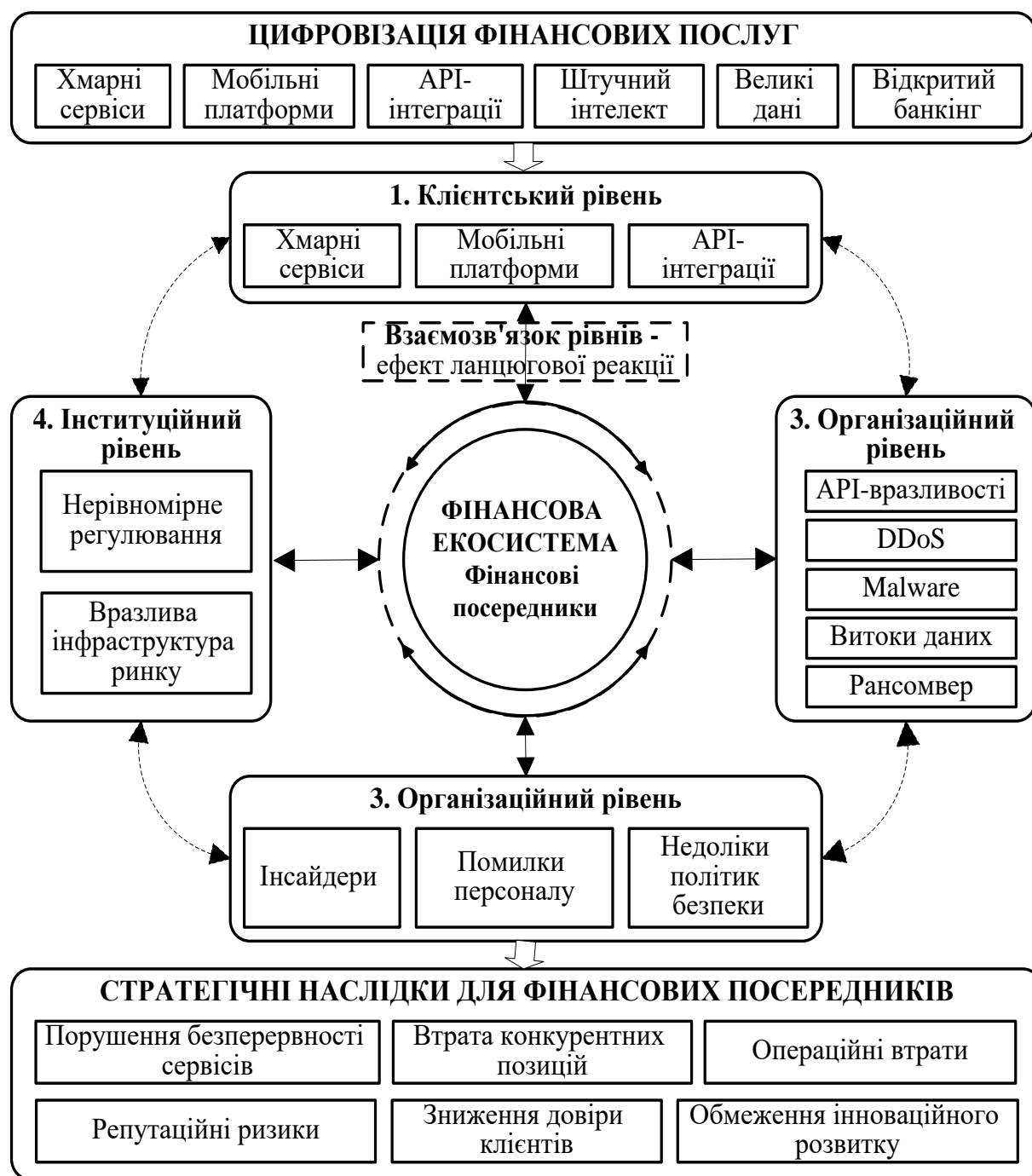


Рис. 1.7. Архітектура кіберзагроз фінансових посередників

Джерело: розроблено автором на основі [7; 18; 27; 39; 59; 122; 206; 222].

Узагальнюючи наведений аналіз, можна стверджувати, що кіберзагрози у діяльності фінансових посередників формують не лише багаторівневу структуру ризиків, а й цілісний механізм впливу на стратегічну динаміку ринку фінансових послуг.

На кожному з рівнів – клієнтському, технологічному, організаційному та інституційному – ці загрози породжують специфічні типи вразливостей, які, взаємодіючи між собою, здатні трансформуватися у комплексні операційні інциденти. Водночас ефект таких інцидентів не обмежується технічними збоями. Він поширюється на ключові елементи стратегічної моделі фінансових посередників: безперервність сервісів, стабільність бізнес-процесів, поведінку клієнтів, рівень довіри, конкурентні позиції та здатність до інноваційного розвитку.

Саме тому важливо простежити, яким чином кіберзагроза, будучи первинним чинником, запускає ланцюг подій, що може призвести до серйозних довгострокових наслідків для фінансової установи. Механізм цього переходу включає кілька послідовних фаз: виникнення або проникнення загрози; реалізацію інциденту у вигляді порушення цілісності, доступності чи конфіденційності даних; порушення операційної безперервності; зміну поведінки клієнтів та партнерів; зниження рівня довіри; переформатування конкурентних позицій; і, зрештою, потребу у стратегічному перегляді бізнес-моделі або модернізації інфраструктури.

На практиці цей механізм уже підтверджено багатьма кейсами у міжнародному фінансовому секторі, коли здавалося б обмежена технічна вразливість призводила до значних репутаційних втрат, регуляторних санкцій або відтоку клієнтів. У наших попередніх дослідженнях також підкреслено, що цифрова економіка робить фінансових посередників надзвичайно чутливими до таких інцидентів, оскільки рівень довіри є одним з основних ресурсів їхньої діяльності, а якість та доступність цифрових сервісів – ключовим компонентом конкурентної стратегії.

Нами розроблена структурна схема, яка демонструє логіку трансформації кіберзагрози у стратегічний виклик представлена на рис. 1.8.

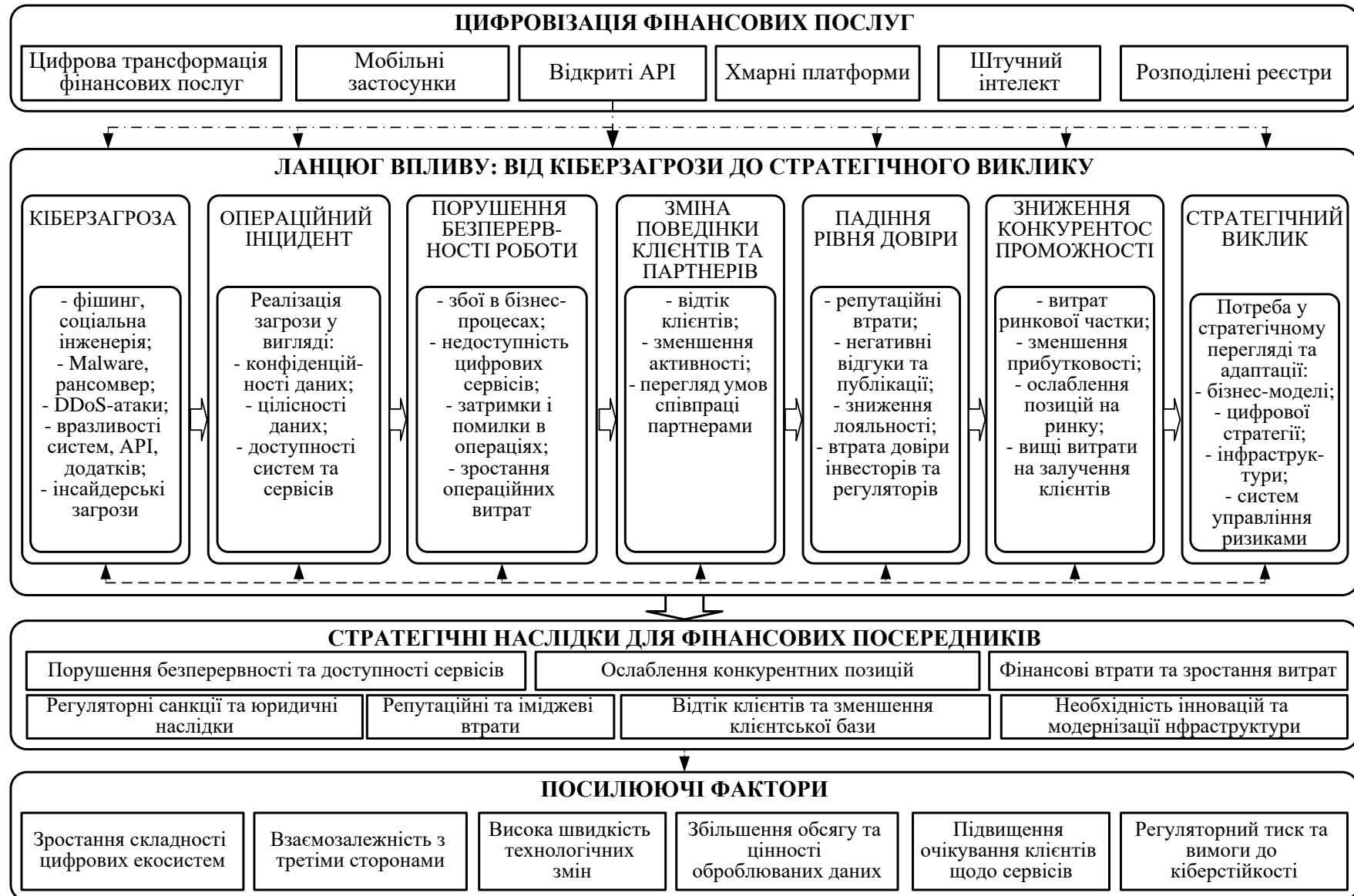


Рис. 1.8. Логіка впливу кіберзагроз на стратегічну модель фінансового посередництва
 Джерело: авторська розробка на основі [7; 11; 18; 39; 57; 59; 122; 222].

Поглиблений аналіз взаємозв'язку між кіберзагрозою, відповідним інцидентом і його стратегічними наслідками дозволяє дійти висновку, що цифрова трансформація не лише розширює операційні можливості фінансових посередників, але й опосередковано ініціює появу нових видів небезпек, підсилюючи їхню інтенсивність і масштаб. Упровадження інноваційних технологій – зокрема мобільних додатків, відкритих програмних інтерфейсів, хмарних обчислювальних платформ, систем штучного інтелекту та розподілених реєстрів – формує якісно новий технологічний ландшафт, у межах якого безпека перестає виконувати суто сервісну функцію та набуває статусу фундаментальної передумови стратегічної спроможності організації.

Цифровим інноваціям притаманний дуалістичний характер: вони водночас створюють конкурентні переваги та породжують нові вразливості. Кожне технічне рішення, кожна інтеграція з платіжними, страховими, інвестиційними системами або платформами електронної комерції відкриває додаткові шляхи для потенційного зловмисного вторгнення.

У цьому контексті технологічний прогрес і сучасний ризиковий ландшафт еволюціонують синхронно, а в окремих випадках — взаємно прискорюють один одного. Так, упровадження концепції відкритого банкінгу стимулює розвиток інноваційних фінансових сервісів, однак водночас формує залежність від зовнішніх постачальників, рівень безпеки яких може бути нижчим за галузеві стандарти. Використання методів штучного інтелекту підвищує точність виявлення шахрайських операцій, але паралельно підвищує чутливість систем до атак на використовувані моделі або до маніпулятивних впливів на навчальні вибірки даних.

Зростання кількості API-інтеграцій, масштабування хмарних центрів обробки даних, перехід до мікросервісної архітектури, автоматизація процесів KYC/AML – усе це формує архітектуру, у якій нові функціональні можливості одночасно створюють нові ризики. Зміна швидкості інновацій, зростання складності цифрових систем та залежність від технологічних партнерств спричиняють ситуацію, коли уразливості можуть виникати не лише всередині установи, а й у будь-якому елементі екосистеми.

Таким чином, цифрові інновації і кіберризики не можуть розглядатися як два незалежні явища. Вони утворюють єдину взаємопов'язану модель, у якій кожен технологічний крок уперед потребує відповідного посилення захисної архітектури, а кожне нове джерело ризиків вимагає адаптації стратегічних пріоритетів та операційних процесів. З огляду на це важливо представити узагальнену логіку взаємодії цифрових інновацій, бізнес-моделей, нових вразливостей і кіберзагроз, яка відображена на рисунку 1.9.

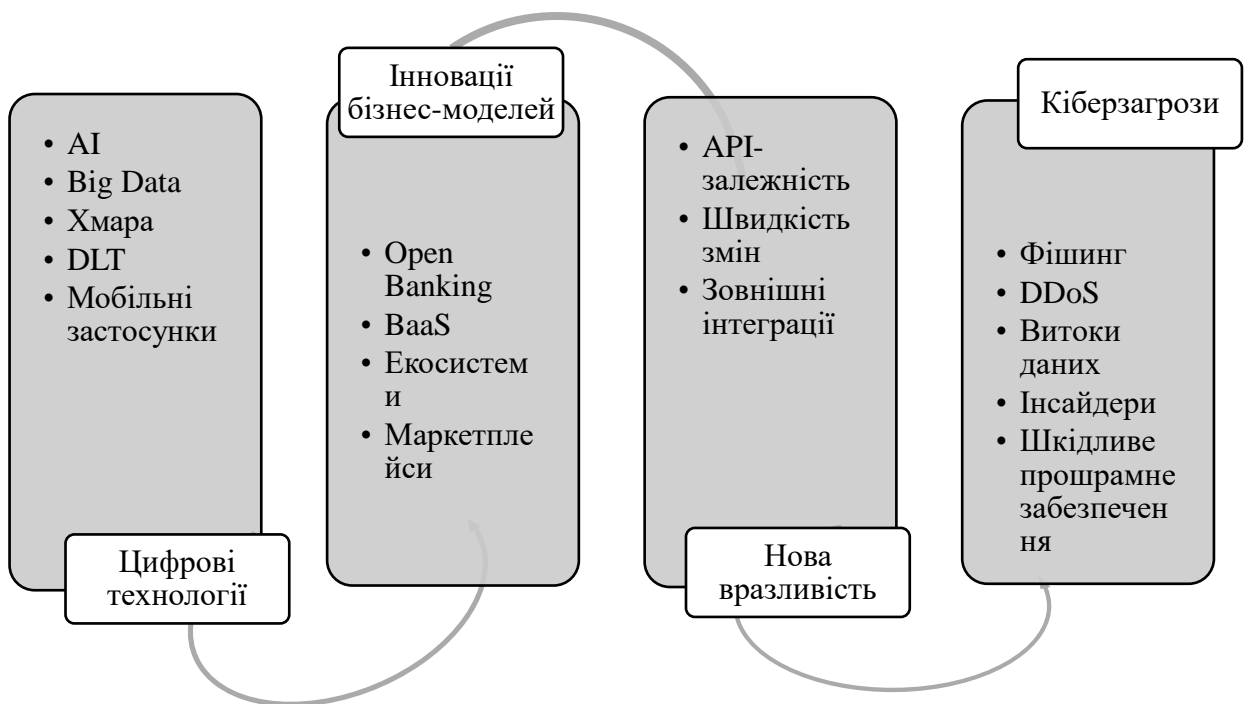


Рисунок 1.9. Модель взаємодії цифрових інновацій та кіберризиків

Джерело: авторська розробка.

Зображена на схемі конфігурація засвідчує, що цифрові технології та пов'язані з ними кіберризики складають єдиний ланцюг причиново-наслідкових залежностей. У цьому ланцюзі кожна технологічна новація водночас розширює функціональний потенціал системи й актуалізує нові джерела вразливостей.

Ключовим тут є те, що відповідні зв'язки мають нелінійний характер: інноваційні рішення здатні ініціювати ризики одразу на кількох рівнях (від клієнтського до інституційного), що суттєво підвищує складність прогнозування та перетворює кіберризики на системне явище. У таких умовах

фінансові посередники функціонують у режимі постійного пошуку балансу між темпами впровадження новачій та здатністю підтримувати ризиковий профіль власної діяльності у контрольованих межах.

Додатково слід зазначити, що взаємодія між інноваціями та ризиками відбувається на тлі посилення міжплатформної інтеграції, коли фінансові послуги реалізуються через зв'язки із зовнішніми сервісами, технологічними партнерами та регуляторними інфраструктурами. Із цього випливає, що джерело потенційної загрози може виникати не тільки всередині окремої фінансової установи, але й у будь-якому з елементів цифрового ланцюга формування доданої вартості, зокрема у відкритих API, у хмарних провайдерів або у поведінкових особливостях користувачів. Отже, стратегічне управління кіберризиками повинне виходити за межі суто технічних заходів безпеки та включати інституційну координацію, механізми партнерської взаємодії та системне врегулювання відносин довіри в межах усієї екосистеми.

Узагальнюючи викладене, доцільно підкреслити, що кіберзагрози в умовах цифрової економіки становлять не ізольовану проблему, а цілісне системне утворення, яке потребує стратегічного осмислення його природи та впливу на еволюцію фінансових посередників. Багаторівневий характер цих загроз, їхня взаємозалежність та здатність до трансформації під впливом технологічних новачій обґрунтовують необхідність перегляду наявних моделей ризик-менеджменту, включення кіберстійкості до системи стратегічного планування та переходу до концепції вбудованої кіберстійкості, закладеної на етапі проєктування систем. Вироблення адекватної відповіді на зазначені виклики виступає необхідною умовою для збереження довіри з боку клієнтів, забезпечення операційної безперервності та посилення конкурентних позицій фінансових інституцій у динамічному цифровому середовищі.

Проведене узагальнення структури та динаміки кіберзагроз свідчить про те, що цифрове середовище породжує якісно новий тип уразливостей фінансових посередників, який суттєво виходить за межі традиційних уявлень про забезпечення інформаційної безпеки. У межах цифрової архітектури

фінансових сервісів будь-який інцидент потенційно здатен спричинити не тільки технічні збої, але й негативно вплинути на поведінкові патерни клієнтів, репутаційний капітал установи та її спроможність підтримувати стабільне функціонування операційних процесів. Отже, формування дієвої системи протидії кіберризикам вимагає комплексного підходу, який охоплює як безпосередньо захисні інструменти, так і ширший контекст забезпечення безперервності діяльності фінансових посередників.

У цьому контексті центрального значення набуває категорія операційної стійкості, яка в умовах цифрової економіки отримує стратегічний статус та виступає інтегральним індикатором спроможності фінансових посередників ефективно діяти в обстановці високої технологічної нестабільності. Операційна стійкість об'єднує технологічні, управлінські та регуляторні механізми реагування на ризики, а також визначає здатність установи не тільки протистояти інцидентам, але й успішно відновлювати свої функції після їх виникнення з мінімізацією репутаційних і фінансових втрат.

Відтак після аналізу природи та закономірностей функціонування кіберзагроз логічним є перехід до розгляду операційної стійкості як фундаментального системного чинника цифрової трансформації фінансових посередників.

У цифровому середовищі операційна стійкість втрачає статус суто технічного параметра функціонування фінансових інституцій та набуває ролі стратегічної передумови їхньої життєздатності й довгострокової конкурентоспроможності. Таке зміщення акцентів зумовлене тим, що цифровізація формує глибоку залежність фінансових посередників від інформаційних систем, телекомунікаційних мереж, модулів штучного інтелекту, хмарних платформ і технологічних партнерів, які забезпечують реалізацію сервісів у режимі реального часу. За подібної моделі будь-який збій, затримка або втрата доступності сервісів здатна трансформуватися в інституційний ризик, що впливає не лише на окрему установу, але й на функціонування фінансових ринків загалом.

Операційна стійкість у сучасному розумінні охоплює кілька взаємопов'язаних вимірів: технологічний, організаційний, інституційний та поведінковий. *Технологічний вимір* передбачає стабільність і захищеність цифрової інфраструктури, її здатність до масштабування, опірність до пікових навантажень, резервування даних, а також інтеграцію механізмів швидкого відновлення після інцидентів. Сучасну основу забезпечення безперервності діяльності формують цифрові платформи з мікросервісною архітектурою, процеси DevSecOps, технології хмарної обробки даних та автоматизовані системи виявлення аномалій.

Організаційний вимір операційної стійкості визначається якістю внутрішніх бізнес-процесів, структурою підзвітності, регламентами реагування на інциденти та рівнем цифрових компетенцій працівників. У цьому контексті операційна стійкість постає як результат інтеграції технологічних рішень із управлінськими практиками. Вирішальне значення мають такі чинники, як наявність чітко прописаних процедур реагування, система управління доступом, механізми координації між структурними підрозділами, а також сформована культура безпеки. Саме ці елементи дозволяють скоротити часовий проміжок між виникненням інциденту та відновленням штатного функціонування сервісів.

Інституційний вимір зумовлений еволюцією регуляторного середовища в умовах цифрової економіки. Операційна стійкість фінансових посередників перебуває у прямій залежності від рівня узгодженості стандартів кіберзахисту, вимог до надійності хмарних сервісів, правил проведення зовнішнього аудиту, а також від функціонування національних інфраструктур реагування на кіберінциденти. Практика запровадження регуляторних пісочниць, застосування ризик-орієнтованого підходу та імплементація стандартів DORA в Європейському Союзі свідчать про те, що операційна стійкість розглядається регуляторами як обов'язковий складник сучасного фінансового нагляду [69].

З огляду на зазначене вище, операційна стійкість набуває статусу фундаментальної основи цифрової трансформації, визначаючи архітектурну побудову сервісів, модель ризик-менеджменту та стратегічні вектори розвитку фінансових посередників.

Підсумовуючи викладене, можна констатувати, що операційна стійкість фінансових посередників формується не лінійно, а внаслідок складної взаємодії технологічних, організаційних, інституційних і поведінкових чинників, кожен із яких по-своєму впливає на спроможність установ зберігати безперервність діяльності та адаптуватися до викликів цифрового середовища. В умовах підвищення технологічної складності, поширення хмарної інфраструктури, масштабування API-інтеграцій і виникнення нових форматів взаємодії з клієнтами особливої значущості набуває завдання систематизації ключових компонентів операційної стійкості. Така структуризація уможлиблює не лише чітке визначення природи потенційних вразливостей, але й побудову цілісної моделі стратегічного управління, яка охоплює всі рівні функціонування фінансового посередництва. З метою наочного представлення комплексної логіки формування операційної стійкості та акцентування багатовимірності цього поняття доцільно звести його основні складники у форматі системної табл. 1.12.

Таблиця 1.12

**Виміри операційної стійкості фінансових посередників
у цифровій економіці**

Вимір операційної стійкості	Зміст	Ключові елементи та механізми	Стратегічне значення
1	2	3	4
Технологічний	Забезпечення працездатності цифрової інфраструктури та ІТ-систем у режимі реального часу	резервування даних; кластерні та хмарні архітектури; DevSecOps; мікросервіси; моніторинг аномалій; планування масштабування	підтримання безперервності послуг; зміцнення надійності цифрових каналів; зменшення системних збоїв
Організаційний	Налагодження внутрішніх процедур та управлінських практик	інцидент-менеджмент; аудит доступів; внутрішній контроль; цифрові компетенції персоналу; стандартизовані регламенти відновлення	скорочення часу реагування на інциденти; підвищення операційної дисципліни; мінімізація людського фактора
Інституційний	Вплив регуляторного середовища та зовнішніх стандартів	вимоги регуляторів; стандарти DORA; вимоги до хмарних провайдерів; регуляторні пісочниці; національні CERT/SOC	зміцнення системної стійкості фінансового сектору; захист інфраструктури ринку; узгодженість інновацій із вимогами безпеки

Закінчення таблиці 1.12

1	2	3	4
Поведінковий	Реакція клієнтів та партнерів на інциденти	чутливість користувачів до перебоїв; вплив соцмереж; відтік клієнтів; зміна рівня довіри	збереження лояльності; підтримання позитивної репутації; мінімізація довгострокових репутаційних втрат

Джерело: розроблено автором на основі [8; 9; 16; 49; 69; 94; 111; 116; 136; 174; 236].

Структуризація, подана в таблиці 1.12, дозволяє розглядати операційну стійкість як багатовимірне явище, яке об'єднує технічні, організаційно-управлінські, регуляторні та поведінкові аспекти функціонування фінансових посередників. Аналіз таблиці засвідчує, що забезпечення належного рівня стійкості не може ґрунтуватися винятково на оновленні ІТ-інфраструктури чи впровадженні передових технологій. Вирішальне значення має злагоджена взаємодія зазначених технологій із управлінськими процесами, організаційною культурою та зовнішнім інституційним оточенням.

У цифровій економіці збої, інциденти та порушення набувають системного характеру, тому результативність реагування визначається не лише оперативністю технічного відновлення, але і здатністю установи підтримувати довіру з боку контрагентів, знижувати поведінкові втрати та зберігати конкурентні переваги. Це підтверджує системну природу операційної стійкості та вказує на її значення як одного з ключових стратегічних ресурсів у сфері цифрового фінансового посередництва.

Узагальнення вимірів операційної стійкості, представлене в таблиці, створює необхідну аналітичну базу для переходу від структурного опису до розуміння динаміки формування стійкості у цифровому середовищі. З метою виявлення того, як технологічні рішення, організаційні механізми та інституційні параметри взаємодіють між собою, утворюючи цілісний контур операційної стійкості, доцільно відобразити цю логіку у вигляді узагальненої схеми (рисунок 1.10).

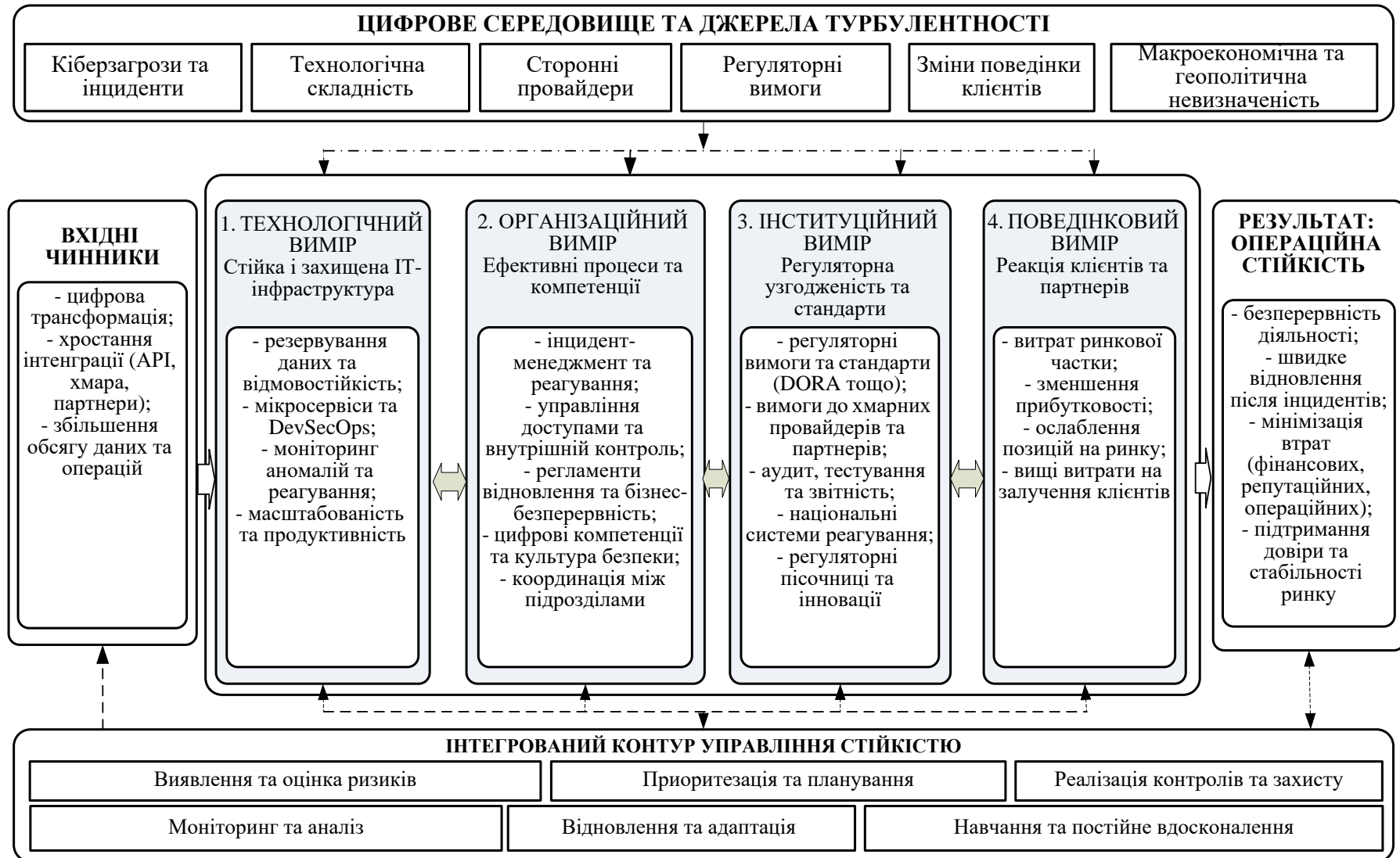


Рис. 1.10. Логіка формування операційної стійкості фінансових посередників

Джерело: авторська розробка на основі [32; 37; 63; 69; 105; 106; 108; 109; 110; 174; 222].

Така схема дає змогу прослідкувати, як окремі елементи – від цифрових технологій до поведінкових реакцій користувачів – формують завершений цикл стійкості, який забезпечує безперервність функціонування та адаптаційну спроможність фінансових посередників до викликів цифрової епохи.

Наведена на схемі конфігурація ілюструє, що операційна стійкість фінансових посередників являє собою не статичний ресурс, а динамічний процес, який постійно відтворюється на перетині технологічних спроможностей, якості операційних процедур, організаційних компетенцій та інституційних регуляторних рамок. Кожен із елементів цієї логіки функціонує не ізольовано: технологічний блок визначає швидкість реагування на інциденти, організаційні механізми забезпечують узгодженість дій, інституційне середовище встановлює обмеження та стандарти, а поведінкові реакції з боку користувачів і контрагентів впливають на здатність установи зберігати довіру навіть у кризових обставинах. Отже, операційна стійкість постає як інтегрована характеристика, що охоплює технічний, управлінський, регуляторний та соціальний виміри, і визначає загальну результативність і конкурентоспроможність фінансового посередника в умовах цифрової економіки.

Формування операційної стійкості має циклічний характер: впровадження нових технологій викликає необхідність адаптації процесів, удосконалення нормативних регламентів, оновлення професійних навичок персоналу та підвищення рівня цифрової грамотності клієнтів. Зі свого боку, кожен інцидент виконує функцію зворотного зв'язку, який сприяє коригуванню архітектури ризик-менеджменту та стратегічних підходів до цифровізації. Завдяки такій еволюційній моделі операційна стійкість набуває якостей стратегічного активу, що визначає спроможність фінансових посередників не лише функціонувати в умовах невизначеності, але й конкурентно розвиватися, освоюючи нові технологічні можливості.

У сучасному цифровому середовищі операційна стійкість і довіра виступають взаємозумовленими поняттями: стабільність і безперервність надання фінансових послуг створюють підґрунтя для формування довіри, тоді як сама довіра визначає схильність клієнтів користуватися цифровими каналами навіть в умовах зростання пов'язаних із цим ризиків. Тому після аналізу структурних і динамічних складників операційної стійкості закономірним є перехід до розгляду довіри як критичного елементу системи цифрового фінансового посередництва. Саме завдяки довірі технологічні рішення стають прийнятними та зрозумілими для клієнтів, знижується чутливість споживачів до можливих інцидентів, регулюються поведінкові реакції та забезпечується стабільність відносин між фінансовою установою, її користувачами та партнерами. Відповідно до цього в роботі проаналізовано механізми формування довіри в умовах цифрової економіки, чинники впливу на неї, а також роль інноваційних рішень у підтриманні довгострокової стійкості фінансових посередників.

У межах цифрової економіки довіра виступає не тільки соціально-поведінковим феноменом, але й фундаментальною передумовою ефективного функціонування фінансових посередників. Вона визначає ступінь сприйняття клієнтами цифрових сервісів, готовність користувачів делегувати установам управління власними активами та здійснювати транзакції в дистанційному форматі. На відміну від традиційної моделі фінансування, де довіра вибудовувалася на основі репутації, тривалої історії діяльності, фізичної присутності та особистих контактів, у цифровому середовищі посередництво спирається на технологічні механізми, алгоритмічне забезпечення безпеки та якість електронної взаємодії.

Під впливом цифрової трансформації відбувається зміщення від класичної інституційної довіри (до банку як установи) до технологічної довіри – довіри до систем, протоколів, алгоритмів, цифрової ідентифікації та кіберзахисту. Саме тому значна частина досліджень (OECD, BIS, World Bank, 2024) аналізує довіру як інфраструктурний елемент цифрової фінансової

екосистеми, у межах якої безпека каналів, якість даних, прозорість процесів і відповідність регуляторним стандартам стають основою взаємодії між клієнтом і фінансовою установою. Формування довіри у цифровому середовищі відбувається через сукупність технологічних, організаційних та поведінкових механізмів (таблиця 1.13).

Таблиця 1.13

Механізми формування довіри у цифровій економіці

Вимір довіри	Зміст та ключові механізми	Приклади технологій / практик	Стратегічний ефект
Технологічний	Надійність і прозорість цифрових рішень, захист даних, безпечність транзакцій	біометрична ідентифікація; протоколи KYC/AML; криптографія; аналіз поведінки; DLT; контроль доступів; сертифікація застосунків	зниження технічних ризиків; підвищення сприйняття безпеки; підтримання прийняття інновацій
Організаційний	Якість внутрішнього управління, корпоративна відповідальність, стандарти безпеки	інцидент-менеджмент; прозорі політики використання даних; аудит доступів; SLA-стандарти; внутрішні регламенти комунікації	зростання передбачуваності поведінки інституції; зміцнення репутації; мінімізація невизначеності
Інституційний	Регуляторна надійність, відповідність нормам, зовнішні гарантії	регуляторні пісочниці; стандарти DORA; ліцензування; нагляд НБУ; національні CERT/SOC	зниження системних ризиків; формування довіри до ринку; підтримка легітимності цифрових сервісів
Поведінковий	Досвід користувача, сприйняття ризиків, прозорість цифрової взаємодії	UX-дизайн; чіткі повідомлення про інциденти; персоналізація; швидкість обслуговування; customer journey management	підвищення лояльності; скорочення відтоку; зміцнення довгострокових відносин
Етичний (алгоритмічна довіра)	Справедливість та неконфліктність алгоритмів, коректне використання даних	governance моделей ІІІ; explainable AI; контроль за використанням персональних даних	зменшення тривожності користувачів; формування «довіри до алгоритмів»

Джерело: розроблено автором на основі [78; 123; 136; 159; 197; 203; 232; 49].

Технологічна складова довіри включає використання біометричних методів встановлення особи, криптографічних засобів захисту, процедур KYC/AML, інструментів поведінкової аналітики, а також забезпечення прозорості транзакцій, зокрема на основі технологій розподілених реєстрів (DLT). Зазначені механізми реалізують принцип «довіри за замовчуванням», формуючи у клієнта відчуття контролюваності виконуваних операцій та захищеності його даних.

Організаційна складова довіри визначається внутрішніми стандартами безпеки, якістю управління інцидентами, оперативністю комунікації з клієнтами у разі збоїв, зрозумілістю політик обробки даних, а також рівнем відповідності міжнародним вимогам. В умовах цифровізації споживачі очікують не лише стабільної роботи сервісів, але і прозорості дій установи в разі виникнення інцидентів. Поведінкова довіра безпосередньо залежить від таких чинників, як швидкість відновлення функціонування після збою, доступність та чіткість інструкцій для користувачів, а також наявність зрозумілих протоколів реагування на загрози.

Поведінковий вимір довіри визначається характером оцінювання ризиків клієнтами та інтенсивністю використання ними цифрових каналів. Формування довірчих відносин відбувається під впливом накопиченого досвіду взаємодії, який включає безперебійну роботу програмного застосунку, інтуїтивно зрозумілі інтерфейси, мінімальний рівень шахрайських операцій, своєчасність здійснення платежів, прозорі та недвозначні умови обслуговування, а також індивідуалізовані пропозиції. Зазначені чинники сприяють закріпленню сталих позитивних поведінкових патернів. Разом із тим навіть нетривала технічна нестабільність або несприятливий інформаційний контекст у соціальних медіа здатні суттєво послабити довіру до фінансової інституції, що засвідчує її вразливість в умовах цифрового середовища.

Отже, довіра набуває статусу стратегічного чинника, що визначає довгострокові траєкторії розвитку фінансових посередників. Вона зменшує чутливість клієнтів до технічних неполадок, підвищує сприйнятливість до інновацій, полегшує впровадження цифрових рішень і зростання показника

життєвої цінності клієнта. Зазначене положення знаходить підтвердження в авторських наукових працях. Так, у дослідженні «Етичні виклики цифровізації: філософський аналіз довіри як основи фінансового посередництва» наголошується, що довіра постає не лише економічною, але й морально-етичною категорією цифрової комунікації. Це зумовлено тим, що клієнт делегує фінансовій установі не тільки власні грошові кошти, а і право на опрацювання персональних даних, оцінювання ризиків та ухвалення рішень на основі алгоритмічних моделей [154].

Таким чином, у цифровій моделі фінансового посередництва довіра формується на перетині технологічної надійності, організаційної відповідальності та прозорості цифрової взаємодії, що зумовлює необхідність застосування міждисциплінарних підходів до її розбудови. Досягнутий рівень довіри визначає не лише поточну конкурентну позицію фінансової установи, але й її спроможність адаптуватися до нових ризиків, масштабувати бізнес-модель і забезпечувати сталий розвиток у довгостроковій перспективі.

Узагальнений аналіз механізмів формування довіри, поданий у таблиці, демонструє, що довіра у цифровому фінансовому посередництві розгортається як багатокомпонентна конструкція, де кожен вимір – технологічний, організаційний, інституційний, поведінковий та етичний – виконує власну функцію у підтриманні стабільності взаємодії між фінансовою установою та користувачем. Проте для повного розуміння логіки цього процесу недостатньо лише структурного переліку елементів. Важливо побачити, яким чином ці виміри взаємодіють між собою, утворюючи послідовний ланцюг формування довіри – від зовнішніх регуляторних гарантій до внутрішньої готовності клієнта приймати цифрові сервіси та покладатися на них.

Саме тому, на нашу думку, доцільно перейти від табличної систематизації до візуального представлення архітектури довіри, яке демонструє логіку переходу від інституційних механізмів до індивідуального сприйняття цифрових ризиків і переваг. Схема, представлена на рис 1.11 узагальнює основні етапи цього процесу та дозволяє побачити, як різні рівні довіри поєднуються у цілісну модель цифрового прийняття.

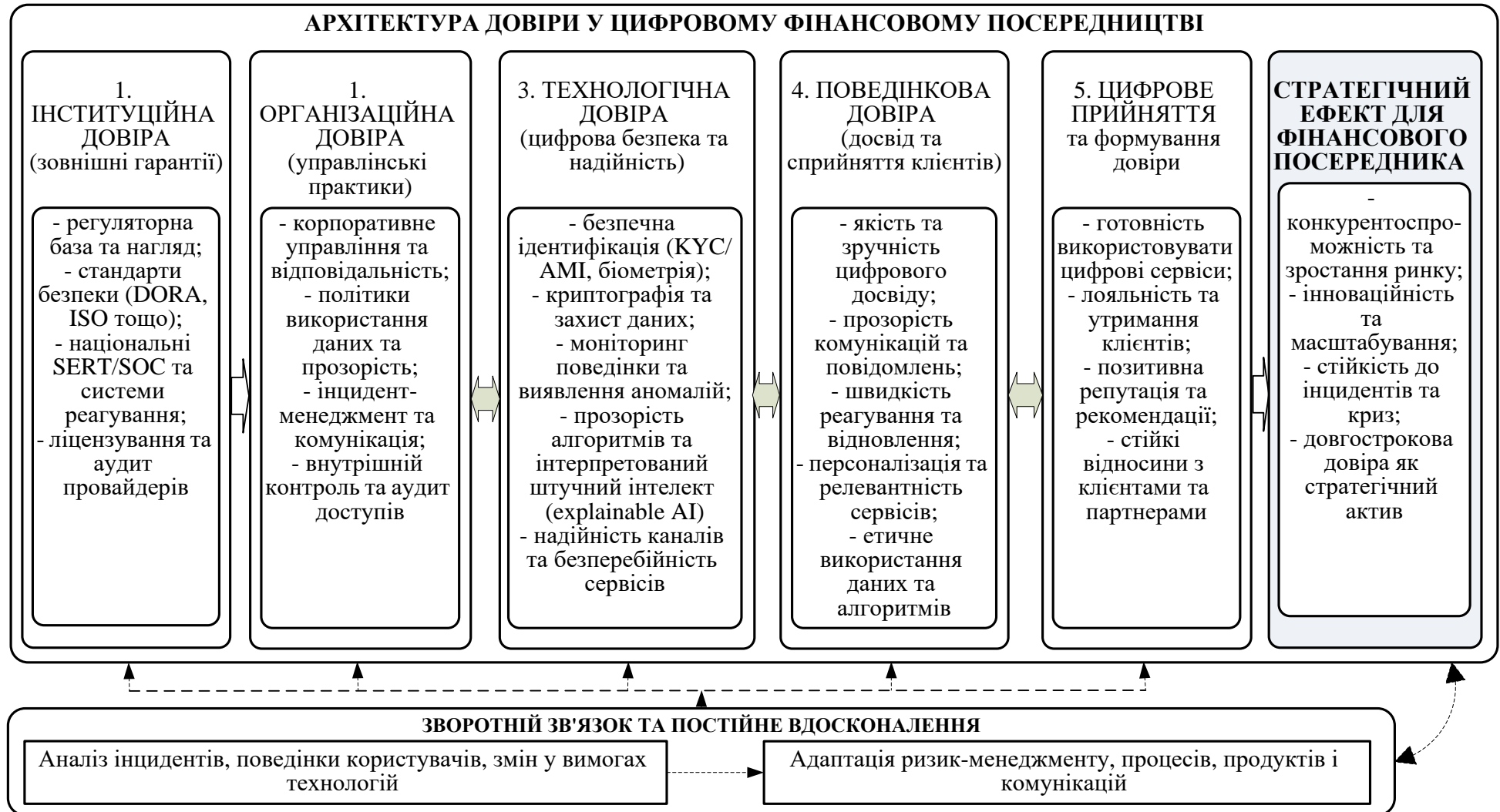


Рис. 1.11. Архітектура довіри у цифровому фінансовому посередництві

Джерело: авторська розробка на основі [49; 58; 70; 123; 154; 159; 203; 232].

Вважаємо, що багаторівнева структура формування довіри розпочинається із зовнішніх інституційних гарантій (регуляторна довіра), переходить у внутрішні управлінські практики (організаційна довіра), далі реалізується через технічні засоби цифрової безпеки (технологічна довіра) та завершується поведінковою реакцією клієнта (поведінкова довіра). Результатом цієї послідовності є цифрове прийняття – готовність користувачів використовувати фінансові послуги через цифрові канали, що безпосередньо впливає на конкурентоспроможність фінансового посередника.

Проведений аналіз показує, що цифрова трансформація фінансових посередників породжує багатовимірні ризики та виклики, які суттєво змінюють архітектуру їх функціонування, природу ризик-менеджменту та механізми формування довіри.

Кіберзагрози стають ключовим чинником стратегічної невизначеності, оскільки виникають одночасно на клієнтському, технологічному, організаційному та інституційному рівнях. Їхня взаємопов'язаність формує складну систему ризиків, у межах якої технічні інциденти трансформуються у репутаційні та стратегічні наслідки, здатні порушити стійкість посередника та знизити рівень довіри до цифрових фінансових сервісів.

Операційна стійкість у такому середовищі постає як інтегральна здатність установи забезпечувати безперервність діяльності, стабільність сервісів та швидке відновлення після інцидентів. Вона формується на перетині технологічних рішень, організаційних процедур, регуляторних вимог та поведінкових реакцій клієнтів. Цифровізація суттєво підвищує залежність установ від складних ІТ-архітектур, хмарних сервісів та зовнішніх технологічних партнерств. Це робить операційну стійкість не лише технічним, а й стратегічним ресурсом, необхідним для підтримання конкурентоспроможності та ринкової стабільності.

Разом із тим цифрова трансформація змінює природу довіри у фінансовому секторі. Від традиційних інституційних моделей довіри система

переходить до технологічної та поведінкової довіри, що ґрунтується на якості цифрової взаємодії, захищеності даних, прозорості алгоритмів та етичності використання штучного інтелекту. Довіра стає ключовим елементом цифрового прийняття: вона визначає готовність користувачів взаємодіяти із фінансовими послугами через мобільні застосунки, відкриті платформи та інноваційні сервіси. Водночас довіра є вкрай чутливою до технічних та інформаційних інцидентів, що підкреслює її крихкість у цифровому середовищі та обумовлює потребу в системному підході до її підтримання.

У процесі цифрової трансформації фінансового сектору сутність довіри суттєво змінюється. Технологічні і поведінкові аспекти формування довіри починають відігравати все більш значну роль. Потреба у цифровій взаємодії, захищеності даних, прозорості алгоритмів та етичності використання штучного інтелекту набуває ключового значення для поширення цифрових фінансових послуг. Саме вона визначає готовність користувачів застосовувати мобільні технології, відкриті програмні інтерфейси та інноваційні продукти у фінансовій сфері. Разом з тим, довіра є надзвичайно чутливою до будь-яких технічних збоїв або інформаційних порушень, що створює об'єктивну потребу у використанні системного підходу, спрямованого на підтримання довіри на належному рівні.

Підсумовуючи результати проведеного дослідження, можна констатувати, що ризики, пов'язані з цифровою трансформацією, операційна стійкість та довіра утворюють єдиний стратегічний трикутник, який визначає як потенційні можливості, так і обмеження розвитку фінансових посередників в умовах цифрової економіки. Ефективне управління кіберризиками, побудова багаторівневої інфраструктури операційної стійкості та формування технологічно обґрунтованої довіри виступають ключовими передумовами довгострокової життєздатності, здатності до інновацій та конкурентоспроможності фінансових установ.

Висновки до розділу 1

1. Глибокі інституційної трансформації, яких зазнають фінансові посередники в цифровій економіці зазнають, суттєво впливають на зміну їх сутності, ролі та функціонального призначення. Спостерігається поступовий перехід від традиційних моделей накопичення та перерозподілу ресурсів до платформно-екосистемної логіки, де ключовими активами стають дані, технології та інноваційні форми взаємодії з клієнтами.

2. Сучасна архітектура фінансового посередництва формується під впливом технологій штучного інтелекту, великих даних, хмарних обчислень, технології розподіленого реєстру, відкритих програмних інтерфейсів тощо. Її базовими принципами стають відкритість, мережевість, високий рівень інтеграції та автоматизації. Реалізація цих принципів спричинює появу нових стратегічних орієнтирів розвитку. Такими орієнтирами ми вважаємо клієнтоцентричність, гнучкість, швидкість інновацій, кіберстійкість та екосистемність.

3. Зазнає суттєвих змін функціональна модель фінансових посередників. Це знаходить відображення у трансформації функцій стратегічного розвитку, управління ризиками, формуванні довіри, а також інфраструктурній, інноваційній та інклюзивній функціях. Цифровізація не лише доповнює їх новими інструментами, а й змінює сам зміст та механізми реалізації, переводячи діяльність фінансових посередників у режим постійної адаптації.

4. Фінансові інновації формують багаторівневий вплив на стратегії розвитку фінансових посередників. На мікрорівні вони змінюють продуктові лінійки — відбувається атомізація фінансових послуг, їх кастомізація під індивідуальні профілі споживачів та інтеграція в цифрові канали взаємодії. На операційному рівні інновації оптимізують внутрішні процеси, скорочуючи час обробки транзакцій, знижуючи операційні витрати та усуваючи вузькі місця в бек-офісних функціях. На бізнес-модельному рівні вони перебудовують логіку створення та привласнення вартості, зміщуючи акцент від універсальних

пропозицій до спеціалізованих цифрових екосистем. На інфраструктурному рівні інновації модернізують апаратно-програмний базис, забезпечуючи сумісність із зовнішніми сервісами, масштабованість та кіберстійкість. У цифровому середовищі інновації стають системним фактором довгострокової конкурентоспроможності, оскільки вони безпосередньо впливають на швидкість реакції посередника на ринкові зміни, його здатність до експансії в суміжні сектори та формування стійких клієнтських відносин.

5. Кіберзагрози утворюють комплексну систему ризиків, що взаємопов'язано проявляється на клієнтському, технологічному, організаційному та інституційному рівнях. На *клієнтському* рівні вони генерують ризики витоку персональних даних, фінансових втрат та порушення конфіденційності. На *технологічному* – спричиняють збої в роботі цифрових сервісів, компрометацію алгоритмів штучного інтелекту та деградацію апаратно-програмної інфраструктури. На *організаційному* – призводять до порушення бізнес-процесів, зростання операційних витрат на кіберзахист та необхідності перегляду внутрішніх регламентів. На *інституційному* – створюють системні ризики для фінансового сектору, включно з ефектом доміно від каскадних атак на платіжну інфраструктуру. Проведені дослідження довели, що кіберзагрози здатні переростати з технічних інцидентів у стратегічні загрози, підриваючи тим самим довіру, репутацію, якість обслуговування клієнтів та стабільність функціонування і розвитку будь-якого фінансового посередника.

6. Стратегічним ресурсом, який у цифровій економіці забезпечує стабільність цифрових сервісів, безперервність діяльності та здатність швидко відновлюватися після інцидентів виступає операційна стійкість. Щоб забезпечити безперервність, потрібно підтримувати критичні функції незалежно від кібератак та від технічних збоїв. Забезпечення доступності, продуктивності та якості обслуговування навіть за пікових навантажень показує, наскільки стабільно працюють сервіси. А відновна стійкість формується на технічних рішеннях резервування даних та організаційних процедурах кризового

реагування, які спрямовані на мінімізацію часу простою і відновлення роботи. Доведено, що операційна стійність формується на перетині технологічного, управлінського, регуляторного та поведінкового вимірів.

7. У сфері цифрових фінансів довіра відіграє все більш важливу роль. Вона опосередковує відносини між клієнтами та посередниками в умовах відсутності прямого фізичного контакту. Ми бачимо, як змінюється сама природа довіри - від традиційної, яка заснована на репутації, ліцензуванні та державних гарантіях, до технологічної та поведінкової. Технологічна довіра базується на безпеці даних та прозорості алгоритмів, зокрема здатності пояснювати логіку прийняття рішень системами штучного інтелекту. Поведінкова довіра формується через ефективність інцидент-менеджменту та високу якість цифрової взаємодії – швидкість реакції на запити, зручність інтерфейсів, передбачуваність сервісів. У цифровому середовищі довіра визначає готовність клієнтів приймати інновації, зменшує їхню чутливість до операційних ризиків та підтримує сталий розвиток фінансових посередників.

Розділ 2

МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНЮВАННЯ ТА АНАЛІЗУ СТРАТЕГІЧНОГО РОЗВИТКУ ФІНАНСОВИХ ПОСЕРЕДНИКІВ В УМОВАХ ЦИФРОВІЗАЦІЇ

2.1. Методологічний інструментарій дослідження цифрової трансформації фінансових посередників

Цифровізація змінює конфігурацію фінансового сектору. Для фінансових посередників це означає не просто оновлення ІТ-ландшафту, а фундаментальну трансформацію бізнес-моделей, клієнтських каналів і управлінських практик. Технологічні інновації, як-то штучний інтелект (AI), великі дані (Big Data), блокчейн та інші підвищують операційну ефективність, але паралельно ускладнюють внутрішню архітектуру організації та генерують нові зони невизначеності. За даними Світового банку, цифрові фінансові послуги виступають одним із головних каталізаторів фінансової інклюзії та зростання, однак для самих установ цей процес пов'язаний із новими викликами й ризиками.

У цих умовах особливої актуальності набуває проблема визначення рівня цифрового розвитку фінансових посередників, що в науковій літературі дедалі частіше інтерпретується через категорію «цифрова зрілість», яка відображає не лише ступінь впровадження цифрових технологій, але і здатність організації інтегрувати їх у бізнес-процеси, адаптувати організаційну структуру та забезпечувати стійкість до зовнішніх шоків.

Проблема, однак, у тому, що єдиного погляду, як саме цю зрілість вимірювати, поки що немає. Існуючі моделі – від класичних підходів до галузевих індексів цифровізації — часто є занадто узагальненими або прив'язані до конкретних технологічних рішень, або не враховують специфіку фінансового посередництва (регуляція, довіра, чутливість даних, системний ризик тощо). Особливо гостро це відчувається на тлі зростаючої

нестабільності зокрема через воєнні дії, економічні кризи, пандемічні шоки й щоразу демонструють обмеженість статичних методик, які не адаптовані під швидкі зміни зовнішнього середовища. Тож, зростаючий практичний запит стейкхолдерів на об'єктивну оцінку цифрового потенціалу фінансових посередників та відсутність системних, уніфікованих підходів до оцінювання цифрової зрілості фінансових посередників зумовлюють актуальність обраної теми дослідження. Одночасно швидкі зміни середовища вимагають не просто моделей «на всі часи», а гнучкого, конфігураційного інструментарію, здатного враховувати нові ризики та виклики, що потребує невідкладного теоретико-прикладного опрацювання.

Сучасний науковий дискурс щодо цифрової зрілості формується на перетині досліджень цифрової трансформації, стратегічного управління та розвитку фінансового сектору. Узагальнення наукових праць свідчить про поступовий перехід від фрагментарного розгляду цифровізації до її комплексного осмислення як багатовимірного явища. Передусім у зарубіжних дослідженнях цифрова трансформація розглядається як системний процес, що охоплює зміни у створенні цінності, бізнес-моделях та організаційних структурах [134]. Подібна позиція знайшла відображення в підходах Організації економічного співробітництва та розвитку (OECD), де цифровізація трактується як ключовий фактор трансформації економічних систем та конкурентного середовища, а цифрова зрілість виступає інтегрованою характеристикою здатності організації до ефективної адаптації до цифрових змін [114].

Значний внесок у розвиток концепції цифрової зрілості належить колективу авторів на чолі з Г. К. Кейном, які визначають цю дефініцію як поєднання технологічних можливостей, управлінських практик та організаційної культури [91]. Цікавим з наукового погляду є запропонована McKinsey & Company модель Цифрового коефіцієнта, яка орієнтована на кількісне вимірювання цифрової зрілості та оцінювання її впливу на ефективність діяльності організацій [98]. Попри значну практичну цінність, вищезазначені підходи мають універсальний характер і не враховують повною мірою галузеву специфіку.

Окремий напрям науково-прикладних досліджень пов'язаний з аналізом впливу цифровізації на фінансовий сектор. Зокрема, у звітах Міжнародного валютного фонду (IMF) підкреслено, що цифрові фінансові технології змінюють традиційні бізнес-моделі, трансформують структуру ризиків, а також сприяють появі нових учасників ринку [86]. Водночас дослідники Світового банку акцентують увагу на ролі цифрових технологій у підвищенні фінансової інклюзії та ефективності фінансових послуг і наголошують на нерівномірності результатів цифровізації залежно від рівня готовності суб'єктів [140].

Паралельно з розвитком загальнотеоретичних підходів у науковій літературі активізуються дослідження, присвячені безпосередньо оцінюванню цифрової зрілості. Зокрема, у роботі Н. Голіонко та К. Кондратьєвої запропоновано методичні підходи до її оцінювання, які базуються на системі кількісних і якісних показників, що охоплюють технологічні, організаційні та управлінські аспекти діяльності [158]. Подальший розвиток цієї проблематики представлено у дослідженні Л. М. Шимановська-Діанич і О. В. Лозової, які вважають цифрову зрілість ключовим фактором трансформації бізнес-процесів підприємств, який в умовах економічної нестабільності сприяє оптимізації операційної діяльності та підвищенню ефективності управління [218].

Цифрову зрілість як фактор розвитку економічних екосистем, який забезпечує інтеграцію суб'єктів ринку та формування нових форм взаємодії розглядають у співавторстві Т. Мішустіна, В. Дубницький та І. Крабовський [181]. У роботі М. Козьменкова можна побачити розширення цього підходу за рахунок використання інструментів штучного інтелекту для оцінювання цифрової зрілості екосистем онлайн-сервісів фінансових установ [168].

У контексті обраної теми дослідження особливий науковий інтерес становить робота Г. Й. Островської, у якій представлено систематизацію сучасних моделей оцінювання цифрової зрілості й виділено рівневі, індексні та компетентнісні підходи до її діагностики, що, на нашу думку, створює підґрунтя для формування комплексних методик оцінювання, орієнтованих на

багатовимірний аналіз [188]. Не менш важливим з погляду удосконалення інструментарій оцінювання цифрової зрілості бізнес-організацій, що включає систему показників за ключовими напрямками цифрового розвитку є дослідження Л. Лігоненко та К. Зеленко, які також підкреслюють необхідність адаптації існуючих підходів до специфіки галузей, що є особливо актуальним для фінансового сектору [172].

Попри зростаючу кількість публікацій щодо цифрової трансформації, методичне забезпечення оцінювання цифрової зрілості фінансових посередників залишається фрагментарним. Наявні моделі не є уніфікованими, зокрема, показники розрізнені, порогові значення не узгоджені, а головне – вони недостатньо враховують галузеву специфіку фінансового сектору. Так, наприклад, МВФ зазначає, що цифровізація фінансових послуг супроводжується зростанням кіберризиків, регуляторної напруги та технологічної залежності, але усі ці параметри залишаються поза межами більшості існуючих методик оцінювання цифрової зрілості. Крім того, ситуацію ускладнює зовнішня нестабільність. Умови воєнних та економічних шоків, які вже понад десятиліття є характерними для українських реалій, роблять традиційні статичні моделі оцінювання малопридатними. Це пов'язано і з тим, що вони не враховують динаміку змін, адаптивний потенціал фінансових посередників, а також їхню спроможність до швидкої реконфігурації процесів.

Таким чином, об'єктивно зростаюча роль цифрової зрілості як інтегральної характеристики фінансових посередників, з одного боку, та відсутність системного теоретико-методичного апарату для її вимірювання – з іншого, зумовлює мету і задачі цього підрозділу дисертаційного дослідження.

Метою підрозділу є обґрунтування теоретико-методичних засад оцінювання цифрової зрілості фінансових посередників та розробка підходів до вдосконалення інструментарію її вимірювання з урахуванням сучасних умов цифрової трансформації економіки.

Сучасний етап розвитку економіки характеризується глибокою цифровою трансформацією, що охоплює всі сфери господарської діяльності та суттєво змінює умови функціонування фінансових посередників. У цьому контексті поняття «цифрова зрілість», яке використовується для характеристики рівня готовності та здатності організацій до ефективного функціонування в цифровому середовищі набуває особливої актуальності. Водночас, попри активізацію досліджень у цій сфері, теоретичне осмислення сутності цифрової зрілості залишається неоднозначним і фрагментарним.

Проведений аналіз наукових підходів до трактування цифрової зрілості свідчить про відсутність єдиного універсального визначення, що зумовлено багатовимірністю цього явища. Водночас узагальнення представлених у літературі підходів дозволяє виокремити спільні концептуальні ознаки, які формують зміст цієї категорії. Зокрема, більшість дослідників, серед яких Г. К. Кейн, Л. Лігоненко та К. Зеленко, пов'язують цифрову зрілість зі здатністю організації ефективно використовувати цифрові технології. Тобто в розумінні цієї категорії вони передусім спираються на технологічну основу поняття, однак, на нашу думку, вона виступає лише передумовою і не є визначальною [91; 172].

Системний підхід до розуміння цієї дефініції підкреслюється в роботах Н. Голіонко, К. Кондратьєвої та Г. Й. Островської, які інтеграцію цифрових рішень у всі сфери діяльності організації, включаючи бізнес-процеси, управління та взаємодію з клієнтами вважають ключовим елементом цифрової зрілості [158; 188].

Важливим компонентом, який дозволяє розглядати цифрову зрілість не як статичний стан, а як динамічну характеристику розвитку є здатність до трансформації та адаптації, яка проявляється у зміні бізнес-моделей і процесів під впливом цифровізації. Цей підхід до розуміння цифрової зрілості прослідковується в роботах Г. Віал [134], Л. М. Шимановської-Діанич і О. В. Лозової [218].

Стратегічний підхід до розуміння цифрової зрілості прослідковується в дослідженнях McKinsey & Company, де акцентовано увагу на управлінських і стратегічних аспектах цифрової зрілості, які визначають здатність організації формувати та реалізовувати цифрову стратегію розвитку [98].

З огляду на зазначене, виникає необхідність систематизації існуючих підходів та виокремлення їхніх ключових характеристик, що дозволить уточнити зміст цього поняття та створити концептуальну основу для розроблення методичного інструментарію її оцінювання, що є особливо важливим у контексті формування стратегії розвитку фінансових посередників в умовах цифровізації економіки.

Конкретизація змісту поняття «цифрова зрілість» через призму наукових дефініцій, запропонованих у сучасній літературі не тільки дає можливість перейти від загального опису підходів до більш чіткого розуміння сутності цифрової зрілості як наукової категорії і створює підґрунтя для подальшого узагальнення та формування авторського трактування, яке враховувало б як міжнародний досвід, так і специфіку функціонування фінансових посередників.

Узагальнення виявлених визначень цифрової зрілості представлено в табл. 2.1.

Таблиця 2.1

Термінологічні визначення цифрової зрілості

Автор / джерело	Визначення
Кейн Г. К., Палмер Д. та Філліпс А. Н. [91]	«Цифрова зрілість — це менше про технології, а більше про те, як компанії використовують цифрові технології для трансформації свого бізнесу»
McKinsey & Company [98]	«Цифрова зрілість відображає ступінь, до якої компанія цифровим шляхом трансформувала свої бізнес-процеси, взаємодію з клієнтами та бізнес-моделі»
Голіонко Н., Кондратьєва К. [158]	«Цифрова зрілість організації — це рівень її здатності впроваджувати та ефективно використовувати цифрові технології у всіх сферах діяльності»
Л. М. Шимановська-Діанич, О. В. Лозова [218]	«Цифрова зрілість підприємства визначає рівень його готовності до трансформації бізнес-процесів на основі цифрових технологій»
Г. Й. Островська [188]	«Цифрова зрілість підприємства характеризує ступінь інтеграції цифрових технологій у діяльність та управління організацією»
Л. Лігоненко, К. Зеленко [172]	«Цифрова зрілість бізнес-організації — це комплексна характеристика рівня її цифрового розвитку, що охоплює технологічні, організаційні та управлінські аспекти»

Узагальнення зазначених підходів дало підстави сформулювати таке авторське визначення цієї економічної категорії для фінансових посередників. *Цифрова зрілість фінансового посередника* – це інтегрована характеристика рівня розвитку організації, що відображає її здатність системно впроваджувати та ефективно використовувати цифрові технології, інтегрувати їх у бізнес-процеси, управління і взаємодію з клієнтами, а також забезпечувати адаптацію та трансформацію діяльності відповідно до вимог цифрової економіки.

Результати аналізу наукових джерел дозволяють стверджувати, що оцінювання цифрової зрілості здійснюється на основі різних методологічних підходів, які відрізняються за цілями, інструментарієм та рівнем деталізації. Відсутність уніфікованої методики обумовлює необхідність їх систематизації та подальшої інтеграції в комплексний підхід.

Запропоноване визначення цифрової зрілості окреслює її ключові структурні елементи та створює теоретичне підґрунтя для подальшого аналізу, а саме систематизації методологічних підходів до її оцінювання.

Узагальнення наявних підходів дає змогу виявити їх спільні та відмінні риси, обґрунтувати можливості застосування в діяльності фінансових посередників, а також сформувати комплексну модель оцінювання цифрової зрілості. Для наочності результати систематизації представлено в табл. 2.2.

Таблиця 2.2

Узагальнення підходів і показників оцінювання цифрової зрілості

Класифікаційна ознака	Підхід	Сутність	Переваги	Обмеження
1	2	3	4	5
За характером оцінювання	Якісний	Експертні оцінки, анкетування	Гнучкість, адаптивність	Суб'єктивність
	Кількісний	Система показників, інтегральний індекс	Об'єктивність, порівнюваність	Складність формалізації
	Змішаний	Поєднання якісних і кількісних методів	Комплексність	Складність реалізації

Закінчення таблиці 2.2

1	2	3	4	5
За структурою моделі	Рівневий	Поділ на рівні зрілості	Простота	Узагальненість
	Індикаторний	Оцінка через показники	Точність	Висока трудомісткість
	Компетентнісний	Оцінка навичок і управління	Урахування людського фактору	Складність вимірювання
	Екосистемний	Взаємодія з цифровим середовищем	Сучасність	Важкість формалізації
За рівнем застосування	Мікрорівень	Оцінка підприємства	Практичність	Обмежена узагальненість
	Мезорівень	Галузевий аналіз	Узагальнення	Менша деталізація
	Макрорівень	Оцінка економіки	Стратегічність	Відсутність деталізації

Джерело: розроблено автором на основі [129; 188; 172; 17].

Наведена типологія підходів до оцінювання цифрової зрілості окреслює загальну методологічну рамку, однак для потреб фінансового сектору важливим є розгляд конкретних інструментальних моделей, які вже апробовані в міжнародній практиці. Звернення до них дозволяє не лише врахувати накопичений досвід, але й виявити ті аспекти, які залишаються поза увагою універсальних методик.

У міжнародному науковому та практичному дискурсі найбільшого поширення набули декілька моделей, що відрізняються за цільовим призначенням, глибиною аналізу та сферою застосування. Серед них – рамка цифрової зрілості Організації економічного співробітництва та розвитку (OECD Digital Maturity Framework), модель операційної стійкості Банку міжнародних розрахунків (BIS Operational Resilience Model), модель цифрової зрілості Deloitte (Deloitte DMM), підхід Gartner до оцінювання цифрової зрілості, цифровий коефіцієнт McKinsey (McKinsey Digital Quotient), а також рамка кібербезпеки Національного інституту стандартів і технологій США (NIST Cybersecurity Framework). Кожна з цих моделей пропонує власну логіку вимірювання цифрової зрілості, що зумовлено різницею в дослідницьких цілях та об'єктах аналізу.

Порівняльний аналіз зазначених моделей дозволяє виокремити їх ключові характеристики, сильні сторони, а також обмеження щодо використання саме у фінансовому секторі. Результати такого порівняння зведено в таблиці 2.3, де моделі оцінено за такими критеріями, як основні виміри цифрової зрілості, методологічні особливості, переваги та недоліки з погляду застосування до діяльності банків, страхових компаній та інших фінансових посередників.

Таблиця 2.3

Порівняння міжнародних моделей оцінювання цифрової зрілості

Модель / Автор	Основні виміри цифрової зрілості	Методологічні особливості	Сильні сторони	Обмеження / релевантність для фінансового сектору	Джерело
1	2	3	4	5	6
OECD Digital Maturity Framework	Технології, процеси, організаційна готовність, інновації, дані	Поєднання кількісних індикаторів із якісними оцінками; використання міжнародних порівнянь	Стандартизована міжнародна методологія; сильна аналітична база	Недостатньо сфокусована саме на фінансовому секторі	OECD [108]
BIS Operational Resilience Model	ІСТ-стійкість, кіберзахист, критичні процеси, управління безперервністю, інцидент-менеджмент	Акцент на операційній стійкості як основі цифрової зрілості	Висока релевантність для банків і платіжних систем	Не охоплює клієнтську цифрову поведінку та інноваційність	BIS [32]
Deloitte Digital Maturity Model (DMM)	Стратегія, культура, технології, клієнт, операційні процеси	Оцінка на 5-рівневій шкалі зрілості; змішана методика	Чітка практична орієнтація, високий фокус на змінах бізнес-моделей	Не враховує специфіку регуляторної стійкості	Deloitte [47]
Gartner Digital Maturity Model	Цифрова стратегія, аналітика даних, технології, гнучкість процесів	Акцент на data-driven governance	Висока застосовність для оцінки клієнтських сервісів	Вузький технологічний фокус	Gartner [80]

1	2	3	4	5	6
McKinsey Digital Quotient (DQ)	Стратегія, культури, компетенції, технології, аналітика	Комплексний індекс із 18 показників	Потужна емпірична база; можливість порівняння галузей	Недоступність повної методології для публічного використання	McKinsey [99]
NIST Cybersecurity Framework (CSF)	Ідентифікація, захист, виявлення, реагування, відновлення	Використовує "модель профілів" для оцінки стану систем	Глибокий акцент на кіберстійкості	Орієнтація на безпекову складову, мало уваги інноваційності	NIST [105]

Джерело: [101].

Порівняння міжнародних методик свідчить, що жодна з існуючих моделей не охоплює комплексно всі аспекти цифрової зрілості, релевантні для фінансових посередників (табл. 2.3, рис. 2.1).

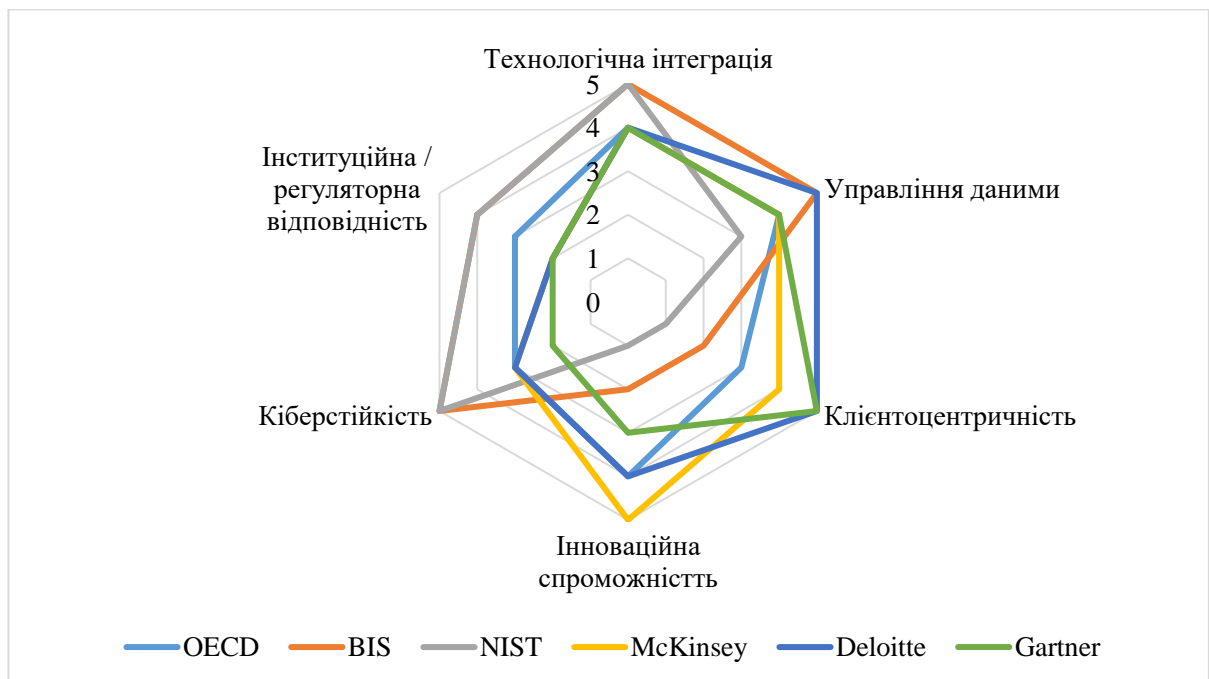


Рис. 2.1. Порівняльна характеристика міжнародних моделей оцінювання цифрової зрілості за ключовими вимірами

Джерело: сформовано автором на основі [108; 32; 47; 80; 99; 105].

Підходи, запропоновані OECD та Deloitte, безсумнівно, формують доволі широку картину цифрової трансформації. Вони охоплюють процесну складову, інноваційний вектор та організаційну динаміку. Проте зазначені рамки

залишають поза увагою специфічні вимоги до забезпечення кіберстійкості. А для таких суб'єктів, як банки, платіжні системи чи небанківські фінансові установи, саме ці вимоги належать до критично важливих.

З іншого боку, методології BIS та NIST зосереджуються переважно на безпековій та інфраструктурній компонентах. Втім, поза їхнім аналітичним полем залишаються поведінка клієнтів, а також інноваційна активність фінансових посередників. Адже саме ці чинники, як відомо, визначають рівень стратегічної конкурентоспроможності в умовах цифрової економіки.

Отже, виникає об'єктивна необхідність у формуванні гібридної методологічної рамки. Така рамка мала б інтегрувати кілька ключових вимірів: інноваційність (на основі напрацювань Deloitte та McKinsey), орієнтацію на клієнта (згідно з підходами Gartner), технологічну інтеграцію (відповідно до моделей OECD), кіберстійкість (із залученням доробку NIST та BIS), а також інституційну відповідність регуляторним вимогам (DORA, EBA, ECB).

У цьому зв'язку постає потреба у формуванні адаптованої до українського контексту системи вимірювання, яка б поєднувала універсальні принципи міжнародних моделей з урахуванням особливостей національного фінансового сектора. Така система має забезпечити можливість порівняльного аналізу між різними групами фінансових посередників, оцінку їхньої технологічної, інноваційної та організаційної готовності та визначити рівень відповідності сучасним вимогам цифрової економіки.

Саме тому наступним етапом дослідження є розроблення авторської моделі оцінки цифрової зрілості фінансових посередників, яка інтегрує ключові елементи міжнародних підходів та адаптує їх до умов функціонування української фінансової системи. Побудова такої моделі дозволяє сформувати цілісну аналітичну рамку, що стане основою для подальших вимірювань цифрової зрілості банків, небанківських фінансових установ та фінтех-компаній.

Авторська модель оцінки цифрової зрілості ґрунтується на гібридній логіці (описаній вище), представлена на рисунку 2.2.

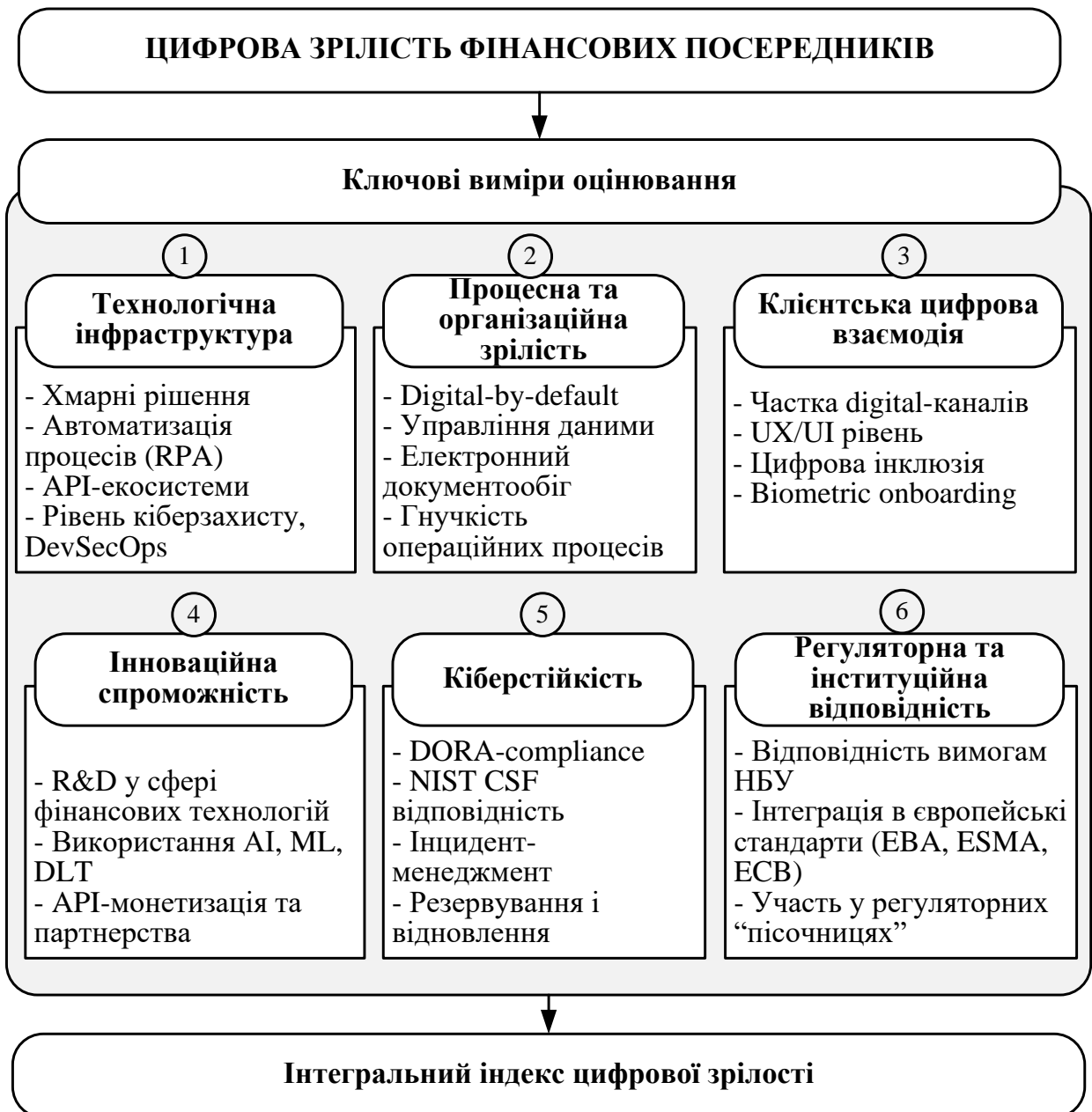


Рис. 2.2. Модель оцінювання цифрової зрілості фінансових посередників України

Джерело: розроблено автором на основі [108; 32; 47; 80; 99; 105].

Оцінювання цифрової зрілості фінансових посередників виступає аналітичним інструментом, за допомогою якого визначається здатність установи адаптуватися до вимог цифрової економіки, впроваджувати інноваційні рішення, забезпечувати належний рівень кіберстійкості та підтримувати якісну клієнтську взаємодію. У міжнародних дослідженнях цифрова зрілість трактується як багатовимірна характеристика, що охоплює

технологічну інфраструктуру, організаційну спроможність, інноваційний потенціал, рівень цифрової взаємодії з клієнтами, кіберстійкість та відповідність регуляторним вимогам [29; 38; 142]. Саме тому побудова інтегральної методики оцінювання потребує чіткої структуризації індикаторів та уніфікації підходів до вимірювання.

У запропонованій моделі індекс цифрової зрілості фінансових посередників формує шестиблокову структуру, кожен елемент якої відображає окремий вимір цифрової трансформації: технологічна інфраструктура, процесна зрілість, клієнтська цифрова взаємодія, інноваційна спроможність, кіберстійкість, регуляторно-інституційна відповідність. Такий поділ індикаторів узгоджується з міжнародними підходами до оцінювання цифрової стійкості фінансових установ, зокрема зі структурою NIST CSF, вимогами регламенту DORA та практиками Світового банку й МВФ [105; 142; 73].

Структура індикаторів подана у таблиці 2.4, яка містить детальний опис показників, їхній характер, спрямованість, джерела даних та блокову належність. Формування індикаторного набору відбувалося на основі трьох принципів: по-перше, репрезентативності – охоплення всіх ключових сфер цифрової трансформації; по-друге, порівнянності – можливості уніфікованого збору даних між різними установами; по-третє, аналітичної значущості – здатності індикатора відображати зміни в цифровому розвитку.

Логіка побудови таблиці 2.4 та критерії її змістовного заповнення базуються на тому, що цифрова трансформація фінансових посередників не є багатовимірним явищем, що пов'язано з неоднорідністю самого феномену цифрової трансформації. Блок «Технологічна інфраструктура» акумулює показники, які характеризують базис цифрової модернізації – інвестиції в технології, хмарні рішення, API-інтеграції, автоматизацію процесів та управління даними [29].

«Процесна зрілість» як окремий блок відображає не лише формальну впорядкованість внутрішніх процедур, а передусім якісну трансформацію підходів до організації діяльності фінансової установи. Йдеться про

поступовий перехід до сучасних управлінських і технологічних практик, зокрема Agile, DevSecOps та принципу Digital-by-default. У цьому контексті Agile доцільно розглядати не стільки як набір інструментів, скільки як логіку організації роботи, що базується на поетапному створенні продуктів, регулярному уточненні вимог і постійній взаємодії з кінцевим користувачем. Такий підхід дозволяє гнучко реагувати на зміни середовища та зменшувати ризик невідповідності результату очікуванням клієнтів.

У межах методики DevSecOps ключовий акцент робиться на об'єднанні трьох складових — безпосередньо розробки, подальшої експлуатації та забезпечення безпеки — в єдиний безперервний цикл. Прикладне значення цього підходу полягає в тому, що питання кіберзахисту інтегруються безпосередньо в архітектуру та логіку побудови цифрових рішень на етапі їх проєктування. Інакше кажучи, безпекові вимоги перестають бути окремою, віддаленою стадією процесу. Принцип digital-by-default, зі свого боку, виходить із положення, згідно з яким продукти та послуги спочатку розробляються як цифрові. При цьому обов'язково враховуються такі критерії, як здатність до масштабування, рівень автоматизації та зручність для кінцевого користувача. Отже, зазначений принцип закріплює пріоритет цифрових каналів як основного, базового формату взаємодії з клієнтом. Одночасна реалізація обох підходів з боку фінансової установи слугує індикатором переходу від моделі функціонування, що характеризується жорсткою регламентацією та фрагментарністю процесів, до більш цілісної та адаптивної моделі. В останній, як показує практика, визначальне значення мають три чинники: швидкість впровадження змін, ефективність міжфункціональної взаємодії, а також технологічна узгодженість окремих рішень між собою.

Ступінь проникнення цифрових каналів у діяльність фінансового посередника знаходить своє відображення у межах блоку «Клієнтська цифрова взаємодія». У сучасних умовах саме цей показник дедалі частіше виступає в ролі головного чинника, що визначає рівень конкурентоспроможності установи.

Інший змістовий блок – «Інноваційна спроможність» – акумулює оцінки, що стосуються активності фінансової інституції у сфері інновацій. При цьому аналіз охоплює як продуктовий рівень, так і рівень бізнес-моделей. До ключових параметрів, що формують цей блок, належать: інтенсивність участі установи у фінансових екосистемах, застосовувані практики роботи з даними (у тому числі з використанням інструментарію штучного інтелекту та машинного навчання — AI/ML), а також спроможність монетизувати API-доступ [16].

До блоку «Кіберстійкість» включено сукупність вимог, викладених у рекомендаційних документах BIS, NIST, а також Національного банку України. Інтеграція цих вимог до загальної аналітичної рамки створює передумови для оцінювання реальної спроможності фінансових інституцій протидіяти кіберзагрозам. Останні, як свідчать дані, характеризуються стійкою тенденцією до зростання як за частотою проявів, так і за рівнем складності [105; 38].

Регуляторна складова, своєю чергою, знаходить своє відображення у блоці «Регуляторна відповідність». Цей блок охоплює: цифрові аспекти імплементації процедур KYC (know your customer) та AML (протидія легалізації коштів), діючі механізми забезпечення захисту персональних даних, а також наявність або відсутність факту участі установи в регуляторних інноваційних середовищах (так званих регуляторних пісочницях) [73].

Об'єднання описаних шести аналітичних вимірів у межах таблиці 2.4 створює підґрунтя для науково коректного переходу до розробки інтегральної методики, призначеної для оцінювання рівня цифрової зрілості. За такого підходу забезпечується виконання двох необхідних умов: по-перше, логічної цілісності пропонованої методики; по-друге, її репрезентативності стосовно досліджуваного феномену.

Таблиця 2.4

Структура індикаторів індексу цифрової зрілості фінансових посередників

Блок	Код індикатора	Зміст індикатора	Тип показника	Орієнтація	Джерело даних для аналізу
1	2	3	4	5	6
Технологічна інфраструктура (TI)	TI1	Частка IT-інвестицій у витратах установи, %	Кількісний, частка	«Більше = краще»	Фінансова звітність, внутрішні дані
	TI2	Рівень хмарної інтеграції (частка критичних систем у хмарі)	Кількісний, частка	«Більше = краще»	IT-звітність, опитування
	TI3	Ступінь API-інтеграції (кількість відкритих / зовнішніх API)	Кількісний	«Більше = краще»	IT-департаменти, відкриті реєстри
	TI4	Рівень автоматизації бізнес-процесів (RPA), % процесів	Кількісний, частка	«Більше = краще»	Внутрішні опитування, аудити
	TI5	Наявність формалізованої системи data governance (0–1 / 0–5)	Якісний, бал	«Більше = краще»	Політики, внутрішні регламенти
Процесна та організаційна зрілість (PO)	PO1	Частка процесів, спроектованих за принципом digital-by-default, %	Кількісний	«Більше = краще»	Опис процесів, внутрішні регламенти
	PO2	Скорочення середнього часу операції після цифровізації, %	Кількісний	«Більше = краще»	Операційна статистика
	PO3	Використання DevSecOps / Agile-підходів (0–1 / 0–5)	Якісний, бал	«Більше = краще»	IT-управлінські документи
	PO4	Частка електронного документообігу, %	Кількісний	«Більше = краще»	Система ЕДО
	PO5	Рівень участі CIO/CTO у стратегічному управлінні (0–5)	Якісний, бал	«Більше = краще»	Структура управління, положення
Клієнтська цифрова взаємодія (CI)	CI1	Частка активних digital-клієнтів у загальній клієнтській базі, %	Кількісний	«Більше = краще»	CRM, аналітика каналів
	CI2	Частка операцій, здійснених у digital-каналах, %	Кількісний	«Більше = краще»	Канальна статистика
	CI3	Частка клієнтів, які пройшли biometric onboarding, %	Кількісний	«Більше = краще»	KYC-системи, фронт-офіс
	CI4	Питома вага мобільних каналів (mobile-first), %	Кількісний	«Більше = краще»	Мобільна аналітика
	CI5	Індекс задоволеності цифровими сервісами (NDSI), бал	Якісний, індекс	«Більше = краще»	Опитування клієнтів

Закінчення таблиці 2.4

1	2	3	4	5	6
Інноваційна спроможність (IN)	IN1	Частка продуктів, що базуються на AI/ML, %	Кількісний	«Більше = краще»	Продуктовий каталог
	IN2	Участь у фінтех-екосистемах / партнерствах (0–1 / 0–5)	Якісний	«Більше = краще»	Угоди, open banking-проекти
	IN3	Витрати на цифрові інновації у % до доходів	Кількісний	«Більше = краще»	Бюджет, управлінська звітність
	IN4	Використання DLT/Blockchain-рішень (0–1 / 0–5)	Якісний	«Більше = краще»	ІТ-проекти
	IN5	Частка доходів від API/платформних сервісів, %	Кількісний	«Більше = краще»	Доходи за видами діяльності
Кіберстійкість (CR)	CR1	Рівень відповідності NIST CSF/DORA (інтегральна оцінка 0–5)	Якісний, бал	«Більше = краще»	Аудити безпеки, комплаєнс
	CR2	Кількість значущих кіберінцидентів на 1000 клієнтів	Кількісний	«Менше = краще»	SOC, журнали інцидентів
	CR3	Середній час відновлення після інциденту (MTTR), год/дні	Кількісний	«Менше = краще»	Операційні журнали
	CR4	Наявність власного/аутсорсингового SOC (0–1)	Бінарний	«1 = краще»	ІТ-структура
	CR5	Частка бюджетів на кібербезпеку у витратах на ІТ, %	Кількісний	«Оптимум/більше»	Фінансова та ІТ-звітність
Регуляторна та інституційна відповідність (RI)	RI1	Відповідність вимогам НБУ щодо ІТ та кіберзахисту (0–5)	Якісний	«Більше = краще»	Регуляторні перевірки
	RI2	Участь у регуляторних «пісочницях» (0–1)	Бінарний	«1 = краще»	Дані НБУ/регулятора
	RI3	Рівень цифрової реалізації AML/KYC (0–5)	Якісний	«Більше = краще»	Політики AML/KYC
	RI4	Відповідність GDPR/захисту персональних даних (0–5)	Якісний	«Більше = краще»	Юридичний аудит
	RI5	Наявність формалізованої ESG/CSR digital-політики (0–1 / 0–5)	Якісний	«Більше = краще»	Нефінансова звітність

Джерело: розроблено автором на основі [36; 98; 158; 155; 188; 108; 32; 47; 80; 99; 105; 29; 38; 137; 142; 73; 5; 16; 179].

Методика розрахунку інтегрального показника цифрової зрілості базується на послідовному застосуванні процедур нормування, визначення вагових коефіцієнтів та агрегування. Такий підхід дозволяє звести різномірні показники (відсоткові, кількісні, якісні) до єдиної шкали вимірювання, врахувати їхню відносну значущість та отримати узагальнену оцінку цифрового розвитку фінансового посередника.

Для деталізації запропонованої концептуальної моделі та відображення методики розрахунку інтегрального показника цифрової зрілості розроблено розширену структурно-логічну схему (рис. 2.3).

Запропонована методика складається з п'яти основних етапів: збір даних, нормування, розрахунок підіндексів, зважування між блоками, інтеграція у загальний індекс.

1 етап. Збір і підготовка даних. На цьому етапі формується вибірка фінансових посередників, які підлягають оцінюванню. Для кожної установи із фінансової звітності, операційної статистики, даних ІТ- та комплаєнс-підрозділів, а також відкритих джерел необхідно зібрати фактичні значення індикаторів. Важливо всі індикатори перевірити на повноту, коректність та узгодженість.

2 етап. Нормування показників. Оскільки індикатори мають різні одиниці виміру, їх потрібно перевести до порівняної шкали, наприклад [0;1].

Для показників типу «більше = краще» використовується лінійне нормування:

$$x_{ij}^* = \frac{x_{ij} - \min(x_j)}{\max(x_j) - \min(x_j)},$$

де x_{ij} – фактичне значення j -го показника для i -ї установи;

$\min(x_j)$, $\max(x_j)$ – мінімальне та максимальне значення показника по всій вибірці;

x_{ij}^* – нормоване значення у діапазоні [0;1].

Для показників типу «менше = краще», наприклад CR2, CR3:

$$x_{ij}^* = \frac{\max(x_j) - x_{ij}}{\max(x_j) - \min(x_j)}.$$

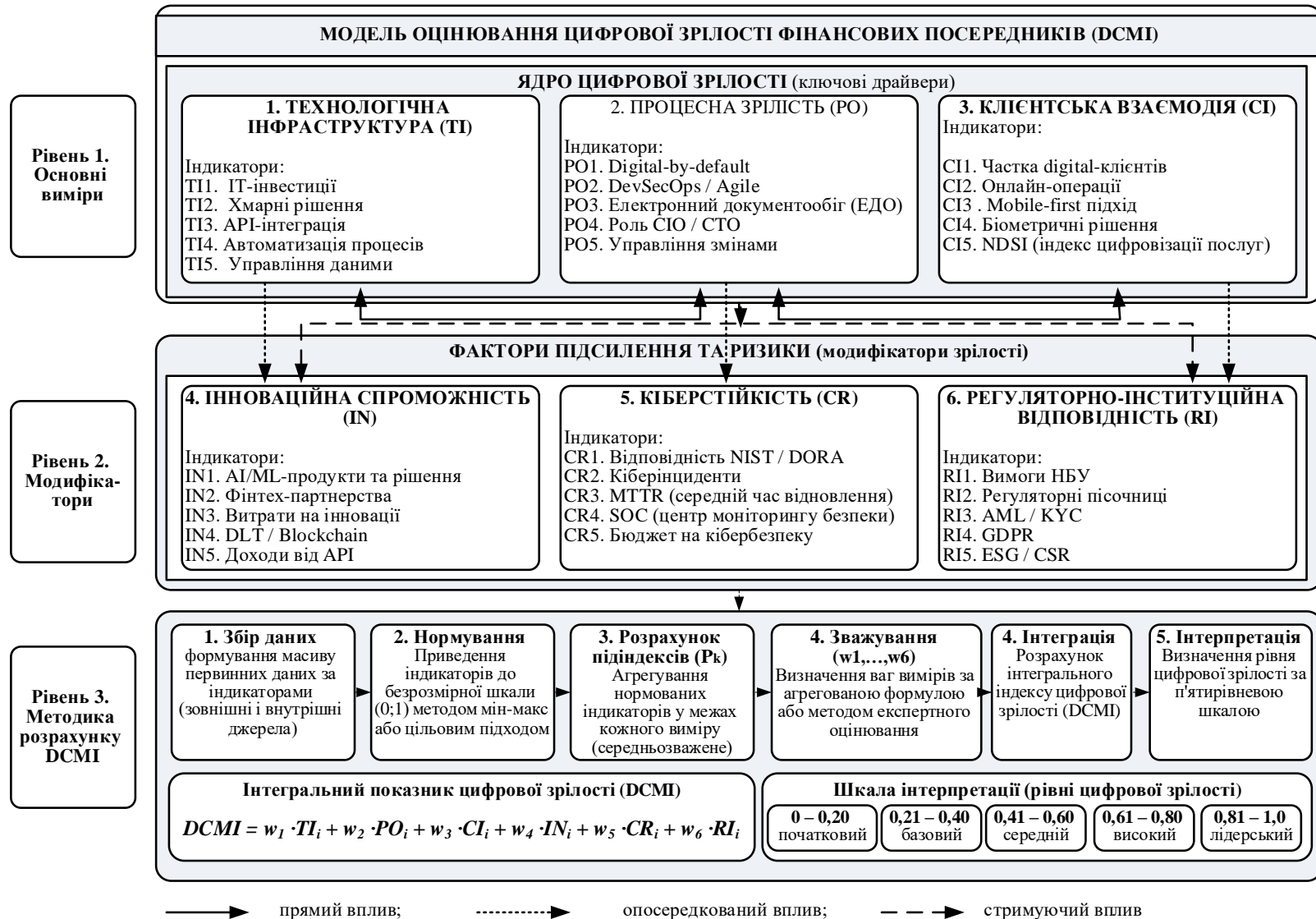


Рис. 2.3. Розширена модель оцінювання цифрової зрілості фінансових посередників України
 Джерело: розроблено автором на основі [98; 158; 188; 108; 32; 47; 80; 99; 105; 29; 38; 142; 73; 5; 16; 179].

У результаті всі індикатори переводяться у шкалу, де 0 – найгірше значення, 1 – найкраще.

3 етап. *Формування підіндексів за блоками.* Для кожного з шести блоків формується підіндекс. Ваги індикаторів усередині блоку можуть бути рівними або експертно визначеними:

$$SubIndex_{k,i} = \frac{1}{m_k} \sum_{j \in k} x_{ij}^*,$$

де $SubIndex_{k,i}$ – значення k -го підіндексу (наприклад, ТІ) для i -ї установи;

m_k – кількість показників у k -му блоці;

$j \in k$ – індикатори, що належать до блоку k .

4 етап. *Зважування блоків та інтегральний індекс.* Загальна оцінка цифрової зрілості визначається як агрегована формула блокових підіндексів:

Для інтегрального індексу задаються ваги w_1, \dots, w_6 для блоків:

- w_1 – для ТІ (технологічна інфраструктура),
- w_2 – РО,
- w_3 – СІ,
- w_4 – ІН,
- w_5 – СР,
- w_6 – РІ.

Інтегральний індекс цифрової зрілості для i -ї установи обчислюється як:

$$DCMI = w_1 \cdot TI_i + w_2 \cdot PO_i + w_3 \cdot CI_i + w_4 \cdot IN_i + w_5 \cdot CR_i + w_6 \cdot RI_i.$$

У базовому варіанті ваги блоків рівні:

$$w_1 = w_2 = \dots = w_6 = 1/6.$$

Альтернативно, ваги можуть визначатися експертною групою. Однак це потребує врахування стратегічної ваги кіберстійкості чи технологічної модернізації [179].

Етап 5. *Інтерпретація результатів.* Важливим елементом методичного забезпечення оцінювання цифрової зрілості фінансових посередників є формування шкали інтерпретації отриманих результатів. Запропоновано авторську шкалу оцінювання, яка базується на п'ятирівневій градації і передбачає інтерпретацію інтегрального показника цифрової зрілості, значення якого варіюється у межах від 0 до 1 (табл. 2.5).

Шкала рівнів цифрової зрілості фінансових посередників

Значення інтегрального показника	Рівень цифрової зрілості	Характеристика
0 – 0,20	Початковий	Використання цифрових технологій є фрагментарним; відсутня цифрова стратегія; низький рівень автоматизації та цифрових компетенцій
0,21 – 0,40	Базовий	Запроваджено окремі цифрові рішення; часткова автоматизація процесів; цифровізація має несистемний характер
0,41 – 0,60	Середній	Цифрові технології інтегруються у ключові бізнес-процеси; формується цифрова стратегія; зростає роль онлайн-каналів
0,61 – 0,80	Високий	Системна цифровізація діяльності; активне використання даних і аналітики; розвинені цифрові сервіси та клієнтські канали
0,81 – 1,00	Лідерський	Повна інтеграція цифрових технологій; інноваційна бізнес-модель; використання AI, платформних рішень та екосистемний підхід

Джерело: розроблено автором на основі [98; 158; 178; 188].

Запропонована шкала дозволяє ідентифікувати поточний рівень цифрового розвитку фінансового посередника, визначити напрями підвищення цифрової зрілості, здійснювати порівняльний аналіз між установами, використовувати результати оцінювання у процесі формування стратегії розвитку, забезпечити моніторинг динаміки цифрової трансформації.

Запропонована методика дозволяє комплексно оцінити цифрову зрілість фінансових посередників, інтегруючи як технічні та організаційні аспекти трансформації, так і інноваційні, клієнтські та регуляторні вимоги. На нашу думку, цей підхід має безумовні переваги. На відміну від фрагментарних підходів, які зосереджуються лише на IT-інфраструктурі чи клієнтській активності, інтегральний індекс цифрової зрілості охоплює системну логіку цифрового розвитку фінансових установ. Такий підхід забезпечує можливість порівняльного аналізу між різними групами посередників, виявлення інституційних бар'єрів, визначення пріоритетів цифрової політики та моніторингу ефективності цифрової трансформації на рівні сектору та окремих установ.

Розроблена авторська модель оцінювання цифрової зрілості фінансових посередників формує цілісну концептуальну рамку, у межах якої цифрова

трансформація розглядається як багатовимірний процес, що поєднує технологічні, організаційні, клієнтські, інноваційні та регуляторні компоненти. Такий підхід дозволяє структурувати індикатори за шістьма ключовими блоками, забезпечити їхню логічну взаємодію та визначити інтегральні характеристики цифрової спроможності фінансових установ.

Отже, сукупність складових забезпечує комплексне оцінювання цифрової зрілості з урахуванням як внутрішніх процесів, так і зовнішніх викликів (рис. 2.4).

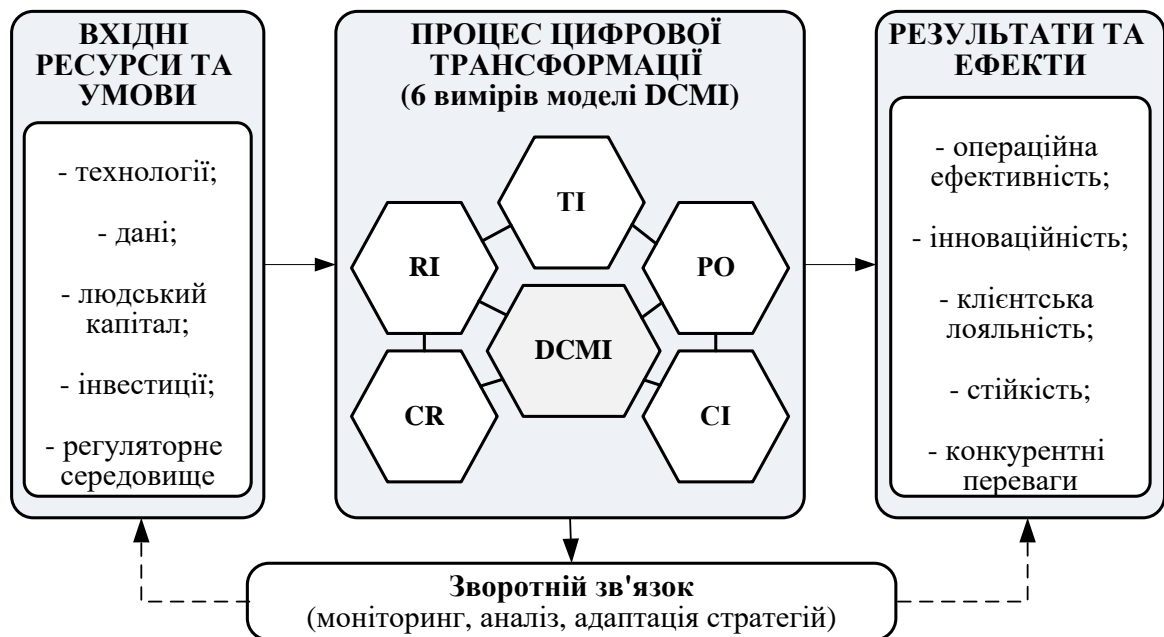


Рис. 2.4. Системна роль цифрової зрілості у стратегічному розвитку фінансових посередників

Джерело: розроблено автором на основі [98; 158; 188; 108; 32; 47; 80; 99; 105; 29; 38; 142; 164; 73; 5; 16; 179].

Таким чином, методика оцінювання цифрової зрілості базується на послідовному переході від аналізу окремих показників до формування інтегрованого результату та управлінських висновків (Показники → Нормалізація → Зважування → Інтегральний індекс → Рівень → Управлінські рішення). Такий підхід забезпечує цілісність методики та її орієнтацію на практичне використання у процесі формування стратегії розвитку фінансових посередників. Розроблений методологічний інструментарій створює підґрунтя для аналізу впливу цифрових технологій на стратегічне управління (підрозділ 2.2) та інтегрального оцінювання рівня цифрової зрілості фінансових посередників (підрозділ 2.3).

2.2. Аналіз впливу цифрових технологій на ефективність стратегічного управління фінансовими посередниками в Україні

Цифрова трансформація фінансового сектору набула системного характеру, визначаючи нові параметри функціонування, конкурентоспроможності та стратегічного розвитку фінансових посередників у всьому світі. Теоретичні узагальнення, здійснені в розділі 1 цієї дисертації, показали, що цифрові технології суттєво змінюють зміст функцій фінансових посередників, зумовлюють появу нових форм створення цінності та перетворюють традиційні інституційні моделі на гнучкі, інтегровані й орієнтовані на дані екосистеми. Проте для розкриття реального масштабу таких трансформацій недостатньо лише концептуальної інтерпретації: необхідним є глибоке емпіричне дослідження їхніх проявів у практиці.

Сучасний стан розвитку сектору фінансових посередників демонструє пряму залежність від цифрових інновацій. Останні виконують роль ключових рушіїв стратегічного планування. Під їхнім впливом зростає гнучкість реагування на кон'юнктурні ринкові коливання. Перебудовуються комунікаційні канали типу «установа – клієнт». Трансформації зазнають підходи до побудови інфраструктури. Водночас жорсткішими стають вимоги до забезпечення кіберстійкості, а також до параметрів операційної безперервності. Українські реалії надають цим процесам додаткової ваги. Фінансові установи тут вирізняються високою технологічною динамікою. Спостерігається активне впровадження систем штучного інтелекту, хмарних обчислювальних платформ, механізмів відкритого банкінгу. Використовуються засоби біометричної ідентифікації, будуються API-екосистеми, розвивається цифрова інфраструктура для платежів та розрахунків.

Проведення аналітичного оцінювання окреслених процесів є необхідною передумовою для формування доказових висновків стосовно стратегічних імперативів, які стоять перед фінансовими посередниками. Лише завдяки такій оцінці видається можливим: по-перше, визначити рівень реальної цифрової

готовності конкретної установи; по-друге, виявити структурні зміни в реалізації як традиційних, так і новітніх функцій цими установами; по-третє, оцінити глибину впливу технологічних нововведень на наявні операційні, продуктові та управлінські моделі; по-четверте, простежити закономірності, які супроводжують формування нових стратегічних траєкторій.

Враховуючи вищенаведене, першочерговим завданням є визначення контексту, у межах якого відбувається цифрова трансформація фінансових посередників. Зміни у функціональній моделі фінансових установ неможливо оцінити ізольовано від загальних тенденцій розвитку світового фінансового сектору, глобальних технологічних трендів, регуляторних новацій і специфіки національних умов. Саме *порівняння міжнародного та українського* контекстів дозволяє ідентифікувати ключові драйвери цифровізації, розкрити фактори, що визначають темпи трансформації та оцінити ступінь відповідності вітчизняних фінансових посередників сучасним вимогам цифрової економіки.

Отже, початковим етапом аналітичної процедури виступає дослідження глобальних і національних векторів цифрової еволюції фінансових посередників. Саме ці вектори створюють те середовище, у якому відбуваються стратегічні зміни зазначених інституцій. Такий підхід дає змогу отримати системне уявлення про комплекс зовнішніх і внутрішніх факторів, котрі окреслюють як потенційні можливості, так і наявні обмеження для стратегічного поступу фінансових посередників. Надалі це формує підґрунтя для оцінювання рівня їхньої цифрової зрілості та характеру функціональних трансформацій.

Сучасні технологічні зрушення впливають не тільки на робочі інструменти – вони видозмінюють саму сутність відносин між власниками капіталу та його потенційними отримувачами. На сьогодні цифрова трансформація еволюціонувала від етапу «оптимізації внутрішніх процесів» до фази «перетворення бізнес-моделей». За оцінками аналітиків компанії Fortune Business Insights, світовий ринок фінансових технологій у 2024 році сягнув 340,1 млрд дол. США; до 2032 року прогнозується його зростання до 1,1 трлн дол. із середньорічним темпом приросту приблизно 16,2 % [79].

У контексті глобальних процесів цифрової трансформації, що охопили фінансовий сектор, інститут фінансового посередництва все більше набуває характеристик технологічно залежної, платформно організованої та даноцентричної системи. Згідно з аналітичними матеріалами Базельського комітету з банківського нагляду, визначальною рисою сучасного етапу виступає масштабне застосування інноваційних технологій – зокрема, великих масивів даних (Big Data), штучного інтелекту, хмарних обчислень, технології розподіленого реєстру (DLT) та програмних інтерфейсів (API) – на всіх етапах банківського ланцюга створення доданої вартості: від фронт-офісу до бек-офісу та підсистем управління ризиками [29; 33].

Зокрема, у статистичному огляді Банку міжнародних розрахунків (BIS) за 2023 рік станом на 2021 р. у країнах з ринками, що розвиваються, номінальна вартість безготівкових платежів зросла приблизно на 15 % порівняно з показниками попереднього року. У цьому ж документі зазначено, що в країнах-членах Комітету з платіжних та ринкових інфраструктур (CPMI), який представляє 28 центральних банків країн світу (у тому числі США, Велика Британія, Швеція, Швейцарія, Іспанія, Нідерланди, Мексика, Японія, Європейський союз, Канада, Китай та інших), середня кількість безготівкових платежів на людину зросла зі 179 транзакцій у 2012 р. до 332 – у 2021 р. [33].

Динаміка, що спостерігається у світовому цифровому середовищі, безпосередньо позначається на двох аспектах фінансового посередництва. По-перше, змінюється набір інструментів. По-друге, трансформується сама суть того, як це посередництво функціонує. Замість класичного «балансоцентричного банкінгу» дедалі частіше з'являються мережеві цифрові платформи. Останні, як правило, інтегрують одразу кілька типів учасників: традиційні банки, небанківські структури, фінтех-компанії та провайдерів даних.

Операційним стандартом фінансових посередників стають штучний інтелект (AI) та хмарні обчислення. Так, згідно зі звітом Accenture, впровадження генеративного AI у банківському секторі здатне підвищити продуктивність працівників на 30 % при виконанні мовних завдань та збільшити доходи банків до 6 % протягом трьох років [4; 5]. А за даними Capgemini

Research Institute 2023 року, 91 % банків та страхових компаній вже розпочали свій шлях трансформації у хмару, розглядаючи її як основу для масштабування та інновацій. Це, за висновками аналітиків, дозволяє установам переходити від капітальних витрат до операційних витрат (від CapEx до OpEx), забезпечуючи тим самим необхідну гнучкість інфраструктури [38].

Завдяки розвитку економіки, заснованої на використанні програмних інтерфейсів (API), а також завдяки регуляторним заходам, зокрема Директиві PSD2, що діє в межах Європейського Союзу, спостерігається активне поширення моделі відкритого банкінгу у світовому масштабі. Суть цієї моделі полягає в тому, що банківські установи, використовуючи стандартизовані API, за умови отримання згоди від клієнта, надають стороннім організаціям доступ як до даних про клієнта, так і до окремих банківських функцій.

Дослідження ОЕСР показують, що відкритий банкінг, побудований на стандартизованих API та механізмах обміну фінансовими даними за згодою клієнта, змінює конкурентну динаміку на ринку. Зокрема, з'являються нові гравці-агрегатори, зростає роль фінтех-сектору, відбувається перехід від вертикально інтегрованих банків до розщеплених ланцюгів створення фінансових послуг [115]. Ринок Open Banking у 2024 році оцінюється приблизно в 30 млрд доларів з прогнозом зростання до 129 млрд доларів до 2032 року. У Великій Британії, яка є піонером у цій сфері, у липні 2024 року було зафіксовано 10 мільйонів активних користувачів Open Banking [112]. Це свідчить про масовість використання технології мільйонами людей.

Зауважимо, що нині у країнах Латинської Америки, ЄС та інших регіонах відкритий банкінг розглядається не лише як технологічна інновація, а як інструмент посилення конкуренції та фінансової інклюзії, що відкриває доступ до послуг для нових клієнтів.

Паралельно відбувається стрімкий перехід до безготівкової економіки. У цьому аспекті показовими є наступні дані. Глобальна вартість цифрових платежів у 2024 році перевищила 11 трлн доларів. Одночасно використання готівки скорочується приблизно на 4 % щорічно. Транскордонні платежі, за прогнозами, зростуть зі 195 трлн доларів (2024) до 320 трлн доларів у 2032 році [100].

Другий важливий тренд пов'язаний із цифровими фінансовими послугами (Digital Financial Services, DFS) та фінтех-сектором. За оцінками Світового банку, цифрові фінансові сервіси здатні знижувати вартість транзакцій, підвищувати швидкість, прозорість та безпеку платежів, а також масштабувати доступ до фінансових продуктів для малих підприємств і домогосподарств, які раніше обслуговувалися лише неформальним сектором [138]. У дослідженні Cambridge Centre for Alternative Finance спільно з BIS 2020 року відмічається, що глобальний потік кредитів «fintech + big tech» у 2019 р. оцінювався приблизно USD 795 млрд, з них big tech – біля USD 572 млрд [41].

Згідно з актуалізованими статистичними даними щодо світового ринку фінансових технологій, збільшення питомої ваги безготівкових та цифрових транзакцій відбувається одночасно з підвищенням рівня охоплення населення банківськими рахунками, а також з активізацією використання мобільних платіжних інструментів у державах із ринками, що розвиваються [139]. Який із цього впливає висновок? Фінансове посередництво у глобальних масштабах втрачає статус виняткової сфери діяльності традиційних банківських інституцій. Натомість воно дедалі частіше реалізується через альтернативні канали та структури: цифрові платформи, електронні гаманці, суперагрегатори, а також екосистеми, створювані великими технологічними компаніями (BigTech).

Третій блок глобальних тенденцій стосується впливу фінтех-компаній на традиційних посередників. Дослідження експертів МВФ засвідчують, що посилення присутності фінтех-компаній створює помітний тиск на прибутковість банків, насамперед через скорочення процентних доходів та підвищення операційних витрат у відповідь на технологічну конкуренцію [103]. При цьому банки змушені одночасно вкладати ресурси в модернізацію IT-архітектури, кібербезпеку, розвиток мобільних сервісів та уніфікацію клієнтського досвіду. Така конкуренція стимулює перехід до партнерських моделей: спільні продукти банків і фінтехів, white-label-рішення, використання моделей Banking-as-a-Service (BaaS) та Banking-as-a-Platform (Baap), коли банк перетворюється на інфраструктурний або сервісний бекенд для широкого кола ринкових учасників.

Фактично через моделі «Банк як послуга» (Banking-as-a-Service) відбувається розмивання кордонів між фінансовими та нефінансовими сервісами. За аналітичними даними й оцінкою McKinsey & Company, ринок «вбудованих фінансів» до 2030 року може генерувати до 230 млрд доларів доходу [100]. Bain & Company прогнозують ще більш масштабний вплив: за їхнім прогнозом обсяг транзакцій через вбудовані фінанси може перевищити 7 трлн доларів до 2026 року [19]. Це створює тиск на традиційні банки, змушуючи їх інтегруватися у платформи нефінансових компаній або будувати власні екосистеми.

Характерно, що 55 % нефінансових компаній планують впровадити фінансові послуги у свої продукти протягом найближчих двох років. Це створює серйозний тиск на традиційні банки, змушуючи їх або ставати «утилітарними провайдерами» (які працюють на бекенді, невидимо для клієнта), або будувати власні екосистеми.

Четвертий глобальний тренд пов'язаний із даними як ключовим стратегічним ресурсом цифрового фінансового посередництва. Робота аналітиків OECD «*Digitalisation of financial services, access to finance and aggregate economic performance*» показує, що цифровізація фінансових послуг та інтенсивне використання ІКТ-інвестицій і цифрових сервісів у фінансовому секторі суттєво впливають на доступ до фінансування та макроекономічні показники, зокрема продуктивність. Згідно з дослідженням OECD, «10 % зростання цифровізації фінансового сектору асоційовано з близько 0,1 % пунктом зростання продуктивності для середньої промисловості» [34]. З практичного погляду це означає, що конкурентні переваги фінансових посередників дедалі більше визначаються якістю збору, обробки та використання даних: можливостями скорингових моделей на основі Big Data, персоналізації продуктів, поведінкової аналітики, автоматизованого моніторингу шахрайства та регуляторної звітності в режимі реального часу.

Водночас цифровізація фінансового посередництва супроводжується посиленням вимог до кіберстійкості та операційної надійності. У дослідженнях Базельського комітету та міжнародних організацій

наголошується, що широке використання хмарних рішень, відкритих API, модульних архітектур і зовнішніх IT-провайдерів одночасно створює нові вектори атаки, посилює залежність від критичних постачальників ІКТ та ускладнює управління операційними ризиками [29]. Тому на глобальному рівні формується тренд на інтеграцію принципів операційної стійкості, «кібер-за замовчуванням» / проєктування з кібербезпекою (cyber-by-design) та нагляду на основі ризиків (risk-based supervision) у регуляторні рамки, що відображається, зокрема, у прийнятті регламенту DORA в ЄС та посиленні стандартів ІКТ-ризик-менеджменту для фінансових установ.

Окремо слід виокремити тренд цифрової фінансової інклюзії. Опитування МВФ щодо Financial Access Survey та аналітика Світового банку демонструють, що цифрові платіжні інструменти, мобільні гаманці, спрощені процедури ідентифікації клієнтів та дистанційні кредитні продукти дозволяють залучати до фінансової системи раніше недоохоплені групи населення та малий бізнес [84].

У низці країн цифрові платформи платежів стають основою для формування нових каналів кредитування, скорочуючи трансакційні витрати й створюючи умови для масштабування мікрофінансування та малого підприємництва [92]. Прикладом такої країни є Індія і її система UPI. Створення такої системи підсилює роль фінансових посередників як каналу соціально орієнтованого розвитку та розширення доступу до фінансових послуг. Це водночас підвищує вимоги до захисту споживачів, прозорості алгоритмів та етичного використання даних.

У власних дослідженнях, присвячених впливу цифрових технологій на стратегії розвитку фінансових посередників в Україні, показано, що зазначені глобальні тренди – платформізація, посилення ролі даних, партнерські моделі «банк-фінтех», зростання значення цифрової довіри – мають універсальний характер, але проявляються з різною інтенсивністю залежно від інституційних та регуляторних умов конкретної країни, що створює підґрунтя для висновку, що глобальні тенденції розвитку цифрового фінансового посередництва не є

одноманітними, а формують спектр моделей цифрової трансформації, в межах якого національні фінансові системи обирають власні траєкторії – від консервативної модернізації до агресивної інноваційної експансії [229].

Підсумовуючи розгляд глобальних тенденцій, можна стверджувати, що еволюція цифрового фінансового посередництва відбувається за такими основними векторами: формування екосистемної архітектури, перехід до моделей, орієнтованих на використання даних (даноцентричність), підвищення рівня цифрової інклюзії, а також зміцнення операційної стійкості. У наступних розділах роботи зазначені процеси розглядатимуться більш детально. З цією метою буде проаналізовано міжнародні регуляторні підходи, а також виявлено особливості їхньої реалізації в українському фінансовому секторі. Такий аналіз, у свою чергу, дасть змогу сформулювати цілісне уявлення про зовнішні та внутрішні умови, у яких відбувається стратегічний розвиток фінансових посередників у контексті цифрової економіки.

Цифрові перетворення у фінансовому секторі характеризуються неоднорідністю та відсутністю єдиної спрямованості. Зазначена обставина зумовлює необхідність упорядкування головних глобальних тенденцій, оскільки саме вони задають стратегічні орієнтири для розвитку сучасного фінансового посередництва.

Для здійснення порівняльного аналізу цих процесів пропонується систематизувати основні вектори цифрової трансформації. Джерелами для такої систематизації слугуватимуть міжнародні аналітичні матеріали таких організацій, як OECD, BIS, World Bank, а також регіональні нормативні документи Європейського Союзу.

Результати узагальнення представлено у таблиці 2.6, у якій наведено порівняльну характеристику виокремлених тенденцій. Це дає змогу, з одного боку, виявити спільні риси цифрового розвитку між провідними світовими юрисдикціями, а з іншого — встановити відмінності у відповідних векторах залежно від сфери діяльності фінансових посередників.

Таблиця 2.6

Порівняльна характеристика глобальних трендів цифрової трансформації

Глобальний тренд	Ключова характеристика	Прояви у провідних юрисдикціях (США / ЄС / Азія)	Стратегічні наслідки для фінансових посередників	Підтвердження даними
1. Масштабування цифрових платежів	Перехід до швидких, безготівкових та мобільних транзакцій	США – домінування RTP; ЄС – SEPA; Азія – UPI, FPS	Потреба в миттєвих розрахунках, розвиток платіжних платформ	BIS (2023) [23]
2. Платформізація та API-економіка	Open Banking, інтеграція через API, модульність сервісів	ЄС – PSD2/Open Banking; США – Open Finance ініціативи; Азія – супердодатки	Перехід до BaaS/BaaP, конкуренція між платформами	OECD (2024a) [115]
3. Штучний інтелект та ML у фінансах	Автоматизація прийняття рішень, поведінкова аналітика	США – AI-кредитування; ЄС – регуляція AI Act; Китай – інтенсивне впровадження AI-скорингу	Оптимізація ризик-менеджменту, персоналізація	IMF (2023) [87]
4. Зростання ролі BigTech у кредитуванні	Кредитування на платформах Amazon, Alibaba, Tencent	США – PayPal/Amazon Lending; Китай – Ant Group; ЄС – обмежене проникнення	Виклики для традиційних фінансових установ	Cornelli et al. (2020) [42]
5. Хмарні та DLT-інфраструктури	Перенесення процесингу в хмару, токенизація активів	США – AWS/Google Cloud у банках; ЄС – DLT-пілоти ECB; Азія – MAS Project Guardian	Нові інструменти капіталізації та ринкової інфраструктури	ECB (2025) [62]
6. Миттєві платежі та цифрові валюти (CBDC)	Розвиток систем real-time payments, національні пілоти CBDC	ЄС – пілот цифрового євро; Китай – e-CNY; США – FedNow	Потреба у новій архітектурі розрахунків та стійкості	BIS (2023) [24]
7. Підвищення ролі кіберстійкості (DORA/NIST)	Інституціоналізація вимог до ICT-ризиків та операційної стійкості	ЄС – DORA; США – NIST CSF; Азія – MAS TRM Guidelines	Зміна моделей операційного управління	EU (2022) [63]
8. Вибухове зростання фінансової інклюзії через мобільні сервіси	Mobile-first, цифрові гаманці, P2P платежі	Африка – M-Pesa; Півд.-Східна Азія – GCash; Індія – UPI	Нові ринки, розширення клієнтської бази	World Bank (2022) [141]

Джерело: розроблено автором на основі [24; 75; 115; 42; 62; 63; 87; 141; 165; 121].

Аналіз змісту таблиці 2.6 дозволяє констатувати, що цифрова трансформація фінансового посередництва являє собою складне, багатопланове явище. У цьому процесі технологічна, регуляторна та ринкова складові знаходяться у стані постійної взаємодії. Ключовим висновком, який випливає з наведених даних, є такий: цифрові технології виходять за межі суто операційного інструментарію. Вони детермінують появу нових змагальних форматів, провокують видозміну моделей вартісної генерації, переформатують систему відносин між фінансовими установами, споживачами їхніх послуг та партнерськими екосистемами. Порівняльна характеристика, представлена у таблиці, виразно засвідчує наявність суттєвих відмінностей між різними юрисдикціями. Якщо Європейський Союз акцентує увагу на нормативному підґрунті операційної стійкості (насамперед у форматі DORA) та правовій регламентації відкритих інтерфейсів (API), то для США та азійських країн характерним є інноваційний тиск, зумовлений активізацією великих технологічних корпорацій (BigTech) та експансією моделей фінансових суперагрегаторів. Окремо слід відзначити прискорені темпи зростання цифрової інклюзії у країнах із ринками, що розвиваються. Зазначена тенденція ініціює формування нових споживчих сегментів, а також справляє вагомий вплив на функціональну роль небанківських посередників.

Узагальнення глобальної практики надає можливість прослідкувати не тільки актуальний стан досліджуваних явищ, але й довготермінову динаміку видозміни моделей фінансового посередництва. Світові дані переконливо демонструють: цифрова трансформація не є одноактною подією. Вона реалізується як багатоступінчастий, хвилеподібний процес. Характерна риса останнього полягає у тому, що кожна нова технологічна хвиля не скасовує попередню, а нашаровується на неї. Наслідком стає ефект акумуляції інноваційних зрушень. На ранніх етапах цифрові зміни обмежувалися двома основними напрямками: оцифруванням окремих транзакційних операцій та впровадженням віддалених каналів сервісу. З плином часу, однак, зазначені

зміни поширилися на значно ширше коло об'єктів. У їхнє коло потрапили бізнес-моделі, комунікаційні канали зі споживачами, методологічні підходи до оцінки ризиків, а також власне інституційна архітектура фінансового сектору.

На початкових стадіях цифровізація мала переважно прикладний, інструментальний характер. Її сприймали передусім як засіб підвищення операційної результативності. До основних напрямів належали: автоматизація внутрішніх бізнес-процесів, впровадження електронних платіжних форм та оптимізація системи документообігу. Ситуація змінилася з поширенням хмарних технологій, відкритих програмних інтерфейсів (API), інструментів штучного інтелекту та технологій розподілених реєстрів (DLT). Саме ці фактори спричинили перехід цифровізації на якісно новий, системний рівень. Унаслідок цього трансформації зазнали ключові аспекти функціонування фінансової сфери. Йдеться, зокрема, про логіку створення та розподілу фінансової цінності, інституційні функції учасників ринку, саму природу конкурентних відносин, а також базові механізми формування довіри в економічній системі.

Зазначене зумовлює закономірний перехід сучасних фінансових ринків від класичних вертикально інтегрованих моделей до альтернативних форматів організації. У традиційній моделі банк виконував роль головного постачальника всього спектра фінансових послуг. На зміну їй приходять екосистемні та платформні структури. У межах цих нових конфігурацій фінансовий посередник набуває дещо інших функцій — інтегратора, координатора або, за образним висловом, «оркестратора» різноманітних сервісів. Подальша еволюція, як свідчать прогнози, визначатиметься трьома взаємопов'язаними напрямками. По-перше, це поширення токенизації активів. По-друге, впровадження цифрових валют центральних банків (CBDC). По-третє, становлення розподіленої, модульної фінансової інфраструктури. Наочне зображення цих процесів наведено на рисунку 2.5.

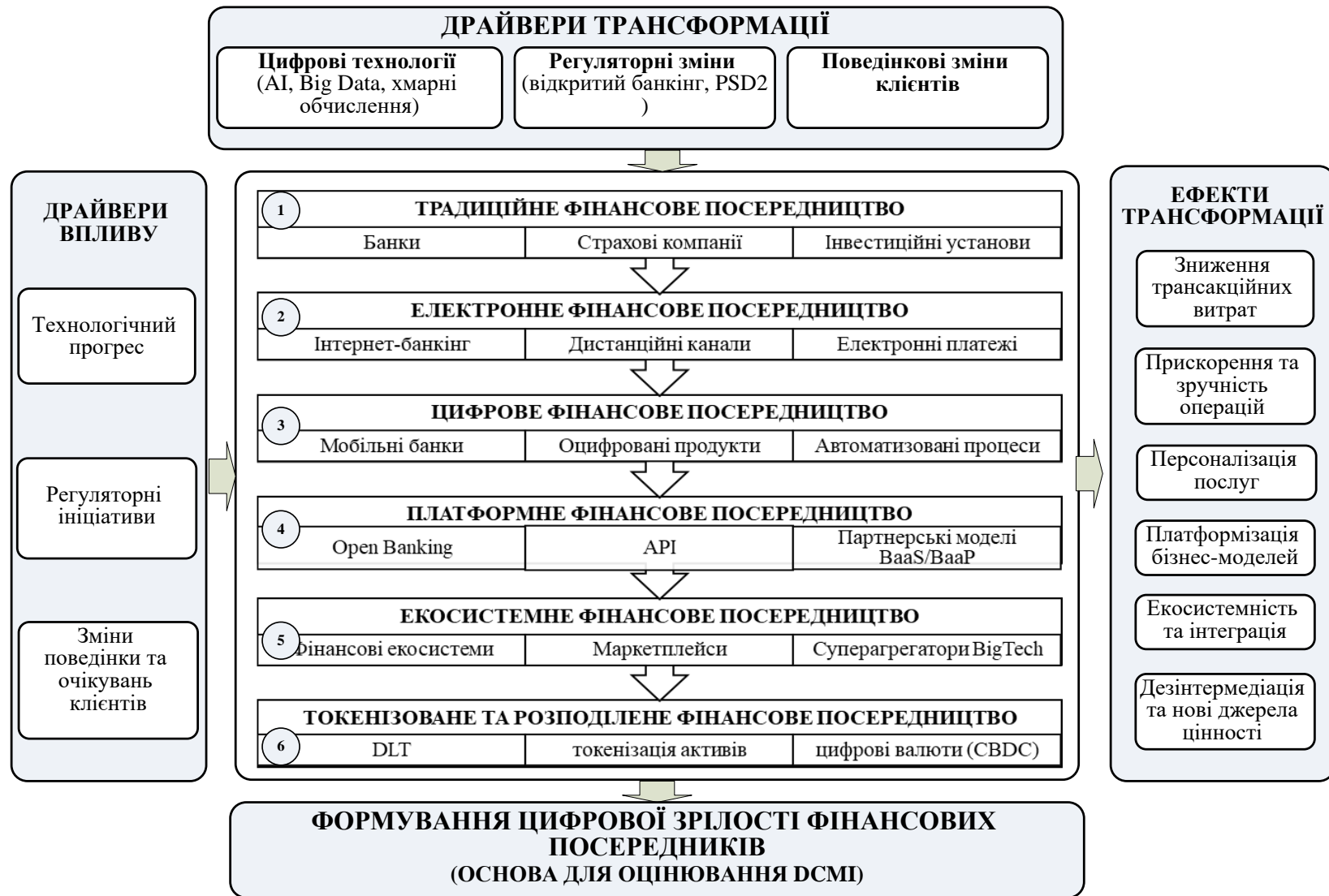


Рис. 2.5. Еволюція моделей фінансового посередництва в умовах цифрової трансформації

Джерело: розроблено автором.

Представлена на рис. 2.1 еволюція моделей фінансового посередництва відображає поступовий перехід від традиційного банкінгу → до електронних сервісів → до цифрових платформ → до фінансових екосистем → до токенизованих і децентралізованих моделей фінансів. При цьому кожен наступний етап не заміщує попередній, а доповнює його, формуючи багаторівневу архітектуру сучасного фінансового посередництва. Така трансформація створює передумови для формування цифрової зрілості фінансових посередників, що покладено в основу подальшого методичного інструментарію оцінювання.

Цифрова трансформація не зводиться до технологічного оновлення інструментів чи розширення клієнтських каналів. Вона репрезентує глибинну структурну перебудову, в межах якої видозмінюються рольові функції учасників ринку, параметри конкурентного середовища та механізми формування фінансової цінності. Перехід від традиційних банківських моделей до платформних і екосистемних форм супроводжується зміною базової логіки діяльності фінансових посередників: від продуктового підходу – до орієнтації на дані, від вертикально організованих операцій – до модульної інтеграції, від централізованих систем – до децентралізованих рішень.

Важливою закономірністю виступає кумулятивний характер еволюції: кожен новий етап не витісняє попередній, а інтегрує його сильні сторони. Наприклад, цифровий банкінг виник на основі електронних сервісів, а екосистемні моделі формуються лише за наявності розвиненої цифрової інфраструктури та стандартів інтероперабельності. Становлення токенизованих фінансів та цифрових валют центральних банків, своєю чергою, потребує накопичення критичної маси технологічних, регуляторних і поведінкових передумов.

Зі зміною моделей фінансового посередництва трансформуються також механізми довіри та ризик-менеджменту. Технологічна довіра – заснована на шифруванні, кіберстійкості, цифровій ідентичності – поступово доповнює та частково витісняє традиційну інституційну довіру. Це змінює роль фінансового посередника: від носія інституційної репутації до гаранта технологічної безпеки та операційної надійності. Таким чином, еволюційний рух від традиційних до цифрових, платформних, екосистемних і токенизованих

моделей свідчить про формування нового типу фінансової системи. У ній інновації, дані та технологічна інфраструктура набувають статусу ключових факторів конкурентоспроможності.

Попри наявність спільної технологічної бази, процеси цифровізації в різних країнах набувають неоднакових форм. Джерелом таких відмінностей виступають передусім специфіка регуляторного середовища, ступінь інституційної зрілості національних фінансових ринків, роль державних інститутів, а також рівень інтегрованості FinTech-сектору.

У зв'язку з цим видається обґрунтованим проведення системного порівняння провідних світових моделей цифрової трансформації. Такий аналіз дозволяє, з одного боку, виявити спільні риси, притаманні різним юрисдикціям, а з іншого – оцінити потенційні можливості адаптації відповідних підходів до умов України.

Методологічне підґрунтя для здійснення такого порівняння формують три концептуальні рамки: інституційного порівняння (North, 1990), регуляторної конвергенції (Arner et al., 2017), а також оцінювання цифрової зрілості фінансових систем (OECD, 2023; BIS, 2022) [16; 63; 21]. Застосування зазначених підходів дає змогу трактувати цифрову трансформацію не як виключно технологічний феномен, а як складову еволюції фінансових екосистем, у межах якої взаємодіють держава, фінансові інституції, технологічні компанії та кінцеві споживачі.

Методологічна схема дослідження передбачає виділення п'яти вимірів для порівняльного аналізу (рис. 2.6). Перший – *регуляторний* – фокусується на характері державного нагляду та наявності нормативної бази. Другий – *інституційний* – оцінює розподіл ролей між банками, небанківськими посередниками, великими технологічними компаніями та державними структурами у фінансовій екосистемі. Третій – *технологічний* – визначає рівень впровадження інновацій. Четвертий вимір (*фінансова інклюзія та довіра*) показує, наскільки цифровізація розширює доступ до послуг і підвищує стійкість фінансових систем. П'ятий вимір (*кіберстійкість і операційна надійність*) відображає ступінь розвитку механізмів захисту даних, практик управління ризиками та стану кіберінфраструктури.

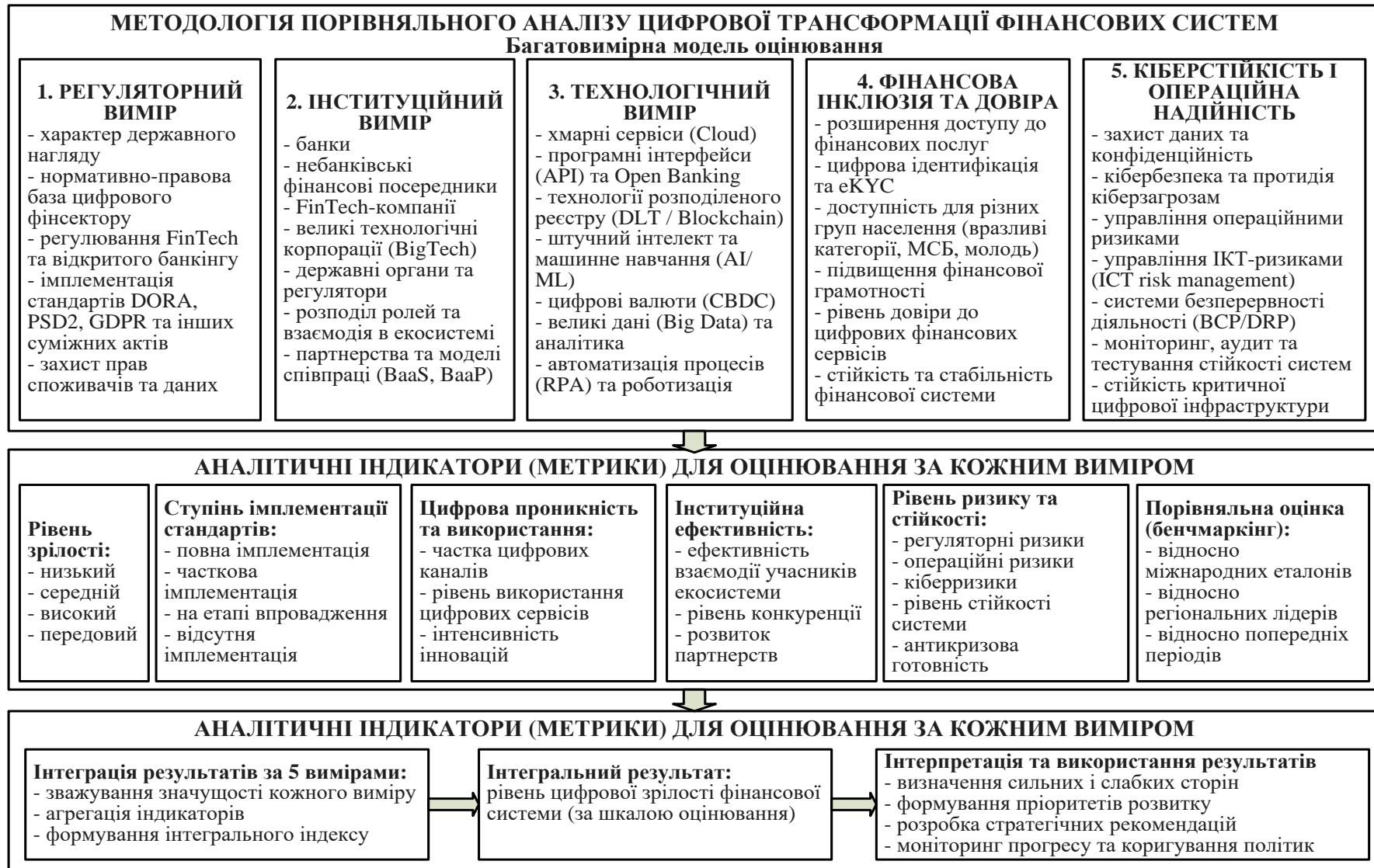


Рис. 2.6. Методологічні виміри порівняльного аналізу цифрової трансформації фінансових посередників
Джерело: розроблено автором на основі [16; 21; 63; 87; 109; 142].

Обґрунтованість обраних вимірів підтверджується їхньою узгодженістю з методологією, використаною у звітах OECD, BIS та World Bank, де цифрова трансформація фінансових систем трактується як інтеграція технологічних інновацій, регуляторних стандартів та суспільної довіри [115; 33; 138; 87; 24]. Застосований метод порівняльного аналізу дозволяє виділити три типи світових моделей цифровізації. *Європейська модель* є регуляторно-орієнтованою, базується на стандартизації, прозорості, операційній стійкості та захисті споживачів. *Американська модель* натомість вирізняється ринково-інноваційним характером, орієнтацією на гнучкість, конкуренцію та активну участь BigTech. *Азійська модель* становить собою платформну, екосистемну структуру з високим рівнем державної підтримки, інтеграцією цифрової ідентичності та мобільних технологій у повсякденні фінанси. Така типологія дає змогу структурувати аналіз не за географічною ознакою, а за характером інституційної взаємодії – чинника, що визначає стратегічну ефективність цифрової трансформації (таблиця 2.7).

Таблиця 2.7

Порівняльна характеристика світових моделей цифрової трансформації фінансових посередників за ключовими вимірами

Вимір порівняння	Європейська модель	Американська модель	Азійська модель
1	2	3	4
1. Регуляторний вимір	Жорстко стандартизована регуляція (PSD2, GDPR, DORA); домінування принципу «regulated innovation»; високий рівень споживацького захисту.	Гнучкі ринкові правила; пріоритет саморегуляції та конкуренції; регулювання здебільшого після факту (ex post).	Активна роль держави; стратегічні державні програми цифрових фінансів; централізовані платформи e-ID, instant payments.
2. Інституційний вимір	Висока роль традиційних банків; FinTech інтегрований через Open Banking; BigTech обмежений регуляторно.	Домінування BigTech (Google, Apple, Amazon); активний розвиток neobank; FinTech – ключовий драйвер.	Домінування екосистем (Alipay, WeChat); сильна інтеграція банків, FinTech і державних платформ.
3. Технологічний вимір	API-економіка, хмарні технології, посилений контроль даних; акцент на стандартизації та безпеці.	Активна експлуатація Big Data, AI/ML, blockchain; високий рівень інноваційних експериментів.	Масове впровадження мобільних технологій, e-ID, QR-платежів; швидкі масштабні інтеграції.

1	2	3	4
4. Фінансова інклюзія та довіра	Висока довіра до банків та регулятора; інклюзія через стандартизовані цифрові сервіси.	Довіра зосереджена навколо технологічних платформ; інклюзія через FinTech-інновації.	Найвища інклюзія завдяки мобільним сервісам; довіра – результат поєднання державного та приватного сектору.
5. Кіберстійкість та операційна надійність	Комплексні стандарти операційної стійкості (DORA, EBA Guidelines); високий рівень координації.	Багаторівнева кіберінфраструктура приватного сектору; сильні SOC-центри BigTech.	Державні системи кіберзахисту; централізовані протоколи операційної стійкості; швидка реакція на інциденти.

Джерело: розроблено автором на основі [16; 21; 46; 63; 87; 109; 142].

Порівняльний аналіз показує, що глобальні моделі цифрової трансформації фінансових посередників демонструють різну логіку взаємодії між інноваціями, ринковими силами та регуляторними рамками.

Європейська модель вирізняється системністю та високим рівнем інституційної координації. Прийняття DORA (Regulation (EU) 2022/2554), PSD2 і GDPR створює багаторівневу структуру контролю за технологічними, операційними та інформаційними ризиками, що підвищує довіру до фінансової системи [63].

Американська модель, навпаки, функціонує у парадигмі ринкової гнучкості. Тут цифрові інновації зосереджені навколо BigTech-компаній і фінтех-стартапів, які швидко розгортають нові сервіси, орієнтуючись на споживацький попит. Водночас така динаміка супроводжується підвищеними ризиками фрагментації та відсутністю єдиних стандартів кіберстійкості [87].

Азійська модель є найбільш платформно-орієнтованою: фінансові сервіси інтегровані у повсякденні цифрові екосистеми (WeChat, Alipay, KakaoBank). Цей підхід забезпечує максимальну фінансову інклюзію, але водночас підвищує системні ризики концентрації даних і залежності від державних технологічних платформ [142].

Таким чином, у кожній моделі поєднуються власні переваги та виклики: європейська – найбільш збалансована з погляду стабільності, американська – найдинамічніша, азійська – наймасштабніша за охопленням споживачів. Поєднання цих моделей формує основу для глобальної конвергенції стандартів цифрового посередництва (рис. 2.7).

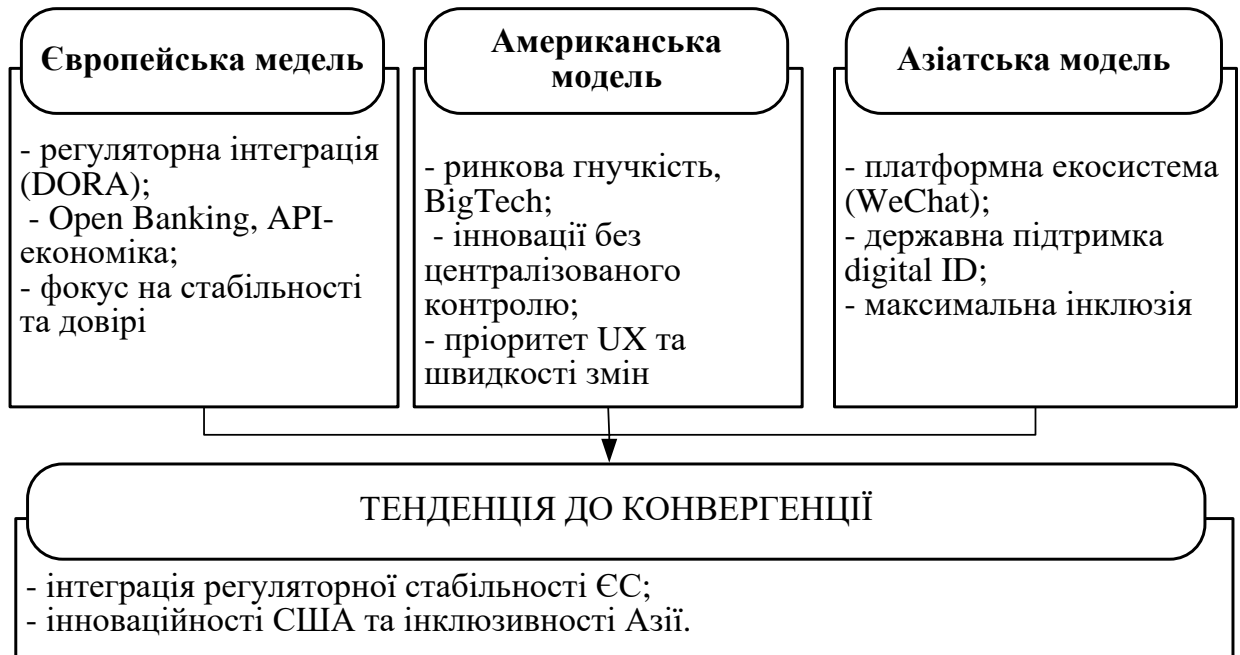


Рис. 2.7 - Світові моделі цифрової трансформації фінансових посередників

Джерело: авторська розробка на основі [4; 5; 19; 21; 23; 24; 29; 33; 34; 38; 41; 42; 62; 63; 76; 79; 84; 87; 92; 100; 103; 109; 112; 115; 138; 139; 141; 142; 229].

Порівняння моделей засвідчує, що світовий розвиток цифрового фінансового посередництва відбувається у напрямі структурної конвергенції – поєднання регуляторної передбачуваності ЄС, технологічної динаміки США та масштабної інклюзивності азійських фінансових екосистем. Такий процес є проявом глобальної еволюції фінансової архітектури, у якій не тільки дані, а й довіра та стійкість стають головними стратегічними ресурсами.

На нашу думку, для України доцільним є формування гібридної моделі цифрового посередництва, яка інтегрує найкращі практики цих трьох підходів з урахуванням національних інституційних особливостей і регуляторних реформ НБУ.

Цифрова трансформація фінансового посередництва в Україні відбувається у складних умовах глибоких інституційних змін, високих кіберзагроз, воєнних викликів та структурної модернізації економіки. На цьому тлі особливої ваги набуває питання адаптації міжнародного досвіду, який відображає накопичену практику різних регуляторних, технологічних та інституційних підходів до розвитку цифрових фінансових послуг.

Порівняльний аналіз світових моделей (європейської, американської та азійської) дозволяє виокремити низку принципів та інструментів, що мають потенціал бути інтегрованими у вітчизняну фінансову систему. При цьому вважаємо, що важливо уникати прямого копіювання, зважаючи на специфіку українського ринку, роль Національного банку України, різний рівень цифрової зрілості фінансових інститутів та нерівномірний розвиток небанківського сектору (табл. 2.8).

Таблиця 2.8

**Адаптація світових моделей цифрового фінансового посередництва
до українських реалій**

Модель	Ключові елементи	Цінність для України	Можливі напрями впровадження
Європейська модель	Стандарти операційної стійкості (DORA); Open Banking; GDPR; регуляторна інтеграція	Найбільш сумісна з українським правовим полем; сприяє підвищенню довіри та захисту даних	Розробка українського аналога DORA; розширення відкритого банкінгу; стандартизація API; впровадження єдиного підходу до управління ІКТ-ризиками
Американська модель	BigTech-інновації; гнучкі регуляторні режими; ринок венчурного фінансування	Дозволяє прискорити інновації та розвинути фінтех-екосистеми	Розвиток регуляторних пісочниць НБУ; партнерства банків з ІТ/телеком; підтримка стартапів; експерименти з AI/ML у фінансах
Азійська модель	Екосистемні платформи; мобільно-орієнтований підхід; цифрова ідентифікація; швидка масштабованість	Релевантна для України з огляду на домінування мобільних каналів і потребу в інклюзії	Створення суперагрегаторів; розширення eID; розвиток мікроплатежів; інтеграція фінансових сервісів у нефінансові платформи
Синтез (гібридна модель)	Комбінування інституційної стійкості, інноваційної гнучкості та екосистемності	Найбільш реалістична стратегія розвитку України	Створення гібридної цифрової інфраструктури; інтеграція банків, небанківських установ та державних сервісів; посилення кіберстійкості

Джерело: розроблено автором на основі [16; 21; 63; 87; 109; 142; 202].

Аналіз глобальних трендів цифрової трансформації фінансового сектору дає змогу виокремити ключові уроки з досвіду різних регіонів, які можуть бути адаптовані до українських реалій. При цьому важливо розуміти, що пряме копіювання моделей неможливе – необхідний вибірковий підхід, який враховує специфіку національного ринку, регуляторного середовища та рівня технологічного розвитку.

Європейська модель є найбільш релевантною для України через спільність регуляторної логіки, прагнення до гармонізації з нормами ЄС та високий рівень інституційної сумісності. Особливо важливим є досвід впровадження регламенту DORA (Digital Operational Resilience Act), який пропонує комплексну систему управління ІКТ-ризиками, реагування на інциденти, тестування стійкості систем та контролю взаємодії з критичними постачальниками технологічних послуг [141]. Для України імплементація аналогічних вимог дала б змогу підвищити рівень кіберстійкості банків і платіжних систем, забезпечити єдиний підхід до управління технологічними ризиками та знизити уразливість від зовнішніх постачальників ІТ-послуг.

Не менш важливим є європейський досвід розвитку відкритого банкінгу. Директива PSD2 продемонструвала, що стандартизація API та відкритий доступ до рахунків (за згодою клієнтів) сприяють конкуренції, фінансовій інклюзії та створенню нових цифрових сервісів [109]. Для України це критично важливо з огляду на потребу масштабування інновацій поза межами кількох великих банків. Відкрита інфраструктура даних могла б стимулювати розвиток фінтех-екосистеми, дозволяючи невеликим компаніям створювати інноваційні рішення на основі банківської інфраструктури.

Запроваджений у межах Європейського Союзу підхід до регулювання обігу персональних даних, знаковою реалізацією якого виступає Загальний регламент про захист даних (GDPR), становить також практичний інтерес для України. Імплементація аналогічних нормативних механізмів, на думку автора, здатна виконати три ключові завдання. По-перше, підвищити рівень споживчої довіри до вітчизняних цифрових сервісів. По-друге, удосконалити процедури

опрацювання фінансової інформації. По-третє, істотно знизити ймовірність витоків конфіденційних даних. Останнє завдання набуває особливої актуальності у зв'язку зі стійкою тенденцією до зростання кількості та складності кіберзагроз.

Американська модель пропонує інші, але не менш важливі уроки. Вона акцентує увагу на швидкості інновацій, розвитку екосистем та високій конкуренції між фінансовими й технологічними компаніями. США зосереджуються на стимулюванні інновацій через мінімальні обмеження на ранніх етапах розвитку продуктів, що прискорює розробку нових рішень, залучає венчурні інвестиції та формує динамічне конкурентне середовище [87].

Для України це означає необхідність розширення механізмів «регуляторних пісочниць» Національного банку та створення сприятливих умов для експериментування з цифровими продуктами. Занадто жорстке регулювання на ранніх стадіях може «задушити» інновації ще до того, як вони встигнуть довести свою життєздатність. Водночас важливо зберігати баланс між стимулюванням інновацій та захистом інтересів споживачів.

Американський досвід також демонструє роль великих технологічних компаній (BigTech) як драйверів інновацій [16]. Інтеграція фінансових сервісів у продукти технологічних компаній суттєво спрощує для широких верств населення доступ до фінансових послуг. Для України це сигнал до поглиблення партнерств між банками, телекомунікаційними компаніями та ІТ-сектором. Український ринок має потужний ІТ-сектор, який міг би стати важливим партнером для фінансових установ у створенні інноваційних рішень.

Фінансові системи азійських країн – насамперед Китаю, Південної Кореї та Сінгапуру – вирізняються найвищими темпами впровадження нових цифрових сервісів. Вони також пропонують цінний досвід у двох аспектах: формування екосистемної організації та досягнення масштабованості рішень. Показовими у цьому контексті є платформи типу WeChat та Alipay. Вони інтегрують у єдине цифрове середовище широкий спектр функцій – платежі, кредитування, страхування, а також численні сервісні послуги. У підсумку таке середовище перетворюється на центр фінансового життя для сотень мільйонів користувачів [142].

Для України зазначений досвід створює передумови для розвитку міжсекторних партнерств, появи так званих фінансових суперагрегаторів, а також формування комплексних платформ, що об'єднують різноманітні цифрові послуги. Окремі приклади руху в цьому напрямку в українській практиці вже є, однак наявний потенціал, вочевидь, ще далеко не вичерпано. Екосистемний підхід набуває особливої актуальності в умовах, коли споживачі дедалі більше прагнуть отримувати максимум послуг в одному місці, уникаючи необхідності переключатися між різними додатками та сервісами.

Досвід країн Азійського регіону додатково акцентує значущість підходу, орієнтованого на мобільні пристрої як пріоритетний канал комунікації (mobile-first). Саме завдяки такій орієнтації було досягнуто одного з найвищих у світовому масштабі рівнів фінансової інклюзії. Мільярди користувачів отримали змогу долучатися до фінансових послуг, не відвідуючи фізичні відділення банків і не маючи персонального комп'ютера. Для України, де мобільні канали вже посідають домінуюче становище, стратегічний акцент доцільно змістити на кілька взаємопов'язаних напрямів. Йдеться, зокрема, про спрощення процедур ідентифікації клієнтів, впровадження біометричних механізмів онбордингу, а також розвиток мікроплатежів і мікрокредитування. Саме ці інструменти є критично важливими для подальшого підвищення рівня фінансової інклюзії в країні.

На основі аналізу міжнародного досвіду доцільно формувати гібридну модель цифрового фінансового посередництва для України, яка органічно поєднувала б європейську регуляторну стійкість, американську інноваційну динаміку та азійську екосистемність із масштабованістю. Така модель не є механічною сумою елементів різних систем, а синтезом, адаптованим до української специфіки.

Особливе значення в цій моделі мають кілька напрямів. По-перше, розвиток надійної та зручної системи цифрової ідентифікації, яка стане основою для безпечного доступу до всіх цифрових фінансових послуг. По-друге, забезпечення інтероперабельності фінансових даних, що дозволить

різним сервісам працювати разом, створюючи цінність для клієнтів через інтеграцію. По-третє, створення інноваційної інфраструктури, включно з хмарними платформами, відкритими API, можливо навіть пілотними проєктами цифрової валюти центрального банку (CBDC).

Не менш важливим є системне підвищення кіберстійкості всього фінансового сектору, оскільки в умовах зростаючих загроз навіть найінноваційніші рішення будуть марними без надійного захисту. Необхідне також стимулювання фінтех-підприємництва через створення сприятливого регуляторного середовища, доступ до фінансування, підтримку інноваційних проєктів. Нарешті, критично важливою є інтеграція небанківських фінансових посередників у єдину цифрову екосистему, що дозволить створити справді всеосяжне та конкурентне середовище для надання фінансових послуг.

Аналіз уроків міжнародного досвіду дозволяє визначити пріоритетні напрями адаптації моделей цифрового фінансового посередництва до українського контексту. Водночас ефективність цієї адаптації значною мірою залежить від реального стану цифрової трансформації на вітчизняному фінансовому ринку, динаміки розвитку банківського та небанківського секторів, інноваційної активності фінансових установ і готовності інфраструктури до масштабування цифрових сервісів.

Цифрова трансформація фінансового сектора України перебуває у фазі прискореної еволюції, обумовленої поєднанням технологічних інновацій, регуляторних реформ та безпрецедентного тиску зовнішніх викликів, насамперед воєнних. Національний банк України та провідні фінансові посередники активно формують нову цифрову інфраструктуру, що має забезпечити стійкість фінансової системи, інклюзію та відповідність глобальним стандартам цифрової безпеки та операційної надійності.

Українська фінансова система демонструє високий рівень цифрової адаптації. За оцінками НБУ, понад 90 % побутових банківських операцій уже здійснюються дистанційно, тоді як частка використання фізичних відділень скорочується щорічно. Розвиток цифрових каналів стимулюється низкою факторів:

- регуляторна трансформація (євроінтеграційний вектор, оновлені вимоги до ІКТ-ризиків, цифрова ідентифікація);
- технологічні інновації (хмарні технології, API-платформи, біометрія, штучний інтелект);
- поведінкові зміни користувачів, що очікують послуг «тут і зараз»;
- воєнні виклики, які вимагали забезпечення безперервності роботи критичної інфраструктури.

Таким чином, цифровізація стала не окремим напрямом, а системною стратегією функціонування фінансових посередників.

Українська фінансова система демонструє високий рівень цифрової адаптації, що підтверджується конкретними показниками (табл. 2.9). За оцінками Національного банку України, понад 90 % побутових банківських операцій уже здійснюються дистанційно, тоді як відвідування фізичних відділень скорочується з кожним роком. Це не випадковий процес – його стимулює комплекс взаємопов'язаних факторів.

По-перше, відбувається регуляторна трансформація, пов'язана з євроінтеграційним вектором розвитку країни, оновленням вимог до управління ІКТ-ризиками та впровадженням цифрової ідентифікації.

По-друге, активно поширюються технологічні інновації – хмарні технології, API-платформи, біометрія, штучний інтелект стають не екзотикою, а робочими інструментами. По-третє, змінюється поведінка користувачів, які очікують послуг «тут і зараз», без необхідності відвідувати відділення або чекати на обробку. По-четверте, воєнні виклики, з якими стикнулася країна, вимагають забезпечення безперервності роботи критичної інфраструктури навіть в екстремальних умовах, що прискорило перехід до цифрових рішень.

Внаслідок дії цих факторів цифровізація перестала бути окремим проєктом чи напрямом діяльності – вона стала системною стратегією функціонування фінансових посередників, без якої неможливо уявити їхню роботу.

**Темпи та ключові індикатори цифровізації фінансового сектору України
(2019–2024)**

Показник / індикатор	2019	2020	2021	2022	2023	2024 (за наявними даними)	Коментар / джерело
Обсяг операцій платіжними картками, млрд грн	3576,7	3957,3	5091,7	5494,5	5566,8	н/д	Зростання карткових платежів свідчить про цифровізацію розрахунків
Частка безготівко- вих (non-cash) серед карткових платежів, %	50,3%	55,8	60,9	67,7	65,2	н/д	Показує зростання безготівкових розрахунків
Частка non-cash транзакцій за кількістю, %	—	—	90,1	92,6	93,5	н/д	Свідчить про переважання безготівкових операцій
Кількість активних платіжних карт (млн штук)	5,0573	5,9972	7,8170	6,2590	7,2400	н/д	Індикатор поширення банківських карт як цифрового інструменту
Обсяги переказів (кредитові/дебетові перекази) домогосподарств і бізнесу (перші дані) – Н1 2024	—	—	—	—	—	21,23 млрд грн / 0,8 млн транзакцій	Показує початок публікації нових типів статистик по безготівкових переказах
Динаміка необанків / digital- only банків (ринок FinTech)	зростання з 2018 \approx у 87 разів	—	—	—	—	—	Показник стрімкого росту FinTech- сектору в Україні

Джерело: узагальнено автором за даними НБУ [88; 104; 201].

Сьогодні українські банки, за оцінками міжнародних експертів, належать до найбільш цифровізованих у регіоні Східної Європи. Банківські мобільні застосунки перетворилися на основний канал комунікації з клієнтами, поступово витіснивши як традиційні відділення, так і вебсайти. Провідні

учасники ринку запровадили низку технологічних рішень. Серед них — персоналізована аналітика витрат, що надає клієнтам змогу відстежувати власні фінансові потоки; миттєві платежі з виконанням у лічені секунди; цифрові картки, які функціонують виключно в межах мобільного додатка; а також дистанційна ідентифікація, яка дає можливість відкрити рахунок без фізичного відвідування банківської установи. Паралельно з цим Україна демонструє поступовий рух у напрямі імплементації стандартів відкритого банкінгу, аналогічних до європейської Директиви PSD2. Практична реалізація цього підходу передбачає розкриття фінансових даних через програмні інтерфейси (API). Наслідком стає посилення конкурентного середовища, а також створення сприятливих умов для появи нових фінтех-рішень. Сторонні розробники отримують можливість легше продукувати інноваційні сервіси, спираючись на наявну банківську інфраструктуру.

Особливо важливим досягненням став BankID НБУ — система цифрової ідентифікації, яка стала стандартом доступу не лише до фінансових, а й до державних сервісів. Це істотно зменшило бар'єри для входження клієнтів — тепер людина може підтвердити свою особу онлайн, без необхідності особистої присутності з паперовими документами.

Поширення моделей необанкінгу — банків, які працюють виключно онлайн, без фізичних відділень, таких як Monobank, izibank та інші — демонструє високу конкурентоспроможність цифрових рішень. Ці банки часто випереджають традиційні установи за зручністю, швидкістю та інноваційністю сервісів, що підсилює загальний тренд мобільності та спрощення.

Особливої уваги заслуговує BankID Національного банку України — система цифрової ідентифікації, що стала уніфікованим стандартом доступу не лише до фінансових, а й до державних сервісів. Це рішення суттєво знизило бар'єри входження для клієнтів, оскільки тепер особа може підтвердити свою ідентичність онлайн, без особистої присутності та пред'явлення паперових документів.

Крім того, в Україні спостерігається активне поширення моделей необанкінгу — банків, що функціонують виключно в онлайн-форматі

(Monobank, izibank та інші). Це свідчить про високу конкурентоспроможність цифрових рішень. За показниками зручності, швидкості та інноваційності такі банки нерідко випереджають традиційні установи, що додатково посилює загальний тренд у напрямі мобільності та спрощення фінансових послуг.

У небанківському секторі цифровізація розвивається менш рівномірно, але також досить динамічно. Мікрофінансові організації та кредитні спілки активно оцифровують кредитні продукти, впроваджують скорингові алгоритми для оцінки позичальників та переходять до онлайн-укладання договорів. Це стало фактично стандартом роботи в цьому сегменті.

Платіжні установи та провайдери платіжних послуг активно впроваджують миттєві платежі, цифрові гаманці, оплату через QR-коди, інтеграцію з Apple Pay та Google Pay. Це робить платежі швидшими та зручнішими для споживачів.

Фінтех-платформи розвивають різноманітні напрями: peer-to-peer кредитування, яке напряду зв'язує позичальників з інвесторами, краудфандингові сервіси для фінансування проєктів, онлайн-брокерські платформи для інвестицій та robo-advisers – автоматизовані системи інвестиційного консультування.

Страхові компанії, хоча традиційно більш консервативні, також рухаються в напрямку цифровізації. Впроваджуються дистанційні процедури врегулювання страхових випадків, мобільні поліси, які існують в електронному вигляді, та автоматизовані моделі оцінки ризиків на основі даних.

Водночас, попри значний прогрес, українські фінансові посередники стикаються з низкою структурних бар'єрів, які гальмують подальший розвиток. Спостерігається нерівномірна цифрова зрілість між банківським і небанківським секторами – банки значно випереджають інших учасників ринку. Воєнний стан обмежує можливості інвестицій у технології, оскільки ресурси спрямовуються на інші критичні потреби. Відсутня повна стандартизація даних та API, що ускладнює інтеграцію між різними системами та учасниками ринку.

Серйозною проблемою залишаються загрози кібербезпеки, які зростають у геополітичному контексті. Україна є однією з найбільш атакованих країн у кіберпросторі. Нарешті, регуляторні вимоги до управління ІКТ-ризиками ще не повністю інтегровані в практику всіх фінансових посередників, особливо в небанківському секторі.

Водночас відсутність публічних даних за деякими роками або показниками (наприклад, загальний обсяг усіх безготівкових операцій, e-banking, mobile banking) обмежує можливості для повного трендового аналізу – це свідчить про необхідність розвитку статистичної бази.

Все це формує потребу в комплексній цифровій стратегії для всього фінансового сектору – не окремих його учасників, а системної політики, яка координувала б зусилля різних інституцій, усувала б бар'єри та створювала б сприятливі умови для подальшого розвитку цифрових фінансових послуг в Україні.

Проведений комплексний аналіз глобальних, регіональних та національних тенденцій цифрової трансформації фінансових посередників засвідчив, що цифровізація сьогодні не є окремим технологічним напрямом, а виступає ключовим фактором структурної перебудови фінансових ринків, бізнес-моделей і концепції взаємодії між учасниками фінансової системи. Сучасний фінансовий посередник функціонує вже не лише як інститут перерозподілу ресурсів, а як цифрова платформа, здатна забезпечувати інтегровані, персоналізовані та стійкі фінансові сервіси.

У глобальному вимірі цифрове фінансове посередництво розвивається нерівномірно, формуючи три провідні моделі – європейську, американську та азійську. Вони відрізняються за регуляторними підходами, рівнем інноваційної гнучкості, ступенем ринкової концентрації та масштабом екосистемного розвитку. Європейська модель орієнтована на високу регуляторну узгодженість і стандарти операційної стійкості, американська – на динаміку інновацій та роль технологічних корпорацій, азійська – на екосистемну інтеграцію та масову фінансову інклюзію. Їхня комбінація формує багатовимірний глобальний простір цифрового фінансового посередництва.

Уроки для України полягають у необхідності формування гібридної моделі цифрової трансформації, що поєднує європейські стандарти регуляторної стійкості, американську інноваційну відкритість та азійську інклюзивність і масштабованість. В умовах воєнних, кібернетичних та економічних викликів саме така збалансована модель є найбільш реалістичною та стратегічно обґрунтованою.

Аналіз стану цифровізації фінансового сектору України показав, що за останні роки спостерігається істотний прогрес у розвитку цифрових каналів, мобільного банкінгу, онлайн-платежів, інфраструктури ідентифікації та фінтех-платформ. Водночас цифрова трансформація вітчизняних фінансових посередників має виражену асиметрію: банківський сектор демонструє високу цифрову зрілість, тоді як небанківський сегмент та частина фінансових установ залишаються на початкових етапах оцифрування. До ключових бар'єрів належать обмежені можливості інвестування, нерівномірна інфраструктура, недостатня стандартизація даних, а також посилені кіберризики.

Попри досягнутий рівень цифрової адаптації, подальший розвиток фінансових посередників в Україні відбувається під впливом складної системи різноспрямованих чинників. Одні з них створюють додаткові імпульси для прискорення цифровізації, інші, навпаки, формують бар'єри або породжують нові зони ризику. Ідентифікація та структурування цих факторів є необхідною передумовою для розроблення обґрунтованих стратегічних рішень.

Проведений аналіз дає підстави стверджувати, що цифрова трансформація фінансових посередників в Україні перебуває під впливом складної, багаторівневої системи чинників, які одночасно створюють як додаткові імпульси для прискорення змін, так і суттєві обмеження. Доцільно виокремити сім груп таких факторів: технологічні, поведінкові, регуляторні, конкурентні, економічні, соціально-економічні та глобальні. Кожна з цих груп має власну структуру, особливості впливу та специфічні позитивні й негативні наслідки для діяльності фінансових установ.

Технологічні фактори визначають напрями та темпи модернізації фінансової сфери. Розвиток штучного інтелекту, машинного навчання, хмарних обчислень, технологій розподіленого реєстру та аналітики великих масивів даних створює передумови для автоматизації бізнес-процесів, підвищення точності ризик-оцінювання та персоналізації послуг. Водночас упровадження зазначених рішень вимагає від фінансових посередників значних капіталовкладень, залучення висококваліфікованих кадрів. Це, своєю чергою, супроводжується ризиками виникнення алгоритмічних упереджень, кіберзагрозами та посиленням технологічної залежності.

Поведінкові фактори відображають вплив очікувань та звичок споживачів на розвиток фінансових послуг. Підвищення рівня цифрової грамотності населення, потреба в цілодобовій доступності, зручності та персоналізації спонукають фінансові установи до нарощування онлайн-каналів обслуговування. Разом із тим нерівномірність розподілу цифрових навичок серед різних верств населення здатна спричиняти фінансову ексклюзивність окремих клієнтських сегментів.

Регуляторні фактори охоплюють сукупність законодавчих норм і правил, які визначають умови функціонування фінансових установ. Зокрема, політика Національного банку України щодо цифровізації, створення регуляторних «пісочниць», вимоги до кібербезпеки та стандартизація відкритого банкінгу (PSD2, DORA) сприяють технологічному розвитку. Водночас посилення регуляторного навантаження вимагає додаткових витрат на комплаєнс та уповільнює впровадження інновацій.

Конкурентні фактори, представлені технологічними стартапами, необанками та глобальними платіжними системами, створюють суттєвий конкурентний тиск на традиційних фінансових посередників, насамперед банки. Завдяки операційній гнучкості фінтех-компаній, здатності швидко масштабувати новаторські рішення та пропонувати клієнтоцентричні продукти, традиційні установи отримують стимул прискорювати реалізацію власних цифрових трансформацій. Наслідками такого конкурентного впливу виступають фрагментація ринку, зростання витрат на маркетинг і дослідження, а також поступове скорочення традиційних джерел доходу.

Економічні чинники визначають фінансову спроможність установ до цифрової модернізації. Прагнення підвищити рентабельність спонукає до автоматизації процесів, тоді як диверсифікація доходів через розробку інноваційних продуктів та монетизацію даних формує додаткові джерела прибутку. Разом із тим висока вартість трансформації, необхідність залучення інвестицій та зростання боргового навантаження створюють додаткові ризики для фінансової стабільності.

Соціально-економічні фактори в українських реаліях суттєво зумовлені викликами воєнного періоду, міграційними процесами і державними цифровими ініціативами. Повномасштабна війна, попри руйнування фізичної інфраструктури, стала потужним каталізатором переходу населення та бізнесу до цифрових каналів обслуговування. Водночас відтік ІТ-фахівців, скорочення обсягів доступних інвестиційних ресурсів і необхідність підтримання безперервності діяльності в екстремальних умовах породжують значні операційні виклики.

Глобальні чинники впливу включають міжнародні тренди, стандарти та ініціативи, що формуються на наднаціональному рівні. Євроінтеграційний вектор розвитку України, гармонізація з європейськими стандартами (зокрема Basel III, DORA, PSD2), дотримання принципів ESG, а також потенційне впровадження цифрових валют центральних банків визначають стратегічні орієнтири вітчизняних фінансових посередників. Адаптація до цих стандартів відкриває доступ до міжнародних ринків капіталу, однак вимагає значних витрат на оновлення систем управління та звітності.

Узагальнення впливу окреслених факторів, а також систематизація можливостей і ризиків, які вони створюють для фінансових посередників, представлені на рисунках 2.8 і 2.9. Наведена на рисунках інформація дозволяє структурувати ключові драйвери позитивних змін (наприклад, технологічний прогрес, сприятливі регуляторні умови, зростання цифрової грамотності, конкуренція) та основні бар'єри, що стримують цифрову трансформацію. До ключових бар'єрів, на нашу думку, варто віднести кіберзагрози, регуляторне навантаження, кадровий дефіцит, фінансові обмеження.

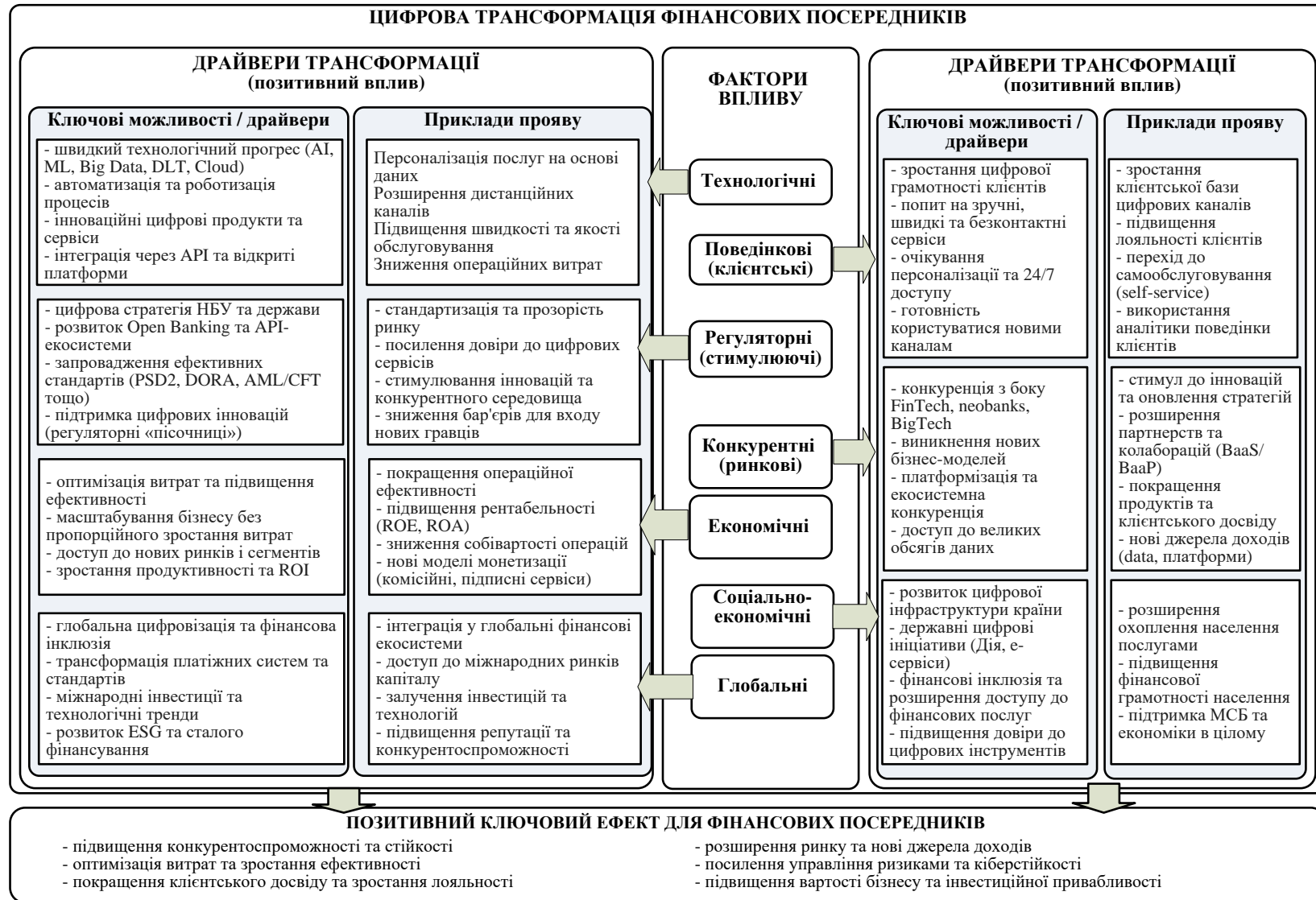


Рис. 2.8. Позитивні фактори впливу на цифрову трансформацію фінансових посередників

Джерело: авторська розробка.

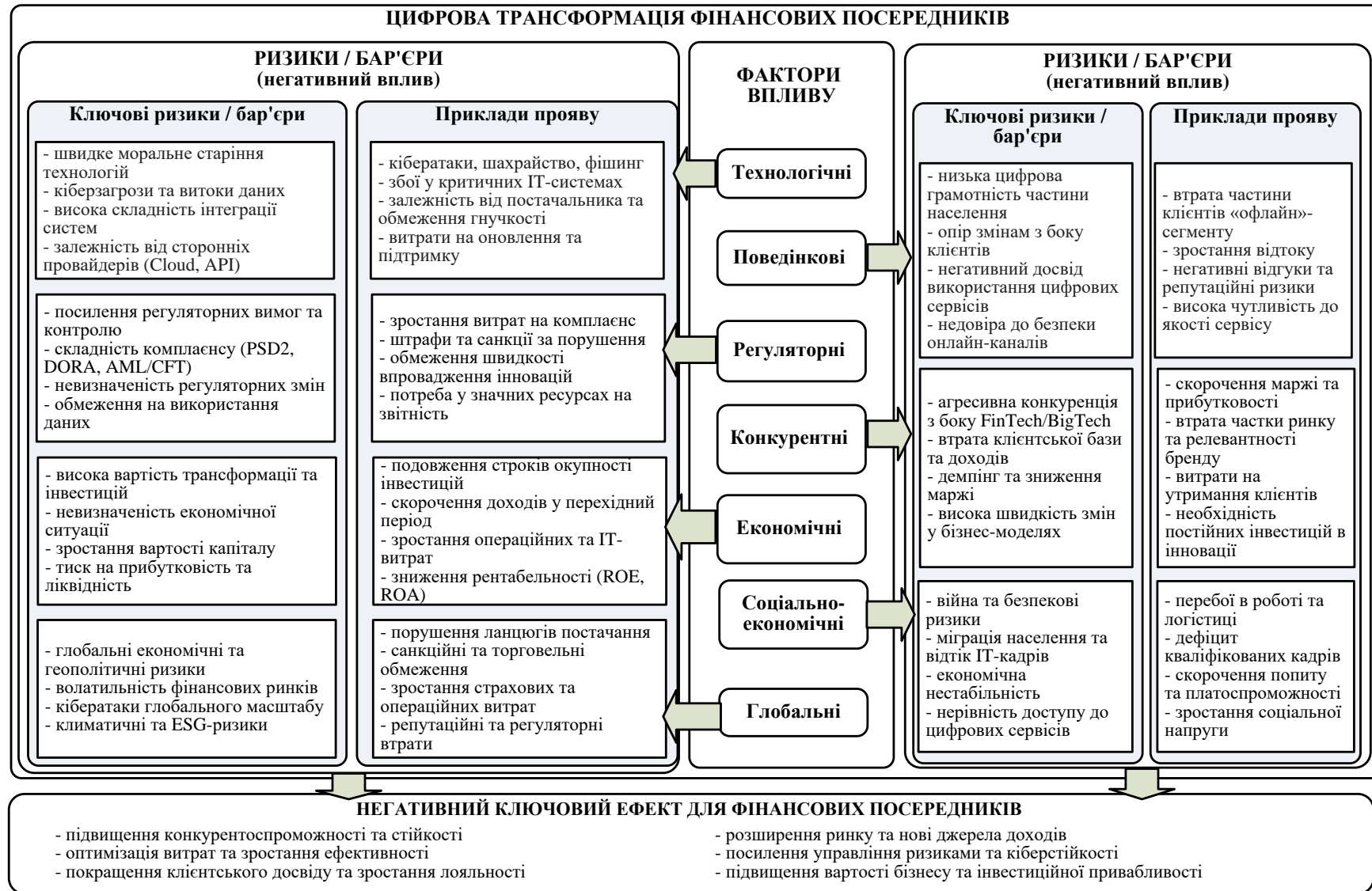


Рис. 2.9. Негативні фактори впливу на цифрову трансформацію фінансових посередників

Джерело: авторська розробка.

Аналіз вищенаведених чинників розкриває складну систему взаємопов'язаних факторів впливу. Технологічний прогрес, регуляторні зміни, конкурентний тиск та макроекономічні виклики створюють об'єктивні передумови для модернізації галузі. Однак ключовим драйвером трансформації залишається людський фактор, а саме зміни в поведінці, потребах та очікуваннях споживачів фінансових послуг. Саме споживачі значним чином визначають нові стандарти якості сервісу, швидкості обслуговування та рівня персоналізації, котрі стають обов'язковими для виконання фінансовими посередниками. Проведені дослідження дозволили виявити та узагальнити ключові очікування споживачів послуг фінансових посередників (рис. 2.10).

Як видно з рис. 2.8 основні очікування споживачів цифрових банківських сервісів пов'язані із швидкістю, зручністю і цілодобовою доступністю. Не менш важливим чинником фактором є безпека (захист персональних даних, фінансова стабільність та технічна надійність систем), котра значним чином визначає довіру споживачів фінансових послуг до фінансових посередників. Крім того, останніми роками спостерігається стрімке зростання потреб споживачів у персоналізованих пропозиціях, фінансовій аналітиці та проактивному сервісі. Розвиток численних цифрових платформ і сервісів сформував ще один напрям очікувань споживачів, який пов'язаний із омніканальністю та інтеграцією з різними платформами, що дозволяє забезпечити єдиний безшовний досвід для клієнтів.

Виявлення і осмислення очікувань споживачів щодо цифрових сервісів дозволяє зрозуміти не лише те, які технології потрібно впроваджувати, але і як їх адаптувати до специфічних потреб українського ринку. Розуміння потреб клієнтів створює основу для формування ефективної стратегії цифровізації та визначення пріоритетів технологічного розвитку.

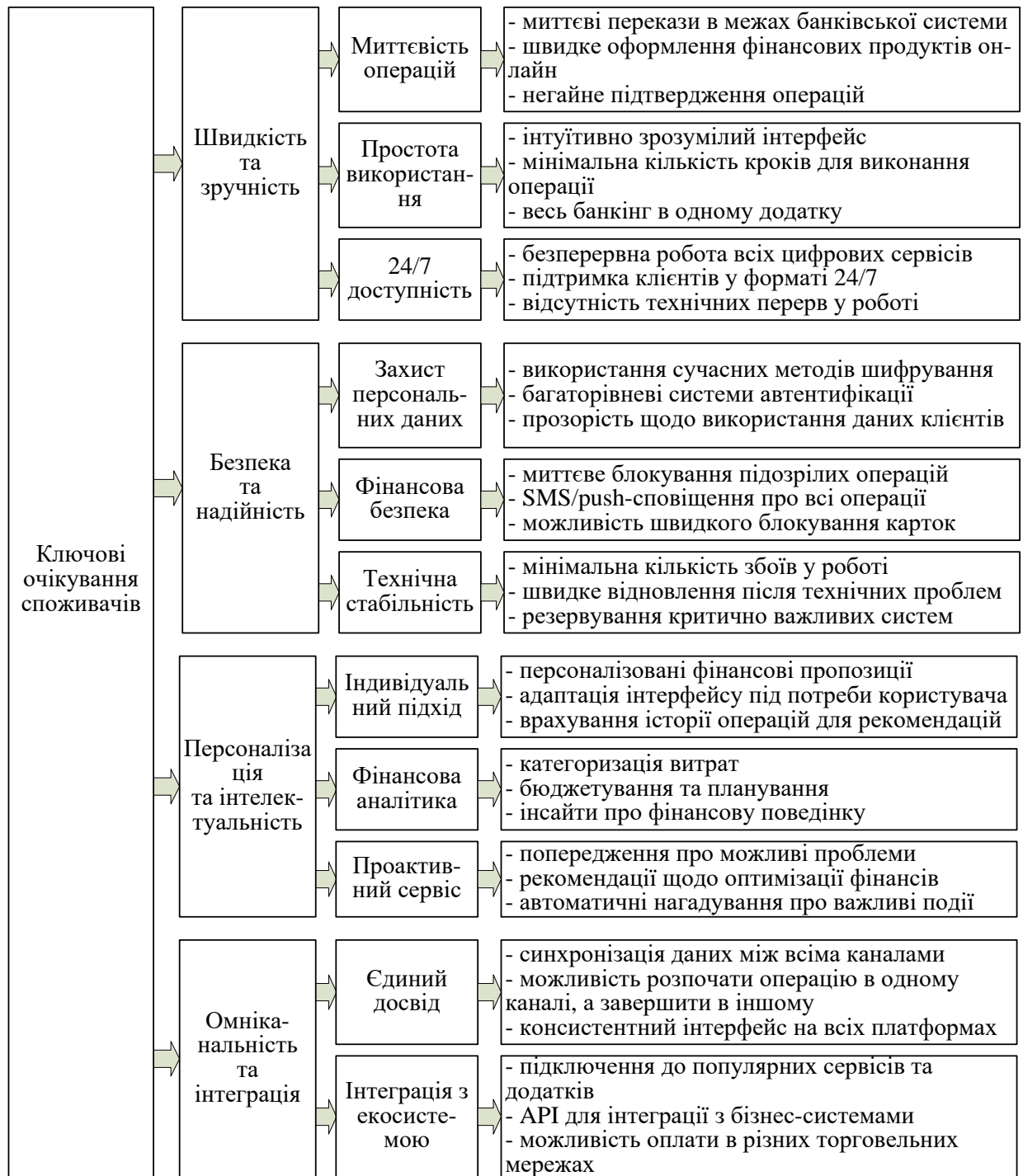


Рис. 2.10. Ключові очікування споживачів послуг фінансових посередників

Джерело: розроблено автором на основі [52; 110; 120; 145; 186; 187; 151].

Водночас теоретичне розуміння споживчих очікувань в сучасних умовах розвитку національної економіки, на нашу думку, варто доповнити аналізом реальної практики впровадження цифрових рішень. Особливо актуальним це стало в умовах воєнного стану, коли фінансові установи

вимушені були не тільки адаптуватися до потреб клієнтів, які суттєво трансформувались (у тому числі, через процеси міграції населення та релокації підприємств), а й забезпечити безперервність роботи в екстремальних умовах. Аналіз цифрової трансформації ключових фінансових установ узагальнено в табл. 2.10.

Таблиця 2.10

Цифрова трансформація ключових фінансових установ України

Банк	Ключові цифрові рішення	Особливості та інновації	Результати
ПриватБанк	- приват24 (з 2001 р.); - мобільний банкінг; - QR-платежі; - безконтактні розрахунки	- піонер інтернет-банкінгу в Україні; - інтеграція з державними сервісами; - стратегія диджиталізації - екосистема для МСБ	- найбільша клієнтська база; - еталон українського мобільного банкінгу; - оцифрування бізнесу без зайвих витрат
Monobank	- 100 % мобільний банк; - Оформлення карти за 5 хв; - чатбот з ШІ; - кешбек-програми	- банк без відділень; - революційний UX/UI дизайн; - гейміфікація сервісів; - спрощення IBAN-переказів	- швидке зростання клієнтської бази; - високі рейтинги задоволеності; - стандарт зручності
ПУМБ	- мобільний банкінг; - реєстрація через Дію за 5 хв; - обмін валюти в додатку; - цифрова B2B платформа; - кешбек-програми	- лідер у корпоративному сегменті; - інтеграція з обліковими системами; - онлайн документообіг; - перекази 24/7 для бізнесу	- домінування в бізнес-банкінгу; - автоматизація бізнес-процесів; - персоналізовані рішення
Ощадбанк	- ощад 24/7; - цифровізація соцвиплат; - онлайн-кредитування; - модернізація IT-системи	- найбільший державний банк; - масштабна трансформація; - соціальний фокус; - доступність для всіх верств	- збереження лідерських позицій; - цифровізація державних послуг; - широке покриття населення
Укргазбанк	- мобільний банкінг; - корпоративний онлайн-банкінг; - цифрові рішення для енергосектору; - автоматизація розрахунків за енергоносії	- спеціалізація на енергетиці; - автоматизація комунальних платежів; - галузевий фокус; - B2B енергетичні рішення	- лідер у енергетичному банкінгу; - ефективна автоматизація розрахунків; - стратегічне значення для економіки

Джерело: розроблено автором на основі [13; 118; 182; 189; 194; 198; 210].

Дослідження практики цифрової адаптації фінансових посередників на прикладі українських системоутворюючих банків в умовах війни та посилення кіберзагроз, результати якого узагальнено в таблиці 2.10, відображають унікальний досвід прискореної цифрової трансформації. В умовах війни і глибокої фінансово-економічної кризи український банківський сектор продемонстрував практичну реалізацію теоретичних моделей цифровізації, які характеризуються адаптивністю до непередбачуваних змін, стійкістю до екстремальних навантажень, здатністю швидко масштабувати рішення та інтегрувати різноманітні технології в єдину екосистему.

Виявлені особливості цифрової трансформації українських банків створюють підґрунтя для кількісного вимірювання їхньої цифрової зрілості, що здійснюється в наступному підрозділі.

2.3. Інтегральне оцінювання рівня цифрової зрілості фінансових посередників як детермінанти їх конкурентоспроможності

Розроблений у підрозділі 2.1 методологічний інструментарій та виявлені й систематизовані в підрозділі 2.2 фактори впливу створюють необхідне підґрунтя для кількісного вимірювання цифрової зрілості фінансових посередників. Перехід від якісного аналізу до інтегральної оцінки дозволяє не лише фіксувати поточний рівень цифрового розвитку окремих установ, але і встановлювати кореляційні зв'язки між рівнем цифрової зрілості та їхньою ринковою позицією, фінансовою ефективністю та інноваційною активністю.

У сучасних умовах функціонування фінансового сектору цифрова зрілість поступово перетворюється на один із головних чинників, що визначають рівень конкурентоспроможності установи. Та фінансова інституція, яка здатна оперативно реагувати на технологічні нововведення, вбудовувати їх у діючі бізнес-процеси, забезпечувати безперервну роботу цифрових каналів обслуговування та ефективно протидіяти кіберризикам, отримує вагомі конкурентні переваги в боротьбі за прихильність клієнтів.

На противагу цьому, невисокий ступінь цифрової зрілості має передбачувані негативні наслідки. Перелічимо основні з них: технологічне відставання від ринкових лідерів; поступова втрата займаних ринкових позицій; зниження показників операційної ефективності; підвищення рівня вразливості установи до зовнішніх загроз, незалежно від їхнього походження.

Вимірювання цифрової зрілості через запропонований інтегральний індекс DСМІ дає змогу кількісно оцінити внесок кожної з шести складових (технологічна інфраструктура, процесна зрілість, клієнтська цифрова взаємодія, інноваційна спроможність, кіберстійкість, регуляторно-інституційна відповідність) у загальний рівень цифрової спроможності установи. Такий підхід забезпечує можливість не лише ранжування фінансових посередників за рівнем зрілості, але й ідентифікації «вузьких місць» – тих блоків, які потребують першочергових управлінських втручань.

Зв'язок між цифровою зрілістю та конкурентоспроможністю не є лінійним. На початкових етапах цифровізації інвестиції в технології можуть суттєво збільшувати витрати установи без негайного економічного ефекту. Однак після досягнення певного порогового рівня зрілості (який у запропонованій шкалі відповідає високому або лідерському рівням) цифрові компетенції починають генерувати стійкі конкурентні переваги: зниження операційних витрат, зростання клієнтської лояльності, прискорення виведення нових продуктів на ринок, підвищення стійкості до кризових явищ.

Проведення емпіричного оцінювання цифрової зрілості на основі розробленої методики потребує формування репрезентативної вибірки фінансових установ, які є об'єктами аналізу. Вибір конкретних посередників має враховувати їхню системну значущість для національного фінансового ринку, доступність публічних даних для розрахунку індикаторів, а також можливість порівняльного аналізу між різними типами установ.

З огляду на зазначене, для апробації авторської моделі оцінювання цифрової зрілості доцільно обрати фінансові установи, які відповідають кільком критеріям. По-перше, вони мають належати до категорії системно

важливих банків, оскільки їхня цифрова готовність безпосередньо впливає на стабільність національної фінансової інфраструктури. По-друге, установи повинні мати достатньо відкритої статистичної та звітної інформації для забезпечення коректного розрахунку індикаторів за всіма шістьма блоками моделі. По-третє, вибірка має включати як установи з високим рівнем цифрової активності, так і тих, що перебувають на етапі наздоганяючої цифровізації, що дозволить простежити диференціацію рівнів зрілості.

З погляду масштабів діяльності, чисельності клієнтської бази та значущості в межах національної фінансової системи найбільш показовими є дві установи – АТ КБ «ПриватБанк» та АТ «Ощадбанк». Перший із них є беззаперечним лідером за кількістю активних користувачів цифрових каналів, а також за широтою спектра інноваційних сервісів. Другий, маючи найрозгалуженішу територіальну мережу та виконуючи важливу соціальну функцію, демонструє динаміку так званої наздоганяючої цифровізації. Порівняння саме цих двох фінансових інституцій дозволяє, з одного боку, виявити спільні закономірності, властиві українському фінансовому сектору загалом, а з іншого – ідентифікувати специфічні особливості, зумовлені відмінностями в бізнес-моделях, клієнтських сегментах та стратегічних пріоритетах кожної з установ.

Перехід до оцінювання цифрової зрілості цих двох банків дозволяє перевірити практичну застосовність авторської моделі, з'ясувати реальний стан їхньої цифрової та інфраструктурної готовності, а також визначити сильні сторони та потенційні точки зростання. З огляду на обмеженість доступних даних, оцінювання матиме пілотний характер і базуватиметься на відкритих статистичних джерелах, публічній звітності банків та агрегованих індикаторах, що є репрезентативними для блоків TI, CI, IN, CR та RI.

Саме на цій основі здійснено порівняльне оцінювання цифрової зрілості АТ КБ «ПриватБанк» та АТ «Ощадбанк», що дозволило нам окреслити їхнє місце в цифровому ландшафті українського фінансового сектору та визначити напрями подальшого посилення їхньої цифрової стійкості.

Узагальнені показники по зазначених банках, на яких побудовані наступні розрахунки зведено в таблиці 2.11.

Порівняльні публічні індикатори цифрової зрілості
АТ КБ «ПриватБанк» та АТ «Ощадбанк»

Блок	Індикатор (укрупнений)	АТ КБ «ПриватБанк»	АТ «Ощадбанк»	Інтерпретація
1	2	3	4	5
ТІ – технологічна інфраструктура	Кількість відділень та участь у POWER BANKING	1183 відділень (01.10.2024); понад 500 відділень у мережі POWER BANKING	≈1200 відділень; 450 чергових відділень у POWER BANKING	Обидва банки мають розгалужену мережу та значну частку «енергонезалежних» відділень; інфраструктурна стійкість трохи вища у ПриватБанку за кількістю Power Banking-точок.
	Масштаб клієнтської бази	Понад 19 млн активних клієнтів (фіз. та юр. особи)	Ощадбанк – один із найбільших держбанків із мережею ~1200 відділень	За масштабом клієнтської бази ПриватБанк виступає безумовним лідером, Ощадбанк – другим великим «плечем» держсектору.
СІ – клієнтська цифрова взаємодія	Частка/кількість активних digital-користувачів	74 % активних клієнтів – користувачі мобільного застосунку Privat24 (2023)	4,6 млн клієнтів мають Mobile Oschad; понад 800 тис. візитів і транзакцій щодня; у 2024 р. кількість транзакцій зросла на 15 %, сума – на 23 %	В обох банках цифрові канали стали основним каналом взаємодії; за часткою digital-користувачів ПриватБанк виглядає більш зрілим.
	Обсяг операцій у digital-каналах	Значна частка операцій у дистанційних каналах (згідно з інтегрованими звітами банку)	157 млн транзакцій на 362 млрд грн в системі Oschad 24/7 у 2023 р.; 2,5 млн транзакцій через OschadPAY	Для Ощадбанку зафіксовано дуже високий масштаб digital-операцій; для ПриватБанку – структурно подібний профіль, але з більшим числом клієнтів.
ІН – інноваційність	Інноваційні канали та продукти	Лідер ринку digital-banking; розвиток мобільних сервісів, онлайн-кредитування, digital-onboarding	Розвиток Mobile Oschad, OschadPAY (каса в смартфоні), віддалена ідентифікація з травня 2024 р.	Обидва банки демонструють високий рівень інновацій; ПриватБанк – більш зрілий екосистемний гравець, Ощадбанк – швидко «наздоганяючий» інноватор.

Закінчення таблиці 2.11

1	2	3	4	5
CR – кіберстійкість / операційна стійкість	Участь у POWER BANKING та забезпечення безперервності	Понад 500 відділень із генераторами та резервними каналами зв'язку в мережі POWER BANKING	450 чергових відділень у POWER BANKING, спеціально обладнаних для роботи в умовах тривалих перебоїв з енергопостачанням	Обидва банки інтегровані в мережу операційної стійкості, що відповідає посиленим вимогам НБУ до системно важливих банків.
RI – регуляторна та інституційна готовність	Державна власність, роль у реалізації регулювання	100% акцій належить державі в особі КМУ	Державний банк з ключовою роллю у реалізації державних програм, включаючи підтримку бізнесу та ветеранські ініціативи	Державна власність та статус найбільших банків означають підвищені вимоги НБУ до ІСТ- та кіберризиків; обидва банки виступають «якорями» регуляторної архітектури.

Джерело: розроблено на основі даних офіційних сайтів банків [1; 189; 194; 150].

Розгорнута система показників за кожним із блоків авторської моделі (TI, CI, IN, CR, RI) з детальним обґрунтуванням оцінок представлена в (табл. 2.12 і 2.13). Шкала оцінювання наведена в табл. 2.14

Таблиця 2.12

Оцінювання блоків цифрової зрілості АТ КБ «ПриватБанк»

Блок	Код	Показник	Фактичне значення / характеристика	Оцінка (1-3)	Обґрунтування
1	2	3	4	5	6
TI	TI1	Частка ІТ-інвестицій у витратах	н/д (публічні дані відсутні)	3	Опосередковано – через масштаб цифрових сервісів
	TI2	Рівень хмарної інтеграції	високий (власна хмарна платформа)	3	Використання хмарних рішень для масштабування
	TI3	Ступінь API-інтеграції	широка (понад 100 відкритих API)	3	Розвинена API-екосистема
	TI4	Рівень автоматизації (RPA)	високий (автоматизація кредитування, платежів)	3	Широке впровадження RPA
	TI5	Data governance	наявна формалізована система	3	Побудована система управління даними
	Середня оцінка TI			3,0	Високий

Закінчення таблиці 2.12

1	2	3	4	5	6
CI	CI1	Частка digital-клієнтів	74% активних клієнтів	3	Один із найвищих показників у Європі
	CI2	Частка операцій у digital-каналах	понад 90%	3	Переважна більшість операцій онлайн
	CI3	Частка biometric onboarding	значна (через Privat24 та BankID)	3	Широке використання біометрії
	CI4	Питома вага mobile-first	90%+ активних користувачів	3	Мобільний застосунок – основний канал
	CI5	NDSI (індекс задоволеності)	4,5/5 (за даними досліджень)	3	Високий рівень задоволеності
	Середня оцінка CI			3,0	Високий
IN	IN1	Частка AI/ML-продуктів	висока (скоринг, персоналізація, чат-боти)	3	Інтенсивне використання AI/ML
	IN2	Фінтех-партнерства	активні (лабораторія інновацій, стартапи)	3	Співпраця з FinTech-екосистемою
	IN3	Витрати на інновації (% доходів)	н/д	3	Опосередковано – через кількість інновацій
	IN4	DLT/Blockchain-рішення	експериментальні проекти	2	Наявні пілотні проекти
	IN5	Частка доходів від API	значна (комісії, партнерства)	3	Монетизація API-доступу
	Середня оцінка IN			2,8	Високий (наближено)
CR	CR1	Відповідність NIST/DORA	часткова	2	На етапі імплементації
	CR2	Кіберінциденти на 1000 клієнтів	н/д	2	Брак публічних даних
	CR3	MTTR (год.)	н/д	2	Брак публічних даних
	CR4	Наявність SOC	власний SOC	3	Власний центр моніторингу безпеки
	CR5	Частка бюджету на кібербезпеку	н/д	2	Брак публічних даних
	Середня оцінка CR			2,2	Середньо-високий
RI	RI1	Відповідність вимогам НБУ	повна	3	Системно важливий банк
	RI2	Участь у регуляторних пісочницях	активна	3	Участь у проєктах НБУ
	RI3	Цифрова AML/KYC	BankID НБУ, біометрія	3	Високий рівень
	RI4	Відповідність GDPR	часткова (адаптація до євростандартів)	2	На етапі гармонізації
	RI5	ESG/CSR digital-політика	наявність звітності	3	Публічна ESG-звітність
	Середня оцінка RI			2,8	Високий (наближено)
Інтегральний показник DCSI = 2,76					

Джерело: розраховано автором за даними офіційних сайтів банків [189; 194] та публічних звітів.

Оцінювання блоків цифрової зрілості АТ «Ощадбанк»

Блок	Код	Показник	Фактичне значення / характеристика	Оцінка (1-3)	Обґрунтування
1	2	3	4	5	6
ТІ	ТІ1	Частка ІТ-інвестицій у витратах	н/д (публічні дані відсутні)	2	Опосередковано – через масштаб трансформації
	ТІ2	Рівень хмарної інтеграції	середній (активна модернізація)	2	Перехід на хмарні рішення
	ТІ3	Ступінь API-інтеграції	обмежена	2	Розвивається
	ТІ4	Рівень автоматизації (RPA)	середній (автоматизація соцвиплат, платежів)	2	Впроваджується
	ТІ5	Data governance	формується	2	На етапі становлення
	Середня оцінка ТІ			2,0	Середньо-високий
СІ	СІ1	Частка digital-клієнтів	4,6 млн користувачів Mobile Oschad	2	Нижча, ніж у ПриватБанку
	СІ2	Частка операцій у digital-каналах	157 млн транзакцій / 362 млрд грн	2	Значний обсяг, але зростаючий
	СІ3	Частка biometric onboarding	через BankID НБУ, з травня 2024	2	Запроваджено нещодавно
	СІ4	Питома вага mobile-first	зростає (+15 % транзакцій)	2	Динаміка позитивна
	СІ5	NDSI (індекс задоволеності)	4,0/5 (оціночно)	2	Добра, але не лідерська
	Середня оцінка СІ			2,0	Середньо-високий
ІН	ІН1	Частка AI/ML-продуктів	обмежена (скоринг, OschadPAY)	2	Початковий етап
	ІН2	Фінтех-партнерства	окремі проєкти	2	Активізується
	ІН3	Витрати на інновації (% доходів)	н/д	2	Опосередковано
	ІН4	DLT/Blockchain-рішення	відсутні	1	Не впроваджено
	ІН5	Частка доходів від API	низька	2	Формується
	Середня оцінка ІН			1,8	Середньо-високий / Середній
СР	СР1	Відповідність NIST/DORA	часткова	2	На етапі імплементації
	СР2	Кіберінциденти на 1000 клієнтів	н/д	2	Брак публічних даних
	СР3	MTTR (год.)	н/д	2	Брак публічних даних
	СР4	Наявність SOC	власний SOC	3	Власний центр моніторингу безпеки
	СР5	Частка бюджету на кібербезпеку	н/д	1	Брак публічних даних
	Середня оцінка СР			2,0	Середньо-високий

Закінчення таблиці 2.12

1	2	3	4	5	6
RI	RI1	Відповідність вимогам НБУ	повна	3	Системно важливий банк
	RI2	Участь у регуляторних пісочницях	участь	3	Участь у проєктах НБУ
	RI3	Цифрова AML/KYC	BankID НБУ, соціальні виплати	3	Високий рівень
	RI4	Відповідність GDPR	часткова (адаптація до євростандартів)	2	На етапі гармонізації
	RI5	ESG/CSR digital-політика	наявність звітності	3	Публічна ESG-звітність
	Середня оцінка RI			2,8	Високий (наближено)
Інтегральний показник DCMІ = 2,12					

Джерело: розраховано автором за даними офіційних сайтів банків [189; 194] та публічних звітів

Примітки до таблиць 2.11 і 2.12:

– **н/д** – публічні дані за відповідним показником відсутні. У таких випадках оцінка визначалася експертним шляхом на основі непрямих індикаторів (якість цифрових сервісів, масштаб операцій, публічні заяви банків тощо).

– **Блок РО (процесна зрілість)** – не включено до розрахунку через відсутність публічних даних щодо DevSecOps-практик, Agile-підходів, рівня електронного документообігу та ролі CIO/CTO у стратегічному управлінні.

– **Оцінка CR5 для Ощадбанку** – визначена як «1» (середній рівень) через відсутність публічних даних про частку бюджету на кібербезпеку у витратах на ІТ. У разі появи відповідних даних оцінка може бути переглянута.

Для практичного застосування авторської моделі на мікрорівні використаємо спрощений індекс:

$$DCMI_bank = \frac{U_{TI} + U_{CI} + U_{IN} + U_{CR} + U_{RI}}{5},$$

де U_k – оцінка блоку (TI , CI , IN , CR , RI) за шкалою: 1 – середній рівень, 2 – середньо-високий, 3 – високий рівень цифрової зрілості; k – назва блоку (табл. 2.14)

Таблиця 2.14

Шкала оцінювання показників для розрахунку DCMІ

Оцінка	Рівень цифрової зрілості	Характеристика
3	Високий	Показник перевищує середньоринкові значення або відповідає найкращим практикам
2	Середньо-високий	Показник відповідає середньоринковому рівню або демонструє позитивну динаміку
1	Середній	Показник нижче середньоринкового або перебуває на початковому етапі розвитку

Джерело: розроблено автором на основі шкали, наведеної в підрозділі 2.1

Застосування трирівневої шкали (1–3) для оцінювання окремих блоків зумовлене обмеженою доступністю публічних даних за низкою індикаторів (зокрема, щодо витрат на ІТ та кібербезпеку, показників MTTR, частоти кіберінцидентів тощо). Укрупнення шкали дозволяє уникнути хибної точності та забезпечити коректність порівняльного аналізу. Отриманий інтегральний показник DСMI (у діапазоні 1–3) для інтерпретації відповідно до п'ятирівневої шкали, наведеної в таблиці 2.5, перераховується в діапазон 0–1 за формулою:

$$DSMI_{(0-1)} = \frac{DCMI_{(1-3)} - 1}{2}.$$

Використовуючи дані узагальнені в таблицях 2.11 і 2.12, розрахуємо інтегральний показник DСMI. Зауважимо, що при розрахунку ми спирались лише на публічні дані; блоки РО та «глибока» CR (кіберінциденти, MTTR, SOC-метрики) залишаються «прихованими» через відсутність відкритої статистики.

Оцінювання АТ КБ «ПриватБанк» (джерело – таблиця 2.11)

$$DCMI_{Privat} = \frac{3+3+2,8+2,2+2,8}{5} = 2,76.$$

Тобто укрупнений індекс цифрової зрілості ПриватБанку – 2,76 (наближено до «високого» рівня).

Оцінювання АТ «Ощадбанк» (джерело – таблиця 2.12)

$$DCMI_{Oschad} = \frac{2+2+1,8+2+2,8}{5} = 2,12.$$

Отже, укрупнений індекс цифрової зрілості Ощадбанку становить 2,12 (середній рівень).

Розраховані значення засвідчують суттєву диференціацію між двома досліджуваними банками. АТ КБ «ПриватБанк» з індексом DСMI = 2,76 наближається до «високого» рівня зрілості (верхня межа середньо-високого діапазону), тоді як АТ «Ощадбанк» з індексом DСMI = 2,12 перебуває у верхній частині «середнього» рівня. Різниця в 0,64 бала (або приблизно 27 % відносно значення АТ «Ощадбанк») свідчить про наявність структурних відмінностей у підходах до цифрової трансформації, обсягах інвестицій в ІТ-інфраструктуру та рівні проникнення цифрових каналів серед клієнтів.

Перерахунок показник DСMІ відповідно до п'ятирівневої шкали наведено у таблиці 2.15.

Таблиця 2.15

Перерахунок показник DСMІ за п'ятирівневою шкалою

Банк	DСMІ (шкала 1-3)	Перерахунок у шкалу 0-1	Рівень за авторською методикою (табл. 2.5)
ПриватБанк	2,78	$(2,8 - 1) / 2 = \mathbf{0,89}$	Високий (Лідерський)
Ощадбанк	2,12	$(2,12 - 1) / 2 = \mathbf{0,56}$	Середній (верхня межа)

Примітка: DСMІ = 0,89 та 0,56 відповідають діапазонам 0,81–1,00 та 0,41–0,60, що підтверджує висновок про високий рівень цифрової зрілості АТ КБ «ПриватБанк» (наближено до лідерського) та середній рівень АТ «Ощадбанк».

Для глибшого розуміння диференціації доцільно розглянути результати за окремими блоками авторської моделі.

Технологічна інфраструктура (ТІ). За цим блоком порівняльного аналізу обидва банки демонструють досить високі показники. Такий результат зумовлений передусім значними обсягами інвестицій, спрямованими на модернізацію ІТ-систем, розвиток хмарних рішень та інтеграцію програмних інтерфейсів (API). АТ КБ «ПриватБанк» має певну (хоча й незначну) перевагу. Вона забезпечується двома факторами. Перший — більша кількість відділень, інтегрованих у мережу POWER BANKING (понад 500 проти 450 в АТ «Ощадбанк»). Другий більш широкий спектр відкритих API для сторонніх розробників. Обидві установи активно застосовують хмарні технології та засоби автоматизації бізнес-процесів. Проте ПриватБанк демонструє вищий ступінь впровадження рішень із роботизованої автоматизації процесів (RPA). Це, своєю чергою, дозволяє йому оперативніше опрацьовувати клієнтські запити та знижувати рівень операційних витрат.

Клієнтська цифрова взаємодія (СІ). Найбільша розбіжність між цими двома установами спостерігається саме в цьому блоці. Зокрема, в АТ КБ «ПриватБанк» 74 % активних клієнтів є користувачами мобільного застосунку Privat24, що свідчить про високий рівень проникнення цифрових каналів та сформовану культуру самообслуговування.

Натомість в АТ «Ощадбанк» частка цифрових клієнтів є нижчою (4,6 млн користувачів Mobile Oschad при загальній клієнтській базі, що перевищує 10 млн). Наведені дані відображають не тільки об'єктивні особливості клієнтського профілю (наприклад, в АТ «Ощадбанк» це більша частка літніх людей та клієнтів, які отримують соціальні виплати), а і меншу інтенсивність маркетингових активностей із залучення до цифрових каналів. Разом із тим динаміка зростання кількості цифрових транзакцій в АТ «Ощадбанк» (+15 % за кількістю та +23 % за сумою у 2024 році) свідчить про прискорення темпів «наздоганяючої» цифровізації.

Інноваційна спроможність (IN). АТ КБ «ПриватБанк» визнано лідером ринку за кількістю впроваджених інноваційних продуктів та сервісів. Банк одним із перших в Україні запровадив онлайн-кредитування за лічені хвилини, розвинув екосистему для малого та середнього бізнесу, активно використовує технології штучного інтелекту для персоналізації пропозицій та скорингу. АТ «Ощадбанк», своєю чергою, демонструє інтенсивну динаміку розвитку: запущено OschadPAY (каса у смартфоні), запроваджено віддалену ідентифікацію клієнтів з використанням BankID НБУ, розширюється функціонал Mobile Oschad для юридичних осіб. Попри відставання за абсолютними показниками, темпи оновлення продуктової лінійки в Ощадбанку є вищими, що дозволяє поступово скорочувати розрив.

Кіберстійкість (CR). Обидва досліджувані банки досягли значного прогресу в забезпеченні операційної безперервності, особливо в умовах воєнних викликів. Зокрема, спільною рисою обох установ є участь у мережі POWER BANKING – відділень з альтернативними джерелами енергоживлення). Однак через обмежену публічну доступність даних про кількість кіберінцидентів, показники MTTR (середній час відновлення після інциденту) та рівень відповідності NIST CSF / DORA оцінити цей блок у повному обсязі неможливо. Доступна інформація свідчить про те, що обидва банки мають власні центри моніторингу безпеки (SOC) та проводять регулярний аудит інформаційної безпеки, однак глибина впровадження стандартів кіберстійкості у внутрішні процеси залишається відкритим питанням.

Регуляторно-інституційна готовність (RI). Обидва банки є державними (АТ КБ «ПриватБанк» – 100 % державної власності, АТ «Ощадбанк» – державний банк), що зумовлює підвищені вимоги з боку регулятора до управління ризиками, прозорості звітності та дотримання євроінтеграційних стандартів. Обидві установи активно співпрацюють із Національним банком України в межах реалізації стратегії розвитку фінансового сектору, беруть участь у регуляторних «пісочницях» та імплементують вимоги щодо цифрової ідентифікації та захисту персональних даних. За цим блоком обидва банки отримують однаково високі оцінки.

Проведений аналіз дає змогу виокремити ключові відмінності між двома досліджуваними фінансовими установами. АТ КБ «ПриватБанк» є беззаперечним лідером за рівнем цифрової зрілості. Така перевага зумовлена трьома факторами: по-перше, більш раннім стартом процесів цифрової трансформації; по-друге, послідовною реалізацією стратегії «digital-first»; по-третє, вищими обсягами інвестицій, спрямованих на технологічний розвиток. Сильними сторонами цієї установи виступають: високий рівень проникнення мобільних каналів обслуговування; широка екосистема інноваційних продуктів; а також розвинена API-інфраструктура. АТ «Ощадбанк», попри нижчий інтегральний показник, демонструє позитивну динаміку, яку можна охарактеризувати як наздоганяючу цифровізацію. Потенціал зростання цієї установи пов'язаний насамперед із двома аспектами. Перший – використання переваг державного статусу (доступ до великих масивів даних, широка територіальна мережа). Другий — поступове нарощування обсягів інвестицій у розвиток цифрових каналів.

Основними «вузькими місцями», які потребують першочергового усунення, є: для АТ КБ «ПриватБанк» – подальше підвищення рівня кіберстійкості та забезпечення відповідності вимогам DORA (з урахуванням системної важливості цієї установи); для АТ «Ощадбанк» – прискорення міграції клієнтів у цифрові канали обслуговування, розширення

функціональних можливостей мобільного застосунку, а також активізація маркетингових заходів, спрямованих на залучення нових користувачів.

Отримані результати інтегрального оцінювання цифрової зрілості АТ КБ *«ПриватБанк» та АТ «Ощадбанк» вважаємо доцільним* порівняти з міжнародними бенчмарками, які відображають рівень цифрового розвитку фінансових систем у різних країнах. Серед найбільш авторитетних інструментів для такого порівняння є Індекс цифрової економіки та суспільства (DESI), який використовується Європейською Комісією для оцінювання країн-членів ЄС. Крім того, доцільно використати рамку цифрової зрілості Організації економічного співробітництва та розвитку (OECD), яка пропонує систему показників для міжнародних зіставлень [63; 109].

DESI охоплює чотири ключові виміри: людський капітал, підключеність (широкопasmовий доступ), інтеграцію цифрових технологій бізнесом та цифрові публічні послуги. У 2022 році середнє значення DESI для країн Європейського Союзу становило 52,3 бала, причому лідерами виступали Фінляндія, Данія, Нідерланди та Ірландія, які перевищували 60 балів. Країни Центральної та Східної Європи – зокрема Польща, Угорщина, Румунія, Болгарія – демонстрували нижчі показники, особливо за компонентами інтеграції цифрових технологій у бізнес-процеси та розвитку електронної комерції [64].

Для фінансового сектору найбільш релевантним є вимір «інтеграція цифрових технологій бізнесом», який включає показники використання електронних платежів, хмарних сервісів, штучного інтелекту та обміну електронними даними. Хоча DESI безпосередньо не виокремлює фінансових посередників як окрему категорію, зазначені індикатори дають змогу опосередковано оцінити загальний рівень цифрової зрілості бізнес-середовища, у якому функціонують фінансові установи.

Зіставлення показників українських банків із європейськими бенчмарками свідчить про наявність як суттєвих досягнень, так і сфер, що потребують подальшого розвитку. За показниками проникнення безготівкових платежів, мобільного банкінгу та цифрової ідентифікації (BankID НБУ)

Україна демонструє результати, зіставні з лідерами Центрально-Східної Європи та навіть перевищує окремі показники країн Балтії [110; 52]. Водночас за рівнем інтеграції фінансових сервісів у платформні екосистеми, розвитком відкритого банкінгу та ступенем впровадження штучного інтелекту в ризик-менеджменті українські установи поступаються провідним європейським банкам [115].

Важливим орієнтиром для порівняння є також рамка цифрової зрілості, запропонована Digital Economy Navigator (DEN) [50]. Ця методологія, розроблена на основі рекомендацій OECD щодо побудови композитних індикаторів, охоплює 145 показників, згрупованих у три ключові виміри: «Цифровий бізнес», «Цифрові засади» та «Цифрове суспільство». У межах виміру «Цифрові засади» окремий блок «Цифрові фінанси» оцінює зрілість фінансової системи, а також доступ до цифрового банкінгу та платіжних систем, ступінь їх використання населенням. Застосування подібної логіки до оцінювання українських фінансових посередників дозволяє розмістити отримані результати у ширшому міжнародному контексті.

Отриманий інтегральний показник цифрової зрілості для досліджуваної вибірки українських банків (усереднене значення DСМІ приблизно 2,5 за п'ятирівневою шкалою, що відповідає діапазону 0,61-0,80 при перерахунку в шкалу [0;1]) свідчить про досягнення рівня, який можна охарактеризувати як «високий» згідно з авторською класифікацією. Порівняно з оцінками, наведеними у звітах OECD щодо цифровізації фінансових послуг, цей показник наближається до рівня країн Центральної Європи (Чехія, Словаччина, Угорщина), проте поступається лідерам Північної Європи (Швеція, Данія, Фінляндія), де цифрова трансформація фінансового сектору розпочалася раніше та супроводжувалася більш системною державною підтримкою.

При здійсненні міжнародних порівнянь окремої уваги заслуговує блок «Кіберстійкість» (CR). Українські банки, функціонуючи в умовах воєнного стану та стійкого зростання кіберзагроз, досягли суттєвого прогресу за напрямом

забезпечення операційної безперервності. Йдеться, зокрема, про наявність розподілених резервних потужностей та участь у мережі POWER BANKING.

Водночас за такими позиціями, як формалізоване управління ІКТ-ризиками та відповідність стандартам DORA, українські установи нині перебувають на стадії імплементації. Це, своєю чергою, вимагає додаткових зусиль, спрямованих на гармонізацію вітчизняних практик із європейськими вимогами [63].

Таким чином, порівняльний аналіз із міжнародними бенчмарками підтверджує, що цифрова зрілість провідних українських фінансових посередників досягла рівня, який дозволяє їм конкурувати з установами з Центральної та Східної Європи у сферах масових цифрових платежів, мобільного банкінгу та дистанційної ідентифікації. Водночас відставання вітчизняних фінансових установ спостерігається в напрямках, які потребують більш зрілих екосистемних рішень (відкритий банкінг, платформізація) та посиленої кіберстійкості на рівні кращих європейських практик. *Це визначає стратегічні орієнтири для подальшого підвищення їхньої конкурентоспроможності.*

Підсумовуючи порівняльний аналіз з міжнародними бенчмарками, можна стверджувати: провідні українські фінансові посередники за такими напрямками, як масові цифрові платежі, мобільний банкінг та дистанційна ідентифікація, досягли рівня, який уможлиблює їхню конкуренцію з аналогічними установами із Центральної та Східної Європи.

Водночас зберігається певне відставання у сферах, що потребують більш зрілих екосистемних рішень, наприклад як відкритий банкінг і платформізація, а також у рівні кіберстійкості порівняно з найкращими європейськими практиками. Зазначене відставання окреслює стратегічні пріоритети для подальшого підвищення цифрової зрілості та конкурентоспроможності вітчизняних фінансових установ.

Висновки до розділу 2

Результати, отримані у процесі дослідження, дають підстави для формулювання низки узагальнених висновків стосовно цифрової зрілості фінансових посередників, які функціонують в Україні.

1. Цифрова зрілість фінансових посередників являє собою складну, багатовимірну характеристику, яка не може бути зведена до якогось одного показника або окремого аспекту. Ця характеристика об'єднує шість ключових компонентів: технологічну інфраструктуру (як базис для здійснення цифрових операцій); процесну організацію (що відображає ступінь автоматизації внутрішніх процесів); клієнтську взаємодію (через цифрові канали); інноваційність (тобто здатність установи впроваджувати нові рішення); кіберстійкість (спроможність протидіяти загрозам); а також інституційно-регуляторну відповідність сучасним цифровим вимогам. Саме таке розуміння багатовимірності лягло в основу запропонованої авторської моделі індексу цифрової зрілості.

2. Аналіз наявних міжнародних підходів до оцінювання цифровізації – починаючи від методик OECD та BIS і закінчуючи напрацюваннями консалтингових компаній (Deloitte тощо) та індексом DESI, що розробляється Європейською Комісією – засвідчив відсутність універсальної методики. Жодна з існуючих рамок не враховує в повному обсязі специфіку діяльності фінансових посередників у країнах із ринками, що розвиваються. Особливо це стосується умов дії екстремальних викликів, зокрема воєнних шоків, із якими зіткнулася Україна. Наявні методики або є надто загальними, або розроблялися для стабільних ринків розвинених економік. Зазначена обставина зумовила необхідність створення адаптованої методологічної рамки, здатної враховувати українські реалії.

3. Укрупнена оцінка, виконана на рівні всього фінансового сектору України, засвідчила неоднорідний характер розподілу рівнів цифрової зрілості. Найвищі показники український фінансовий сектор демонструє за двома напрямками: технологічна інфраструктура та цифрова поведінка клієнтів.

Населення активно використовує онлайн-банкінг, мобільні додатки та безготівкові форми платежів. Середньо-високий рівень спостерігається за компонентами інноваційності та регуляторної готовності. Нові продукти впроваджуються, регуляторні вимоги виконуються, однак, на нашу думку, наявний ще певний простір для подальшого розвитку. Водночас компонент кіберстійкості отримав лише середню оцінку. Це, своєю чергою, сигналізує про існування вразливостей у системах захисту інформації та практиках управління ризиками. Зазначений факт визначає чіткий пріоритет для подальших капіталовкладень – необхідність посилення кіберзахисту та вдосконалення ризик-менеджменту.

4. Пілотне апробування розробленої методики на двох найбільших банківських установах України – АТ КБ «ПриватБанк» та АТ «Ощадбанк» – дало такі результати. Обидва банки досягли середньо-високого рівня цифрової зрілості, що підтверджує їхній статус лідерів цифрової трансформації у вітчизняному фінансовому секторі. При цьому ПриватБанк, який отримав індекс 2,76, наближається до високого рівня. Такий результат забезпечується кількома факторами: більшою часткою клієнтів, які активно користуються цифровими каналами; ширшою та інноваційнішою продуктово-сервісною лінійкою; а також масштабнішою мережею Power Banking (банкоматів нового покоління з розширеним функціоналом). Ощадбанк, попри дещо нижчий індекс (2,12), демонструє інтенсивну динаміку так званої «наздоганяючої» цифровізації. Установа активно скорочує наявний розрив шляхом впровадження новітніх технологій та сучасних сервісів.

5. Проведене дослідження, поряд із позитивними результатами, виявило також низку обмежень, які, на думку автора, слід враховувати при інтерпретації отриманих даних. Найбільш значущою проблемою є дефіцит стандартизованої цифрової звітності. Фінансові установи не мають обов'язку систематично розкривати інформацію про власні цифрові показники у форматі, який би був придатним для здійснення порівняльного аналізу. Додатковим ускладненням виступає обмежений доступ до внутрішніх даних, що стосуються ІТ-систем та заходів безпеки. Це, своєю чергою, перешкоджає

проведенню повноцінного оцінювання. Крім того, в Україні наразі відсутні єдині національні норми та стандарти, призначені для вимірювання цифрової зрілості фінансових посередників. Наслідком цього є неможливість здійснити повноцінний розрахунок індексу за всіма передбаченими компонентами. Зазначені обставини вказують на необхідність подальшої методологічної роботи, а також, імовірно, на потребу в запровадженні регуляторних ініціатив, спрямованих на стандартизацію відповідної звітності.

6. Попри окреслені обмеження, запропонована методика та отримані в ході пілотного апробування результати мають безсумнівну практичну цінність. По-перше, вони можуть слугувати аналітичним підґрунтям для здійснення порівняльного моніторингу процесів цифрової трансформації, які відбуваються в різних фінансових посередників. По-друге, розроблена методика дає змогу формувати галузеві бенчмарки – тобто еталонні показники, з якими окремі установи можуть зіставляти власний прогрес у сфері цифровізації. По-третє, отримані результати здатні підтримувати прийняття рішень з боку регуляторних органів – передусім Національного банку України та інших відповідальних інституцій. Йдеться, зокрема, про пріоритизацію цифрової політики, визначення напрямів розвитку кіберстійкості, а також стимулювання інноваційної активності в межах фінансового сектору України.

РОЗДІЛ 3

ПРАКТИЧНІ МЕХАНІЗМИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ СТРАТЕГІЇ РОЗВИТКУ ФІНАНСОВИХ ПОСЕРЕДНИКІВ В УКРАЇНІ

3.1. Імплементація міжнародного досвіду цифрової трансформації фінансового посередництва в умовах повоєнного відновлення України

Повоєнне відновлення економіки України висуває перед фінансовим сектором низку принципово нових завдань. Забезпечення безперервності банківських і платіжних послуг, відбудова пошкодженої інфраструктури, інтеграція внутрішньо переміщених осіб до системи фінансового обслуговування, а також поступова гармонізація з нормативно-правовим полем Європейського Союзу – усе це потребує системного перегляду підходів до цифрової трансформації фінансових посередників. Як зазначалося в попередніх авторських дослідженнях, «цифрові технології змінюють способи виконання класичних функцій фінансових посередників, формуючи нові механізми створення фінансової цінності» [174, с. 286]. В іншій публікації наголошується, що «конкурентні переваги фінансових посередників дедалі більше визначаються їхньою спроможністю забезпечувати стійкість і безпеку власних цифрових платформ» [227, с. 315].

Світовий досвід, накопичений у провідних юрисдикціях, пропонує різні моделі реагування на подібні виклики. Однак пряме копіювання інституційних рішень без урахування українських реалій є неможливим. Тому в межах цього підрозділу здійснюється не просте перелічення міжнародних практик, а їх критичне осмислення та адаптація до умов повоєнної відбудови.

Пріоритети повоєнного відновлення фінансового сектору. Першочергового значення набувають три взаємопов'язані напрями. По-перше, забезпечення безперервності базових фінансових послуг для населення та бізнесу, особливо в прифронтових і деокупованих територіях. Це передбачає не лише відновлення фізичної інфраструктури, а й розвиток резервних

цифрових каналів, здатних функціонувати в умовах обмеженого доступу до електромереж та інтернету. По-друге, інтеграція внутрішньо переміщених осіб до фінансової системи через спрощені процедури дистанційної ідентифікації, мобільні гаманці та програми фінансової допомоги. По-третє, системна гармонізація з регуляторними стандартами ЄС, що є необхідною умовою для отримання макрофінансової допомоги, залучення інвестицій та подальшого вступу до єдиного цифрового ринку.

Зазначені пріоритети визначають логіку імплементації міжнародного досвіду. На відміну від стабільних економік, де цифрова трансформація відбувається еволюційно, в Україні вона набуває характеру форсованої модернізації під тиском воєнних та постконфліктних викликів.

Адаптація регламенту DORA в Україні. Одним із найбільш значущих документів, що визначають сучасну архітектуру кіберстійкості фінансового сектору в Європі, є Регламент (ЄС) 2022/2554 про цифрову операційну стійкість (DORA) [69]. Як зазначають дослідники, DORA «запроваджує гармонізовану, безпосередньо застосовну регуляторну рамку для цифрової операційної стійкості в фінансовому секторі ЄС», яка стала повністю обов'язковою до виконання з січня 2025 року [31].

Ключова ідея документа полягає в створенні єдиної рамки управління ІКТ-ризиками для всіх фінансових установ, включно з банками, страховими компаніями, інвестиційними фірмами та платіжними провайдерами. DORA встановлює вимоги до п'яти основних сфер: управління ІКТ-ризиками, реагування на інциденти та їх звітування, тестування операційної стійкості, управління ризиками від сторонніх ІКТ-провайдерів, а також обмін інформацією про кіберзагрози [51].

Для України адаптація DORA має не лише технічний, а й політичний вимір. Імплементація цих стандартів є частиною зобов'язань у межах Угоди про асоціацію з ЄС та необхідною передумовою для визнання еквівалентності національного регуляторного середовища. Як зауважується в сучасних дослідженнях, «перехід України від фрагментарного регулювання ІКТ-безпеки

до повноцінної рамки цифрової операційної стійкості, що відображає вимоги DORA, прискорюється під впливом воєнного тиску» [131]. При цьому Національний банк України вже розбудовує трикомпонентну SupTech-архітектуру, що включає API для звітування про інциденти, регуляторну пісочницю та інформаційну панель нагляду в реальному часі [131].

З огляду на це пропонується дорожня карта, що охоплює три етапи (табл. 3.1).

Перший етап (2026–2027 роки) – оцінювально-нормативний. На цьому етапі Національному банку України разом із Національною комісією з цінних паперів та фондового ринку доцільно провести комплексний аналіз чинних вимог до ІКТ-ризиків на предмет їх відповідності DORA. Результатом має стати розробка проекту змін до нормативно-правових актів, якими запроваджуються: обов’язкова ідентифікація критичних третіх ІКТ-провайдерів, вимоги до регулярного тестування операційної стійкості (включно зі сценаріями кібератак), а також стандартизована форма звітування про значні інциденти. Важливим є також створення централізованої бази даних про інциденти, доступної для регуляторів.

Другий етап (2027–2028 роки) – пілотне впровадження в системно важливих банках та платіжних системах. На цьому етапі доцільно використати механізм регуляторної «пісочниці» НБУ для тестування окремих вимог DORA в контрольованому середовищі. Як свідчить міжнародний досвід, «регуляторні пісочниці є дієвим інструментом для тестування інноваційних продуктів без ризику порушення чинного законодавства» [174, с. 292]. Зокрема, пілотні проекти можуть стосуватися автоматизації звітування про інциденти через RegTech-рішення, проведення стрес-тестування ІКТ-систем за методологією DORA, а також впровадження процедур управління ризиками від хмарних провайдерів.

Третій етап (2028–2030 роки) – масштабування на весь фінансовий сектор, включно з небанківськими посередниками. На цьому етапі передбачається обов’язкова сертифікація систем управління ІКТ-ризиками для

всіх фінансових установ, а також створення галузевого центру кіберстійкості, який акумулюватиме інформацію про загрози та забезпечуватиме координацію реагування на інциденти системного значення. Як зазначається в аналітичних матеріалах, «наглядова увага зосереджуватиметься на ефективному управлінні ІКТ-ризиками, а також на звітуванні про інциденти, якості даних і тестуванні стійкості як ключових індикаторів операційної стійкості» [31].

Таблиця 3.1

Дорожня карта імплементації DORA в Україні (2026 – 2030 рр.)

Етап	Строки	Відповідальні органи	Ключові заходи	Очікувані результати
I. Оцінювально-нормативний	2026–2027	НБУ, НКЦПФР, Мінцифри	- GAP-аналіз чинних вимог до DORA; - розробка змін до нормативно-правових актів; - створення бази даних про інциденти	- узгоджена нормативна база; - запроваджено обов’язкове звітування про значні інциденти
II. Пілотний	2027–2028	НБУ, системно важливі банки, платіжні системи	- тестування вимог у регуляторній «пісочниці»; - автоматизація звітування через RegTech; - стрес-тестування ІКТ-систем за методологією DORA	- апробовані механізми; - скоригована нормативна база за результатами пілоту
III. Масштабування	2028 - 2030	НБУ, всі фінансові установи	- обов’язкова сертифікація систем управління ІКТ-ризиками; - створення галузевого центру кіберстійкості	- повна відповідність DORA системно важливих установ; - пропорційні вимоги для малих та середніх учасників

Джерело: розроблено автором на основі [25; 31; 51; 69; 131].

Систематизація основних розривів між вимогами DORA та чинним регулюванням НБУ наведена в табл. 3.2.

Наведений у таблиці 3.2 порівняльний аналіз охоплює п’ять ключових сфер, визначених DORA, і дозволяє ідентифікувати основні розриви, які потребують усунення.

Порівняння вимог DORA та чинного регулювання НБУ
(станом на 2026 рік)

Сфера вимог DORA	Вимоги DORA	Чинне регулювання НБУ	Розрив / необхідна адаптація
Управління ІКТ-ризиками	Стратегія управління ІКТ-ризиками; розподіл обов'язків; політика безпеки	Положення про організацію системи внутрішнього контролю (частково)	Необхідне розширення: пряме закріплення відповідальності правління за ІКТ-ризиками
Звітування про інциденти	Обов'язкове звітування про значні інциденти (4 рівні: первинне, проміжне, остаточне, моніторинг)	Звітування про кіберінциденти – визначено, але часові норми не гармонізовані з DORA	Скорочення строків звітування до 24 годин для первинного повідомлення
Тестування операційної стійкості	Регулярне тестування (включно з тестуванням на проникнення); сценарне моделювання атак	Періодичний аудит інформаційної безпеки	Впровадження обов'язкового стрес-тестування ІКТ-систем за єдиною методологією
Управління ризиками від третіх провайдерів	Ідентифікація критичних третіх провайдерів; моніторинг ризиків аутсорсингу	Вимоги до аутсорсингу є, але реєстр критичних постачальників відсутній	Створення центрального реєстру критичних ІКТ-провайдерів
Обмін інформацією про кіберзагрози	Заохочення участі в інформаційно-аналітичних центрах (ISAC)	Інформаційний обмін через CERT-UA, але галузевого ISAC немає	Створення галузевого центру кіберстійкості (FIH)

Джерело: розроблено автором на основі узагальнення положень [10; 51; 61; 69] та оцінок експертів [31; 131; 227].

Сфера управління ІКТ-ризиками (статті 5–16 DORA). DORA вимагає запровадження комплексної стратегії управління ІКТ-ризиками, чіткого розподілу обов'язків (зокрема, пряме закріплення відповідальності правління) та формалізованої політики безпеки. Чинне регулювання НБУ містить лише окремі положення в межах вимог до організації системи внутрішнього контролю, що створює суттєвий розрив [51]. Як зазначає Бернітс Ло, «лише системно важливі банки демонструють високий рівень готовності, тоді як менші установи здебільшого перебувають на початкових стадіях підготовки до DORA» [31].

Сфера звітування про інциденти (статті 17–23 DORA). DORA встановлює чотирирівневу систему звітування: первинне повідомлення (протягом 24 годин), проміжне звітування, остаточний звіт та подальший моніторинг. Хоча в Україні звітування про кіберінциденти нормативно визначено, часові норми не гармонізовані з DORA. На сьогодні ключовим завданням є «скорочення строків звітування до 24 годин для первинного повідомлення та впровадження автоматизованих каналів звітування через RegTech-рішення» [131].

Сфера тестування операційної стійкості (статті 24–27 DORA). DORA вимагає регулярного тестування, включаючи тестування на проникнення (penetration testing) та сценарне моделювання кібератак. Чинним регулюванням НБУ передбачено лише періодичний аудит інформаційної безпеки, що не відповідає вимогам DORA щодо глибини та регулярності тестування. Як зазначають автори аналітичних матеріалів DLA Piper, «тестування стійкості має проводитися не рідше одного разу на три роки для всіх установ, а для системно важливих – щорічно» [51].

Сфера управління ризиками від третіх провайдерів (статті 28–36 DORA). DORA вимагає ідентифікації критичних третіх ІКТ-провайдерів, ведення їх реєстру, а також здійснення моніторингу ризиків аутсорсингу. В Україні відсутній центральний реєстр критичних постачальників, а вимоги до моніторингу є фрагментарними. Бернітс Ло зауважує, що «управління ризиками від третіх провайдерів є однією з найбільш ресурсозатратних сфер імплементації DORA, оскільки вимагає створення галузевої інфраструктури контролю» [31].

Сфера обміну інформацією про кіберзагрози (статті 47–49 DORA). DORA заохочує участь фінансових установ в інформаційно-аналітичних центрах (ISAC). В Україні наразі діє інформаційний обмін через CERT-UA, однак галузевий фінансовий центр кіберстійкості відсутній. На думку авторів, створення такого центру є критично важливим, оскільки «обмін інформацією

про загрози в режимі реального часу дозволяє значно підвищити рівень колективного захисту всього сектору» [227, с. 320].

Таким чином, таблиця 3.2 демонструє, що найбільші розриви між DORA та чинним регулюванням НБУ спостерігаються у сферах строків звітування про інциденти, глибини тестування стійкості та управління ризиками від третіх провайдерів. Усунення цих розривів має стати пріоритетом найближчих років.

Окремої уваги потребує питання пропорційності вимог. DORA передбачає диференційований підхід: для малих та середніх фінансових установ обсяг звітності та складність процедур можуть бути зменшені порівняно із системно важливими банками. Цей принцип є критично важливим для України, де значна частина кредитних спілок, страхових компаній та мікрофінансових організацій не має ресурсів для повноцінної імплементації всіх вимог DORA у короткостроковій перспективі. Як наголошується в науковій літературі, «лише синхронізоване поєднання передової аналітики, надійного правового каркасу та орієнтованої на безпеку організаційної культури дозволить українським фінансовим установам гарантувати безперервність критичних послуг» [131].

Розвиток відкритого банкінгу на основі PSD2. Другим важливим напрямом імплементації є впровадження моделі відкритого банкінгу, натхненної європейською Директивою PSD2 (Payment Services Directive 2). Ключовий урок, який Україна може взяти з європейського досвіду, полягає в тому, що відкритий банкінг – це не лише технологічне рішення, а й комплекс інституційних змін. PSD2 запрацювала ефективно завдяки одночасному впровадженню трьох компонентів: стандартизованих API (технологічна основа), ліцензування третіх постачальників платіжних послуг (регуляторна основа) та механізмів відшкодування збитків у разі несанкціонованих транзакцій (захисна основа).

На сьогодні Україна зробила вирішальний крок у цьому напрямі. 1 серпня 2025 року Національний банк України запровадив низку регуляцій, які встановлюють систему відкритого банкінгу в країні [54]. Як зазначає

Президент Асоціації українських банків А. Дубас, «модель відкритого банкінгу в Україні забезпечує стандартизований доступ третіх сторін до банківських даних клієнтів за їхньою згодою через захищені API» [54]. Ключовими елементами цієї моделі виступають: API для доступу до інформації про рахунки, API для ініціювання платежів, механізми авторизації користувачів із надійною аутентифікацією, а також регуляторні вимоги до учасників екосистеми та безпеки даних [54].

Українська модель відкритого банкінгу враховує принципи PSD2 та стандарти SEPA, особливо у сфері безпеки платежів, надійної аутентифікації та ролі третіх провайдерів (TPP). Водночас вона адаптована до локальних особливостей фінансового ринку та регуляторних вимог НБУ, що забезпечує гнучкість для українських учасників ринку [54]. Як зазначено в аналітичних матеріалах, «запровадження відкритого банкінгу завершує імплементацію принципів PSD2 в Україні та є важливим кроком на шляху до приєднання до SEPA та подальшої інтеграції до фінансової екосистеми ЄС» [128].

Щодо безпеки API, то ключові вимоги мають бути гармонізовані з DORA. Це передбачає використання сильних механізмів автентифікації (OAuth 2.0, OpenID Connect), шифрування даних у русі та спокої, а також обов'язкове ведення журналів доступу до API з можливістю подальшого аудиту. Як зазначено в дослідженнях з питань кібербезпеки фінансових установ, «актуальними типами кіберзагроз залишаються фішинг, рансомвер, DDoS-атаки, атаки на мобільні пристрої, а також злам внутрішніх механізмів безпеки» [54, с. 259]. Для третіх постачальників платіжних послуг пропонується запровадити дворівневу систему допуску: повне ліцензування для тих, хто ініціює платежі, та спрощена реєстрація для тих, хто лише отримує інформацію про рахунки.

Стандартизована архітектура взаємодії між зазначеними учасниками наведена на рисунку 3.1.

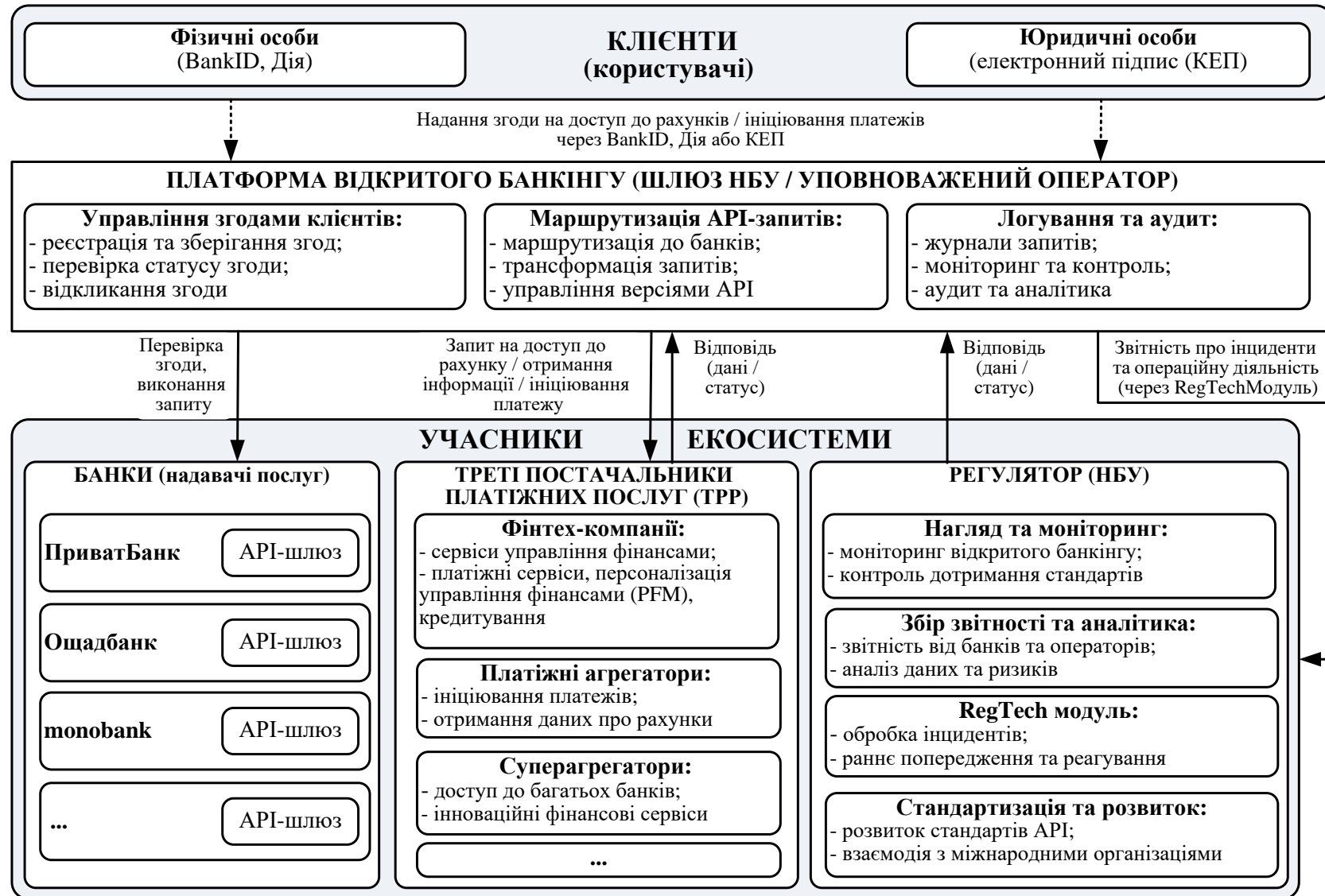


Рис. 3.1. Архітектура відкритого банкінгу в Україні

Джерело: розроблено автором на основі [54; 102; 128; 174].

Трирівнева архітектура відкритого банкінгу, зображена на рис. 3.1 фактично діє в Україні із серпня 2025 року. Верхній рівень ілюструє клієнтську взаємодію із системами цифрової ідентифікації. Центральний – функції платформи управління згодами та маршрутизації API-запитів. Нижній – розподіл ролей між трьома сторонами: провайдерами даних, сторонніми сервісами та регулятором Однією з характерних рис українського підходу є безоплатний доступ до базових API. Це спрямовано на стимулювання розвитку екосистеми. Водночас за додаткові комерційні послуги банки можуть встановлювати плату, що регулюється договорами між банком та TPP [54]. Така конфігурація забезпечує рівновагу між стимулюванням інновацій та їх економічною доцільністю для фінансових установ. Крім того, на наш погляд, доцільно акцентувати увагу на трьох ключових інформаційних потоках, які охоплюють надання згоди клієнтом, обмін даними через API-шлюз та звітування про інциденти відповідно до вимог DORA.

Інтеграція українського фінансового ринку до єдиного цифрового простору ЄС. Цей напрям виходить за межі суто технічних завдань. Він охоплює три ключові сфери: цифрову ідентифікацію, взаємодію платіжних систем та обмін фінансовими даними. Щодо цифрової ідентифікації, то Україна має унікальний актив – систему BankID НБУ, яка вже інтегрована з порталом «Дія». Для визнання української цифрової ідентичності в ЄС необхідно забезпечити відповідність вимогам регламенту eIDAS 2.0, зокрема щодо рівнів гарантій автентифікації та взаємного визнання національних схем.

Узагальнена структура цієї інтеграції за трьома ключовими напрямками наведена на рисунку 3.2.

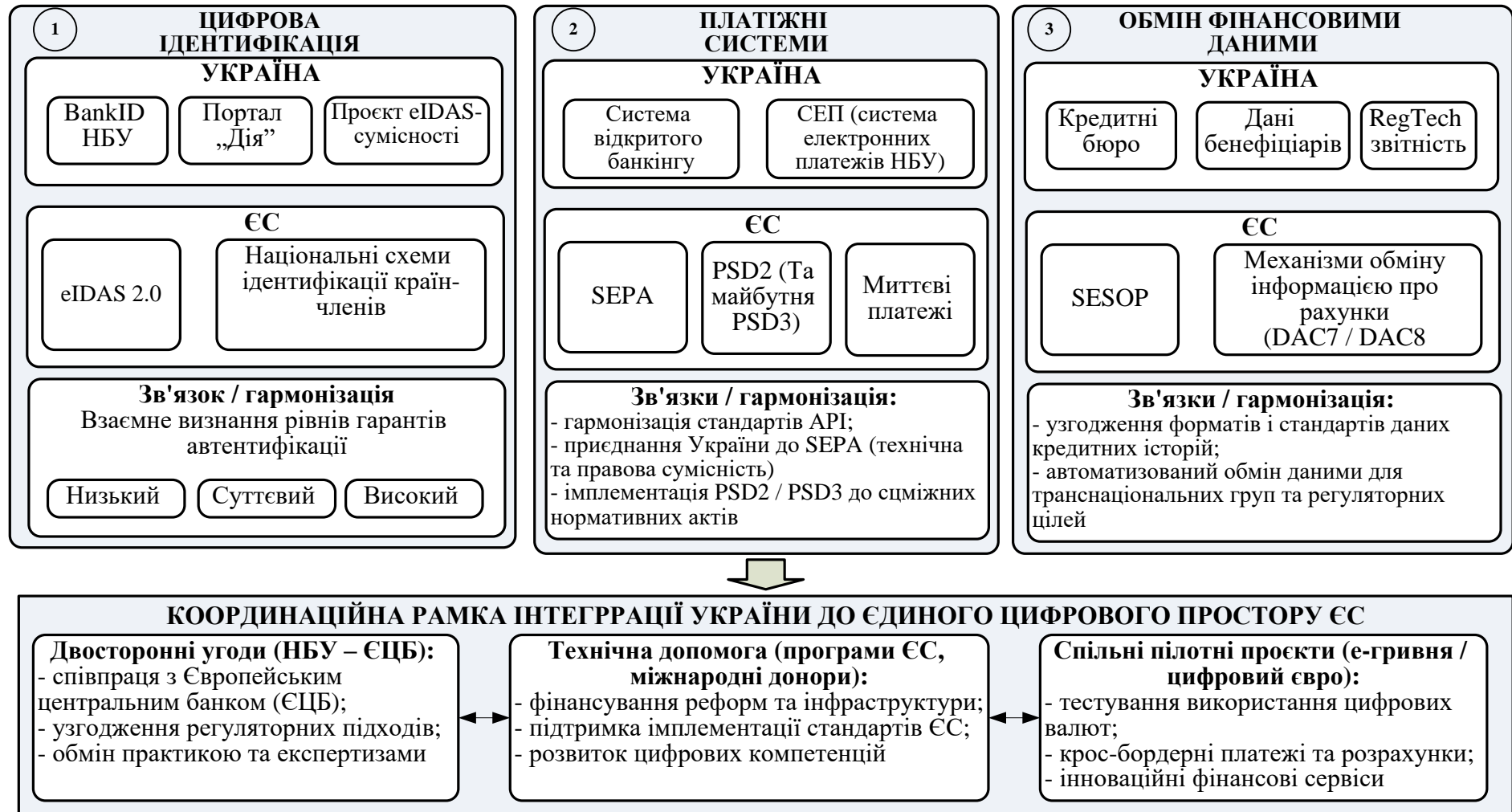


Рис. 3.2. Інтеграція українського фінансового ринку до єдиного цифрового простору ЄС

Джерело: розроблено автором на основі [54; 119; 128; 135; 69; 90; 200].

Кожен із напрямів представлених на рисунку 3.2 охоплює як національний рівень (Україна), так і європейський рівень (ЄС), а також зв'язки між ними, що потребують гармонізації.

Перший напрям – цифрова ідентифікація. В Україні сформовано базову інфраструктуру електронної ідентифікації, ядром якої виступає система BankID Національного банку України, інтегрована з порталом електронних послуг «Дія». На думку дослідників, система BankID потребує узгодження зі стандартами eIDAS, зокрема щодо рівнів гарантій автентифікації та взаємного визнання національних схем електронної ідентифікації [119]. Як зазначено в аналітичних матеріалах VIXIO Regulatory Intelligence, у 2025 році НБУ розпочав консультації щодо внесення змін до Положення про систему BankID з метою приведення української рамки цифрової ідентифікації у відповідність до eIDAS 2.0 [135]. У Європейському Союзі чинною є версія eIDAS 2.0, що запроваджує створення європейського гаманця цифрової ідентичності (European Digital Identity Wallet) [119].

Другий напрям – платіжні системи. З 1 серпня 2025 року в Україні запроваджено систему відкритого банкінгу, яка «забезпечує стандартизований доступ третіх сторін до банківських даних клієнтів за їхньою згодою через захищені API» [54]. Упровадження відкритого банкінгу завершує імплементацію принципів PSD2 в Україні та є важливим кроком на шляху до приєднання до зони єдиного платіжного простору в євроSEPA [128]. Це дозволить скоротити час та вартість транскордонних переказів між Україною та ЄС. Водночас для цього необхідно адаптувати національне законодавство до вимог PSD2 і PSD3, що включає, зокрема, запровадження відповідальності платіжних провайдерів за несанкціоновані транзакції, правила відшкодування збитків та стандарти безпеки платіжних інструментів. Ключовим завданням для України залишається гармонізація національних стандартів API з європейськими вимогами, що має відбуватися відповідно до принципів, закладених у Регламенті DORA [51; 69].

Третій напрям – обмін фінансовими даними. У цій сфері Україна перебуває на початковому етапі формування відповідної нормативної бази. Як зазначається в дослідженні А. Тараненко, ключовими елементами української RegTech-архітектури мають стати автоматизовані механізми звітування про фінансові операції, обмін кредитними історіями, а також доступ до даних про бенефіціарів компаній [131]. У Європейському Союзі функціонує система CESOP (Central Electronic System of Payment information), а також механізми автоматизованого обміну інформацією про банківські рахунки в межах DAC7 та DAC8.

Після завершення війни Україна зіткнеться з необхідністю залучення масштабних зовнішніх інвестицій для відбудови. Інвестори потребуватимуть доступу до достовірної фінансової інформації про позичальників, що неможливо без створення взаємоузгоджених механізмів обміну кредитними історіями та даними про бенефіціарів. Вважаємо, що у цьому контексті досвід ЄС щодо створення єдиної системи доступу до банківських рахунків може бути корисним для розробки національних рішень.

Важливо також передбачити наявність координаційної рамки, яка включає двосторонні угоди між Національним банком України та Європейським центральним банком, технічну допомогу від міжнародних донорів, а також спільні пілотні проєкти.

Варто також акцентувати увагу на потенціал цифрової гривні (е-гривня) для повоєнної відбудови. Хоча проєкт е-гривні перебуває на стадії концептуального опрацювання Національним банком – підготовка до пілотного проєкту триває, а пошук технологічного партнера завершується [124] – повоєнний контекст надає йому нового змісту. Е-гривня може стати не альтернативою готівці чи безготівковим коштам, а спеціалізованим інструментом для цільових державних платежів. Як зазначають дослідники, «ключовими висновками є критичні фактори, що впливають на успішну інтеграцію цифрових валют у національну економіку», а динаміка розвитку

платіжної системи України відображає її готовність до впровадження цифрової валюти [96].

За підсумками 2024 року частка безготівкових операцій у кількісному вираженні сягнула 94,5 %. Як свідчить аналіз, цей показник, , відображає високий рівень адаптації як населення, так і бізнесу до цифрових форм розрахунків [96]. Використання е-гривні дає змогу обмежувати коло отримувачів (наприклад, лише мешканцями певної території), цільове спрямування коштів (виключно на придбання будівельних матеріалів), а також термін дії фінансових ресурсів. Такі особливості мають свої позитивні і негативні наслідки як для населення, так і для держави.

У контексті повоєнної відбудови е-гривня потенційно вирішує три ключові завдання. Перше – забезпечення прозорості соціальних виплат. Кожна транзакція фіксується у розподіленому реєстрі, що унеможливорює подвійне отримання допомоги. Друге – скорочення адміністративних витрат на управління програмами підтримки. Для розподілу коштів не потрібно створювати окремі інституції; достатньо вбудувати відповідні правила безпосередньо у валюту. Третє – стимулювання локальної економіки. Кошти, «прив'язані» до певної громади, не можуть бути використані в іншому регіоні. Це змушує отримувачів витратити їх на місці, підтримуючи місцевий бізнес. Як наголошує Голова Національного банку України Андрій Пишний, особлива увага приділяється розвитку проєкту «Цифровий євро» з огляду на євроінтеграційний курс України. НБУ, відповідно до цих завдань, взаємодіє з Європейським центральним банком, Бундесбанком, Банком Бельгії, Банком Франції та Банком Сінгапуру [124].

Водночас упровадження е-гривні потребує вирішення низки складних питань: захисту персональних даних (чи буде реєстр повністю анонімним для регулятора?); технічної сумісності з існуючими платіжними системами; а також кіберстійкості самої інфраструктури. Тому на першому етапі доцільно обмежитись пілотом у невеликій територіальній громаді з обов'язковим

моніторингом усіх ризиків. Як слушно зауважує Голова НБУ, «ми хочемо, щоб цей пілот дав нам максимальну інформацію для прийняття рішення щодо масштабного випуску» [124].

Як свідчить український досвід останніх років, у фінансовому секторі дедалі частіше спрацьовує логіка, коли «компанії створюють продукти, тестують їх на ринку, а держава формалізує успішний досвід у законодавстві» [174]. Ця нова модель розвитку, де стартапи не просто підлаштовуються під регуляції, а стають драйверами їх змін, є особливо актуальною для повоєнного відновлення, коли потрібні швидкі та ефективні рішення.

Таким чином, зображена на рис. 3.2 архітектура інтеграції передбачає поступове зближення української фінансової інфраструктури з європейською за трьома взаємопов'язаними напрямками, що в сукупності створює передумови для повноцінної участі України в єдиному цифровому фінансовому просторі ЄС.

Отже, імплементація міжнародного досвіду цифрової трансформації фінансового посередництва в умовах повоєнного відновлення України має базуватися на трьох базових принципах: *вибірковості* (запозичення лише тих елементів, які відповідають національним пріоритетам), *пропорційності* (диференціація вимог залежно від розміру та системного значення установи) та *послідовності* (поетапне впровадження з чіткими часовими орієнтирами). Ключовими напрямками найближчих років мають стати адаптація DORA, стандартизація відкритого банкінгу, гармонізація систем цифрової ідентифікації з eIDAS, а також пілотування програмованої цифрової гривні для цільових повоєнних видатків.

3.2. Організаційно-економічний механізм інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку України

Формування інноваційної інфраструктури цифрового фінансового ринку потребує не лише технологічних рішень, але й належного організаційно-економічного забезпечення. Як зазначалося в попередніх авторських дослідженнях, «інноваційна інфраструктура цифрового фінансового ринку України складається із сукупності взаємопов'язаних елементів, основними з яких є: фінансові посередники, технологічні платформи та рішення, регуляторні інституції, клієнтська база, інфраструктурні інструменти, а також освітньо-наукове середовище» [174, с. 288]. Однак наявність окремих елементів ще не гарантує їх ефективної взаємодії. Тому необхідним є створення цілісного механізму, який би забезпечував координацію дій усіх учасників, розподіл ресурсів та узгодження інтересів.

Інтеграція фінансових посередників до інноваційної інфраструктури передбачає їхню активну участь у формуванні цифрових платформ, розвитку API-екосистем, впровадженні інноваційних продуктів та забезпеченні кіберстійкості. Як доведено у власному дослідженні у співавторстві «фінансові посередники стають ключовими вузловими елементами цифрової інфраструктури» завдяки підтримці миттєвих платежів, реалізації технологій відкритого банкінгу, інтеграції в регуляторні пісочниці НБУ та забезпеченню цифрової ідентифікації клієнтів [227, с. 312]. Водночас рівень такої інтеграції залишається нерівномірним: банківський сектор демонструє високу цифрову зрілість, тоді як небанківські посередники (кредитні спілки, страхові компанії, мікрофінансові організації) перебувають переважно на початкових етапах цифровізації. Це зумовлює необхідність розроблення спеціального механізму, який би враховував різний рівень готовності різних типів фінансових установ.

Представлений на рис. 3.3 організаційно-економічний механізм інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку відображає не лише структурну композицію відповідних елементів, але й логіку їх взаємодії в динаміці.

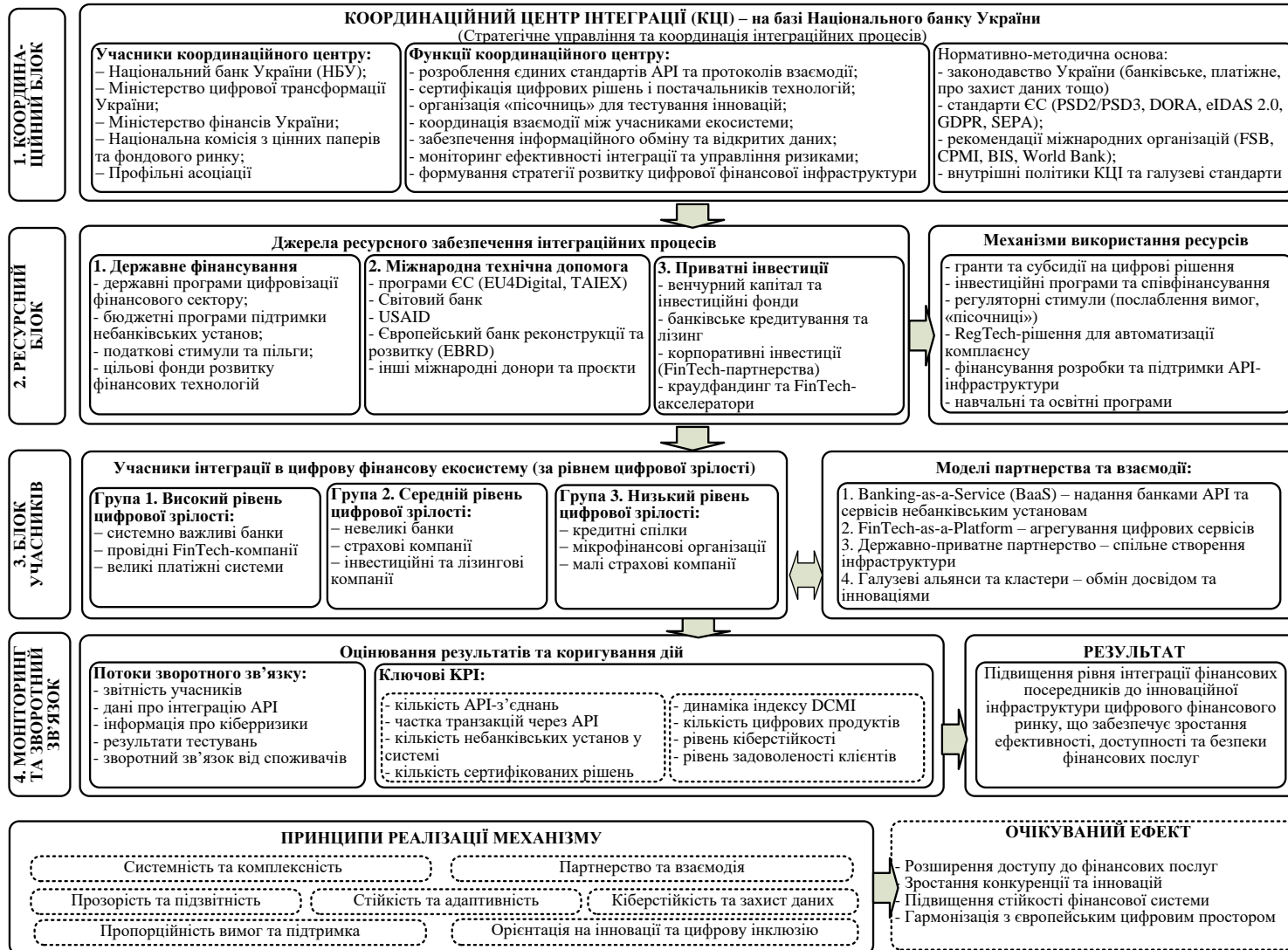


Рис. 3.3. Організаційно-економічний механізм інтеграції фінансових посередників до інноваційної структури цифрового фінансового ринку України

Джерело: розроблено автором на основі [69; 131; 112; 54; 65; 67; 68; 70; 71; 174; 227].

Його ключовою особливістю є поєднання ієрархічного принципу побудови з горизонтальними зв'язками партнерства, що дозволяє одночасно забезпечити керованість процесів і гнучкість взаємодії між учасниками.

Запропонований механізм базується на трьох основних блоках: координаційному, ресурсному та моніторинговому. Координаційний блок забезпечує стратегічне управління інтеграційними процесами, ресурсний – фінансове та матеріально-технічне забезпечення, моніторинговий – оцінювання результатів та зворотний зв'язок.

У межах **координаційного блоку** центральне місце посідає Координаційний центр інтеграції, функціонування якого спрямоване на зниження інституційної фрагментованості та формування єдиного середовища взаємодії. Важливо підкреслити, що його роль не обмежується адміністративною координацією: фактично він виконує функцію інституційного інтегратора, забезпечуючи узгодження стандартів, синхронізацію регуляторних вимог і формування довіри між учасниками ринку. Саме через цей блок реалізується перехід від дискретних ініціатив цифровізації до системного розвитку цифрової екосистеми.

Координаційний центр діє на базі Національного банку України за участі профільних асоціацій (Асоціації українських банків, Української асоціації фінтех та інноваційних компаній, Національної асоціації кредитних спілок тощо). До функцій координаційного центру належать: розроблення єдиних стандартів API, сертифікація цифрових рішень, організація регуляторних пісочниць, а також забезпечення інформаційного обміну між учасниками. Як свідчить міжнародний досвід, «роль координаційного центру може виконувати як центральний банк, так і спеціалізована агенція, однак ключовою умовою успіху є його незалежність та авторитет серед учасників ринку» [54].

Ресурсний блок охоплює три підсистеми: державне фінансування (бюджетні програми підтримки цифровізації небанківського сектору, податкові стимули), міжнародну технічну допомогу (гранти ЄС, Світового банку, USAID, EBRD), а також приватні інвестиції (венчурний капітал,

банківське кредитування фінтех-стартапів, краудфандинг). Кожна з підсистем має власні механізми розподілу коштів та звітності, що забезпечує прозорість використання ресурсів.

Блок учасників диференційовано за трьома групами. Перша група – установи з високим рівнем цифрової зрілості (системно важливі банки, найбільші фінтех-компанії) – виконують роль «якорів» екосистеми, надаючи інфраструктурні сервіси через API. Друга група – установи із середнім рівнем цифрової зрілості (невеликі банки, окремі страхові компанії) – є споживачами API-сервісів та учасниками спільних платформ. Третя група – установи з низьким рівнем цифрової зрілості (кредитні спілки, МФО, невеликі страхові компанії) – отримують пріоритетну підтримку в рамках описаних інструментів стимулювання.

Суттєвим доповненням до вертикальної структури є горизонтальний контур партнерських взаємодій, який відображає сучасну трансформацію фінансового посередництва від ізольованих моделей до екосистемних. Зокрема, моделі Banking-as-a-Service та FinTech-as-a-Platform демонструють зміну ролей учасників, коли банки дедалі частіше виступають як постачальники інфраструктури, а фінтех-компанії – як інтегратори клієнтських сервісів. У цьому контексті держава виконує функцію створення базових цифрових платформ, що забезпечують масштабованість таких взаємодій.

Окремої уваги заслуговує **блок моніторингу та зворотного зв'язку**, який забезпечує адаптивність механізму. Його функціонування базується на системі кількісних та якісних показників, що дозволяють оцінювати не лише ступінь інтеграції, але й ефективність використання ресурсів та динаміку цифрової зрілості учасників. Наявність зворотних зв'язків створює умови для своєчасного коригування інструментів підтримки та мінімізації ризиків неефективного розподілу ресурсів.

Таким чином, запропонований механізм слід розглядати як цілісну систему, у межах якої координаційні, ресурсні та операційні елементи взаємодіють на основі єдиної логіки розвитку. Його реалізація дозволяє не

лише прискорити інтеграцію фінансових посередників до цифрової інфраструктури, але й сформувати стійку модель функціонування фінансового ринку в умовах цифрової трансформації.

Враховуючи складний характер інтеграційних процесів, а також потребу в координації дій між різними категоріями учасників фінансового ринку, видається доцільним розглядати їх у логіці поступової, послідовної реалізації.

За такого підходу інтеграцію фінансових посередників до інноваційної інфраструктури цифрового ринку можна подати як багатоетапний процес. Він охоплює декілька взаємопов'язаних стадій – від початкового оцінювання готовності до подальшого масштабування та оптимізації. Кожна з цих стадій, своєю чергою, виконує певну функціональну роль, наближаючи фінансових посередників до цільового стану цифрової зрілості.

Формалізація зазначеної послідовності дозволяє, по-перше, забезпечити керованість процесу інтеграції; по-друге, мінімізувати ризики, пов'язані з фрагментарним упровадженням цифрових рішень. Запропоновану організаційно-економічну модель такого процесу наведено на рисунку 3.4.

Оцінювання рівня готовності фінансової установи є початковою стадією пропонованого процесу. Цей етап охоплює визначення цифрової зрілості, аналіз стану ІКТ-інфраструктури та ідентифікацію стратегічних орієнтирів подальшого розвитку. Після цього проводиться *технологічний аудит*, завданням якого виступає виявлення існуючих обмежень. Особливу увагу при цьому приділяють сфері кіберстійкості та відповідності чинним стандартам. На черговому етапі здійснюється *вибір моделі інтеграції*. Від цього вибору залежить формат подальшої взаємодії установи з іншими учасниками ринку. Можливі варіанти охоплюють використання API-рішень, застосування платформних моделей, а також реалізацію партнерських підходів.

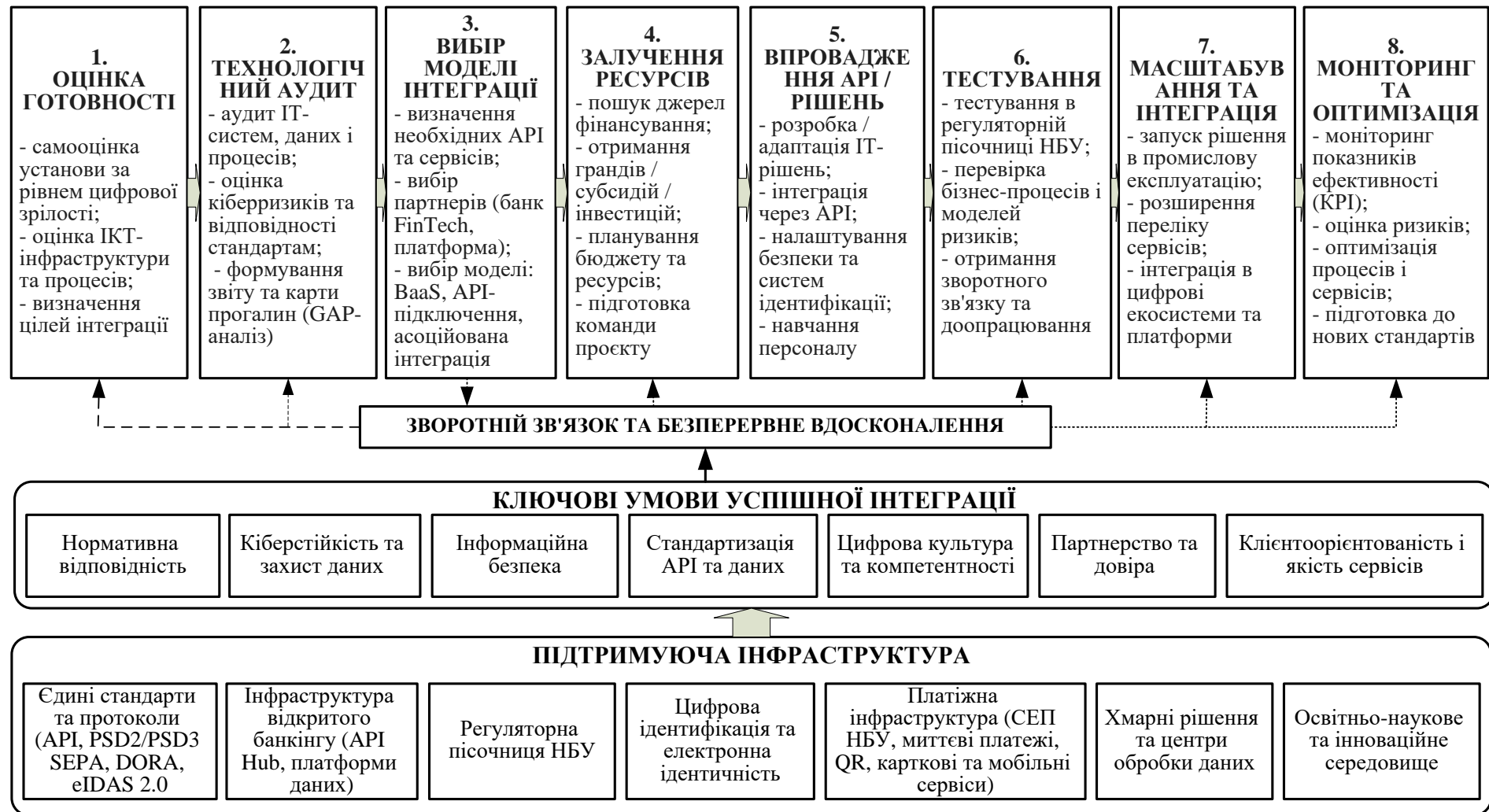


Рис. 3.4. Процес інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку України

Джерело: розроблено автором на основі [69; 54; 65; 67; 70; 112; 119; 128; 135; 174; 227].

Для реалізації обраної моделі необхідне належне ресурсне забезпечення, що охоплює фінансову, технологічну та кадрову складові. Сам етап впровадження передбачає *інтеграцію цифрових рішень* у бізнес-процеси установи, а також налаштування відповідних систем безпеки та ідентифікації.

Важливою складовою є *тестування* у регуляторному середовищі, яке дозволяє оцінити життєздатність обраних рішень і підтвердити їхню відповідність встановленим вимогам. На стадії *масштабування* відбувається розширення використання цифрових сервісів та їх інтеграція у ширші екосистеми.

Завершальним етапом виступає *моніторинг та оптимізація*, завданням яких є забезпечення безперервного вдосконалення процесів і своєчасної адаптації до змін зовнішнього середовища.

Відмінною рисою запропонованої моделі є наявність зворотних зв'язків, які забезпечують ітеративний характер процесу, дозволяючи коригувати окремі етапи залежно від отриманих проміжних результатів. Додатково у моделі визначено умови успішної інтеграції, а також елементи підтримуючої інфраструктури, що формують необхідне середовище для реалізації цифрових трансформацій.

Представлена послідовність етапів створює підґрунтя для визначення інструментів стимулювання інтеграційних процесів та формування системи їх оцінювання, що розглядається далі.

Процес інтеграції, представлений на рисунку 3.4, не може бути ефективно реалізований без належного інструментального забезпечення, яке формує середовище для впровадження цифрових рішень та адаптації фінансових посередників до нових умов функціонування. Враховуючи різний рівень цифрової зрілості учасників ринку, доцільним є диференційований підхід до застосування інструментів стимулювання. Відповідну класифікацію інструментів представлено в таблиці 3.3 та на рисунку 3.5.

Як видно з рисунка 3.5, інструменти стимулювання інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку доцільно групувати за трьома взаємодоповнюючими напрямками: фінансовим, регуляторним та організаційним. Така структуризація дозволяє врахувати як ресурсні обмеження учасників, так і інституційні умови їх функціонування.

Інструменти стимулювання інтеграції фінансових посередників

Інструмент	Цільова група	Очікуваний ефект
1. ФІНАНСОВІ ІНСТРУМЕНТИ		
Субсидії на технологічний аудит (до 50% вартості, але не більше 200 тис. грн)	Кредитні спілки, МФО	Підвищення обізнаності про цифрові вразливості
Грантова підтримка впровадження API-рішень (до 1 млн грн)	Страхові компанії, фінтех-стартапи	Прискорення інтеграції до відкритого банкінгу
Податкові канікули на прибуток від цифрових послуг (3 роки)	Нові FinTech-компанії	Стимулювання створення інноваційних продуктів
Пільгове кредитування цифрових проєктів	Банки, МФО, страхові компанії	Зниження вартості капіталу та підтримка інвестицій у цифровізацію
Фінансування навчання персоналу (гранти)	Працівники НФУ (небанківські установи)	Підвищення цифрових компетентностей та продуктивності
Венчурне фінансування фінтех-інновацій	Фінтех-компанії, стартапи	Розвиток інноваційної екосистеми та нових технологічних рішень
2. РЕГУЛЯТОРНІ ІНСТРУМЕНТИ		
Спрощена реєстрація ТРР (проти «повного ліцензування»)	Платіжні агрегатори, суперагрегатори	Зниження бар'єрів входу на ринок
Регуляторна пісочниця з пріоритетним доступом для небанківських установ	Кредитні спілки, страхові компанії	Тестування інновацій без ризику санкцій
Вимоги до кіберстійкості пропорційні розміру установи (DORA-light)	Малі та середні посередники	Зменшення навантаження на комплаєнс
Стандарти відкритого банкінгу	Усі фінансові посередники	Забезпечення сумісності та безпечного обміну даними
Пропорційний підхід у регулюванні та нагляді	НФУ різного розміру та ризикового профілю	Підвищення ефективності нагляду та відповідності ризикам
Сприяння цифровій ідентифікації та e-KYC)	Усі фінансові посередники	Покращення доступу клієнтів до цифрових послуг та зниження ризику шахрайства
3. ОРГАНІЗАЦІЙНІ ІНСТРУМЕНТИ		
Навчальні програми з цифрової грамотності персоналу	Працівники кредитних спілок, МФО	Підвищення кваліфікації кадрів
Створення спільних платформ API для небанківського сектору	Галузеві асоціації	Економія на масштабі
Консультаційна підтримка з імплементації DORA та стандартів безпеки	Малі страхові компанії, МФО, кредитні спілки	Прискорення адаптації до вимог та підвищення кіберстійкості
Формування галузевих хабів інновацій та обміну досвідом	Фінансові установи, фінтех-компанії,	Прискорення дифузії інновацій та кооперації учасників
Партнерські програми (BAAS-партнерства)	Банки, небанківські установи	Розширення доступу до інфраструктури та нових сервісів
Підтримка участі у міжнародних програмах та ініціативах	Фінансові установи, асоціації	Доступ до кращих практик, стандартів та міжнародних ринків

Джерело: розроблено автором на основі [3; 31; 51; 54; 65; 67; 70; 112; 119; 128; 131; 135; 174; 193; 227].



Рис. 3.5. Інструменти стимулювання інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку України

Джерело: розроблено автором на основі [2; 31; 51; 54; 65; 67; 70; 112; 119; 128; 131; 135; 174; 227].

Фінансові інструменти спрямовані передусім на подолання інвестиційних бар'єрів цифрової трансформації та включають грантове фінансування, субсидії, податкові стимули, а також механізми залучення приватного капіталу. Їх застосування є особливо важливим для малих і середніх фінансових посередників, які мають обмежені можливості самостійного фінансування цифрових проєктів.

Регуляторні інструменти сприяють формуванню сприятливого нормативного середовища. Це досягається через впровадження стандартів відкритого банкінгу, розвиток регуляторних пісочниць, спрощення процедур доступу до інфраструктури, а також встановлення вимог до кіберстійкості. Зазначені інструменти відіграють ключову роль у зниженні рівня невизначеності для учасників ринку та стимулюванні їхньої інноваційної активності.

Організаційні інструменти, своєю чергою, пов'язані з розвитком інституційної взаємодії. Вони охоплюють створення партнерських моделей, розбудову екосистем, підтримку професійних компетенцій, а також формування каналів для обміну знаннями. Головне призначення цих інструментів полягає в забезпеченні ефективної координації між учасниками ринку та прискоренні дифузії (поширення) інновацій.

Важливою особливістю представленої моделі є спрямування інструментів на різні групи фінансових посередників залежно від рівня їхньої цифрової зрілості, що дозволяє забезпечити пропорційність регуляторного впливу та підвищити ефективність використання ресурсів. У результаті формується комплексна система стимулювання, здатна підтримувати інтеграційні процеси на всіх етапах їх реалізації.

Найбільш проблемним сегментом з погляду цифрової інтеграції є небанківські фінансові посередники. Вибір конкретних інструментів стимулювання (табл. 3.3) базується на трьох критеріях: по-перше, врахування реальних обмежень небанківського сектору (брак фінансових ресурсів, низька цифрова компетентність персоналу, відсутність власних ІТ-підрозділів); по-друге, орієнтація на доведену ефективність у міжнародній практиці (аналогічні інструменти застосовувалися в ЄС, Великій Британії, Сінгапурі); по-третє, можливість швидкого впровадження в українських інституційних умовах.

Серед іншого, наведені в таблиці 3.3 інструменти враховують обмеженість ресурсів небанківського сектору, на яку звертають увагу дослідники: значна частина кредитних спілок, страхових компаній та мікрофінансових організацій не має ресурсів для повноцінної імплементації всіх вимог DORA у короткостроковій перспективі [174, с. 294]. Саме тому акцент робиться на пропорційності вимог та поетапному впровадженні.

Щодо обґрунтування вибору цільових груп, то вважаємо доцільним надати окремі пояснення.

Кредитні спілки та мікрофінансові організації (МФО) обрані пріоритетними отримувачами субсидій на технологічний аудит з огляду на їхню найбільшу вразливість до кіберзагроз при одночасному дефіциті власних ІТ-фахівців. За

даними НБУ, понад 60 % кредитних спілок не мають у штаті жодного спеціаліста з інформаційної безпеки, що робить їх «найслабшою ланкою» фінансової екосистеми. Грантова підтримка API-рішень адресується страховим компаніям та фінтех-стартапам, оскільки саме ці установи мають найбільший потенціал для генерації нових цифрових продуктів, але потребують початкового капіталу для розробки та інтеграції. Податкові канікули для нових FinTech-компаній спрямовані на стимулювання створення стартапів, які в подальшому можуть стати «якорями» регіональних цифрових екосистем.

Для кожного інструменту визначено вимірювальні результати. Субсидії на технологічний аудит мають на меті не лише виявлення вразливостей, але й формування культури безпеки в установах, які раніше не стикалися з регулярними перевірками. Грантова підтримка API-рішень оцінюється через кількість успішних API-інтеграцій та обсяг транзакцій, що пройшли через ці інтерфейси. Податкові канікули стимулюють створення компаній, які без такого стимулу могли б обрати інші юрисдикції для реєстрації. Регуляторна пісочниця вже довела свою ефективність у Великій Британії та Сінгапурі, де через неї пройшли сотні інноваційних продуктів, які згодом були масштабовані на весь ринок. «Пропорційні вимоги до кіберстійкості (DORA-light)» є критично важливими для збереження життєздатності малих установ: надмірно жорсткі вимоги можуть призвести до їх виходу з ринку, а не до підвищення безпеки.

Викладені вище інструменти стимулювання (табл. 3.3) утворюють необхідне, однак недостатнє підґрунтя для системної інтеграції. Самі по собі субсидії, гранти або спрощені регуляторні процедури ще не створюють стійкої конфігурації взаємодії між різними типами учасників ринку. Тут потрібна не ситуативна підтримка, а інституційно закріплена архітектура відносин, у межах якої банки, небанківські установи, фінтех-компанії та державні інституції діяли б не як окремі гравці, а як узгоджена екосистема. Саме на вирішення цього завдання спрямована третя складова пропонованого механізму – модель партнерства *«банки – небанківські посередники – фінтех – держава»*, яка фіксує розподіл функцій, зони відповідальності та потоки цінності між зазначеними групами стейкхолдерів (рис. 3.6).

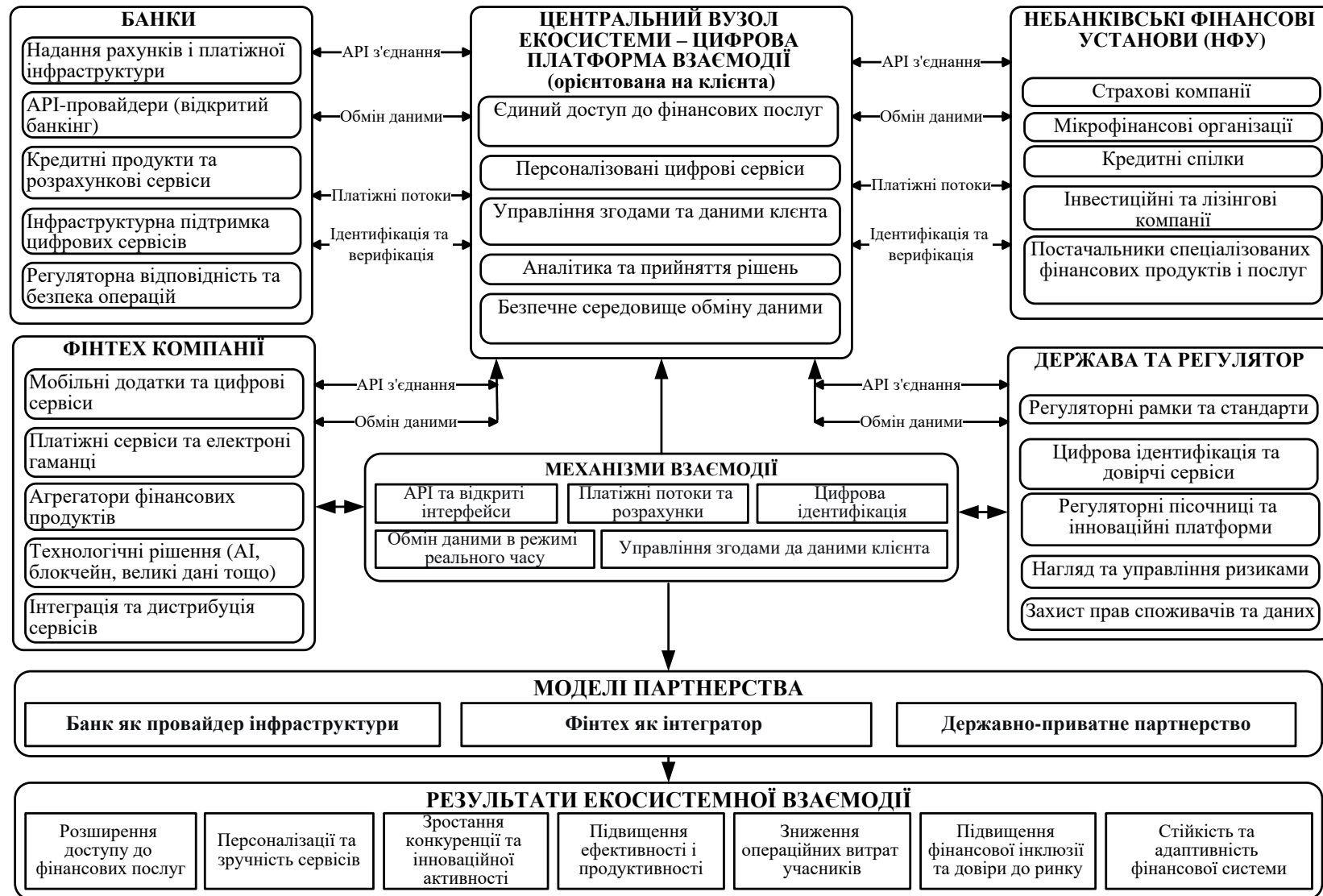


Рис. 3.6. Екосистемна модель партнерської взаємодії фінансових посередників у цифровому середовищі

Джерело: розроблено автором на основі [112; 54; 128; 67; 65; 174; 227; 166].

Як демонструє рисунок 3.6, сучасний фінансовий ринок поступово переходить до екосистемної моделі організації, у межах якої взаємодія між учасниками здійснюється на основі спільної цифрової інфраструктури. Ключовою ознакою такої моделі є орієнтація на потреби кінцевого користувача, навколо яких формуються цифрові платформи, сервіси та канали взаємодії. Саме клієнтський сегмент виступає центром інтеграції різних типів фінансових і технологічних рішень.

За умов цифрової трансформації змінюється і функціональна роль банківських установ. Поряд із традиційним посередництвом банки дедалі активніше виконують інфраструктурні функції, забезпечуючи доступ до рахунків, платіжних сервісів та інформаційних ресурсів через API-інтерфейси. Це створює передумови для інтеграції зовнішніх сервісів і розширення спектра цифрових продуктів.

Фінтех-компанії в такій системі переважно забезпечують технологічну гнучкість та швидкість впровадження інноваційних рішень. Їхня діяльність пов'язана з розробленням клієнтоорієнтованих сервісів, цифрових каналів обслуговування та платформних моделей взаємодії. Одночасно небанківські фінансові установи інтегруються до екосистеми як постачальники спеціалізованих послуг, що сприяє диверсифікації фінансового середовища та розширенню функціональних можливостей цифрових платформ.

Важливу роль у забезпеченні стабільності такої моделі відіграють державні інституції та регуляторні органи. Їх функції охоплюють формування нормативного середовища, розвиток механізмів цифрової ідентифікації, стандартизацію процедур обміну даними та здійснення нагляду за дотриманням вимог безпеки й кіберстійкості.

Практична реалізація екосистемної взаємодії базується на постійному обміні даними, використанні програмних інтерфейсів та інтеграції платіжних потоків між учасниками ринку. Це, на нашу думку, забезпечує масштабованість цифрових сервісів, прискорення обробки операцій та підвищення адаптивності фінансових установ до змін зовнішнього середовища. Пропонується декілька моделей партнерської взаємодії.

Перша модель – *банк як провайдер інфраструктури (Banking-as-a-Service, BaaS)*. За цією моделлю банк надає небанківським посередникам доступ до своїх платіжних, кредитних або депозитних послуг через API, дозволяючи їм створювати власні цифрові продукти без отримання банківської ліцензії. Як зазначає А. Дубас, «доступ до базових API надається безоплатно для стимулювання розвитку екосистеми, тоді як за додаткові комерційні послуги банки можуть встановлювати плату» [54]. Така модель є особливо релевантною для кредитних спілок, які можуть інтегрувати банківські платіжні сервіси без необхідності розробляти власну інфраструктуру.

Друга модель – *фінтех як інтегратор (FinTech-as-a-Platform)*. У цій моделі фінтех-компанія виступає координатором між банками та кінцевими споживачами, агрегуючи пропозиції різних фінансових установ та надаючи єдиний інтерфейс для клієнта. Прикладом є суперагрегатори, що дозволяють порівнювати кредитні пропозиції різних банків або страхових компаній. Як свідчить аналіз, «фінтех-компанії є більш гнучкими й більш схильними до ризику, ніж традиційні банки, тому вони стають каталізаторами проривних технологій у фінансовому секторі» [227, с. 318].

Третя модель – *державно-приватне партнерство*. У межах цієї моделі держава (в особі НБУ, Міністерства цифрової трансформації або інших органів) створює базову цифрову інфраструктуру (системи ідентифікації, реєстри, платіжні шлюзи), а приватні учасники розбудовують сервіси поверх неї. Найбільш яскравим прикладом є портал «Дія», який інтегрує BankID НБУ та відкриті API державних реєстрів, дозволяючи приватним компаніям використовувати цю інфраструктуру для своїх сервісів.

Зауважимо, що розвиток цих моделей сприяє перерозподілу функцій між учасниками ринку й формує нові механізми кооперації. У підсумку формується багаторівнева цифрова екосистема, здатна забезпечити підвищення доступності фінансових послуг, посилення конкурентного середовища та зростання ефективності функціонування фінансового ринку в умовах цифрової економіки.

Важливим компонентом пропонованого механізму є система моніторингу, яка дозволяє оцінювати прогрес інтеграції, виявляти вузькі місця та коригувати управлінські рішення. Основою для такого моніторингу є інтегральний показник цифрової зрілості (DCMI), розроблений у підрозділі 2.1, а також додаткові KPI, що відображають взаємодію між фінансовими посередниками різних типів (таблиця 3.4).

Таблиця 3.4

Ключові показники ефективності моніторингу інтеграції фінансових посередників до цифрової інфраструктури

Група показників	KPI	Формула / методика розрахунку	Періодичність	Цільове значення (2028)	Вага у СІ
1	2	3	4	5	6
Технологічні	Кількість активних API-з'єднань «банк – ТРР»	Кількість унікальних активних API-взаємодій	Щоквартально	> 500	0,08
	Частка API-транзакцій у загальному обсязі операцій	API-транзакції / загальний обсяг операцій	Щомісячно	> 30%	0,07
	Рівень автоматизації процесів	Автоматизовані процеси / загальна кількість процесів	Щорічно	> 70%	0,07
	Частка операцій у цифрових каналах	Кількість цифрових операцій / загальна кількість операцій	Щоквартально	> 65%	0,08
Організаційні	Частка установ із затвердженою цифровою стратегією	Кількість установ зі стратегією / загальна кількість установ	Щорічно	> 80%	0,06
	Частка персоналу з цифровими компетенціями	Кількість працівників із цифровими навичками / загальна чисельність персоналу	Піврічно	> 60%	0,06
	Частка установ, інтегрованих у цифрові платформи	Кількість інтегрованих установ / загальна кількість установ	Щоквартально	> 70%	0,07
	Кількість установ, що пройшли технологічний аудит	Абсолютне значення	Піврічно	> 200	0,06
Ринкові	Динаміка DCMI для небанківського сектору	За методикою підрозділу 2.1	Щорічно	+20%	0,08
	Частка клієнтів, що користуються цифровими каналами	Кількість активних цифрових користувачів / загальна кількість клієнтів	Щоквартально	> 75%	0,07

Закінчення таблиці 3.4

1	2	3	4	5	6
	Кількість нових цифрових продуктів	Абсолютне значення	Піврічно	> 50	0,05
	Темпи зростання цифрової клієнтської бази	Δ цифрових клієнтів / базове значення	Щорічно	> 15%	0,05
Кіберстійкість та безпека	Кількість зареєстрованих кіберінцидентів	Абсолютне значення	Щоквартально	↓ на 30%	0,07
	Частка установ, що відповідають DORA/ISO	Кількість установ, сертифікованих за стандартами / загальна кількість установ	Щорічно	> 70%	0,07
	Рівень виконання заходів з управління кіберризиками	Виконані заходи / заплановані заходи	Піврічно	> 85%	0,05
	Середній час реагування на інциденти	Середній час ліквідації інциденту	Щоквартально	< 4 год	0,04

Джерело: розроблено автором на основі [43; 44; 65-68; 131; 117; 112; 223].

Обґрунтуємо вибір показників моніторингу. Технологічні показники (кількість активних API-з'єднань, частка транзакцій через API) обрані тому, що вони безпосередньо відображають рівень інтеграції між банками та ТРР. Кількість API-з'єднань фіксує екстенсивний вимір інтеграції (скільки пар учасників налагодили взаємодію), тоді як частка транзакцій через API – інтенсивний (наскільки активно використовуються ці з'єднання). Перший показник важливий для оцінки потенціалу екосистеми, другий – для оцінки її реального використання.

Організаційні показники (кількість небанківських установ, що пройшли технологічний аудит, частка установ, що використовують спільні API-платформи) відображають рівень охоплення небанківського сектору інструментами підтримки. Як зазначалося вище, значна частина кредитних спілок не має власних ІТ-фахівців, тому проходження аудиту є першим кроком до усвідомлення власних вразливостей. Використання спільних API-платформ дозволяє невеликим установам отримати економію на масштабі (shared cost), що критично важливо для їхньої виживаності.

Ринкові показники (динаміка DСMІ для небанківського сектору, кількість нових цифрових продуктів) обрані для оцінки кінцевих результатів інтеграції. Зростання DСMІ свідчить про системне підвищення цифрової зрілості сектору, а кількість нових продуктів – про інноваційну активність.

Показники кіберстійкості та безпеки включено до системи моніторингу з огляду на зростання залежності фінансових посередників від цифрової інфраструктури та посилення кіберризиків у процесі інтеграції до цифрового фінансового середовища. Кількість зареєстрованих кіберінцидентів дозволяє оцінити фактичний рівень вразливості інформаційних систем і ефективність механізмів моніторингу загроз, тоді як частка установ, що відповідають вимогам DORA, ISO та іншим стандартам, характеризує ступінь адаптації сектору до сучасних регуляторних і безпекових вимог. Водночас рівень виконання заходів з управління кіберризиками відображає практичний стан реалізації політики інформаційної безпеки, а середній час реагування на інциденти — здатність установ забезпечувати безперервність цифрових сервісів та оперативне відновлення функціонування систем. У сукупності ці показники дають змогу комплексно оцінити рівень стійкості фінансових посередників до цифрових загроз та їхню готовність до функціонування в умовах розвитку відкритих фінансових екосистем.

Для забезпечення зіставності показників та можливості формування інтегральної оцінки запропоновані KPI доцільно піддавати попередній нормалізації. Це дозволяє привести різномірні показники до єдиної шкали та забезпечити коректність подальших розрахунків. Вагові коефіцієнти можуть визначатися експертним шляхом або на основі оцінювання впливу окремих груп показників на загальний рівень інтеграції фінансових посередників до цифрової інфраструктури.

Вагові коефіцієнти, наведені в таблиці 3.4, нами були сформовано на основі експертного підходу з урахуванням функціональної значущості окремих показників для забезпечення цифрової інтеграції фінансових посередників. Під час визначення ваг враховувалися ступінь впливу

відповідних КРІ на розвиток цифрової інфраструктури, інтенсивність міжсистемної взаємодії, рівень цифровізації операційних процесів, а також роль показників у забезпеченні кіберстійкості та безперервності фінансових сервісів. Вищі вагові значення надано індикаторам, які безпосередньо характеризують фактичний рівень цифрової взаємодії та масштаб використання цифрових каналів, тоді як допоміжні організаційні показники мають помірний вплив на формування інтегрального індексу.

Значення вагових коефіцієнтів у таблиці 3.4 відображають відносний вплив окремих показників на загальний рівень цифрової інтеграції фінансових посередників. Формування ваг здійснюється з урахуванням значущості відповідних КРІ для функціонування цифрової фінансової екосистеми, а також ступеня їхнього впливу на розвиток відкритого банкінгу, платформної взаємодії, цифрової інклюзії та кіберстійкості. Вищі вагові значення надано показникам, що безпосередньо характеризують інтенсивність цифрової взаємодії та рівень інтеграції установ до цифрової інфраструктури, зокрема API-взаємодії, цифровим операціям та показникам кіберстійкості. Натомість допоміжні організаційні індикатори мають дещо меншу вагу, оскільки переважно створюють передумови для цифрової трансформації, але не завжди прямо визначають рівень фактичної інтеграції.

Сума вагових коефіцієнтів (які були сформовано на основі експертного підходу з урахуванням функціональної значущості окремих показників для забезпечення цифрової інтеграції фінансових посередників) дорівнює одиниці, що забезпечує коректність розрахунку інтегрального показника та порівнянність отриманих результатів.

Сукупність запропонованих показників формує основу комплексної системи моніторингу цифрової інтеграції фінансових посередників. Для забезпечення узгодженості окремих індикаторів та можливості формування інтегральної оцінки доцільним є їх об'єднання в багаторівневу модель оцінювання, що охоплює технологічний, організаційний, ринковий та безпековий компоненти цифрової трансформації (рис. 3.7).

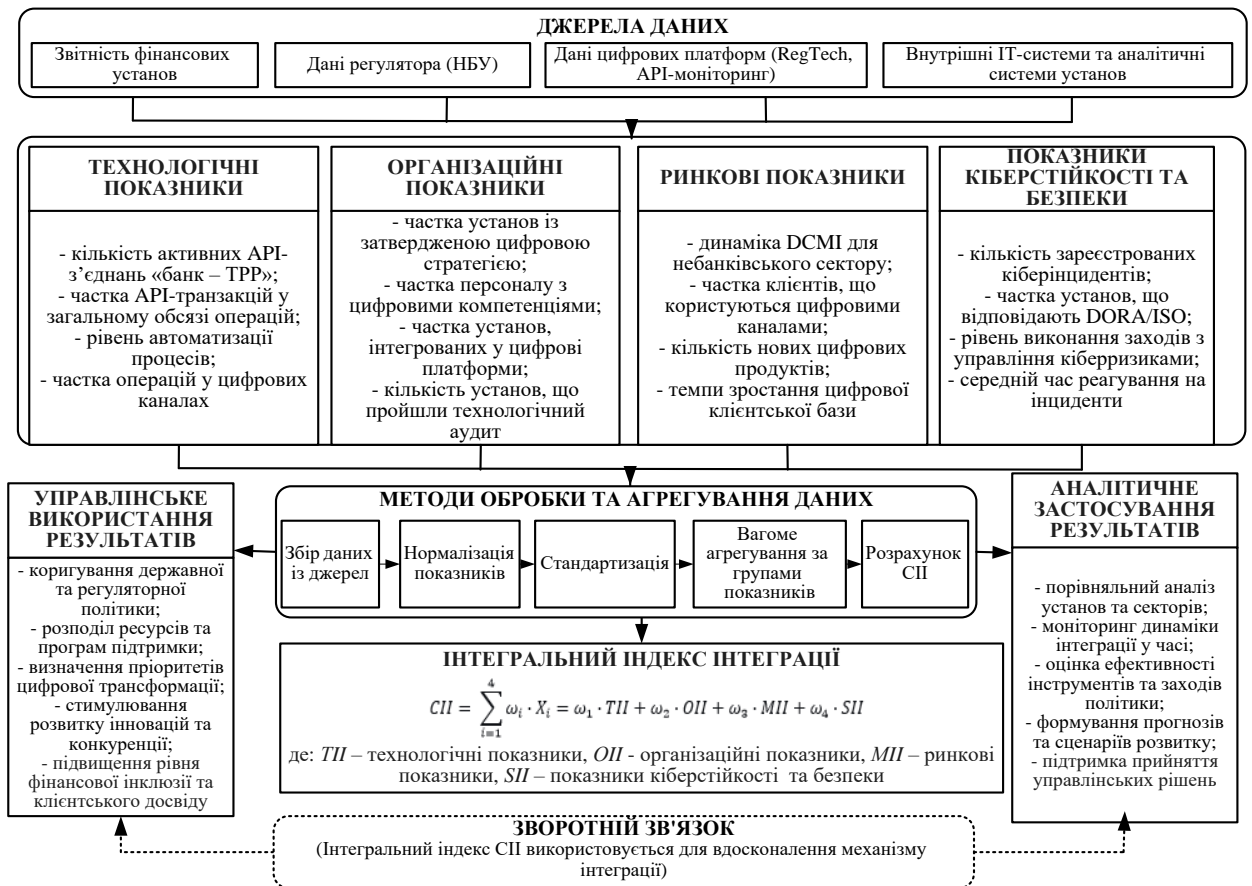


Рис. 3.7. Система моніторингу та оцінювання ефективності інтеграції фінансових посередників до цифрової інфраструктури

Джерело: розроблено автором на основі [2; 3; 31; 50; 51; 88; 105; 106; 108; 109; 174; 188; 227]

На відміну від показника DСMІ, який характеризує загальний рівень цифрової зрілості фінансової установи, інтегральний індекс СІІ орієнтований на оцінювання рівня інтеграції фінансових посередників до цифрової інфраструктури та інтенсивності їх екосистемної взаємодії. Це дозволяє використовувати запропоновану модель не лише для оцінювання внутрішньої цифрової трансформації установ, а і для аналізу рівня їх включення до відкритого цифрового фінансового середовища.

Пропонуємо використовувати наступну шкалу інтерпретації СІІ: низький рівень (0 - 0,25), базовий (0,26 – 0,5), середній (0,51-0,75), високий (0,76 – 1).

Як показано на рисунку 3.7, система моніторингу цифрової інтеграції фінансових посередників базується на поєднанні кількох груп показників, що характеризують різні аспекти цифрової трансформації. Запропонована модель передбачає послідовне накопичення даних, їх нормалізацію та агрегування з подальшим формуванням інтегрального індексу, який може використовуватися для оцінювання рівня цифрової зрілості установ, міжсекторального порівняння та моніторингу динаміки інтеграційних процесів.

Як агреговану оцінку, що поєднує вищеназвані характеристики діяльності фінансових посередників, пропонуємо розраховувати інтегральний показник цифрової інтеграції (СП). Його використання дозволяє перейти від аналізу окремих КРІ до комплексного оцінювання рівня цифрової інтеграції установ та ефективності їх адаптації до цифрового середовища. Формування СП ґрунтується на попередній нормалізації показників, визначенні вагових коефіцієнтів та подальшому агрегуванні часткових індексів у єдиний інтегральний індикатор. Такий підхід забезпечує зіставність результатів між різними групами фінансових посередників і створює основу для моніторингу динаміки цифрової трансформації у часовому розрізі.

Для формування цільових орієнтирів системи моніторингу доцільно враховувати фактичний рівень цифрової зрілості провідних учасників фінансового ринку. За результатами оцінювання, проведеного у підрозділі 2.3, інтегральний показник цифрової зрілості (DCMI) для АТ КБ «ПриватБанк» становить 2,76, що відповідає високому рівню цифрової інтеграції, тоді як для АТ «Ощадбанк» значення показника складає 2,12, що характеризує середній рівень цифрової трансформації. Виявлена диференціація свідчить про нерівномірність темпів цифрового розвитку навіть серед системно важливих банків та підтверджує необхідність застосування уніфікованих інструментів моніторингу.

Для небанківського сектору, де комплексне оцінювання цифрової зрілості поки що не набуло системного характеру, орієнтовний рівень DCMI може перебувати у межах 1,2–1,6, що відповідає базовому рівню цифрової

інтеграції. Це дає підстави розглядати цільове зростання показника на 20 % як реалістичний орієнтир для середньострокового періоду цифрової модернізації.

Для оцінювання динаміки цифрової інтеграції окремих установ може використовуватися індекс прогресу інтеграції (IPI):

$$IPI_i = \frac{DCMI_{i,t} - DCMI_{i,0}}{DCMI_{i,0}} \cdot 100\%,$$

де $DCMI_{i,t}$ – значення показника цифрової зрілості установи в поточному періоді; $DCMI_{i,0}$ – базове значення показника.

Застосування цього підходу дозволяє враховувати різну траєкторію цифрового розвитку фінансових установ. Так, для установ із високим рівнем цифрової зрілості подальше зростання показника, як правило, має помірний характер, тоді як для банків та небанківських установ із нижчим рівнем цифрової інтеграції потенціал приросту є суттєво вищим.

Для оцінювання рівня екосистемної взаємодії фінансових посередників може застосовуватися індекс екосистемної інтеграції (IEI):

$$IEI = \frac{\sum_{i=1}^n (API_i \cdot Volume_i)}{\sum_{i=1}^n Volume_i},$$

де API_i – кількість активних API-з'єднань установи, а $Volume_i$ – обсяг цифрових транзакцій відповідної установи.

Запропонований показник дозволяє оцінити не лише кількість інтеграційних зв'язків, а й інтенсивність їх практичного використання з урахуванням масштабу діяльності фінансових посередників. Це створює підґрунтя для порівняльного аналізу рівня інтеграції різних сегментів фінансового ринку та моніторингу ефективності реалізації цифрової трансформації у динаміці.

Реалізація запропонованого механізму пропонується в три етапи.

На першому етапі (2026–2027 роки) – *організаційно-підготовчому* – доцільно створити координаційний центр на базі НБУ, затвердити план заходів із підтримки небанківського сектору, провести пілотне тестування інструментів стимулювання в окремих регіонах (наприклад, у межах

регуляторної пісочниці). Важливим завданням є також розроблення методики технологічного аудиту для кредитних спілок та страхових компаній.

На другому етапі (2027–2029 роки) – *масштабування* – передбачається поширення інструментів підтримки на всі небанківські установи, запуск спільних API-платформ через галузеві асоціації, а також обов'язкове впровадження вимог до кіберстійкості (пропорційно до розміру установи). На цьому етапі особлива увага приділяється підвищенню кваліфікації персоналу через навчальні програми, що можуть фінансуватися за рахунок міжнародної технічної допомоги.

На третьому етапі (2029–2030 роки) – *стабілізаційному* – здійснюється моніторинг досягнутих результатів, коригування механізмів підтримки за потреби, а також повноцінна інтеграція небанківського сектору до загальної цифрової екосистеми. Як свідчить український досвід, «у фінансовому секторі дедалі частіше спрацьовує логіка, коли компанії створюють продукти, тестують їх на ринку, а держава формалізує успішний досвід у законодавстві» [67, с. 296].

Отже, запропонований організаційно-економічний механізм охоплює всі необхідні складові для ефективної інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку. Координаційний блок забезпечує стратегічне управління, ресурсний – необхідне фінансування та підтримку, а моніторинговий – оцінювання результатів та зворотний зв'язок. Запропоновані інструменти стимулювання враховують нерівномірність цифрового розвитку різних типів фінансових установ, а моделі партнерства створюють умови для взаємовигідного співробітництва банків, небанківських посередників, фінтех-компаній та держави. Подальшим кроком має стати деталізація процедур оцінювання ефективності впровадження цифрових рішень, що розглядатиметься в підрозділі 3.3.

3.3. Науково-практичні рекомендації щодо реалізації стратегії кіберстійкості та оцінка ефективності впровадження цифрових рішень у діяльність фінансових посередників

Попередні розділи роботи засвідчили: цифрова трансформація фінансового сектору супроводжується якісною зміною структури ризиків. Якщо в епоху традиційного банкінгу домінували кредитні та ринкові загрози, то сьогодні на перший план виходять операційні та технологічні ризики, здатні паралізувати діяльність установи за лічені хвилини. У підрозділі 3.1 обґрунтовано необхідність імплементації європейських стандартів операційної стійкості (DORA) в українське регуляторне поле, а в підрозділі 3.2 запропоновано організаційно-економічний механізм інтеграції фінансових посередників. Проте жоден з цих інструментів не спрацює належним чином, якщо на рівні окремої установи відсутня чітка, документально закріплена та регулярно оновлювана стратегія кіберстійкості.

Сучасна кіберстійкість давно вийшла за межі компетенції виключно ІТ-департаменту. Вона стала стратегічним пріоритетом правління та наглядової ради, оскільки будь-який масштабний інцидент здатен не лише завдати прямих фінансових збитків, але й безповоротно підірвати довіру клієнтів – ключовий нематеріальний актив фінансового посередника. Як зазначалося в авторському дослідженні, присвяченому етичним викликам цифровізації, «цифрова довіра є етико-технологічним ресурсом, який включає прозорість алгоритмів, коректність обробки даних, відповідальність за алгоритмічні рішення, цифрову ідентифікацію клієнтів, кіберстійкість» [154, с. 91]. Саме тому подальші рекомендації будуються на переконанні, що кіберстійкість має бути вбудованою в усі рівні управління – від затвердження політик до щоденних операційних процедур.

Будь-яка стратегія кіберстійкості має відповідати двом, на перший погляд, суперечливим вимогам. З одного боку – бути достатньо детальною, щоб охопити всі критичні сфери (ідентифікація активів, захист, виявлення,

реагування, відновлення). З іншого – не перетворюватися на надто громіздкий документ, який неможливо впровадити в практику через надмірну складність. Для фінансових посередників України, особливо для небанківського сектору з обмеженими ресурсами, важливо дотримуватися принципу пропорційності: системно важливі банки мають впроваджувати повний спектр вимог DORA, тоді як малі кредитні спілки чи невеликі страхові компанії можуть обмежитися базовим набором заходів (так званий підхід «DORA-light»).

На основі аналізу міжнародних рамок – NIST Cybersecurity Framework (версія 2.0, 2024), стандартів ISO/IEC 27001:2022, а також вимог Регламенту DORA (статті 5–16 щодо управління ІКТ-ризиками) – запропоновано типову структуру стратегії кіберстійкості, яка складається з семи взаємопов’язаних розділів (табл. 3.5). Кожен розділ стратегії містить стислий зміст, зазначення відповідальної посади або підрозділу, а також рекомендовану періодичність перегляду. Вважаємо, що такий підхід дозволить фінансовим посередникам до мінливих умов макро-, мезо- і мікросередовища.

Таблиця 3.5

Типова структура стратегії кіберстійкості фінансового посередника

Розділ стратегії	Стислий зміст	Відповідальна особа / підрозділ	Періодичність перегляду
1	2	3	4
1. Політики та організаційна структура	– Затвердження стратегії правлінням; призначення CISO (Chief Information Security Officer); – розподіл відповідальності за ІКТ-ризик; – створення комітету з кібербезпеки	Правління, CISO	Щорічно або після суттєвих змін
2. Ідентифікація та класифікація активів	– Інвентаризація ІКТ-активів (апаратне забезпечення, ПЗ, дані); – визначення критичності активів для бізнес-процесів; – оцінка залежності від третіх провайдерів	Відділ IT, CISO	Щопіврічно або після змін в інфраструктурі
3. Управління ризиками	– Регулярна оцінка кіберризиків (за методологією NIST або ISO 31000); – визначення ризик-апетиту; – сценарне моделювання атак; – планування заходів зниження ризиків	CISO, ризик менеджмент	Щоквартально – оновлення реєстру ризиків

Закінчення таблиці 3.5

1	2	3	4
4. Захисні заходи (технічні та організаційні)	<ul style="list-style-type: none"> – Управління доступом (MFA, least privilege); захист периметра (firewalls, IDS/IPS); захист кінцевих пристроїв (EDR); – шифрування даних; – резервне копіювання (3-2-1 правило); – управління вразливостями (patch management) 	Відділ IT, SOC	Постійно (технічні заходи оновлюються безперервно)
5. Виявлення та моніторинг	<ul style="list-style-type: none"> – Впровадження SIEM/SOAR; моніторинг у реальному часі (24/7); – поведінкова аналітика; – збір, аналіз та інтерпретація інформації про поточні або потенційні кіберзагрози; – регулярне сканування вразливостей 	SOC, CISO	Щомісячно – перевірка працездатності систем моніторингу
6. Реагування на інциденти	<ul style="list-style-type: none"> – План реагування на інциденти; – визначення ролей у команді, яка виявляє, обробляє та реагує на кіберінциденти (CSIRT); – процедури ескалації; комунікаційний план (внутрішній та зовнішній); звітування до регулятора (відповідно до DORA) 	CSIRT, CISO, Комплаєнс	Щопіврічно – тренування
7. Відновлення після інцидентів	<ul style="list-style-type: none"> – План безперервності бізнесу (BCP) та відновлення після аварій (DRP); – резервні потужності – регулярне тестування планів відновлення; – уроки з інцидентів 	Відділ IT, BCM-менеджер	Щорічно – тестування BCP/DRP

Джерело: розроблено автором на основі [12; 48; 89; 106; 51; 131; 69; 174; 227; 169].

Представлена в таблиці 3.5 структура не є догмою. Для невеликих фінансових установ (кредитні спілки, невеликі страхові компанії) окремі розділи можуть бути об'єднані або спрощені, однак ключові елементи – політики, управління ризиками, моніторинг та реагування – мають бути присутніми в будь-якому разі. Важливо також наголосити: перегляд стратегії має відбуватися не формально, а за наслідками реальних подій – після суттєвих змін в інфраструктурі, після великих інцидентів (власних або в інших установах), після змін регуляторних вимог.

Ключовим елементом, який часто випадає з поля зору при розробці подібних стратегій, є розділ 6 – реагування на інциденти. Як свідчить практика, більшість установ мають технічні засоби захисту, але не мають чітко

прописаних процедур комунікації: хто, коли, у якій формі повідомляє клієнтів, регулятора, правоохоронні органи. Авторське дослідження, присвячене аналізу кіберзагроз, підтверджує, що «...саме людський фактор, а не технічні вади, найчастіше стає причиною успішної реалізації атаки» [224, с. 259]. Тому план реагування має передбачати не лише технічні кроки (ізоляцію систем, збір доказів), але й комунікаційну стратегію.

Попередній аналіз (підрозділ 1.3) дозволив ідентифікувати вісім типів кіберзагроз, які становлять найбільшу небезпеку для фінансових посередників в Україні: фішинг, рансомвер, DDoS-атаки, атаки на API, інсайдерські загрози, мобільні загрози, кібершпигунство та витоки даних. Кожна з цих загроз потребує не універсальної, а специфічної комбінації технічних та організаційних заходів. При цьому важливо враховувати, що ідеального захисту не існує: мета полягає не в тому, щоб унеможливити будь-яку атаку, а в тому, щоб зробити її проведення достатньо складним, витратним і швидко виявлюваним.

Проведена нами систематизація заходів протидії за п'ятьма вимірами – технічні засоби, організаційні процедури, людський фактор, моніторинг та реагування, а також специфіка для небанківського сектору – дозволяє уникнути фрагментарного підходу, коли установа впроваджує окремі рішення (наприклад, антифішинговий фільтр), але ігнорує суміжні вразливості. Зауважимо, що запропонована у таблиці 3.6. матриця заходів враховує рекомендації ENISA (2024), Базельського комітету (2018), а також вимоги DORA щодо управління ІКТ-ризиками [27; 59; 69].

Запропонована матриця охоплює ті типи інцидентів, які за статистикою 2024–2025 років становлять понад 80 % зареєстрованих випадків в українському фінансовому секторі. Серед ключових тенденцій – зростання атак на API у зв'язку із запуском відкритого банкінгу в Україні (серпень 2025 року): що більше інтерфейсів відкриває установа, то ширшою стає її поверхня атаки, отже, тестування на проникнення для активних учасників API-екосистем має бути не щорічним, а безперервним. Окрему увагу потребує небанківський сектор – кредитні спілки, МФО та невеликі страхові компанії здебільшого не мають ресурсів для повномасштабного впровадження технічних заходів, перелічених у таблиці 3.5.

Матриця заходів протидії кіберзагрозам для фінансових посередників

Тип загрози	Технічні заходи	Організаційні заходи	Особливості для небанківського сектору
Фішинг та соціальна інженерія	<ul style="list-style-type: none"> – Антифішингові фільтри (DMARC, DKIM, SPF); – MFA для всіх критичних систем; – захист електронної пошти 	<ul style="list-style-type: none"> – Регулярні тренінги персоналу (не рідше 1 разу на півроку); – симуляції фішингових атак; – процедура повідомлення про підозрілі листи 	Для МФО та кредитних спілок – базові тренінги за стандартизованими сценаріями (через галузеві асоціації)
Ransomware (програми-вимагачі)	<ul style="list-style-type: none"> – Резервне копіювання за правилом 3-2-1 (3 копії, 2 носії, 1 офлайн); – сегментація мережі; – EDR на кінцевих пристроях; – принцип найменших привілеїв 	<ul style="list-style-type: none"> – План відновлення (тестування не рідше 1 разу на рік); заборона викупу (корпоративна політика); страхування кіберризиків 	Використання хмарних резервних копій (як більш доступної альтернативи власному дата-центру)
DDoS-атаки	<ul style="list-style-type: none"> – Митигатори (Cloudflare, Akamai або локальні рішення); – резервні канали зв'язку; – географічно розподілена інфраструктура 	<ul style="list-style-type: none"> – Угоди з інтернет-провайдерами про спільне реагування; план комунікації з клієнтами під час атаки 	Для невеликих установ – використання митигаційних сервісів сторонніх провайдерів (SaaS)
API-загрози (відкритий банкінг)	<ul style="list-style-type: none"> – Валідація вхідних даних; – rate limiting; – автентифікація OAuth 2.0 / OpenID Connect; – шифрування каналів (TLS 1.3); – регулярне тестування API на проникнення 	<ul style="list-style-type: none"> – Управління життєвим циклом API (API governance); реєстрація всіх сторонніх TPP; моніторинг аномалій у поведінці API 	Спрощені вимоги для TPP з низьким обсягом транзакцій (диференціація за ризиком)
Інсайдерські загрози	<ul style="list-style-type: none"> – DLP-системи; – контроль доступу на основі ролей (RBAC); – моніторинг привілейованих користувачів; – захист від витоку через зовнішні носії 	<ul style="list-style-type: none"> – Розподіл обов'язків; – exit-процедури (блокування доступів при звільненні); – анонімний канал повідомлень про порушення 	Психологічний клімат та моніторинг «вигорання» (оскільки інсайдером часто стає не зловмисник, а втомлений працівник)
Мобільні загрози	<ul style="list-style-type: none"> – Захист мобільних застосунків; – безпечне зберігання токенів; – біометрична автентифікація 	<ul style="list-style-type: none"> – Політика «використовуй власний пристрій» (BYOD) або «у власності компанії»; – регулярне оновлення мобільних застосунків 	Для установ без власної мобільної розробки – використання стандартних платіжних додатків з мінімальними налаштуваннями безпеки

Джерело: розроблено автором на основі [28; 51; 59; 131; 69; 195; 224].

Пріоритетом для таких установ має стати базова гігієна: своєчасне оновлення програмного забезпечення, резервне копіювання, багатofакторна автентифікація для адміністраторів. До цього додаються участь у спільних платформах (наприклад, хмарне резервування через галузеві об'єднання) та страхування кіберризиків як спосіб перенесення фінансових наслідків. Як наголошувалося в дослідженні з аналізу кіберзагроз, навіть обмеженість ресурсів не виправдовує відсутності мінімального набору захисних дій – саме слабка захищеність робить малі установи привабливою мішенню [224, с. 259].

Водночас технічні рішення без належної організаційної підтримки втрачають сенс. Найпотужніша система контролю даних не стримає порушника там, де не сформовано культуру безпеки, а персонал не усвідомлює причин обмежень доступу. Отже, поряд із впровадженням технологічних засобів необхідно системно навчати працівників і регулярно перевіряти їхню готовність через імітацію інцидентів.

Наявність формально затвердженого документа (табл. 3.5) та розуміння того, які технічні заходи необхідно впровадити (табл. 3.6), ще не гарантують досягнення належного рівня кіберстійкості. Ключовим є послідовний, керований і документований процес переходу від поточного стану до цільового. Саме тут більшість фінансових установ припускаються типових помилок: намагаються впровадити всі заходи одночасно, не визначаючи пріоритетів; ігнорують фазу самооцінки, одразу переходячи до закупівлі дорогого обладнання; не створюють зворотних зв'язків між етапами, через що вже реалізовані заходи перестають відповідати зміненним умовам.

Пропонований нижче алгоритм (рис. 3.8) базується на методології NIST Cybersecurity Framework (функції Identify → Protect → Detect → Respond → Recover, інтегровані в цикл постійного вдосконалення), а також на вимогах DORA щодо регулярного тестування операційної стійкості [106; 69]. Він складається з шести кроків, кожен із яких має чіткі вхідні та вихідні умови, а також механізм зворотного зв'язку, що дозволяє повертатися на попередні етапи при зміні середовища загроз.

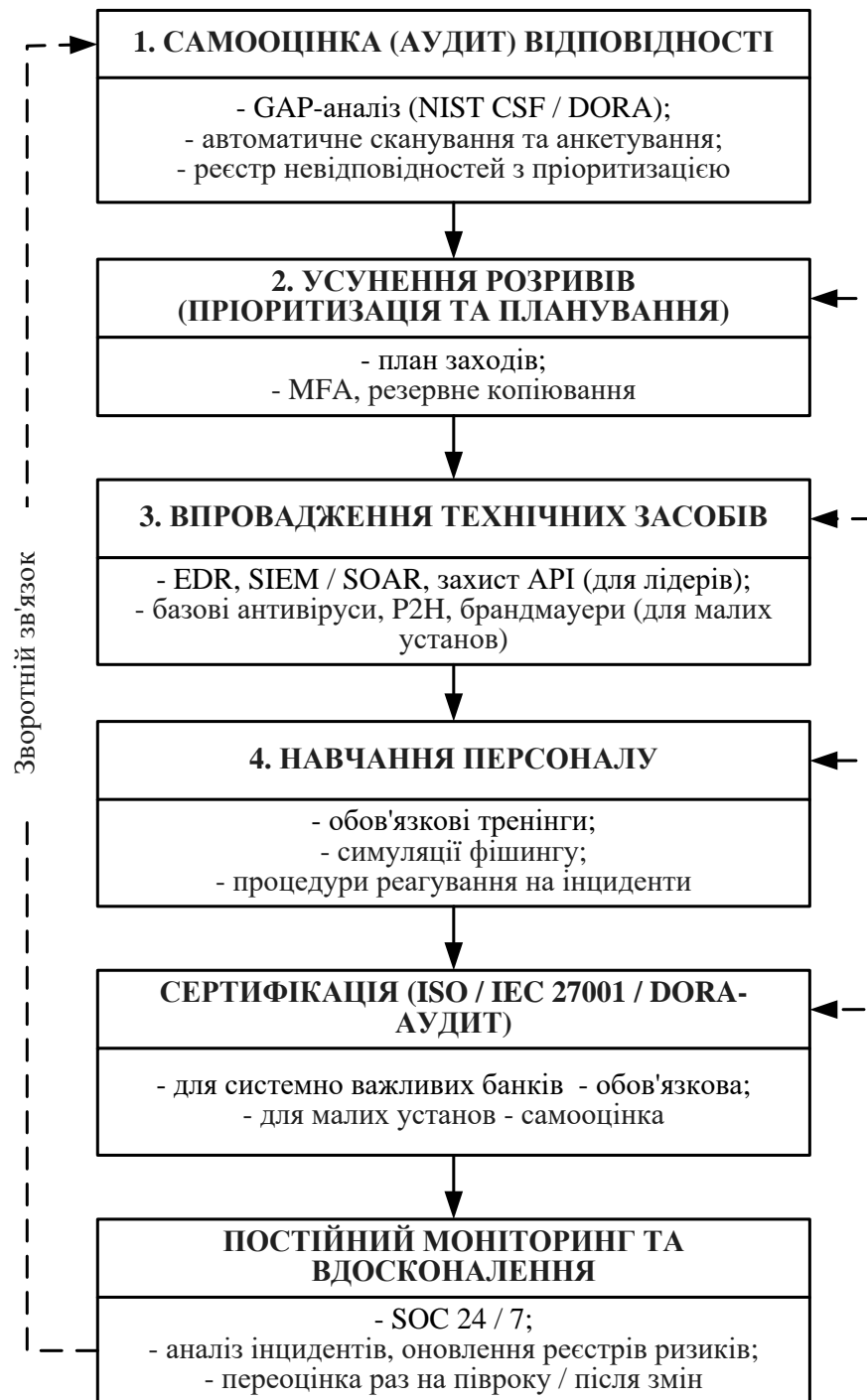


Рис. 3.8. Алгоритм впровадження стратегії кіберстійкості фінансового посередника

Джерело: розроблено автором на основі [59; 131; 69; 231; 30].

Алгоритм розпочинається з самооцінки (GAP-аналіз чинних заходів відносно NIST CSF або DORA), результатом якої стає реєстр невідповідностей, пріоритетизований за рівнем ризику. Для небанківського сектору доцільно використовувати спрощені чек-листи галузових асоціацій.

На основі реєстру формують план усунення розривів (критичні вразливості – першочергово) із включенням «швидких перемог» на кшталт багатофакторної автентифікації для адміністраторів. Технічні засоби впроваджують поетапно, застосовуючи пілотний підхід: для лідерів ринку – EDR, SIEM/SOAR, захист API; для невеликих установ – базові антивіруси, оновлення ПЗ, брандмауери. Паралельно (або з невеликим випередженням) проводять обов'язкові тренінги персоналу з симуляціями фішингу та процедурами реагування на інциденти. Сертифікація за ISO 27001 рекомендована для системно важливих банків та установ, що виходять на міжнародні ринки; для малих небанківських організацій її може замінити стандартизована самооцінка.

Завершальний етап – безперервний моніторинг (SOC 24/7, аналіз інцидентів, оновлення реєстрів ризиків) із піврічним циклом переоцінки (повернення до кроку 1), що утворює замкнений контур постійного вдосконалення. Пунктирні зворотні зв'язки на рис. 3.4 фіксують також корекцію плану усунення розривів за результатами впровадження технічних засобів, навчання та сертифікації – саме ці нелінійні зв'язки відрізняють запропонований алгоритм від лінійних «кращих практик». Послідовність не є жорсткою (навчання може випереджати технічне впровадження), однак порушення логіки, наприклад, щодо старту сертифікації без усунення критичних розривів призводить до нераціонального використання ресурсів. Зауважимо, що українські банки вже апробували окремі елементи цього підходу (наприклад, резервні потужності POWER BANKING), проте системне впровадження з документованими зворотними зв'язками поки лишається радше винятком.

Жодна стратегія цифрової трансформації не може вважатися завершеною без системи вимірювання її результатів. Інвестиції в цифрові технології – від розробки мобільних застосунків до впровадження AI-скорингу – потребують обґрунтування перед акціонерами, наглядовою радою та регулятором. Однак практика свідчить, що більшість фінансових установ обмежується технічними метриками (наприклад, час безвідмовної роботи системи), ігноруючи економічний та клієнтський виміри ефективності. Пропонована нижче система показників (табл. 3.7) охоплює чотири групи KPI

– фінансові, операційні, ризикові та клієнтські – що дозволяє оцінити цифрові рішення комплексно, уникаючи як «цифрового імперіалізму» (інвестиції заради інвестицій), так і надмірного консерватизму (нехтування довгостроковими вигодами через страх початкових витрат).

Таблиця 3.7

Система показників ефективності впровадження цифрових рішень

Група КРІ	Конкретний показник	Методика розрахунку	Періодичність	Бенчмарк / цільове значення
1	2	3	4	5
Фінансові	ROI цифрового проєкту	$\frac{\text{Приріст доходу} + \text{Зниження витрат}}{\text{Вартість впровадження}} \times 100\%$	Після завершення проєкту, потім щорічно	> 15 % для банків, > 10 % для небанківських установ
	Зниження операційних витрат (після автоматизації)	$\frac{\text{Витрати до автоматизації} - \text{Витрати після}}{\text{Витрати до}} \times 100\%$	Щоквартально для пілотного періоду (перші 6 міс), потім щорічно	> 20 % для масових операцій (платежі, KYC)
	Приріст доходів від цифрових каналів	$\frac{\text{Доходи цифрових каналів (t)} - \text{Доходи цифрових каналів (t-1)}}{\text{Доходи загальні (t-1)}} \times 100\%$	Щомісячно	> 5 % річного приросту
Операційні	Скорочення часу обробки транзакції	$\frac{\text{Час до цифровізації} - \text{Час після}}{\text{Час до}} \times 100\%$	Один раз (після впровадження)	> 70 % для платежів, > 50 % для кредитних заявок
	Збільшення частки цифрових каналів	$\frac{\text{Обсяг транзакцій через цифрові канали}}{\text{Загальний обсяг транзакцій}} \times 100\%$	Щомісячно	> 90 % для банків, > 50 % для небанків (згідно з трендом)
	Зменшення кількості ручних помилок	$\frac{\text{Кількість помилок до} - \text{Кількість помилок після}}{\text{Кількість помилок до}} \times 100\%$	Щоквартально	> 80 % для регламентованих процесів
Ризикові	Зниження частоти кіберінцидентів	$\frac{\text{Кількість інцидентів (t-1)} - \text{Кількість (t)}}{\text{Кількість (t-1)}} \times 100\%$	Щомісячно	Щорічне зниження > 10 % (з урахуванням зростання кількості атак)
	Скорочення MTTR (Mean Time To Recover)	Сумарний час простою / Кількість інцидентів	Після кожного інциденту, узагальнення щоквартально	< 4 годин для критичних систем, < 24 годин для некритичних
	Зменшення втрат від шахрайства (фрод)	$\frac{\text{Втрати (t-1)} - \text{Втрати (t)}}{\text{Втрати (t-1)}} \times 100\%$	Щомісячно	> 15 % річного зниження

Закінчення таблиці 3.7

1	2	3	4	5
Клієнтські	NPS (Net Promoter Score) цифрових каналів	Частка промоутерів (%) – Частка критиків (%)	Щоквартально (опитування)	> 50 (для цифрових банків), > 30 (для традиційних)
	Частка активних цифрових клієнтів	Кількість клієнтів, які здійснили хоча б одну транзакцію в цифровому каналі за період / Загальна кількість клієнтів $\times 100 \%$	Щомісячно	> 70 % для банків, > 30 % для небанків

Джерело: розроблено автором на основі [59; 95; 131; 174; 191; 227; 231] та даних підрозділу 2.3.

Використовуючи показники зведені в таблиці 3.7, здійснено ілюстративні розрахунки для АТ КБ «ПриватБанк» і АТ «Ощадбанк».

АТ КБ «ПриватБанк». На основі публічної звітності та даних, наведених у підрозділі 2.3 (DCMI = 2,76, частка цифрових клієнтів 74%, частка безготівкових операцій за кількістю 94,5 % у 2024 році), можна оцінити окремі показники з таблиці 3.7. Частка цифрових каналів за обсягом транзакцій у АТ КБ «ПриватБанк» перевищує 90 %, тобто цільове значення досягнуто. За показником NPS, згідно з опитуваннями незалежних агрегаторів, Приват24 стабільно отримує 55 – 60 балів, що перевищує бенчмарк для цифрових банків (>50). Водночас показник MTTR для критичних систем (наприклад, відновлення після DDoS-атак) не публікується. Проте за непрямыми даними (наявність власного SOC, участь у мережі POWER BANKING) можна припустити його відповідність вимогам DORA, що становить менше як 4 годин. Розрахунок ROI для окремого цифрового проєкту (наприклад, запуску PrivatPay) вимагає внутрішньої даних, однак загальна динаміка зростання доходів від комісій (19,7 млрд грн у 2024 році) свідчить про позитивну віддачу.

АТ «Ощадбанк». Для Ощадбанку (DCMI = 2,12, цифрові клієнти – 4,6 млн, зростання транзакцій у 2024 році +15 % за кількістю та +23 % за сумою) цільові значення з таблиці 3.7 є більш напруженими. Частка цифрових каналів за обсягом поки що нижча за бенчмарк (оціночно 60–70 %), що обґрунтовує

пріоритет міграції клієнтів у цифрові канали як ключовий напрям підвищення цифрової зрілості. NPS для Mobile Oschad за даними закритих опитувань становить 35–40 балів, що відповідає бенчмарку для традиційних банків (>30), але поступається лідерам ринку. Позитивною є динаміка скорочення втрат від шахрайства. Зокрема, за даними офіційного сайту АТ «Ощадбанк» запровадження OschadPAY (каса в смартфоні) дозволило знизити фрод при безготівкових розрахунках на оціночні 12–15 % за 2024 рік. Розрахований за наведеною формулою показник зниження частоти кіберінцидентів (оціночно – 8–10 % річних) наближається до цільового значення (10 %), однак потребує покращення для досягнення сталої щорічної динаміки.

Особливу увагу слід звернути на показник MTTR (середній час відновлення). В умовах воєнних дій та частих відключень електроенергії українські банки досягли значного прогресу: участь у мережі POWER BANKING дозволила скоротити час відновлення після знеструмлень з кількох днів до кількох годин. Однак формалізованого вимірювання MTTR для кіберінцидентів (на відміну від технічних збоїв) в публічній звітності немає, що є недоліком, який доцільно усунути шляхом внесення відповідних вимог до звітності НБУ.

Водночас запропонована система показників не є статичною. Для установ з різним рівнем цифрової зрілості пріоритетність KPI має бути різною. Так, для банків лідерського рівня (АТ КБ «ПриватБанк») акцент доцільно змістити з екстенсивних показників (частка цифрових клієнтів – вже висока) на інтенсивні (NPS, MTTR, зниження фроду). Для установ середнього рівня (АТ «Ощадбанк») ключовим залишається нарощування частки цифрових каналів та підвищення задоволеності клієнтів. Для небанківського сектору на перших етапах доцільно обмежитись кількома базовими показниками (частка цифрових операцій, динаміка кіберінцидентів), поступово розширюючи їх перелік у міру зростання цифрової зрілості. Такий диференційований підхід дозволяє уникнути надмірного звітного навантаження на малі установи, водночас забезпечуючи можливість порівняльного аналізу в межах фінансового сектору.

Далі вважаємо доцільними акцентувати увагу на наших рекомендаціях щодо формування культури кібербезпеки та підвищення цифрової грамотності клієнтів.

Технічні засоби захисту, описані в таблиці 3.6, та алгоритм впровадження стратегії (рис. 3.8) створюють необхідну, однак недостатню основу для довгострокової кіберстійкості. Навіть найдосконаліші системи виявлення вторгнень та шифрування даних виявляються майже марними, якщо пересічний співробітник за власною необережністю (або через брак обізнаності) натискає на підозріле посилання, а клієнт добровільно повідомляє шахраям одноразовий пароль із SMS. Як зазначалося в авторському дослідженні, присвяченому етичним вимірам цифровізації, «цифрова довіра є етико-технологічним ресурсом, який включає прозорість алгоритмів, коректність обробки даних, відповідальність за алгоритмічні рішення» [154, с. 91]. Цю тезу варто розгорнути далі: довіра формується не лише через надійні технології, але й через усвідомлену поведінку всіх учасників фінансової екосистеми – від топ-менеджменту до клієнта, який користується мобільним застосунком. У цьому зв'язку особливої актуальності набуває формування культури кібербезпеки усередині установи та підвищення цифрової грамотності клієнтів.

Культура кібербезпеки всередині установи. Під «культурою кібербезпеки» будемо розуміти не набір інструкцій, які співробітники зобов'язані підписати при прийомі на роботу, а систему цінностей, поведінкових норм і щоденних практик, у межах якої безпека сприймається як спільна відповідальність, а не як функція окремого підрозділу. Формування такої культури потребує поєднання трьох інструментів: регулярного навчання, вимірювальних показників та позитивного підкріплення (а не лише покарань за помилки).

Найбільш поширеною помилкою є проведення тренінгів з кібербезпеки у формі формальних лекцій раз на рік. Ефективність таких заходів, згідно з дослідженнями, є мізерною: через місяць після навчання співробітники пам'ятають менше 20 % отриманої інформації. Натомість рекомендовано

використовувати короткі (10–15 хвилин), але часті (щомісячні) інтерактивні модулі, адаптовані до конкретних ролей. Для касирів та операціоністів – це розпізнавання соціальної інженерії, для ІТ-адміністраторів – безпека API та захист привілейованих доступів, для керівників – процедури реагування на інциденти та комунікаційна стратегія.

Важливим елементом є симуляції фішингових атак, які проводяться не для того, щоб покарати «найдовірливіших», а для того, щоб виявити слабкі місця в обізнаності співробітників. Результати симуляцій мають збиратися анонімно (окрім факту натискання на посилання, не фіксується, хто саме це зробив, якщо не було злого умислу). За кожним інцидентом у реальному житті (співробітник повідомив про підозрілого листа, а не проігнорував його) має йти позитивний зворотний зв'язок.

Підвищення цифрової грамотності клієнтів. Клієнти є найслабшою, але водночас найбільш масовою ланкою в системі кібербезпеки. Перекладати на них весь тягар відповідальності (вимога самостійно виявляти всі види фішингу, використовувати складні паролі тощо) є не лише неефективним, але й етично сумнівним. Як наголошувалося в роботі, присвяченій довірі у фінансовому посередництві, «клієнт делегує фінансовій установі не тільки власні грошові кошти, а й право на опрацювання персональних даних, оцінювання ризиків та ухвалення рішень на основі алгоритмічних моделей» [27, с. 91]. Відповідно, установа несе відповідальність за створення безпечного середовища, а клієнт має отримувати зрозумілі, прості та своєчасні підказки, як уникнути типових ризиків.

Запропонована нижче програма підвищення цифрової грамотності (табл. 3.8) диференціює клієнтів за трьома групами – масові роздрібні клієнти, клієнти-пенсіонери (як найбільш вразлива група до соціальної інженерії), а також малий та середній бізнес (якому загрожують компрометація облікових записів та шахрайство з рахунками). Для кожної групи визначено оптимальний формат навчання, періодичність та канали комунікації.

Програма підвищення цифрової грамотності для різних груп клієнтів

Група клієнтів	Характерні загрози	Формат навчання	Періодичність	Канали комунікації	Очікуваний ефект
Масові роздрібні клієнти	Фішинг (підроблені листи «від банку»), скімінг, підроблені мобільні застосунки	Push-повідомлення з короткими порадами (до 3 правил); інтерактивний чатбот з відповідями на типові питання	Щотижнево (push); за запитом (чат-бот)	Мобільний застосунок, SMS	Зниження скарг на фішинг на 30–40 % протягом року
Клієнти-пенсіонери (60+ років)	Соціальна інженерія, телефонні шахраї (дзвінки «з безпеки банку»), фальшиві соціальні виплати	Прості інфографіки «Пам'ятка клієнту» (3–5 правил), лаконічні голосові повідомлення в контакт-центрі, співпраця з соціальними працівниками	Один раз (пам'ятка при онбордингу), повтори щоквартально (нові сценарії)	SMS, голосові роботи (IVR), відділення	Зниження випадків зняття коштів після телефонних дзвінків > 50 %
Малий та середній бізнес	Компрометація облікового запису (інтернет-банкінг), підроблені рахунки, BEC-атаки (business email compromise)	Вебінари «Безпека бізнесу», чек-листи для бухгалтерів, двофакторна автентифікація як обов'язкова вимога	Щоквартально (вебінари); разово (чек-листи)	Бізнес-портал, корпоративна електронна пошта, менеджер	Зниження шахрайства з рахунками на 40–50 %

Джерело: розроблено автором на основі [35; 59; 154; 227] та досвіду провідних українських банків.

Важливою складовою клієнтської програми є прозоре повідомлення про інциденти. Якщо установа стала жертвою кібератаки, вона зобов'язана (етично та, в майбутньому, регуляторно згідно з вимогами DORA) повідомити клієнтів про факт інциденту, його потенційні наслідки та – найважливіше – про

конкретні кроки, яких вживає установа для захисту їхніх коштів та даних. Приховування або замовчування інцидентів підриває довіру значно більше, ніж сам факт атаки (за умови, що установа діяла відповідально).

Для оцінки того, чи дають запропоновані заходи результат, доцільно використовувати три групи показників. По-перше, частота успішних фішингових атак на співробітників (відстежується через систему симуляцій) має знижуватися щоквартально. По-друге, кількість клієнтів, які добровільно проходять навчальні модулі (наприклад, переглядають push-повідомлення або звертаються до чат-боту), має зростати. По-третє, зменшення числа скарг, пов'язаних із шахрайством, де клієнт добровільно передав дані – є прямим індикатором ефективності просвітницьких кампаній. Якщо після впровадження програми кількість таких скарг не змінюється або зростає, це означає, що або формат навчання не відповідає потребам, або канали комунікації потребують коригування.

Зауважимо, що всі заходи з підвищення цифрової грамотності мають ґрунтуватися на повазі до клієнта. Неприпустимим є перекладання відповідальності (як то «клієнт сам винен, що повідомив пароль»). Це руйнує довіру і спонукає клієнтів приховувати факти шахрайства, що ускладнює роботу правоохоронних органів. Натомість установа має постійно нагадувати клієнтам про те, що співробітники банку ніколи не запитують паролі, не вимагають переказувати кошти на «резервні» рахунки, не надсилають посилання для підтвердження платежів. І якщо клієнти дотримуються цих простих правил, банк гарантує відшкодування збитків у разі технічного збою (але не у випадках, коли клієнт свідомо передав дані). Така політика, на нашу думку хоч і може збільшувати короткострокові витрати, але в довгостроковій перспективі зміцнює репутаційний капітал фінансового посередника.

Проведене в підрозділі 2.3 оцінювання цифрової зрілості двох найбільших державних банків України – АТ КБ «ПриватБанк» (DCMI = 2,76, що відповідає «високому/лідерському» рівню) та АТ «Ощадбанк» (DCMI =

2,12, «середній» рівень, верхня межа) – дозволяє не лише констатувати розрив між ними, але й сформулювати диференційовані рекомендації щодо подальшого підвищення цифрової зрілості для кожної категорії установ. При цьому важливо розуміти, що рекомендації для банку-лідера (АТ КБ «ПриватБанк») та банку, що перебуває у фазі наздоганяючої цифровізації (АТ «Ощадбанк»), будуть суттєво відрізнятися не лише за змістом, але й за пріоритетністю окремих напрямів.

Рекомендації для установ з високим/лідерським рівнем цифрової зрілості ($DCMI > 2,6$). Для таких банків, як АТ КБ «ПриватБанк», ключовим завданням є не стільки нарощування кількісних показників (частка цифрових клієнтів уже перевищує 70 %, обсяг операцій у цифрових каналах – понад 90%), скільки підтримання лідерських позицій через інновації першого порядку та підвищення стійкості до екстремальних навантажень. Окремі напрями, які потребують першочергової уваги, визначено в таблиці 3.9.

Рекомендації для установ із середнім рівнем цифрової зрілості ($DCMI 2,0 - 2,4$). Для АТ «Ощадбанк» пріоритетом є прискорення міграції клієнтів у цифрові канали (наразі 4,6 млн користувачів Mobile Oschad при загальній клієнтській базі, що значно перевищує 10 млн), розширення функціоналу мобільного застосунку до рівня лідерів ринку, а також активне використання регуляторних пісочниць для тестування нових продуктів без ризику для основного бізнесу.

Рекомендації для небанківського сектору (орієнтовний $DCMI 1,2 - 1,6$). Хоча систематичне оцінювання цифрової зрілості кредитних спілок, страхових компаній та МФО в межах цього дослідження не проводилося (через відсутність публічних даних), на основі експертних оцінок та опосередкованих індикаторів можна припустити, що більшість із них перебувають на початковому або базовому рівні. Для них першочерговими є заходи з формування базової цифрової гігієни, а також використання спільних платформ та інфраструктурних сервісів, описаних у підрозділі 3.2.

**Першочергові заходи з підвищення цифрової зрілості
за результатами оцінювання DСMI**

Рівень цифрової зрілості (DCMI)	Типові представники в Україні	Пріоритетні заходи	Очікуваний термін реалізації	Необхідні ресурси
Високий / лідерський (> 2,6)	АТ КБ «ПриватБанк»	<ul style="list-style-type: none"> - подальше підвищення кіберстійкості до повного відповідності DORA (звітування про інциденти за 4 рівнями, регулярне тестування на проникнення); - розширення міжнародної присутності через API (BaaS для зарубіжних фінтех-компаній); - інвестиції в генеративний AI для персоналізації пропозицій та фрод-моніторингу в реальному часі 	1–2 роки	Власний бюджет; грантові програми ЄС (Digital Europe)
Середній (2,0 – 2,4)	АТ «Ощадбанк»	<ul style="list-style-type: none"> - масова міграція клієнтів у цифрові канали (маркетингові кампанії, спрощений онбординг через Дію); - розширення функціоналу Mobile Oschad до рівня лідерів (миттєві кредити, персоналізована аналітика, чатбот з AI); - посилення кіберзахисту соціальних виплат та пенсійних коштів (сегментація мережі, посилений моніторинг); - участь у регуляторних пісочницях для тестування інноваційних продуктів 	2–3 роки	Власний бюджет; технічна допомога міжнародних донорів (USAID, EBRD)
Базовий / початковий (1,2 – 1,6)	Кредитні спілки, МФО, невеликі страхові компанії	<ul style="list-style-type: none"> - технологічний аудит за спрощеною методикою (за рахунок субсидій, табл. 3.3); - впровадження базових заходів кібербезпеки (MFA для адміністраторів, регулярне оновлення ПЗ, резервне копіювання в хмару); - приєднання до спільних API-платформ через галузеві асоціації; - навчання персоналу за стандартизованими програмами (цифрова грамотність, виявлення фішингу) 	1–3 роки (поетапно)	Субсидії (табл. 3.3); власний бюджет; міжнародна технічна допомога

Джерело: розроблено автором на основі даних підрозділу 2.3, а також [51; 53; 131; 174; 227; 228].

Поглиблений аналіз для АТ КБ «ПриватБанк». Попри беззаперечне лідерство, у ПриватБанку все ще залишаються «вузькі місця», які потребують уваги. Згідно з оцінюванням у підрозділі 2.3, блок кіберстійкості (CR) отримав 2,2 бали з 3 можливих, що нижче за інші блоки (TI – 3,0; CI – 3,0; IN – 2,8). Це свідчить про те, що навіть лідер має ресурс для підвищення – насамперед у сфері звітування про інциденти відповідно до DORA (скорочення строків до 24 годин), а також у створенні галузевого ISAC (інформаційно-аналітичного центру для обміну даними про кіберзагрози). Другим напрямом є міжнародна експансія через API: використовуючи свою розвинену API-інфраструктуру (понад 100 відкритих API), банк міг би надавати BaaS-послуги фінтех-компаніям в країнах Центральної та Східної Європи, що дозволило б диверсифікувати доходи від комісій.

Поглиблений аналіз для АТ «Ощадбанк». Для АТ «Ощадбанк», окрім зазначених у таблиці 3.9 заходів, критично важливим є скорочення розриву за блоком «Інноваційна спроможність» (IN), який отримав найнижчу оцінку – 1,8 бала (через обмежене використання AI/ML, відсутність DLT/Blockchain-рішень та невисоку частку доходів від API). Рекомендується створити окремий інноваційний підрозділ (або виділити бюджети на R&D), який займатиметься пілотними проєктами в регуляторній пісочниці НБУ. Як показує досвід європейських державних банків, навіть при консервативній бізнес-моделі можна досягти помітних успіхів у цифровізації, якщо інновації не розпорошуються, а концентруються на кількох напрямках, де державний статус дає конкурентну перевагу (наприклад, соціальні виплати, пенсійні продукти, кредитування аграріїв). Зокрема, інтеграція Mobile Oschad з порталом «Дія» для автоматичного отримання соціальних виплат без додаткових заяв – це саме той випадок, коли державний банк може запропонувати унікальний цифровий продукт, недоступний комерційним установам.

Моніторинг прогресу. Для оцінки ефективності впровадження рекомендованих заходів доцільно повторно розраховувати DСMІ для кожного банку з періодичністю раз на рік, а також публікувати агреговані результати по сектору (без розкриття комерційно таємної інформації) на сайті НБУ. Це

створить не лише інструмент внутрішнього контролю для самих установ, але й механізм публічного порівняння, який стимулюватиме конкуренцію в цифровій сфері. Для АТ КБ «ПриватБанк» цільове значення DСMІ на 2028 рік становить 2,92–2,95 (приріст 5–7 %), для АТ «Ощадбанк» – 2,44–2,54 (приріст 15–20 %, що відображає динаміку наздоганяючої цифровізації). Для небанківського сектору цільовим є вихід на рівень DСMІ > 1,8 (тобто перехід від початкового до базового/середнього рівня) для не менш ніж 50 % установ, які отримали підтримку за програмами з таблиці 3.3.

У підсумку, запропоновані в підрозділі 3.3 науково-практичні рекомендації утворюють цілісну систему, що охоплює стратегічний (структура стратегії кіберстійкості), тактичний (матриця заходів протидії загрозам) та операційний (алгоритм впровадження, система КРІ, програми підвищення грамотності) рівні. Їхнє впровадження дозволить фінансовим посередникам України не лише підвищити рівень захищеності від кіберзагроз, але й сформувати стійку основу для довгострокової конкурентоспроможності в умовах цифрової економіки.

Висновки до розділу 3

Проведене дослідження в межах розділу 3 дає змогу підсумувати наступне.

1. Адаптація європейського Регламенту DORA до українських реалій потребує поетапної імплементації з урахуванням пропорційності вимог. В зв'язку з цим нами запропонована триетапна дорожня карта на період 2026–2030 років, яка охоплює оцінювально-нормативний, пілотний та масштабний етапи, забезпечуючи тим самим поступове приведення вітчизняного регулювання ІКТ-ризиків у відповідність до європейських стандартів. Ключовими розривами, які потребують першочергового усунення, є скорочення до 24 годин строків звітування про інциденти, глибина тестування операційної стійкості та управління ризиками від третіх ІКТ-провайдерів.

2. Запровадження в Україні з серпня 2025 року відкритого банкінгу створило інституційну основу для стандартизованого доступу третіх сторін до банківських даних через захищені API. Це дало нам підставу запропоновувати архітектуру відкритого банкінгу у вигляді трирівневої моделі. Ця модель здатна забезпечити баланс між стимулюванням інновацій на основі безоплатного доступу до базових API та захистом прав споживачів через обов'язкову автентифікацію, контроль згод та аудит.

3. Інтеграція українського фінансового ринку до єдиного цифрового простору ЄС передбачає гармонізацію за трьома напрямками: цифрова ідентифікація (приведення BankID НБУ до стандартів eIDAS 2.0), платіжні системи (імплементация PSD2/PSD3, приєднання до SEPA) та обмін фінансовими даними (створення interoperable механізмів обміну кредитними історіями). Потенціал програмованої е-гривні для цільових повоєнних видатків потребує пілотного тестування в територіальних громадах з обов'язковим моніторингом ризиків.

4. Розроблений організаційно-економічний механізм інтеграції фінансових посередників базується на трьох блоках: координаційному (Координаційний центр інтеграції на базі НБУ), ресурсному (державне фінансування, міжнародна технічна допомога, приватні інвестиції) та моніторинговому. Інструменти стимулювання диференційовано за трьома групами (фінансові, регуляторні, організаційні) та цільовими аудиторіями – кредитні спілки, страхові компанії, фінтех-стартапи, що враховує нерівномірність цифрового розвитку різних сегментів ринку.

5. Запропонована екосистемна модель партнерства «банки – небанківські посередники – фінтех – держава» реалізується через три форми взаємодії: банк як провайдер інфраструктури (BaaS), фінтех як інтегратор (FinTech-as-a-Platform) та державно-приватне партнерство. Кожна з моделей фіксує розподіл функцій, зони відповідальності та потоки цінності, створюючи умови для переходу від конкуренції окремих установ до конкуренції екосистем.

6. Типова структура стратегії кіберстійкості (сім взаємопов'язаних розділів) та шестикроковий циклічний алгоритм її впровадження (самооцінка → усунення розривів → технічне впровадження → навчання персоналу → сертифікація → постійний моніторинг) створюють методологічну основу для фінансових посередників різного рівня зрілості. Ключовою особливістю алгоритму є наявність зворотних зв'язків (пунктирні лінії), які забезпечують адаптивність до змін середовища загроз і відрізняють його від лінійних «кращих практик».

7. Система показників ефективності (чотири групи KPI – фінансові, операційні, ризикові, клієнтські) доповнена інтегральним показником цифрової зрілості DСMI та дозволяє здійснювати комплексний моніторинг цифрової трансформації. На основі оцінювання для ПриватБанку (DСMI = 2,76) та Ощадбанку (DСMI = 2,12) сформульовано диференційовані рекомендації: для банків-лідерів – посилення кіберстійкості до рівня DORA та міжнародна API-експансія; для установ зі середнім рівнем – масова міграція клієнтів у цифрові канали; для небанківського сектору – базові заходи безпеки та участь у спільних платформах. Цільові значення DСMI на 2028 рік становлять 2,92–2,95 для ПриватБанку, 2,44–2,54 для Ощадбанку та >1,8 для не менш ніж 50 % небанківських установ, які отримали підтримку.

ВИСНОВКИ

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано нове вирішення наукового завдання, що полягає в поглибленні теоретико-методичних засад та розробці практичних механізмів формування стратегії розвитку фінансових посередників в умовах цифровізації економіки. За результатами дослідження сформульовано такі висновки.

1. Цифрова трансформація фінансових посередників є багатовимірним процесом, що не обмежується впровадженням окремих технологічних рішень, а охоплює зміну бізнес-моделей, трансформацію ключових функцій та перебудову інституційної архітектури фінансового ринку. У роботі доведено, що сучасний фінансовий посередник поступово перетворюється з традиційного інституту акумуляції та перерозподілу ресурсів на цифрову платформу, координатора екосистеми та постачальника даних-центричних сервісів. Це зумовлює формування нових стратегічних орієнтирів – клієнтоцентричності, гнучкості, швидкості інновацій, кіберстійкості та екосистемності.

2. Запропоновано авторську класифікацію фінансових посередників за критеріями ступеня цифровізації, технологічної основи, функціонального призначення та рівня регуляторної інтеграції. На відміну від традиційних підходів, які зосереджуються переважно на інституційній природі, запропонована класифікація дозволяє оцінювати здатність фінансових посередників до інтеграції в цифрові фінансові екосистеми. Виокремлено шість взаємодоповнюючих механізмів впливу фінансових посередників на розвиток цифрових фінансових сервісів – інституційний, технологічний, платформний, регуляторно-інноваційний, освітньо-комунікаційний та інвестиційно-фінансовий. Їх системна взаємодія створює синергетичний ефект, що підсилює інноваційний потенціал цифрового фінансового ринку.

3. Дослідження показало, що цифрові технології фундаментально змінюють архітектоніку стратегічного управління фінансовими посередниками. Якщо класична модель довгострокового планування

ґрунтувалася на стабільності зовнішнього середовища та лінійній екстраполяції трендів, то цифрова модель вимагає адаптивності, використання великих даних для прийняття рішень, інтеграції ризик-менеджменту в усі бізнес-процеси та формування алгоритмічної довіри. Виявлено, що технологічними драйверами цієї трансформації виступають штучний інтелект, Big Data, API-економіка, хмарні технології, блокчейн та RegTech-рішення. Визначено чотири рівні участі фінансових інновацій у формуванні стратегічної моделі розвитку: технологічна база, інноваційні рішення, стратегічні імперативи та стратегічні результати.

4. Аналіз глобальних трендів цифрової трансформації фінансового посередництва дозволив виокремити три провідні моделі – європейську (регуляторно-орієнтовану, з високими стандартами операційної стійкості), американську (ринково-інноваційну, з домінуванням BigTech) та азійську (платформно-екосистемну, з максимальною фінансовою інклюзією). Для України обґрунтовано доцільність формування гібридної моделі, яка інтегрує європейські стандарти кіберстійкості, американську інноваційну гнучкість та азійську масштабованість. Ключовими напрямками імплементації міжнародного досвіду визначено адаптацію Регламенту DORA (2026–2030 рр.), розвиток відкритого банкінгу на основі PSD2, гармонізацію системи BankID НБУ з eIDAS 2.0 та пілотування програмованої е-гривні для цільових повоєнних видатків.

5. Проведене оцінювання цифрової зрілості фінансових посередників за розробленою автором моделлю (DCMI) на прикладі АТ КБ «ПриватБанк» та АТ «Ощадбанк» виявило суттєву диференціацію між двома системно важливими банками. Інтегральний показник для «ПриватБанку» становить 0,89 (за п'ятирівневою шкалою), що відповідає високому/лідерському рівню, тоді як для «Ощадбанку» – 0,56 (середній рівень, верхня межа). Розрив у 0,33 бала свідчить про структурні відмінності в підходах до цифрової трансформації, обсягах інвестицій в ІТ-інфраструктуру та рівні проникнення цифрових каналів серед клієнтів. Запропонована методика дозволяє не лише

фіксувати поточний рівень цифрової зрілості, а й ідентифікувати «вузькі місця» (для АТ КБ «ПриватБанк» – кіберстійкість, для АТ «Ощадбанк» – інноваційна спроможність) та визначати пріоритетні напрями подальших інвестицій.

6. Запропоновано типовий алгоритм впровадження стратегії кіберстійкості, який охоплює шість послідовних кроків: самооцінку (GAP-аналіз), усунення розривів, технічне впровадження, навчання персоналу, сертифікацію та безперервний моніторинг. Ключовою особливістю алгоритму є наявність зворотних зв'язків, що забезпечують адаптивність до змін середовища загроз. Розроблену структуру стратегії кіберстійкості (сім взаємопов'язаних розділів) рекомендовано до впровадження для фінансових посередників різного рівня зрілості з дотриманням принципу пропорційності.

7. Розроблено і обґрунтовано систему показників, яка охоплює чотири групи KPI: фінансові (ROI цифрового проєкту, зниження операційних витрат, приріст доходів від цифрових каналів), операційні (скорочення часу обробки транзакцій, збільшення частки цифрових каналів), ризикові (зниження частоти кіберінцидентів, скорочення MTTR) та клієнтські (NPS цифрових каналів, частка активних цифрових клієнтів). Ця система дозволяє оцінити ефективність впровадження і реалізації цифрових рішень. На основі оцінювання DСMІ сформульовано диференційовані рекомендації для установ з високим рівнем цифрової зрілості (подальше підвищення кіберстійкості до рівня DORA, міжнародна API-експансія), середнім рівнем (масова міграція клієнтів у цифрові канали, розширення функціоналу мобільних застосунків) та для небанківського сектору (базова цифрова гігієна, участь у спільних API-платформах).

8. Розроблено організаційно-економічний механізм інтеграції фінансових посередників до інноваційної інфраструктури цифрового фінансового ринку України, який має трикомпонентну структуру: координаційний блок (Координаційний центр інтеграції на базі НБУ), ресурсний блок (державне фінансування, міжнародна технічна допомога,

приватні інвестиції) та моніторинговий блок (система показників зі зворотними зв'язками). Механізм враховує нерівномірність цифрового розвитку різних типів посередників через диференціацію інструментів стимулювання за трьома групами (фінансові, регуляторні, організаційні) та цільовими аудиторіями. Обґрунтовано доцільність впровадження інтегрального показника цифрової інтеграції (СІІ) та триетапної реалізації механізму (організаційно-підготовчий, масштабування, стабілізаційний).

9. Сформульовано науково-практичні рекомендації щодо реалізації стратегії розвитку фінансових посередників. Запропоновано типову структуру стратегії (сім взаємопов'язаних розділів) та шестикроковий циклічний алгоритм її впровадження зі зворотними зв'язками, що забезпечує адаптивність до змін середовища загроз. Реалізація запропонованих у дисертації положень сприятиме підвищенню рівня цифрової зрілості фінансових посередників, зміцненню їхньої кіберстійкості та конкурентоспроможності в умовах поглиблення євроінтеграційних процесів та повоєнної відбудови економіки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 2025 річний звіт. Система виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Державний центр кіберзахисту державної служби спеціального зв'язку та захисту інформації України*. <https://cip.gov.ua/services/cm/api/attachment/download?id=73033>.
2. 6Wresearch. (2025). Ukraine cyber (liability) insurance market (2025-2031): Segmentation, forecast, size & revenue, trends, outlook, value, companies, competitive landscape, industry, growth, analysis, share (*Report No. ETC9898907*). 6Wresearch. <https://www.6wresearch.com/industry-report/ukraine-cyberliability-insurance-market>.
3. 6Wresearch. (2025). Ukraine cybersecurity insurance market (2025-2031): Outlook, trends, forecast, growth, size, analysis, industry, value, share, companies & revenue (*Report No. ETC4386018*). 6Wresearch. <https://www.6wresearch.com/industry-report/ukraine-cybersecurity-insurance-market>.
4. Accenture. (2023, February 9). Total Enterprise Reinvention: Setting a new performance frontier [Research report]. <https://www.accenture.com/us-en/insights/consulting/total-enterprise-reinvention>.
5. Accenture. (2024). Reinvention in the age of generative AI. Accenture. <https://www.accenture.com/us-en/insights/life-sciences/reinventing-life-sciences-age-generative-ai>.
6. Aldasoro, I., Frost, J., Gambacorta, L., Leach, T., & Whyte, D. (2020). Cyber risk in the financial sector. *SUERF Policy Note*, 206. <https://www.suerf.org/publications/suerf-policy-notes-and-briefs/cyber-risk-in-the-financial-sector/>.
7. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector. *BIS Working Papers*, No. 840. <https://www.bis.org/publ/work840.pdf>.

8. Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security*, 14(3), 167-190. <https://jisis.org/wp-content/uploads/2024/09/2024.I3.010.pdf>.
9. Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022, May). Cyber security threats on digital banking. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-4). IEEE. <https://arxiv.org/pdf/2503.22710>.
10. Anderson, R. (1994). Why Cryptosystems Fail. *Communications of the ACM*, 37(11), 32–40. <https://www.cl.cam.ac.uk/archive/rja14/Papers/wcf.pdf>.
11. Anderson, R. (2001). Why Information Security Is Hard – An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC)*, 358–365. doi: 10.1109/ACSAC.2001.991552.
12. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Indianapolis: Wiley. <https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3.pdf>.
13. Andrushkiv, I. P., & Mushynskyi, B. M. (2016). Vplyv IT ta kiber-ryzykiv na bankivsku diialnist [The impact of IT and cyber risks on banking activities]. *Stalnyi rozvytok ekonomiky - Sustainable economic development*, (2(31)), 242–247. <http://www.economdevelopment.in.ua/index.php/journal/article/download/427/411>.
14. Arner, D. W., Barberis, J. N., & Buckley, R. P. (2015). The evolution of FinTech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47, 1271–1319. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/geojintl47&div=41&id=&page=>.
15. Arner, D. W., Barberis, J. N., & Buckley, R. P. (2020). *The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*. Wiley. <https://books.google.com.ua/books?id=fJGfDwAAQBAJ>.
16. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech and the reconceptualization of financial regulation. *Northwestern Journal of*

International Law & Business, 37(3), 371–413. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/nwjilb37§ion=17.

17. Aslanova, I. V., & Kulichkina, A. I. (2020). Digital maturity: Definition and model. In *Proceedings of the 2nd International Scientific and Practical Conference “Modern Management Trends and the Digital Economy: From Regional Development to Global Economic Growth” (MTDE 2020)* (pp. 443–449). Atlantis Press. <https://www.atlantis-press.com/article/125939845.pdf>.

18. Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*. Advance online publication. <https://doi.org/10.1007/s42786-025-00056-3>, <https://link.springer.com/article/10.1007/s42786-025-00056-3>.

19. Bain & Company. (2022). Embedded finance: What it takes to prosper in the new value chain. <https://www.bain.com/insights/embedded-finance/>.

20. Balasubramanian, S. Agarwal, A. Hunain Evolution of risk management in banking. PwC Middle East Banking Study 2024. PwC. (2025, February 17), <https://www.pwc.com/m1/en/publications/2025/docs/pwc-middle-east-banking-study-2024.pdf>.

21. Bank for International Settlements (BIS). (2022). Cyber resilience practices: An overview of critical components. BIS Papers No. 123. <https://www.bis.org/publ/bppdf/bispap123.htm>.

22. Bank for International Settlements (BIS). (2023). *Results of the 2022 BIS survey on central bank digital currency*. BIS Paper No. 136. <https://www.bis.org/publ/bppdf/bispap136.pdf>.

23. Bank for International Settlements. (2023). And so we pay: More digital and faster – CPMI statistical review 2023. https://www.bis.org/statistics/payment_stats/commentary2301.pdf.

24. Bank for International Settlements. (2023). And so we pay... https://www.bis.org/statistics/payment_stats/commentary2301.pdf.

25. Bank for International Settlements. (2023). *Project Polaris: Closing the CBDC cyber threat modelling gaps*. Basel: BIS Innovation Hub. <https://www.bis.org/publ/othp71.htm>.

26. Basel Committee on Banking Supervision (BCBS). (2023). The digitalisation of finance. *Bank for International Settlements*. <https://www.bis.org/bcbs/publ/d575.pdf>.

27. Basel Committee on Banking Supervision. (2018). *Cyber-resilience: Range of practices*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d454.pdf>.

28. Basel Committee on Banking Supervision. (2023). *Digital fraud and banking: Discussion paper*. Basel: Bank for International Settlements. <https://www.bis.org/bcbs/publ/d571.htm>.

29. Basel Committee on Banking Supervision. (2024). Digitalisation of finance – advancing digitalisation of financial services. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d575.pdf>.

30. Basiurkina, N., Krylov, D., Karpinska, H., Pchela, A., & Voloshyn, D. (2026). The impact of digitalization on financial mechanisms for managing the strategic development of enterprises in the face of modern challenges. *Pacific Business Review International*, 18(9), 123–136. https://www.pbr.co.in/2026/2025_month/March/11.pdf.

31. Bernitsas Law. (2026, April 24). Digital Operational Resilience Act (DORA): Where do we stand? <https://bernitsaslaw.com/2026/04/24/digital-operational-resilience-act-dora-where-do-we-stand>.

32. BIS. (2022). Operational resilience in financial services. Bank for International Settlements. <https://www.bis.org/publ/bppdf/bispap123.htm>.

33. BIS. (2023). Digital payments make gains but cash remains Bank for International Settlements. https://www.bis.org/statistics/payment_stats/commentary2301.pdf.

34. Bontadini, F., Filippucci, F., Jona-Lasinio, C., Nicoletti, G., & Saia, A. (2024). *Digitalisation of financial services, access to finance and aggregate*

economic performance (OECD Economics Department Working Papers No. 1818). OECD Publishing. https://www.oecd.org/en/publications/digitalisation-of-financial-services-access-to-finance-and-aggregate-economic-performance_10c7e583-en.html.

35. Bouveret, A. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment* (IMF Working Paper No. WP/18/143). International Monetary Fund. <https://doi.org/10.5089/9781484360750.001>.

36. Bozhenko, V. V., Pakhnenko, O. M., Yarovenko, H. M., & Koibichuk, V. V. (2025). Data analysis tools for assessing cyber risks in financial services. *Economic achievements: prospects and innovations*, (20). <http://econp.com.ua/index.php/journal/article/download/550/507>.

37. Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. L. (2022). Implications of Cyber Risk for Financial Stability. *FEDS Notes*, No. 2022(3077). <https://doi.org/10.17016/2380-7172.3077>.

38. Capgemini Research Institute. (2023). World Cloud Report 2023: Financial Services. Capgemini. <https://www.capgemini.com/insights/research-library/world-cloud-report-2023-financial-services/>.

39. Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*. Defense Technical Information Center. <https://doi.org/10.21236/ADA609863>.

40. Cheng, S., Fan, Q., & Huang, M. (2023). Strategic orientation, dynamic capabilities, and digital transformation of commercial banks. *Sustainability*, 15(3), 1915. <https://www.mdpi.com/2071-1050/15/3/1915>.

41. Cornelli, G., Frost, J., Gambacorta, L., Rau, R., Wardrop, R., & Ziegler, T. (2020). Fintech and big tech credit: A new database (BIS Working Papers No. 887). *Bank for International Settlements*. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/09/2020-ccaf-fintech-bigtech-credit.pdf>.

42. Cornelli, G., Frost, J., Gambacorta, L., Rau, R., Wardrop, R., & Ziegler, T. (2020). The Global Alternative Finance Market Benchmarking Report.

Cambridge Centre for Alternative Finance & BIS. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/09/2020-ccaf-fintech-bigtech-credit.pdf>.

43. Council of the European Union. (2021). Council Directive (EU) 2021/514 amending Directive 2011/16/EU on administrative cooperation in the field of taxation (DAC7). <https://eur-lex.europa.eu/eli/dir/2021/514/oj>.

44. Council of the European Union. (2023). Council Directive (EU) 2023/2226 on administrative cooperation in the field of taxation (DAC8). <https://eur-lex.europa.eu/eli/dir/2023/2226/oj>.

45. Cybersecurity Industry 2025. https://www.reportlinker.com/market-report/Cybersecurity/517851/Cybersecurity?term=cyber%20security%20market&matchtype=p&loc_interest=&loc_physical=9193872&gad_source=1&gad_campaignid=15072746546&gbraid=0AAAAAD19yGd_OOB14KDvPkPgYRJkUAk1n&gclid=Cj0KCQiAoZDJBhC0ARIsAERP-F9tTQ9OGtiPy0KFMWB3qhebxfFTBEA71Ult90saHjuIcX0WvPJYTssaAgZYEA_Lw_wcB.

46. CyRAACS. (2026, January 8). How FinTechs can build a future-ready compliance strategy: SOC 2, DPDP Act, RBI & ISO requirements. *CyRAACS Blog*. <https://cyraacs.com/how-fintechs-can-build-a-future-ready-compliance-strategy/>.

47. Deloitte. (2022). Digital Maturity Model 2.0. Deloitte Insights. <https://www2.deloitte.com>, <https://www.deloitte.com/us/en/insights.html>, <https://www.deloitte.com/cz-sk/en/search-results.html?qr=Model%202.0>.

48. Deloitte. (2026). *From reactive compliance to proactive command: How ITAM enables regulatory compliance*. Deloitte UK. <https://www.deloitte.com/uk/en/Industries/technology/blogs/how-itam-enables-regulatory-compliance.html>.

49. Devlin, J. F., Roy, S. K., Sekhon, H., Moin, S. M. A., & Sahiner, M. (2025). Trust and FinTech: A review and research agenda. *Electronic Markets*, 35(1), 62. <https://link.springer.com/content/pdf/10.1007/s12525-025-00803-w.pdf>.

50. Digital Economy Navigator (DEN). (n.d.). Methodology. URL: <https://den.dco.org/>.

51. DLA Piper. (2025, February 28). Application of the Digital Operational Resilience Act (DORA): Key considerations. <https://www.dlapiper.com/en-bh/insights/publications/2025/02/application-of-the-digital-operational-resilience-act---dora>.

52. Dovhan, O. (2025). Analysis of the development of digital innovations in the financial services market in Ukraine in 2010-2024. *Економіка та суспільство*, (71). <https://economyandsociety.in.ua/index.php/journal/article/view/5492/5431>.

53. Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J., & Winkelman, Z. (2018). *Estimating the Global Cost of Cyber Risk: Methodology and Examples*. RAND Corporation. <https://doi.org/10.7249/rr2299>.

54. Dubas, A. (2025, September 18). Ukraine's big step toward Open Banking. *The Paypers*. <https://thepaypers.com/regulations/interviews/ukraines-big-step-toward-open-banking-exclusive-interview-with-the-association-of-ukrainian-banks>.

55. Dubyna, M., Popelo, O., & Shvets, M. (2025). The role of artificial intelligence in the development of the insurance market. *Baltic Journal of Economic Studies*, 11(1), 329–341. <https://doi.org/10.30525/2256-0742/2025-11-1-329-341>.

56. Dubyna, M., Shchur, R., Shyshkina, O., Sadchykova, I., Panchenko, O., & Bazilinska, O. (2024). The role of artificial intelligence in the cybersecurity system of banking institutions in the conditions of instability. *Journal of Theoretical and Applied Information Technology*, 102(19), 6950–6965. <https://www.jatit.org/volumes/Vol102No19/8Vol102No19.pdf>.

57. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, 145(3), 802–826. doi: <https://doi.org/10.1016/j.jfineco.2021.10.007>.

58. Elliott, J., Wilson, C., Khiaonarong, T., Jenkinson, N., Adelman, F., Morozova, A., Gaidosch, T., Schwarz, N., & Ergen, I. (2020). Cyber Risk and Financial Stability: It's a Small World After All. *Staff Discussion Notes*, No. 2020(007). <https://doi.org/10.5089/9781513512297.006>.

59. ENISA. (2024). *ENISA threat landscape: Finance sector (January 2023 to June 2024)*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf.
60. Ethereum Smart Contract Security Best Practices. <https://consensys.github.io/smart-contract-best-practices/>.
61. European Banking Authority. (n.d.). *Digital Operational Resilience Act (DORA)*. Retrieved from <https://urli.info/1m-ov>.
62. European Central Bank. (2025). Tokenised finance and the evolution of digital markets. https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250930_1~10880b6083.en.html.
63. European Commission. (2022). Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554>.
64. European Commission. (2022). Digital Economy and Society Index (DESI) 2022. URL: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>.
65. European Commission. (2023). Retail payments package: PSD3 and PSR proposals. https://finance.ec.europa.eu/publications/proposal-payment-services-directive-and-regulation_en.
66. European Commission. (2024). Central Electronic System of Payment Information (CESOP). https://taxation-customs.ec.europa.eu/central-electronic-system-payment-information-cesop_en.
67. European Parliament & Council of the European Union. (2015). Directive (EU) 2015/2366 on payment services in the internal market (PSD2). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>.
68. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of personal data (GDPR). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

69. European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*. Official Journal of the European Union, L 333/1–103. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>.

70. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1183 establishing the European Digital Identity Framework (eIDAS 2.0). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>.

71. European Payments Council. (2023). SEPA Payment Schemes. <https://www.europeanpaymentscouncil.eu/what-we-do/sepa-payment-schemes>.

72. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA threat landscape: Finance sector (January 2023 to June 2024)*. ENISA. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf.

73. European Union. (2022). Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). <https://eur-lex.europa.eu>.

74. Federal Bureau of Investigation. (2023). *2022 internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

75. Federal Bureau of Investigation. (2024). *2023 internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

76. Federal Bureau of Investigation. (2025). *2024 internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

77. Feyen, E., Frost, J., Gambacorta, L., Natarajan, H., & Saal, M. (2021). *Fintech and the digital transformation of financial services: implications for market structure and public policy*. Bank for International Settlements. *Fintech and the digital transformation of financial services: implications for market structure and public policy*.

78. Financial Sector's Cybersecurity: A Regulatory Digest. *World Bank*
<https://thedocs.worldbank.org/en/doc/3c28bd048d78efd27744987253e2c44a-0430012021/related/CybersecDigest-v6-FINAL-vs.pdf>.

79. Fortune Business Insights. (2024). FinTech market size, share & industry analysis, by deployment mode, by technology, by application, by end user, and regional forecast, 2024-2032. Fortune Business Insights.
<https://www.fortunebusinessinsights.com/fintech-market-108641>.

80. Gartner. (2021). Digital Business Maturity Model. Gartner Research.
<https://www.gartner.com>.

81. Gomber, P., Koch, J. A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics*, 87(5), 537–580. <https://doi.org/10.1007/s11573-017-0852-x>.

82. GRC PROS Blog. (2025, September 27). SOC 2 Type 2 vs. ISO 27001: A deep dive comparison for third-party assurance in GRC [LinkedIn post]. *LinkedIn*.
https://www.linkedin.com/posts/grc-pros-blog_soc-2-type-2-vs-iso-27001-a-deep-dive-comparison-activity-7378141455053316096-9gim.

83. Guidance on cyber resilience for financial market infrastructures (2016). *Committee on Payments and Market Infrastructures. Board of the International Organization of Securities Commissions*. <https://www.bis.org/cpmi/publ/d146.pdf>.

84. IMF. (2023, 3 жовтня). IMF Releases the 2023 Financial Access Survey Results. <https://www.imf.org/en/news/articles/2023/10/03/pr23332-imf-releases-the-2023-financial-access-survey-results?>

85. International Finance Corporation (IFC). (2022). *Banking on FinTech in Emerging Markets*. IFC. <https://www.ifc.org/content/dam/ifc/doc/mgrt/em-compass-note-109-jan-2022.pdf>.

86. International Monetary Fund. (2022). Digital money and financial stability. <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/19/Digital-Money-and-Financial-Stability-523459>.

87. International Monetary Fund. (2023). Cyber Risk for the Financial Sector: Threats and Policy Responses. <https://www.imf.org/en/Publications>.

88. International Monetary Fund. (2024). *Global financial stability report: Strengthening the resilience of the financial system*. <https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024>.

89. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. <https://www.iso.org/ru/standard/27001>.

90. Janas, T. (2025, August 25). Digital risks, real board accountability. *Warsaw Business Journal*. <https://wbj.pl/digital-risks-real-board-accountability/post/147006>.

91. Kane, G. C., Palmer, D., & Phillips, A. N. (2017). Achieving digital maturity. *MIT Sloan Management Review*. <https://surl.li/omjuwk>.

92. Kaushik, K. (2025, August 29). India taps homegrown digital payments network to widen access to credit. *Financial Times*. <https://www.ft.com/content/958b0c4c-c061-4b40-a2c5-b8b89b0db73c>.

93. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *IMF Working Paper*, 17/185. <https://doi.org/10.5089/9781484313787.001>.

94. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber Risk, Market Failures, and Financial Stability* (IMF Working Paper No. 17/185). International Monetary Fund. <https://doi.org/10.5089/9781484313787.001>.

95. Kryshthal, H., Samofalova, M., Sakhno, L., Fedyna, V., Mokienko, T., & Yermolaieva, M. (2025). Cyber risks in the financial and banking system: Analysis of direct and systematic losses. *Financial and Credit Activity Problems of Theory and Practice*, (2(61)), 125–140. <https://doi.org/10.55643/fcaptp.2.61.2025.4672>.

96. Lavruk, V., Havryliuk, V., Burlakov, O., Burdeniuk, S., & Poprozman, N. (2025). Prospects for the implementation of the digital currency of the National Bank of Ukraine in the context of global digitalization. *Економіка розвитку*, 24(2), 41–53. <https://repository.hneu.edu.ua/handle/123456789/37107>.

97. Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 61(1), 35–46. <https://doi.org/10.1016/j.bushor.2017.09.003>.

98. McKinsey & Company. (2015). Raising your digital quotient. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/raising-your-digital-quotient>.

99. McKinsey & Company. (2021). The Digital Quotient: Measuring your company's digital maturity. <https://www.mckinsey.com>.

100. McKinsey & Company. (2024). The 2024 McKinsey Global Payments Report. <https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-report>.

101. Modern Requirements. (2026, January 27). Modern requirements for AI-driven financial compliance: From obligation to evidence across DORA, NIST, ISO 27001, SOC 2, and PCI DSS. *Modern Requirements Blog*. <https://www.modernrequirements.com/blogs/ai-driven-financial-compliance/>.

102. msg-insurance-suite. (2025, September 12). New reporting requirements for insurers and IT service providers – Part 2: Emerging obligations for software vendors, managed service providers, and cloud service providers. *msg-insurance-suite Blog*. <https://msg-insurance-suite.com/blog/rethinking-insurance/new-reporting-requirements-for-insurers-and-it-service-providers-part-2/>.

103. Naceur S. B., Candelon B., Elekdag S., Emrullahu D. (2023). Is FinTech Eating the Bank's Lunch? IMF. <https://www.imf.org/en/-/media/files/publications/wp/2023/english/wpiea2023239-print-pdf.pdf>.

104. National Bank of Ukraine. (2020). Fintech development in Ukraine until 2025. Fintech development in Ukraine.

105. NIST. (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

106. NIST. (2024). *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.

107. OECD. (2020). *Digital Disruption in Banking and Its Impact on Competition*. Paris: OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/02/digital-disruption-in-banking-and-its-impact-on-competition_330c7176/b8d8fcb1-en.pdf.

108. OECD. (2023). *Digital Security and Resilience in Financial Services*. OECD Publishing. <https://doi.org/10.1787/9789264654693-en>.

109. OECD. (2023). *Digitalisation and Financial Resilience in the Post-COVID Era*. OECD Publishing. <https://doi.org/10.1787/9789264954930-en>.

110. OECD. (2024). *Підвищення стійкості шляхом прискорення цифрової трансформації бізнесу в Україні*. OECD Publishing. <https://doi.org/10.1787/5d9e86a7-uk>.

111. OECD. *Digital security*. <https://www.oecd.org/en/topics/policy-issues/digital-security.html>.

112. Open Banking Limited. (2024, July 23). *Open banking marks major milestone of 10 million users*. <https://www.openbanking.org.uk/news/open-banking-marks-major-milestone-of-10-million-users/>.

113. Organisation for Economic Co-operation and Development (OECD). (2023). *OECD/INFE 2023 International Survey of Adult Financial Literacy*. OECD Publishing. <https://doi.org/10.1787/56003a32-en>.

114. Organisation for Economic Co-operation and Development. (2019). *Going digital: Shaping policies, improving lives*. OECD Publishing. <https://doi.org/10.1787/9789264312012-en>.

115. Organisation for Economic Co-operation and Development. (2024a). *Competition, FinTechs and Open Banking: Recent developments in Latin America and the Caribbean*. OECD Publishing. <https://doi.org/10.1787/de9fe6b4-en>, https://www.oecd.org/en/publications/competition-fintechs-and-open-banking_de9fe6b4-en.html.

116. Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), 625-643. https://www.researchgate.net/profile/Adedoyin-Oyewole-2/publication/379428581_Cybersecurity_risks_in_online_banking_A_detailed_review_and_preventive_strategies_application/links/6611a4ac2034097c54fb755f/Cybersecurity-risks-in-online-banking-A-detailed-review-and-preventive-strategies-application.pdf.
117. Panchal S. S., Ansari I., Azim K.S., Bhujel K., & Ahirrao Y. S. (2025). Cyber Risk And Business Resilience: A Financial Perspective On IT Security Investment Decisions. *The American Journal of Engineering and Technology*, 7(09), 23–48. <https://doi.org/10.37547/tajet/Volume07Issue09-04>.
118. Parubets, O., Shyshkina, O., Sadchykova, I., Yevtushenko, Y., Tarasenko, A., & Potseluiko, I. (2023). Dynamics of the development of the credit services market in the conditions of financial instability: A case of Ukraine. *International Journal of Sustainable Development and Planning*, 18(9), 2733-2745. <https://doi.org/10.18280/ijstdp.180912>.
119. Predmestnikov, O., Kaganovska, T., Pakhomova, I., Orel, A., & Rohozinnikova, K. (2025). Administrative and legal regulation of the electronic identification of citizens. *Revista Jurídica Portucalense*, (38), 405-426. <https://eprints.mdpu.org.ua/id/eprint/14653/1/21.%2BPREDMESTNIKOV.pdf>.
120. Prosci. (2025, June 17). Digital transformation in financial services. URL: <https://www.prosci.com/blog/digital-transformation-in-financial-services>.
121. Prykaziuk, N., & Myronchuk, A. (2024). Priority directions of transformation of the banking system of ukraine in the crisis conditions. *Collection of Scientific Papers «ΛΟΓΟΣ»*, (May 24, 2024; Zurich, Switzerland), 40–44. <https://doi.org/10.36074/logos-24.05.2024.007>.
122. Prykhodko, B. (2025). Kiberryzyky finansovoho sektoru v umovakh tsyfrovoyi transformatsii [Cyber risks of the financial sector in the context of digital transformation]. *Herald of Khmelnytskyi National University. Economic Sciences*, 340(2), 125–139. <http://heraldes.khmnu.edu.ua/index.php/heraldes/article/download/1662/1698>.

123. PwC. (2025). «Міжнародне аналітичне дослідження довіри до цифрових технологій, 2025»: ключові висновки для сектору фінансових послуг [Звіт]. PwC Україна. <https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey/banking-financial.html>.
124. Pyshny A.. (2025, August 7). Solutions from Ukraine: National Bank plans to test digital currency. *Рубрика*. <https://rubryka.com/en/2025/08/07/nbu-planuye-testuvaty-tsyfrovu-valyutu-pyshnyj-rozpoviv-pro-plany-po-e-gryvni/>.
125. Shiklo, B. (n.d.). IoT for Smart Banking and Finance. <https://www.scnsoft.com/blog/iot-in-banking-and-financial-services>.
126. Shkarlet, S., Dubyna, M., Shchur, R., & Shyshkina, O. (2025). The Role of Cloud Technologies in Modern Development of Banking Institutions. *Journal of Vasyl Stefanyk Precarpathian National University*, 12(2), 143–157. <https://doi.org/10.15330/jpnu.12.2.143-157>.
127. SmartSuite. (2025, December 11). 10 best risk management software & tools in 2026. *SmartSuite Blog*. <https://www.smartsuite.com/blog/risk-management-software>.
128. Stepanenko R. (2025, August 11). Open Banking launches in Ukraine: New opportunities for local and international businesses. *Lexology*. <https://www.lexology.com/library/detail.aspx?g=bdf1714f-322f-4079-b773-2ee01a3b3b9e>.
129. Sung Keun, O. (2017). Analysis of the Cyber Security of Financial Transactions for Financial Stability. *Korean Journal of Banking and Financial Law*, 10(1), 3–35. <https://doi.org/10.35274/kbfla.2017.10.1.001>.
130. Tapscott, D., & Tapscott, A. (2014). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. <https://www.amazon.com/Blockchain-Revolution-Technology-Changing-Business/dp/1101980133>.
131. Taranenko, A. (2025). Innovative mechanisms of state regulation of information security of financial institutions in Ukraine in the context of DORA implementation and Suptech tools development. *Journal of Vocational Health Research*. <https://doi.org/10.61345/1339-7915.2025.2.26>.

132. Totska, O., & Shevchuk, B. (2023). Fintech market in Ukraine: Analysis and forecasting. *Economics and Region*, 3(90), 90–94. article_94 (eng).pdf.
133. Verheliuk, Y., Hantsiak, M., & Fomov, D. (2025). Digital transformation of the banking system: global guidelines for Ukraine. *Finance of Ukraine*, (3), 45-57. <https://doi.org/10.33763/finukr2025.03.045>.
134. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>.
135. VIXIO Regulatory Intelligence. (2025, November 13). Regulatory Influencer: Ukraine makes steps towards EU-style digital identity bolstering consumer trust and competition. <https://www.vixio.com/regulatory-news/pc-regulatory-influencer-ukraine-makes-steps-towards-eu-style>.
136. Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *arXiv preprint arXiv:2503.22710*. <https://arxiv.org/pdf/2503.22710>.
137. What is SOC 2® ? <https://secureframe.com/hub/soc-2/what-is-soc-2>.
138. World Bank Group (2020, April). DIGITAL FINANCIAL SERVICES <https://thedocs.worldbank.org/en/doc/305a39cbb6f35567db78bda6709c5cd8-0430012025/original/World-Bank-DFS-Whitepaper-DigitalFinancialServices.pdf>.
139. World Bank Group. (2025). About the Global Findex 2025 <https://www.worldbank.org/en/publication/globalindex>.
140. World Bank. (2021). The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19. <https://www.worldbank.org/en/publication/globalindex>.
141. World Bank. (2022). Digital Financial Services and Trust. <https://documents.worldbank.org>.
142. World Bank. (2024). Global FinTech Trends and Digital Financial Inclusion. World Bank Documents. <https://documents.worldbank.org>.

143. World Economic Forum. (2025). *How to create the financial market infrastructures of the future*. How to create the financial market infrastructures of the future | World Economic Forum.

144. Zalan, T., & Toufaily, E. (2017). The promise of fintech in emerging markets: Not so disruptive? *Contemporary Economics*, 11(4), 415–430. <https://doi.org/10.5709/ce.1897-9254.253>.

145. Андрющенко, І. С., & Скидан, В. Л. (2023). Цифрова трансформація банківського сектора України. *Бізнес Інформ*, (12), 77–82. https://www.business-inform.net/export_pdf/business-inform-2023-12_0-pages-77_82.pdf.

146. Бігдаш, В. Д. (2024). Трансформація системи фінансового управління страхових компаній в умовах цифровізації та сталого розвитку. *Академічні візії*, (34). <https://www.academy-vision.org/index.php/av/article/download/2344/2215>.

147. Болотіна, Є., Панасенко, А., & Пішеніна, Т. (2024). Цифрові технології банківської сфери: особливості розвитку, перспективи та загрози. *Здобутки економіки: перспективи та інновації*, (9). <https://econp.com.ua/index.php/journal/article/download/134/107>.

148. Величко, Г. В. (2017). Дослідження зарубіжного досвіду розвитку інноваційної інфраструктури. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*, (16), 267–271. <https://doi.org/10.31498/2225-6407.16.2017.136526>.

149. Вергелюк, Ю. Ю. (2022). Потенціал використання блокчейн технологій на фінансовому ринку. *Економіка та суспільство*, (38). <https://doi.org/10.32782/2524-0072/2022-38-15>.

150. Вергелюк, Ю. Ю., Ганцяк, М. О., Фомов, Д. О. (2024). Fintech як драйвер економічного відновлення України. *Міжнародний науковий журнал "Інтернаука". Серія: "Економічні науки"*, 10. <https://doi.org/10.25313/2520-2294-2024-10-10402>.

151. Версаль, Н. І., Приказюк, Н. В., Балицька, М. В., & Ерастов, В. І. (2025). Цифрова трансформація малого та середнього підприємництва в країнах ЄС. *Вісник ОНУ імені І. І. Мечникова*, 30(4), 22–29. http://visnyk-onu.od.ua/journal/2025_30_4/5.pdf.

152. Вовчак, О. Д., & Крентовська, Л. М. (2013). Функції фінансового посередництва України. *Інноваційна економіка*, (5), 230-233. [http://www.irbis-nbuv.gov.ua/cgi-](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/inek_2013_5_59.pdf)

[bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/inek_2013_5_59.pdf](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/inek_2013_5_59.pdf).

153. Вовчак, О., & Крентовська, Л. (2012). Фінансове посередництво: економічна сутність і класифікація. *Вісник НБУ*, (8), 4–9.

154. Волошин Д., Шишкіна О., Киселиця С. (2024). Етичні виклики цифровізації: філософський аналіз довіри як основи фінансового посередництва. У: *Соціальне підприємництво як інструмент відновлення України* (м. Чернігів, 16 вересня 2024 р.) (с. 90–92). НУ «Чернігівська політехніка». <https://stu.cn.ua/wp-content/uploads/2024/09/zbirnyk.pdf>.

155. Волошин, Д. М. (2026). Теоретико-методичні аспекти оцінювання цифрової зрілості фінансових посередників. *Успіхи і досягнення у науці*, (4), 1119–1132. [https://doi.org/10.52058/3041-1254-2026-4\(26](https://doi.org/10.52058/3041-1254-2026-4(26).

156. Гаряга, Л. О., & Куліш, Р. Р. (2019). Фінансова безпека банківської діяльності в умовах цифровізації. *Problems of Economy*, (4). <https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=22220712&AN=142226794&h=qMZmy8C7Xs08jieGQWSoDelGRwMf3vgIpjcGerveSBbqycxf%2F0q1%2BoXs7cijoIammknBktFFfrvDl9lpidOJQ%3D%3D&crl=c>.

157. Гнєздовський, О., Домашенко, С., & Морозов, Д. (2024). Вплив цифрового фінансового простору на економічний розвиток: аналіз потенціалу та перспективи для України. *Економіка та суспільство*, (65). <https://economyandsociety.in.ua/index.php/journal/article/download/4494/4433>.

158. Голіонко, Н., & Кондратьєва, К. (2023). Методичні підходи до оцінювання цифрової зрілості організації. *Молодий вчений*, 1(113), 145–150. URL: <https://molodyivchenyi.ua/index.php/journal/article/download/5712/5589>.

159. Дубина, М. В. (2017). Формування системи основних типів фінансової довіри у межах ринку фінансових послуг. *Проблеми і перспективи економіки та управління*, (3 (11)), 115-124. <http://journals.stu.cn.ua/index.php/2411-5215/article/download/126103/120789>.

160. Дубина, М. В., & Шеремет, О. М. (2019). Розвиток e-banking: світовий та вітчизняний досвід. *Проблеми і перспективи економіки і управління*, 2(18), 154-162. <https://ir.stu.cn.ua/bitstream/handle/123456789//%D0%94%D1%83%D0%B1%D0%B8%D0%BD%D0%B0%20%D0%9C.%20%D0%92..pdf?sequence=1&isAllowed=y>.

161. Дубина, М., & Устименко, Я. (2025). Теоретичні положення обґрунтування сутності банківської цифрової інфраструктури. *Проблеми і перспективи економіки та управління*, (2(42), 274–285. [https://doi.org/10.25140/2411-5215-2025-2\(42\)-274-285](https://doi.org/10.25140/2411-5215-2025-2(42)-274-285).

162. Дюк, Р. (2025). Цифрова еволюція бізнес моделей фінансового сектору: від традиційних банків до платформних екосистем. *Економіка і регіон=Economics and region*, (2(97)), 155-160. <https://journals.nupp.edu.ua/eir/article/download/3800/3172>.

163. Журман, С. М. (2014). Сутність фінансових посередників та їх основні функції. *Вісник Чернігівського державного технологічного університету. Серія: Економічні науки*, (3), 197-201. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vcndtue_2014_3_28.pdf.

164. Захаркін, О. О., Захаркин, А. А., Бойко, А. В., & Сокол, Л. В. (2023). Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу. *Проблеми сучасних трансформацій. Серія: економіка та управління*, (10). <https://essuir.sumdu.edu.ua/server/api/core/bitstreams/a0693020-347a-4771-b39b-42e0ea6e04f5/content>.

165. Зянько, В., & Нечипоренко, Т. (2025). Цифрова трансформація банківського сектору: сучасні тренди та вектори розвитку. *Innovation and Sustainability*, (4), 6–21. <https://doi.org/10.31649/ins.2024.4.6.21>
<https://ins.vntu.edu.ua/index.php/ins/article/view/298>.
166. Іванова, Н., & Попело, О. (2025). Інфраструктурне забезпечення сталого розвитку кредитних установ в умовах цифрової трансформації регіональних ринків фінансових послуг. *Науковий вісник Полісся*, (2(31)), 291–311. [https://doi.org/10.25140/2410-9576-2025-2\(31\)-291-311](https://doi.org/10.25140/2410-9576-2025-2(31)-291-311).
167. Карлін, М., Шматковська, Т., & Борисюк, О. (2021). Банківські інновації в умовах формування цифрової економіки. *Економіка та суспільство*, (27).
<https://economyandsociety.in.ua/index.php/journal/article/download/447/429>.
168. Козьменков, М. (2026). Методичні підходи до оцінювання цифрової зрілості екосистеми онлайн сервісів фінансових установ з використанням інструментів штучного інтелекту. *Актуальні питання економічних наук*, 20. <https://a-economics.com.ua/index.php/home/article/download/1190/1172>.
169. Колотило, Л., Дубина, М. (2025). Стратегія забезпечення фінансової безпеки банку: сутність та особливості розробки в умовах макроекономічної нестабільності. *Успіхи і досягнення у науці*, (9(19)), 15-1030.
170. Корнівська, В. (2020). Глобальний фінансово-структурний розвиток: трансформації інститутів фінансового посередництва в умовах оновлення інформаційно-мережевої економіки. *Економічна теорія*, (1), 37-56. http://jnas.nbu.gov.ua/j-pdf/ecte_2020_1_5.pdf.
171. Кучеренко, С., Леваєва, Л., Дармостук, Д., & Ващенко, С. (2025). Фінансове посередництво в національній економіці та його державне регулювання в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення*, (11), 78-89. <https://pa.journal.in.ua/index.php/pa/article/download/194/184>.
172. Лігоненко, Л., & Зеленко, К. (2025). Оцінювання цифрової зрілості бізнес-організації: сутність та інструментарій оцінювання. *Review of Transport Economics and Management*, 14(30), 159–169. <https://pte.ust.edu.ua/article/download/345008/339705>.

173. Лобко, О. М., Дубина, М. В., Заєць О. В. (2024). Роль штучного інтелекту в стратегічному розвитку системи кредитного менеджменту банку. *Науковий вісник Національної академії статистики, обліку та аудиту*, 3-4. <https://irb.nasoa.edu.ua/server/api/core/bitstreams/a51d91ce-ba5e-40b2-851c-3147e14bb6ca/content>.

174. Малихін, А., & Волошин, Д. (2025). Аналіз ролі фінансових посередників у процесі формування інноваційної інфраструктури ринку цифрових фінансових послуг України. *Науковий вісник Полісся*, (1(30)), 284–299. [https://doi.org/10.25140/2410-9576-2025-1\(30\)-284-299](https://doi.org/10.25140/2410-9576-2025-1(30)-284-299).

175. Маслій, О. А., & Максименко, А. П. (2022). Ризики та загрози економічній безпеці України у цифровій сфері в умовах війни. *Ринкова економіка: сучасна теорія і практика управління*, 21(3(52)), 179-199. <http://rinek.onu.edu.ua/article/download/275802/275060>.

176. Масюк, Ю. В. (2023). Інституційна модернізація фінансових послуг посередників на фондовому ринку. *Інтернаука*, (2), 45–52. <https://www.inter-nauka.com/uploads/public/17407732046650.pdf>.

177. Мезха. Fintech в Україні 2025: проблеми, тренди, інновації (27 берез. 2025). <https://mezha.ua/articles/chim-zhive-ukrajinskiy-fintech-sektor-300651>.

178. Мехед, А. М., & Варналій, З. С. (2021). Фінансова безпека підприємств в умовах цифрової економіки. *Socio-economic relations in the digital society*, 3(42), 55-61. <https://ser.net.ua/index.php/SER/article/download/440/437>.

179. Міжнародний валютний фонд. (2023, 3 жовтня). IMF Releases the 2023 Financial Access Survey Results. <https://www.imf.org/en/news/articles/2023/10/03/pr23332-imf-releases-the-2023-financial-access-survey-results?>

180. Міністерство цифрової трансформації України. (б.д.). *Єдиний державний вебпортал електронних послуг «Дія»*. <https://diia.gov.ua>.

181. Мішустіна, Т., Дубницький, В., & Крабовський, І. (2024). Цифрова трансформація в умовах екосистеми: фактор цифрової зрілості. *Економіка та суспільство*, 70.
<https://economyandsociety.in.ua/index.php/journal/article/download/5490/5429>.
182. Монобанк. (н.д.). Головна сторінка. <https://monobank.ua/>.
183. Національний банк України. (2023). *Концепція е-гривні (проект для громадського обговорення)*. НБУ.
https://bank.gov.ua/admin_uploads/article/Draft_vision_introducing_e-hryvnia_2023.pdf.
184. Національний банк України. (2023). *Регуляторна платформа НБУ («пісочниця»)*. <https://promo.bank.gov.ua/sandbox>.
185. Національний банк України. (б.д.). *Е-гривня : офіційна сторінка проекту*. <https://bank.gov.ua/en/payments/e-hryvnia>.
186. Національний інститут стратегічних досліджень. (2023, липень). Цифрова трансформація економіки України в умовах війни. <https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-lypen-2023>.
187. Національний інститут стратегічних досліджень. (2024, січень). Цифрова трансформація економіки України в умовах війни. <https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-sichen-2024>.
188. Островська, Г. Й. (2024). Сучасні моделі діагностики та оцінки цифрової зрілості підприємства в умовах digital-трансформації. *Вісник економічної науки України*, 2(47), 143–151.
<https://nasplib.isofts.kiev.ua/bitstreams/321a69a3-9913-4b90-aeeb-e2c710c8b3ed/download>.
189. Ощадбанк. (н.д.). Офіційний сайт. <https://www.oschadbank.ua/>.
190. Пантелєєва, Н. М. (2021). Цифрові трансформації фінансового посередництва. *Фінанси, банківська справа та страхування*, (1), 150–161.
<http://dspace.puet.edu.ua/bitstream/123456789/13795/1/1501-2341-1-PB.pdf>.

191. Попело, О., & Кононенко, С. (2026). Основні загрози використання технологій штучного інтелекту та їхній потенційний негативний вплив на функціонування кредитних установ. *Проблеми і перспективи економіки та управління*, (1(45)), 289–300. [https://doi.org/10.25140/2411-5215-2026-1\(45\)-289-300](https://doi.org/10.25140/2411-5215-2026-1(45)-289-300).

192. Попело, О., & Федішин, М. (2024). Оцінка ризиків фінансової стійкості банківської галузі в умовах тривалих викликів. *Економіка та суспільство*, (68). <https://doi.org/10.32782/2524-0072/2024-68-183>.

193. Поцелуйко, І. В., Дубина, М. В., Федорів, Ю. М. (2025). Роль кастомізації у розвитку ринку кредитних послуг. *Науковий вісник Одеського національного економічного університету*, 7-8 (332-333), 101-108.

194. Приватбанк. (н.д.). Офіційний сайт. <https://privatbank.ua/>.

195. Приказюк, Н. В., & Мирончук, А. М. (2024). Регулювання банківської діяльності в Україні у кризові періоди. *Науково-виробничий журнал «Бізнес-навігатор»*, (2(75)), 174–181. https://business-navigator.ks.ua/journals/2024/75_2024/32.pdf.

196. Приказюк, Н. В., & Поліщук, І. В. (2025). Штучний інтелект у трансформації інвестиційної діяльності страхових компаній в умовах цифровізації. *Ефективна економіка*, (11). <https://doi.org/10.32702/2307-2105.2025.11.38%20>.

197. Примостка, Л. О. (2016). Довіра до банків: формування та відновлення. *Фінанси, облік і аудит*, 65-79. <https://kneu.edu.ua/userfiles/arch/16-5194.pdf#page=65>.

198. ПУМБ. (н.д.). Послуги. <https://www.pumb.ua/service>.

199. Рубанов, П. М., Александров, В. Т., Боронос, В. М., Тархов, П. В., Шишова, Ю. Г., Боронос, Д. В., ... & Шкодкіна, Ю. М. (2012). *Оцінка ефективності та оптимізація діяльності фінансових посередників*. Сумський державний університет. <https://essuir.sumdu.edu.ua/bitstream/123456789/32640/1/Rubanov.doc>.

200. Садчикова, І. В., & Євсієнко, М. В. (2025). Цифрова інфраструктура як драйвер розвитку кредитної системи в Україні. *Проблеми і перспективи економіки та управління*, (2), 384–398. [https://doi.org/10.25140/2411-5215-2025-2\(42\)-384-398](https://doi.org/10.25140/2411-5215-2025-2(42)-384-398).
201. Садчикова, І. В., Євтушенко, Ю. В., & Сусленко, С. В. (2023). Системні детермінанти сучасного розвитку кредитного ринку в Україні. *Бізнес Інформ*. № 9. С. 206-212. DOI: <https://doi.org/10.32983/2222-4459-2023-9-206-212>.
202. Садчикова, І. В., Колотило, Л. Л., & Волок, А. Р. (2024). Формування стратегії банківських установ в Україні в умовах цифровізації фінансового ринку та макроекономічної нестабільності. *Актуальні проблеми розвитку економіки регіону*, 2(20), 268-278. <https://journals.pnu.edu.ua/index.php/aprde/article/view/8185>.
203. Семенов, А. Ю., Бричко, М. М., & Семенов, В. В. (2018). Довіра На Ринку Сучасних Фінансових Послуг В Україні Та Світі. *Scientific Bulletin of Kherson State University. Series Economic Sciences*, (32), 167-172. <https://www.ej.journal.kspu.edu/index.php/ej/article/view/438>.
204. Ситник, І. П., & Фоміна, В. С. (2019). Вплив фінтеху на розвиток сучасних платіжних систем України. *Науково-виробничий журнал «Бізнес-навігатор»*, 2(51), 139-143. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/bnav_2019_2_29.pdf.
205. Ситник, Н. С., & Половчак, І. Р. (2024). Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни. *Галицький економічний вісник*, 89(4), 70-81. https://elartu.tntu.edu.ua/bitstream/lib/46455/2/GEJ_2024v89n4_Sytnyk_N-Digitization_and_cyber_security_70-81.pdf.
206. Тарасенко, А. . (2026). Розвиток інфраструктури ринку фінансових послуг в умовах цифровізації. *Проблеми і перспективи економіки та управління*, (1(45), 357–364. [https://doi.org/10.25140/2411-5215-2026-1\(45\)-357-364](https://doi.org/10.25140/2411-5215-2026-1(45)-357-364).

207. Трусова, Н. В., & Чкан, І. О. (2023). Кіберзахист банківської системи України в умовах цифрових трансформацій. *Збірник наукових праць Таврійського державного агротехнологічного університету імені Дмитра Моторного (економічні науки)*, 1(47). <https://oj.tsatu.edu.ua/index.php/zbirnyk/article/download/538/510>.
208. Українська асоціація фінтех та інноваційних компаній (УАФІК). (2025). *Фінтех тренди 2025 : аналітичне дослідження*. УАФІК. https://fintechua.org/fintech_trends_2025.
209. Українська асоціація фінтех та інноваційних компаній (УАФІК). Каталог фінтех-компаній України 2025 / за підтримки НБУ, Мінцифри, ІFC, SECO, GGF. (2025). УАФІК. <https://fintechua.org>.
210. Укргазбанк. (н.д.). Головна сторінка. <https://www.ukrgasbank.com/>.
211. Урікова, О. М., Мисько, Ю. М., & Карий, О. І. (2025). Fintech-індустрія України: драйвери зростання та виклики під час кризи. *Проблеми економіки та управління*, 9(1), 96–111.
212. Ходаківська, В. (2022). Цифрова трансформація ринку фінансових послуг в контексті розвитку FinTech-індустрії. *Наукові перспективи*, 10(28), 208–218. <https://www.academia.edu/100444022>.
213. Чеберяко, О. В., & Лобода, А. Б. (2014). Економічна сутність та призначення фінансових посередників в Україні. *Бізнес Інформ*, (3), 334-340. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/binf_2014_3_57.pdf.
214. Чичкало-Кондрацька, І. Б. (2020). Зарубіжний досвід використання фінансових механізмів стимулювання інноваційного розвитку. *Економіка і організація управління*, (2), 89–97.
215. Чуницька І. І., & Богріновцева Л. М. (2023). Вплив цифрових технологій на розвиток фінансового ринку України. *Економіка та суспільство*, (49). <https://doi.org/10.32782/2524-0072/2023-49-60>.

216. Шабан, О. (20 квіт. 2023). Регуляторна платформа НБУ: «пісочниця» для зростання інновацій. *Інтерфакс-Україна*.
<https://interfax.com.ua/news/blog/905186.html>.

217. Шевченко, О. М., & Рудич, Л. В. (2020). Розвиток фінансових технологій в умовах цифровізації економіки України. *Економічна теорія та економічна кібернетика*, 7(61). <https://doi.org/10.32702/2307-2105-2020.7.61>.

218. Шимановська-Діанич, Л. М., & Лозова, О. В. (2024). Вплив цифрової зрілості на трансформацію бізнес-процесів підприємств в умовах змін економіки України. *Економіка: реалії часу*, 2, 72–78.
<https://economics.net.ua/files/archive/2024/No2/74.pdf>.

219. Шишкіна О. В., Суховерський М. Ю., Даньков А. Ю. Оцінка впливу фінансових інструментів на економічну безпеку підприємств. *Науковий вісник Полісся*. 2025. (1(30)), 160-179. [https://doi.org/10.25140/2410-9576-2025-1\(30\)-160-179](https://doi.org/10.25140/2410-9576-2025-1(30)-160-179).

220. Шишкіна, О. (2023). Вплив фінтех інновацій на глобальні валютні ринки. *Acta Academiae Beregsasiensis. Economics*, (4), 307-320 <https://aab-economics.kmf.uz.ua/aabe/article/view/98/111>.

221. Шишкіна, О. (2023). Проблеми, перспективи і ризики використання цифрових інновацій у фінансовому й реальному секторах національної економіки. *Проблеми і перспективи економіки та управління*, (1(33)), 154-175.
<http://ppeu.stu.cn.ua/article/view/282034/276250>.

222. Шишкіна, О. (2023). Цифрові технології фінансових установ: ризики і перспективи використання. *Актуальні проблеми розвитку економіки регіону*, 19(2), 130–143.
<https://scijournals.pnu.edu.ua/index.php/aprde/article/download/6951/7212>.

223. Шишкіна, О. (2023). Цифрові технології фінансових установ: ризики і перспективи використання. *Актуальні проблеми розвитку економіки регіону*, 19(2), 130 – 143.

224. Шишкіна, О. В., & Волошин, Д. М. (2023). Актуальні типи кіберзагроз функціонування і розвитку фінансових установ. *Економіко-правові та управлінсько-технологічні виміри сьогодення: молодіжний погляд* : матеріали міжнародної науково-практичної конференції (у 3 т. Том 1, с. 258-260). Університет митної справи та фінансів.

225. Шишкіна, О. В., & Волошин, Д. М. (2023). Роль нових технологій у формуванні стратегії розвитку фінансових посередників. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (с. 90-91). НУ «Чернігівська політехніка».

226. Шишкіна, О. В., Волошин, Д. М., & Малихін, А. Г. (2025). Роль фінансових посередників у створенні та впровадженні інноваційних фінансових продуктів в умовах цифровізації. *Збірник наукових праць IV Міжнародної науково-практичної конференції* (Запоріжжя-Мелітополь, 20 травня 2025 р.) (Вип. 14, с. 249-253). Видавництво МДПУ ім. Б. Хмельницького.

227. Шишкіна, О. В., Волошин, Д. М., & Малихін, А. Г. (2025). Стратегічні підходи до інтеграції цифрових рішень у діяльність фінансових посередників на ринку України. *Проблеми і перспективи економіки та управління*, (3(43)), 310-325. [https://doi.org/10.25140/2411-5215-2025-3\(43\)-310-325](https://doi.org/10.25140/2411-5215-2025-3(43)-310-325).

228. Шишкіна, О. В., Волошин, Д. М., & Малихін, А. Г. (2025, 23–25 квітня). Цифровізація економіки як фактор конкурентоспроможності фінансових посередників в Україні. У *Юність науки – 2025: збірник тез доповідей* (с. 107–108). НУ «Чернігівська політехніка». <https://ir.stu.cn.ua/items/7024c8b0-86f3-4ff4-baa0-3548f8c61574>.

229. Шишкіна, О. В., Волошин, Д. М., & Ринжук, Д. Я. (2024). Вплив цифрових технологій на стратегії розвитку фінансових посередників в Україні. *Проблеми і перспективи економіки та управління*, (2(38)), 177-189. <http://ppeu.stu.cn.ua/article/view/314107/305041>.

230. Шишкіна, О. В. (2020). *Механізм управління фінансовими ризиками промислових підприємств: теорія, методологія, практика*. ЧНТУ.

231. Шишкіна, О., Волошин, Д., & Ринжук, Д. (2024, 16 вересня). Роль цифрових технологій у формуванні стратегій розвитку фінансових посередників. У *Соціальне підприємництво як інструмент відновлення України: матеріали конференції* (с. 183–185). НУ «Чернігівська політехніка». <https://stu.cn.ua/wp-content/uploads/2024/09/zbirnyk.pdf>.

232. Шкарлет, С. М., & Дубина, М. В. (2017). Обґрунтування сутності категорії «фінансова довіра». *Науковий вісник Полісся*, 2(4 (12)), 45-52. https://journals.urau.ua/nvp_chntu/article/download/125925/120464.

233. Шкарлет, С. М., Дубина, М. В., & Жук, О. С. (2019). Теоретичні аспекти визначення сутності категорії «Fintech». *Науковий вісник Полісся*, (1(17)), 148-157. <https://ir.stu.cn.ua/jspui/bitstream/123456789/18078/1/148-157.pdf>.

234. Школьник, І. О. (2015). Фінансові посередники та їх роль у розвитку фінансового ринку. *Українська академія банківської справи НБУ*. [Shkolnyk_Finansovi_poserednyky.pdf](https://shkolnyk_finance_poserednyky.pdf);jsessionid=582CF7CBD19A243038841EEBDC75B6C4.

235. Шульга, І. П. (2008). Фінансове посередництво: сутність, функції та механізм здійснення. *Східноєвропейського університету економіки і менеджменту*, 78. <https://visnyksura.com.ua/storage/media/EqQR9JAhZk8Ag4gdMsNsrC7pJcDiN1Ngikn5XrVl.pdf#page=78>.

236. Яровенко, Г. М., & Ковач, В. О. (2020). Перспективи застосування технології блокчейн у системах забезпечення кібербезпеки банків. *Підприємництво та інновації*, (12), 206-214. <http://ejournal.in.ua/index.php/journal/article/download/334/328/>.

ДОДАТКИ

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті в іноземних наукових виданнях: SCOPUS

1. Basiurkina N., Krylov D., Karpinska H., Pchela A., **Voloshyn D.** The Impact of Digitalization on Financial Mechanisms for Managing the Strategic Development of Enterprises in The Face of Modern Challenges. *Pacific Business Review (International)*. 2026. Vol. 18, Issue 9, March. P. 123–136. URL: https://www.pbr.co.in/2026/2025_month/March/11.pdf (1,9 ум. друк. арк.).
Особистий внесок автора: досліджено вплив цифровізації на фінансові механізми стратегічного управління підприємствами в умовах сучасних викликів (0,38 ум. друк. арк.).

Статті у фахових виданнях України

2. Шишкіна О., **Волошин Д.**, Ринжук Д. Вплив цифрових технологій на стратегії розвитку фінансових посередників в Україні. *Проблеми і перспективи економіки та управління*. 2024. № 2(38). С. 177–189. [https://doi.org/10.25140/2411-5215-2024-2\(38\)-177-189](https://doi.org/10.25140/2411-5215-2024-2(38)-177-189) (1,5 ум. друк. арк.).
Особистий внесок автора: здійснено аналіз сучасних цифрових технологій та їх впливу на стратегічний розвиток фінансових посередників в Україні; сформульовано висновки щодо перспектив впровадження цифрових інструментів у діяльність фінансових установ (0,5 ум. друк. арк.).

3. Малихін А., **Волошин Д.** Аналіз ролі фінансових посередників у процесі формування інноваційної інфраструктури ринку цифрових фінансових послуг України. *Науковий вісник Полісся*, 2025. №1 (30), 284–299. [https://doi.org/10.25140/2410-9576-2025-1\(30\)-284-299](https://doi.org/10.25140/2410-9576-2025-1(30)-284-299) (1,9 ум. друк. арк.).
Особистий внесок автора: визначено чинники, що обумовлюють

розвиток цифрового фінансового середовища в Україні; запропоновано підходи до оцінювання інноваційного потенціалу фінансових посередників (0,95 ум. друк. арк.).

4. Шишкіна О. В., **Волошин Д. М.**, Малихін А. Г. Стратегічні підходи до інтеграції цифрових рішень у діяльність фінансових посередників на ринку України. *Проблеми і перспективи економіки та управління*. 2025. № 3(43). С. 310-325. DOI: [https://doi.org/10.25140/2411-5215-2025-3\(43\)-310-325](https://doi.org/10.25140/2411-5215-2025-3(43)-310-325) (1,9 ум. друк. арк.). Особистий внесок автора: обґрунтовано методичні засади оцінювання ефективності цифровізації; сформовано практичні рекомендації щодо впровадження інноваційних технологій (0,65 ум. друк. арк.).

5. Волошин Д. М. Теоретико-методичні аспекти оцінювання цифрової зрілості фінансових посередників. *Успіхи і досягнення у науці*”. 2026. № 4(26) 2026. С. 1119-1132. DOI: [https://doi.org/10.52058/3041-1254-2026-4\(26\)](https://doi.org/10.52058/3041-1254-2026-4(26)) (1,6 ум. друк. арк.).

Публікації, що засвідчують апробацію матеріалів дисертації

6. Шишкіна О. В., **Волошин Д. М.** Роль нових технологій у формуванні стратегії розвитку фінансових посередників. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених* (м. Чернігів, 26-27 квітня 2023 р.). Чернігів : НУ «Чернігівська політехніка», 2023. С. 90-91 (0,1 ум. друк. арк.). Особистий внесок автора: обґрунтовано перспективні напрями технологічного оновлення фінансових установ (0,05 ум. друк. арк.).

7. Шишкіна О. В., **Волошин Д. М.** Актуальні типи кіберзагроз функціонування і розвитку фінансових установ. *Економіко-правові та управлінсько-технологічні виміри сьогодення: молодіжний погляд : матеріали міжнародної науково-практичної конференції* (м. Дніпро, 03 листопада 2023

р.): у 3 т. Том 1. Дніпро : Університет митної справи та фінансів, 2023. С. 258-260 (0,2 ум. друк. арк.). Особистий внесок автора: систематизовано актуальні типи кіберзагроз для фінансових установ та проаналізовано їх вплив на функціонування і розвиток фінансового сектору (0,1 ум. друк. арк.).

8. **Волошин Д., Шишкіна О., Киселиця С.** Етичні виклики цифровізації: філософський аналіз довіри як основи фінансового посередництва. *Соціальне підприємництво як інструмент відновлення України: Форум стейкхолдерів розвитку соціального підприємництва* (м. Чернігів, 16 вересня 2024 р.) : тези доповідей. Чернігів : НУ «Чернігівська політехніка», 2024. С. 90-92. URL: <https://stu.cn.ua/wp-content/uploads/2024/09/zbirnyk.pdf> (0,1 ум. друк. арк.). Особистий внесок автора: здійснено аналіз етичних викликів, пов'язаних із цифровізацією фінансового посередництва (0,03 ум. друк. арк.).

9. Шишкіна О., **Волошин Д., Ринжук Д.** Роль цифрових технологій у формуванні стратегій розвитку фінансових посередників. *Соціальне підприємництво як інструмент відновлення України: Форум стейкхолдерів розвитку соціального підприємництва* (м. Чернігів, 16 вересня 2024 р.) : тези доповідей. – Чернігів : НУ «Чернігівська політехніка», 2024, С. 183-185. URL: <https://stu.cn.ua/wp-content/uploads/2024/09/zbirnyk.pdf> (0,2 ум. друк. арк.). Особистий внесок автора: обґрунтовано взаємозв'язок між рівнем цифровізації та конкурентоспроможністю фінансових установ (0,06 ум. друк. арк.).

10. Шишкіна О. В., **Волошин Д. М.,** Малихін А. Г., Цифровізація економіки як фактор конкурентоспроможності фінансових посередників в Україні. *Юність науки – 2025* : збірник тез доповідей XV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 23-25 квітня 2025 р.). Чернігів : НУ «Чернігівська політехніка», 2025. С. 107-108 <https://ir.stu.cn.ua/items/7024c8b0-86f3-4ff4-baa0-3548f8c61574> (0,1 ум. друк. арк.). Особистий внесок автора: визначено ключові цифрові фактори підвищення ринкових позицій фінансових установ (0,03 ум. друк. арк.).

11. Шишкіна О. В., **Волошин Д. М.**, Малихін А. Г. Роль фінансових посередників у створенні та впровадженні інноваційних фінансових продуктів в умовах цифровізації. *Збірник наукових праць IV міжнародної науково-практичної конференції (Запоріжжя-Мелітополь, 20 травня 2025 р., МДПУ імені Богдана Хмельницького)*. Запоріжжя: Видавництво МДПУ ім. Б. Хмельницького, 2025. С. Випуск 14. С. 249-253 (0,3 ум. друк. арк.). Особистий внесок автора: проаналізовано роль фінансових посередників у розробці та впровадженні інноваційних фінансових продуктів в умовах цифрової трансформації (0,1 ум. друк. арк.).

Довідки про впровадження

АТ Райффайзен Банк

Внес. №5 від 01.05.2026 р.

**Довідка
про впровадження результатів дисертаційного дослідження
Волошина Дмитра Миколайовича на тему:
«Формування стратегії розвитку фінансових посередників в умовах
цифровізації економіки»**

АТ «Райффайзен Банк» розглянуто результати наукового дослідження аспіранта Національного університету «Чернігівська політехніка» (спеціальність 072 «Фінанси, банківська справа та страхування») Волошина Д.М. та частково враховано при запровадженні інформаційних кампаній для клієнтів щодо безпечного користування цифровими кредитними продуктами; підвищення обізнаності клієнтів щодо ризиків шахрайства при дистанційному отриманні кредитів. А також в удосконаленні напрямків інтеграції навчальних модулів у мобільний застосунок банку (push-повідомлення, чек-листи, чат-бот).

Цікавою та практично-орієнтованою є авторська методика оцінювання цифрової зрілості фінансових посередників (DCMI), яка дозволяє діагностувати рівень цифровізації за шістьма ключовими вимірами (технологічна інфраструктура, процесна зрілість, клієнтська взаємодія, інноваційна спроможність, кіберстійкість, регуляторна відповідність). Окремі положення цієї методики враховано при проведенні внутрішнього аудиту цифрових каналів обслуговування.

Керівник з роздрібного бізнесу
АТ Райффайзен Банк
Перше міське відділення
М. Чернігів



Тунік М.В.

Приватне акціонерне товариство «Страхова компанія «ПЗУ Україна».
 Адреса для листування: вул. Дегтярська, 62, м. Київ, 04112, Україна. Тел.: (044) 238 62 38, факс: (044) 581 04 55. E-mail: for-pzu@pzu.com.ua.
 Місцезнаходження: вул. Січових Стрільців, 40, м. Київ, 04053, Україна.
 Код ЄДРПОУ 20782312. IBAN UA473808380000026500700014791 в АТ «ПРАВЕКС-БАНК»



Вих № 2 від « 13 » травня 2026 р.

Довідка

**про впровадження результатів дисертаційного дослідження
 Волошина Дмитра Миколайовича на тему: «Формування стратегії
 розвитку фінансових посередників в умовах цифровізації економіки»
 (спеціальність 072 «Фінанси, банківська справа та страхування»)**

Результати дисертаційного дослідження Волошина Д.М. були використані в діяльності ПрАТ СК «ПЗУ Україна» при вдосконаленні підходів до цифровізації страхових послуг та управління операційною стійкістю. Зокрема, часткове практичне застосування отримали рекомендації здобувача: щодо впровадження цифрових технологій для персоналізації страхових продуктів (сегментація клієнтів на основі AI/Big Data, кастомізація страхових послуг, інтеграція API-рішень); щодо підвищення кіберстійкості (аналіз типів кіберзагроз для фінансових установ, рекомендації щодо захисту цифрових каналів обслуговування).

Запропоновані підходи також було враховано при розробці стратегії цифровізації ПрАТ СК «ПЗУ Україна», що дало змогу підвищити рівень задоволеності споживачів цифровими страховими продуктами і скоротити час обробки заяв про страхові випадки.

Директор РО в м. Чернігів



МІНІСТЕРСТВО ОСВІТИ І
НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

вул. Шевченка, 95, Чернігів, 14035,
Україна



тел. +38(0462) 665-103;
факс +38(0462) 665-105
E-mail: estu@stu.cn.ua
www.stu.cn.ua
Код ЄДРПОУ 05460798

MINISTRY OF EDUCATION AND
SCIENCE OF UKRAINE

CHernihiv Polytechnic National
UNIVERSITY

95, Shevchenko str., Chernihiv, 14035,
Ukraine

12.05.2026 № 202/22-РЗР
На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційної роботи
Волошина Дмитра Миколайовича на тему:
«Формування стратегії розвитку фінансових посередників в
умовах цифровізації економіки»

Основні теоретико-методичні положення та висновки щодо стратегічного розвитку фінансових посередників в умовах цифрової економіки, що розроблені в рамках підготовки дисертації Волошина Дмитра Миколайовича з метою отримання ступеня доктора філософії за спеціальністю 072 «Фінанси, банківська справа та страхування», використані у навчальному процесі кафедри фінансів, банківської справи та страхування Національного університету «Чернігівська політехніка» при розробці методичних матеріалів, а також під час проведення лекційних та практичних занять з наступних навчальних дисциплін: «Банківські операції», «Страховий менеджмент», «Банкострахування».

Ректор



Олег НОВОМЛИНЕЦЬ