

8. Nayve R. M. Jr., Sistoso R., Timbang F. Resilience and Diversity in Financial Economics: A Paradigm Shift towards Ecological Finance Theory. *Jurnal Ilmu Ekonomi dan Manajemen*. 2024. Vol. 11. No. 1. P. 69–78. DOI: <https://doi.org/10.30996/jmm17.v11i1.10820>

REFERENCES

- Łasak P. & Wyciślak S. (2022). Dynamics in Complex Systems Amidst Crisis 2008+: Financial Regulatory and Supervisory Reflections. *Risks*, 2(10), Art. 33. <https://doi.org/10.3390/risks10020033>
- Gutiérrez-López C. & Abad-González J. (2020). Sustainability in the Banking Sector: A Predictive Model for the European Banking Union in the Aftermath of the Financial Crisis. *Sustainability*, 6(12), Art. 2566. <https://doi.org/10.3390/su12062566>
- Khalif J. (2024). The Effect of Macroprudential Policies on Financial Stability. *International Journal of Finance*, 5(9). <https://doi.org/10.47941/ijf.2140>
- Morin S. L. (2025). Regulating for Resilience: Addressing Bank Failures through Enhanced Oversight. *Financial Markets, Institutions and Risks*, 1(9), 43–58. [https://doi.org/10.61093/fmir.9\(1\).43-58.2025](https://doi.org/10.61093/fmir.9(1).43-58.2025)

- Nayve R. M. Jr., Sistoso R. & Timbang F. (2024). Resilience and Diversity in Financial Economics: A Paradigm Shift towards Ecological Finance Theory. *Jurnal Ilmu Ekonomi dan Manajemen*, 1(11), 69–78. <https://doi.org/10.30996/jmm17.v11i1.10820>
- Olulun T. M. (2024). The Impact of Enterprise Risk Management (ERM) on Firm Value in Times of Economic Crisis. *International Journal of Research Publication and Reviews*, 10(5), 242–255. <https://doi.org/10.55248/gengpi.5.1024.2711>
- Oluloni T. M. (2024). ERM Strategies for Navigating Financial Stress: Lessons from US Commercial Banks. *Finance & Accounting Research Journal*, 10(6), 1861–1880. <https://doi.org/10.51594/farj.v6i10.1634>
- Papushvili D. (2023). Cyber Resilience Implications for the Financial System. *Business Administration Research Papers*, 8(a). <https://doi.org/10.62232/barp.8.2023.6774>

Стаття надійшла до редакції / Received: 06.02.2026
Статтю прийнято до публікації / Accepted: 20.02.2026
Оприлюднено / Published: 31.03.2026

УДК 336.71:004.738.5
JEL: G21; G29
DOI: <https://doi.org/10.32983/2222-4459-2026-2-274-282>

ЦИФРОВІЗАЦІЯ БАНКІВСЬКОЇ СИСТЕМИ ТА РОЗВИТОК ОНЛАЙН-БАНКІНГУ

©2026 БЛАЩУК-ДЕВ'ЯТКІНА Н. З., КОЧІШ Т. Р., ГАЛЬЧУК Х. А.

УДК 336.71:004.738.5
JEL: G21; G29

Блащук-Дев'яткіна Н. З., Кочіш Т. Р., Гальчук Х. А. Цифровізація банківської системи та розвиток онлайн-банкінгу

У статті було розглянуто сутність і роль цифровізації банківського сектора як визначального фактора конкурентоспроможності фінансових інститутів у контексті переходу до цифрової економіки. Проаналізовано трансформацію традиційних банківських моделей у цифрові екосистеми, що базуються на дистанційному обслуговуванні, використанні штучного інтелекту та аналізі великих даних (Big Data). Особливу увагу приділено зміні споживчої поведінки, де доступність послуг через смартфон стала базовою потребою клієнта, що підтверджується зростанням рівня застосування мобільних застосунків та готовністю українців до повного переходу на цифровий банкінг. Визначено роль інструментів цифрової трансформації, таких як BankID НБУ та платіжні POS-термінали, у формуванні фізичного та технологічного фундаменту цифрової інфраструктури, що дозволило банкам оптимізувати операційні витрати через скорочення мережі відділень. Оцінено ефективність використання чат-ботів та ШІ-агентів у клієнтській підтримці на прикладі провідних українських банків. Водночас ідентифіковано ключові виклики та ризики, зокрема загрози кібербезпеці, проблему «цифрового розриву» та необхідність адаптації нормативно-правового регулювання до нових технологічних реалій. Отримані результати підтверджують, що успіх банківського бізнесу сьогодні залежить від здатності фінансових установ знайти баланс між інноваційною персоналізацією послуг і високим рівнем кіберстійкості. На основі проведеного аналізу обґрунтовано, що подальша еволюція банківського сектора пов'язана з упровадженням концепції Open Banking і розширенням екосистем вбудованих фінансів (embedded finance). Сформульовані висновки та рекомендації можуть бути використані банківськими установами для вдосконалення стратегій цифрової трансформації, а також державними регуляторами при розробці нормативної бази для забезпечення стабільності та інклюзивності цифрового фінансового середовища в Україні.

Ключові слова: цифровізація банківської системи, онлайн-банкінг, цифрова трансформація, мобільний банкінг, ШІ, кібербезпека, фінансова інклюзія, безготівкові розрахунки.

Рис.: 2. **Табл.:** 1. **Бібл.:** 13.

Блащук-Дев'яткіна Наталія Зіновіївна – доктор економічних наук, доцентка кафедри фінансового менеджменту, Львівський національний університет імені Івана Франка (вул. Університетська, 1, Львів, 79001, Україна)
E-mail: nataliya.blashchuk-devyatkina@lnu.edu.ua
ORCID: <https://orcid.org/0000-0003-1860-3929>

Кочіш Тетяна Романівна – студентка факультету управління фінансами та бізнесу, Львівський національний університет імені Івана Франка (вул. Університетська, 1, Львів, 79001, Україна)

ORCID: <https://orcid.org/0009-0008-3851-0299>

Гальчук Христинна Андріївна – студентка факультету управління фінансами та бізнесу, Львівський національний університет імені Івана Франка (вул. Університетська, 1, Львів, 79001, Україна)

ORCID: <https://orcid.org/0009-0005-3627-3769>

UDC 336.71:004.738.5

JEL: G21; G29

Blashchuk-Deviatkina N. Z., Kochish T. R., Halchuk K. A. The Digitalization of the Banking System and the Development of Online Banking

The article explores the essence and role of digitalization in the banking sector as a key factor in the competitiveness of financial institutions within the context of the transition to a digital economy. The authors analyzed the transformation of traditional banking models into digital ecosystems based on remote services, the use of artificial intelligence, and big data analytics. Particular attention was given to changes in consumer behavior, where the accessibility of services via smartphones has become a fundamental customer need, as evidenced by the growing use of mobile applications and the readiness of Ukrainians to fully transition to digital banking. The article also highlighted the role of digital transformation tools, such as the NBU BankID and POS payment terminals, in establishing the physical and technological foundation of digital infrastructure, which has enabled banks to optimize operational costs by reducing branch networks. The effectiveness of using chatbots and AI agents in customer support was evaluated based on leading Ukrainian banks. At the same time, key challenges and risks were identified, including cybersecurity threats, the «digital divide», and the need to adapt regulatory frameworks to new technological realities. The results confirm that the success of the banking business today depends on the ability of financial institutions to balance innovative service personalization with a high level of cyber resilience. Based on the conducted analysis, it is substantiated that the further evolution of the banking sector is linked to the implementation of the Open Banking conception and the expansion of embedded finance ecosystems. The formulated conclusions and recommendations can be used by banking institutions to refine digital transformation strategies, as well as by State regulators when developing the regulatory framework to ensure the stability and inclusiveness of Ukraine's digital financial environment.

Keywords: digitalization of the banking system, online banking, digital transformation, mobile banking, AI, cybersecurity, financial inclusion, cashless payments. **Fig.:** 2. **Tabl.:** 1. **Bibl.:** 13.

Blashchuk-Deviatkina Nataliia Z. – D. Sc. (Economics), Associate Professor of the Department of Financial Management, Ivan Franko National University of Lviv (1 Universytetska Str., Lviv, 79001, Ukraine)

E-mail: nataliya.blashchuk-devyatkina@lnu.edu.ua

ORCID: <https://orcid.org/0000-0003-1860-3929>

Kochish Tetiana R. – Student of the Faculty of Finance Management and Business, Ivan Franko National University of Lviv (1 Universytetska Str., Lviv, 79001, Ukraine)

ORCID: <https://orcid.org/0009-0008-3851-0299>

Halchuk Khrystyna A. – Student of the Faculty of Finance Management and Business, Ivan Franko National University of Lviv (1 Universytetska Str., Lviv, 79001, Ukraine)

ORCID: <https://orcid.org/0009-0005-3627-3769>

У сучасних умовах глобалізації та стрімкого технологічного розвитку цифрова трансформація стає визначальним фактором конкурентоспроможності фінансових інститутів. Традиційні банківські моделі поступово втрачають актуальність, поступаючись місцем екосистемам, що базуються на дистанційному обслуговуванні, використанні штучного інтелекту та Big Data.

Основна проблема полягає в суперечності між необхідністю швидкого впровадження інноваційних інструментів онлайн-банкінгу для задоволення потреб клієнтів та недостатнім рівнем адаптації нормативно-правового регулювання, а також зростаючими ризиками кібербезпеки. Відсутність єдиних стандартів цифровізації та нерівномірність технологічного розвитку банків створюють бар'єри для формування цілісного цифрового фінансового простору.

Теоретичне підґрунтя переходу до нових економічних моделей та бібліометричний аналіз галузі дослідили у своїх працях Ситник Н. С., Назаркевич І. Б., Мицишин О. Я. та інші, які довели, що

цифрові екосистеми стали стратегічним імперативом для виживання фінансових інститутів. Питання еволюції споживчої поведінки та концепцію «Mobile-First» досліджували N. Miachon, McKinsey and Company та експерти Mastercard, які підтвердили готовність українців до повної відмови від фізичних відділень, тоді як A. Clamp, L. Allen (KPMG) та М. Беркаль зосередилися на впровадженні штучного інтелекту та чат-ботів для створення гіперперсоналізованого сервісу.

Водночас окремий пласт робіт присвячений критичним викликам безпеки, де Р. Мирончук, аналітики «IT-Premium», «Фінансового клубу», «Слово і Діло» та керівництво «ПриватБанку» дослідили вразливість цифрових моделей до хакерських атак, а Національний банк України визначив напрями посилення регуляторного нагляду для забезпечення кіберстійкості всієї фінансової системи.

Стрімка інтеграція інноваційних рішень у повсякденне життя докорінно змінила споживчу поведінку, перетворивши доступність банківських

послуг через смартфон із додаткової переваги на базову потребу клієнта.

Активізація використання сервісів є частиною масштабніших зрушень, спричинених Четвертою промисловою революцією, яка принесла трансформаційні зміни в усі галузі економіки. Саме банківський сектор опинився в епіцентрі цих процесів, ставши головним майданчиком для реалізації цифрової трансформації – стратегічного переосмислення фінансових послуг через упровадження інноваційних практик. Така трансформація виходить далеко за межі звичайної комп'ютеризації, оскільки передбачає повну, клієнтоорієнтовану перебудову організаційних процесів для задоволення динамічних запитів ринку [1, с. 78].

Виклики в галузі ще більше посилюються через активний розвиток фінтех-компаній, які пропонують гнучкі та технологічно орієнтовані альтернативи класичним фінансовим інструментам. Традиційні банківські моделі, що базувалися на паперовому документообігу та фізичній присутності клієнта в касі, хоч і зберігають певну довіру завдяки особистому спілкуванню, дедалі частіше програють у швидкості та вартості обслуговування. Пошук ефективніших рішень зумовив перехід до електронних технологій, таких як інтернет-банкінг, мобільні застосунки та термінали самообслуговування, що забезпечили доступність послуг у режимі 24/7 та суттєву оптимізацію витрат [1, с. 78].

Проте цифровізація не обмежується лише впровадженням ІТ-систем – це глибинна трансформація бізнес-моделей, організаційної структури та культури банку, що вимагає стратегічних змін у всіх ланках діяльності. Цифрова трансформація (ЦТ), хоча й не є новою концепцією, однак вона зуміла привернути значну увагу з початку 2000-х років, коли розпочалися дискусії про Четверту промислову революцію. Сучасний технологічний прогрес зробив її критично важливою проблемою для фінансових установ, які прагнуть підтримувати конкурентоспроможність у банківській сфері [2].

Мобільний банкінг вперше з'явився у 1999 році, пропонуючи базові послуги (такі як запити балансу) через SMS-канали, та революціонував як спосіб управління фінансами в режимі реального часу завдяки інноваційним досягненням у розробці додатків, API відкритого банкінгу та високошвидкісному Wi-Fi-з'єднанню. Ці інновації, включно з платежами між користувачами (P2P), біометричною автентифікацією та штучним інтелектом (ШІ), значно підвищили безпеку та створили безперебійний користувацький досвід. Мобільний зв'язок зараз є воротами до повсякденного банківського обслуговування для

зростаючої більшості споживачів на різних ринках. Тому банкам необхідно розробляти свою систему дистрибуції таким чином, щоб вона лідирувала в мобільному бізнесі [3].

Сьогодні споживачі очікують доступу до фінансових послуг у режимі реального часу, який передбачає гіперперсоналізований досвід, що дозволить їм автоматизувати оплату рахунків, встановлювати цілі заощаджень, інвестувати та складати бюджет тощо. Саме це сьогодні має надзвичайно високий попит у користувачів [3].

Це питання досліджувалося в різних регіонах світу. Зокрема, у В'єтнамі ЦТ у банківському секторі стала стратегічним імперативом для підвищення конкурентоспроможності та задоволення потреб клієнтів. Її виділяють як важливу тенденцію для посилення конкурентних можливостей, максимізації операційної ефективності та покращення адаптивності до ринку, особливо в епоху після COVID-19. У Греції рівень впровадження цифрового банкінгу в банківському секторі був високо оцінений завдяки опитуванням, проведеним серед співробітників грецьких банків (Kitsios et al., 2021). Аналогічно, дослідження, проведене в північній Індії, було зосереджено на ризиках, які цифровий банкінг створює для задоволеності клієнтів, використовуючи опитування клієнтів щодо цифрових послуг (Kaur et al., 2021) [2].

В Україні канали взаємодії з клієнтами в банківській сфері значно розвинулися завдяки інструментам ЦТ, таким як банкомати, термінали самообслуговування та мобільний банкінг. Тому управління технологіями було визначено дослідженням як вирішальний фактор, що впливає на ЦТ у банківській справі, причому ефективне управління технологіями стимулює ініціативи ЦТ і покращує банківську діяльність [2].

В українських реаліях це підтверджується динамікою скорочення кількості мережі відділень банків (рис. 1). Зменшення кількості філій відбулося в усіх групах банків, крім іноземних. Найбільше підрозділів закрили у Дніпропетровській, Донецькій областях і Києві. Кількість структурних підрозділів банків за 2021–2025 роки зменшилася на 36,07%, що свідчить про успішне заміщення традиційних каналів обслуговування інструментами ЦТ, зокрема мобільним банкінгом, що дозволяє банкам не лише задовольняти потреби клієнтів у доступі 24/7, а й суттєво оптимізувати операційні витрати, підвищуючи свою конкурентоспроможність порівняно з фінтех-альтернативами [4].

Цей процес супроводжується дзеркальним зростанням цифрової активності. Зокрема, за підсумками 2025 року кількість успішних ідентифіка-

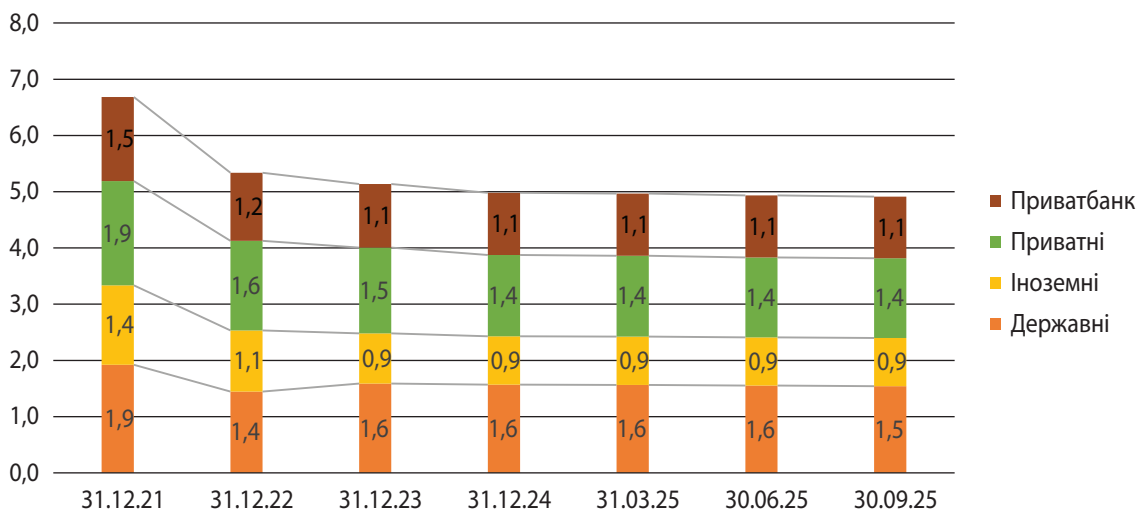


Рис. 1. Кількість структурних підрозділів банків*, тис. од.

Примітка: * – відокремлені структурні підрозділи та головні офіси.

Джерело: побудовано за [4].

цій у Системі BankID НБУ досягла рекордної позначки у 109,4 млн од., що на 25% перевищує показники попереднього року [5]. Це підтверджує, що дистанційна ідентифікація стала повноцінною альтернативою фізичному відвідуванню банку. Розширення функціоналу системи (верифікація віку, посилена безпека) та інтеграція з державними сервісами, такими як «Дія», «Резерв+», остаточно закріпили за онлайн-банкінгом статус базового середовища фінансової життєдіяльності, що корелює з висновками Kaug et al. (2021) щодо визначальної ролі цифрових послуг у задоволеності сучасних клієнтів [2].

Окрім цього, процес трансформації банківського сектора знаходить своє відображення також в динаміці споживчих уподобань. Згідно з дослідженням Mastercard (05.02.23), створеним на основі онлайн-опитування листопада – грудня 2022, готовність понад половини українців (51%) повністю перейти на цифровий банкінг без відвідування фізичних відділень є логічним підґрунтям для оптимізації банківських мереж, зафіксованої у звітах регулятора. Високий рівень проникнення мобільних додатків (75%) і запит на інтегроване управління рахунками в межах одного інтерфейсу (52%) свідчать про те, що український споживач уже зараз формує попит на архітектуру Open Banking. Це перетворює цифровізацію з інструменту зручності на стратегічний фактор стійкості. Адже зараз існує потреба в безперебійному доступі до банківських рахунків та ідентифікації особи в дистанційному режимі, що є критичним для функціонування фінансової системи в умовах надзвичайних викликів [6].

Паралельно з розвитком дистанційної ідентифікації та зміною споживчих уподобань спостерігається інтенсивне розширення інфраструктури безготівкових розрахунків, що є фізичним фундаментом цифрової економіки. Згідно з даними звіту НБУ, кількість платіжних POS-терміналів в Україні зросла з 439,2 тис. од. на кінець 2021 р. до 590,8 тис. од. станом на вересень 2025 р., що становить приріст у 34,5%. У III кварталі лідерами приросту були компанія «НоваПей» та приватні банки (+7,8 тис. і +6,5 тис. од. відповідно). Також серед лідерів зростання традиційно був «ПриватБанк», який забезпечує понад 58% усієї термінальної мережі країни (343 тис. пристроїв). Таке масштабування точок прийому карток безпосередньо корелює з даними Mastercard щодо готовності українців до повної цифровізації свого фінансового життя (рис. 2)[4; 6].

Розширення мережі POS-терміналів у поєднанні з новими гравцями на ринку, зокрема NovaPay, чия частка в категорії «Інші» динамічно зростає, не лише підтримує високу частоту щоденних цифрових операцій, що складає 31% респондентів, а й створює безбар'єрне середовище, де відсутність фізичного банківського відділення повністю компенсується доступністю платіжних сервісів у кожній точці продажу [4].

Спостерігаючи значне зростання кількості терміналів у магазинах, вибір населенням мобільних додатків замість кас, стає зрозуміло, що за цим стоять потужні технології. Сьогоднішні банківські послуги стають зручнішими завдяки застосуванню цифрових інструментів, які роблять застосунки «розумнішими» та безпечнішими. Головна ідея

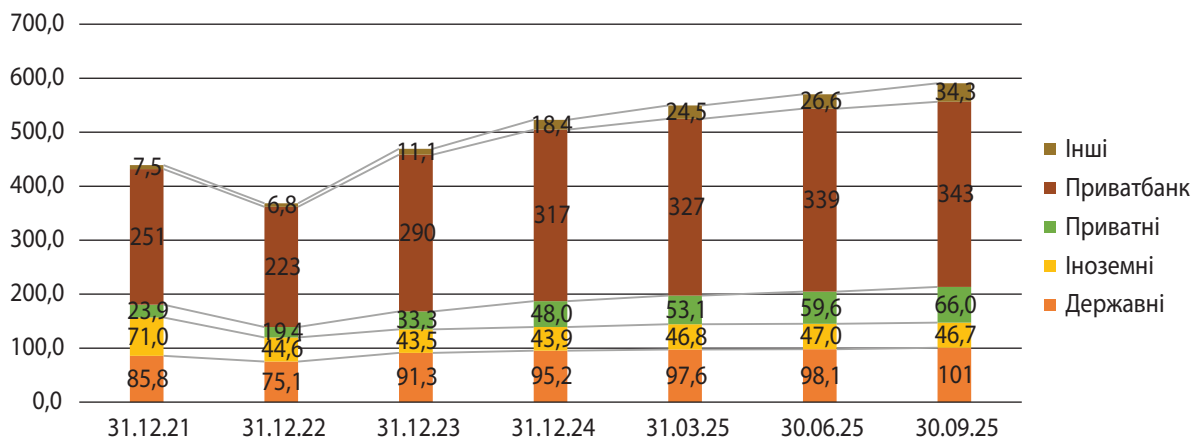


Рис. 2. Кількість платіжних терміналів (POS), тис. од.

Джерело: побудовано за [4].

полягає в тому, що банк підлаштовується під кожного клієнта особисто. Для цього використовують системи, що аналізують великі обсяги інформації та допомагають пропонувати саме ті послуги, які потрібні користувачу в даний момент.

Важливу роль відіграють також нові способи захисту грошей, оскільки більшість користувачів потребують дистанційного користування банківськими послугами. Так, на зміну звичайним паролем приходять відбитки пальців, сканування обличчя та технології захищених записів (блокчейн), які практично неможливо підробити. Завдяки цьому онлайн-банк стає не просто зручною програмою в телефоні, а надійним сейфом, який завжди під рукою. Це і є основою для того, щоб банки в майбутньому стали повністю цифровими.

Глобальні тенденції, викладені у звіті KPMG «Intelligent Banking Report 2025», підтверджують, що наступним етапом розвитку онлайн-банкінгу є перехід до концепції «інтелектуального банку». Це передбачає використання штучного інтелекту не просто для автоматизації відповідей, а для створення гіперперсоналізованого досвіду [7].

Сучасна трансформація банківського сектора базується на переході до моделі «інтелектуального банку», де ШІ стає ключовим елементом операційної ефективності. Згідно з даними KPMG, вже 70% комерційних банків застосовують ШІ у критичних функціях, як-от кредитний скоринг і моніторинг ризиків, причому 78% установ фіксують позитивне повернення інвестицій (ROI) вже протягом перших 18 місяців. В українській практиці цей тренд знаходить відображення у глибокій автоматизації контакт-центрів, де використання голосових ботів та автономних агентів (Agentic AI) дозволяє обробляти до 75% клієнтських звернень без участі персоналу [7].

Такі системи можуть виконувати базові операції, наприклад перевіряти баланс рахунку, блокувати або розблокувати картки та надавати інформацію про банківські послуги. Практика показує, що використання ШІ дозволяє обробляти до 75% звернень клієнтів автоматично, що значно знижує навантаження на персонал і скорочує операційні витрати банку. Крім того, ШІ здатний аналізувати великі обсяги даних клієнтів, що підвищує точність обслуговування та персоналізацію банківських послуг [7].

Іншим стратегічним напрямом визначено використання ШІ для модернізації цифрових каналів (96% банків) та впровадження так званих вбудованих фінансів (*embedded finance*). Завдяки аналізу великих даних банки переходять до гіперперсоналізації, де ШІ-інструменти створюють індивідуальні маркетингові стратегії та контент, що максимально відповідає запитам конкретної аудиторії. Однак таке стрімке технологічне розширення, за якого 52% взаємодій уже здійснюються віртуальними асистентами, неминуче актуалізує питання довіри та безпеки. Поява нових ризиків, пов'язаних із дипфейками та маніпуляціями даними, змушує фінансові інститути інвестувати не лише в розвиток алгоритмів, а й у створення потужних систем кіберзахисту. Таким чином, успіх цифрової трансформації сьогодні залежить від здатності банку знайти баланс між інноваційною персоналізацією послуг та надійним правовим і технічним регулюванням використання штучного інтелекту [7].

Перехід до інтелектуальних систем знаходить своє практичне відображення у функціонуванні систем клієнтської підтримки провідних українських фінансових установ. Зокрема, аналіз досвіду п'яти найбільших банків України – ПриватБанк, Ощад-

банк, Monobank, Sense Bank та ПУМБ – дозволяє оцінити реальний рівень впровадження автоматизованих алгоритмів у щоденну комунікацію з користувачами.

Практично всі великі українські банки використовують автоматизовані системи підтримки клієнтів, що дозволяє швидко надавати інформацію та обробляти запити користувачів.

Аналіз показав, що банківські чат-боти можна умовно поділити на три основні типи [8] (табл. 1).

сервісів для всіх верств населення вкрай актуальним. Водночас швидкість появи нових технологій, як-от ШІ чи блокчейн, вимагає від держави негайної адаптації законів і правил, щоб нові реалії ринку залишалися в межах правового поля та гарантували безпеку всім учасникам процесу.

Важливим етапом у забезпеченні цифрової стійкості фінансового сектора стала активізація регуляторного нагляду з боку Національного банку України. Зокрема, затверджений на 2026 рік план

Таблиця 1

Основні типи банківських чат-ботів та приклади їх застосування

| Назва банку | Тип системи | Характеристика системи |
|----------------------|----------------------------------|---|
| Monobank, Sense Bank | Комбіновані системи | Поєднують автоматичні відповіді з підтримкою живих операторів |
| ПриватБанк | Повністю автоматизовані чат-боти | Працюють виключно на основі алгоритмів або штучного інтелекту |
| Ощадбанк, ПУМБ | Інформаційні чат-боти | Переважно перенаправляють клієнта до відповідних розділів меню або бази знань |

Джерело: складено за [8].

На нашу думку, найбільш ефективними з точки зору зручності користування виявилися Monobank та Sense Bank, оскільки вони використовують змішану модель роботи, яка дозволяє клієнтам отримати допомогу не лише від автоматизованої системи, але й від реального співробітника банку. Це підвищує якість обслуговування та забезпечує можливість уточнення складних питань [8].

Разом із тим, у деяких банках чат-боти мають обмежений функціонал. Наприклад, користувачам необхідно самостійно переходити між пунктами меню для отримання інформації, що знижує зручність використання таких сервісів. Також виявлено проблеми з точністю відповідей і мовними помилками в деяких автоматизованих системах [8].

Попри очевидні переваги та стрімке впровадження інновацій, цифрова трансформація банківського сектора несе в собі низку складних викликів, які можуть стати перешкодою для стабільного розвитку. Оскільки фінансове життя клієнтів майже повністю перейшло у віртуальний простір, на перший план виходять питання кібербезпеки та надійного захисту персональних даних, адже будь-яка вразливість системи ставить під загрозу не лише кошти, а й довіру до всього банківського інституту.

Окрім технічних загроз, існує проблема «цифрового розриву», коли частина населення, особливо старше покоління або мешканці віддалених регіонів, може залишитися без доступу до сучасних послуг через брак навичок або інфраструктури. Це робить питання фінансової інклюзії та доступності

візних перевірок банків із питань інформаційної безпеки та кіберзахисту свідчить про перехід держави до жорсткого аудиту технологічних систем. Такі заходи охоплюють не лише контроль за збереженням коштів, а й перевірку якості електронних довірчих послуг, що є критично важливим в умовах масового переходу клієнтів на дистанційне обслуговування. Це підкреслює необхідність синхронізації темпів технічного розвитку банків із рівнем їхньої кіберстійкості, де державний контроль виступає гарантом захисту персональних даних і стабільності всього цифрового фінансового простору [9].

У сучасних умовах цифровізації фінансового сектора значно зростає роль кібербезпеки, оскільки використання цифрових технологій та штучного інтелекту в банківській системі одночасно створює нові можливості та підвищує рівень кіберризиків. Україна після початку повномасштабної війни стала одним із найбільш атакованих кіберпросторів у світі, що безпосередньо впливає на діяльність фінансових установ та бізнесу загалом. У 2025 році в Україні було зафіксовано понад 4315 кіберінцидентів, що приблизно на 70% більше, ніж до початку повномасштабного вторгнення. При цьому близько 38% усіх атак спрямовані на приватний сектор, включно з фінансовими установами та компаніями, що використовують цифрові фінансові сервіси [9].

Здійснені кіберзлочини були завдяки найпоширенішому способу – фішингу, який становить

понад 60% початкових точок проникнення в інформаційні системи компаній. Суттєво зростає також кількість ransomware-атак (програм-шифрувальників), які у 2025 році збільшилися приблизно на 45% порівняно з попереднім роком [9].

Реалії 2024–2026 років свідчать, що навіть найсучасніші системи захисту стикаються з безпрецедентним тиском. Найбільш вразливою виявилася модель «Digital-only», що підтвердила масштабна хакерська атака на А-Банк у січні 2026 року. Інцидент призвів до критичного збою в роботі мобільного застосунка, залишивши тисячі клієнтів без доступу до платежів. Схожі виклики подолали й інші лідери ринку: так, під час масованих атак наприкінці 2024 та на початку 2025 років «ПриватБанк» та «Ощадбанк» фіксували пікові навантаження на свої системи, що подекуди вимірювалися сотнями мільйонів запитів на секунду (DDoS-атаки). Навіть ПУМБ, маючи потужну IT-інфраструктуру, змушений був посилювати заходи безпеки через технічні збої в партнерів, таких як телеком-оператор «Київстар». Атака на останнього у 2024 році стала найбільш масштабною в історії України, на певний час паралізувавши роботу частини банкоматів та терміналів по всій країні [10; 11].

За даними керівництва «ПриватБанк», з початку повномасштабної війни банк зазнав понад 1,5 млн кібератак, що означає тисячі атак щодня на його інформаційні системи. Така інтенсивність атак пояснюється значною роллю банку у фінансовій системі держави та масштабом його операційної діяльності. Фінансова установа обробляє приблизно 60 тис. транзакцій щохвилини, що робить її важливим елементом платіжної інфраструктури країни та одночасно привабливою мішенню для кіберзлочинців [12].

З метою підвищення кіберстійкості банк впроваджує сучасні підходи до інформаційної безпеки. Зокрема, використовується принцип «нульової довіри» (Zero Trust), який передбачає доступ працівників лише до тих систем і даних, що необхідні для виконання їхніх функціональних обов'язків. Така модель безпеки дозволяє знизити ризики внутрішніх і зовнішніх загроз та підвищити контроль над доступом до критично важливої інформації [12].

Крім того, банк регулярно проводить тестування на вразливість інформаційних систем, залучаючи незалежних міжнародних експертів. Це дозволяє своєчасно виявляти потенційні слабкі місця у цифровій інфраструктурі та оперативно впроваджувати необхідні заходи захисту [12].

Таким чином, досвід «ПриватБанку» демонструє, що в умовах війни кібербезпека стає одним

із ключових факторів стабільності фінансової системи. Постійні атаки вимагають від банківських установ високого рівня технологічної готовності, адаптивності та впровадження сучасних підходів до управління інформаційною безпекою [12].

Важливим етапом у забезпеченні цифрової стійкості фінансового сектора стала активізація регуляторного нагляду з боку Національного банку України. Зокрема, затверджений на 2026 рік план виїзних перевірок банків із питань інформаційної безпеки та кіберзахисту свідчить про перехід держави до жорсткого аудиту технологічних систем. Такі заходи охоплюють не лише контроль за збереженням коштів, а й перевірку якості електронних довірчих послуг, що є критично важливим в умовах масового переходу клієнтів на дистанційне обслуговування. Це підкреслює необхідність синхронізації темпів технічного розвитку банків із рівнем їхньої кіберстійкості, де державний контроль виступає гарантом захисту персональних даних і стабільності всього цифрового фінансового простору [13].

ВИСНОВКИ

Цифрова трансформація українського банківського сектора остаточно закріпила перехід від традиційних фізичних відділень до гнучких мобільних екосистем. Сьогодні банківські послуги стають інтелектуальним сервісом, який завдяки штучному інтелекту та аналізу великих даних підлаштовується під особисті потреби кожного клієнта. Попри виклики, пов'язані з кіберзагрозами та технічними збоями, розвиток технологій захисту, таких як біометрія та блокчейн, створює фундамент для формування безпечного цифрового фінансового простору.

Перспективи подальшого розвитку галузі лежать у площині впровадження архітектури Open Banking, що дозволить клієнтам керувати всіма своїми рахунками з різних банків у межах одного зручного інтерфейсу. Важливим напрямом стане розвиток вбудованих фінансів (*embedded finance*), коли банківські послуги будуть інтегровані безпосередньо в нефінансові платформи та сервіси щоденного вжитку. Окрім цього, фокус зміщуватиметься на досягнення повної фінансової інклюзії, щоб сучасні цифрові інструменти стали доступними та зрозумілими для всіх верств населення, незалежно від їхнього віку чи місця проживання. Подальша адаптація законодавства та посилення кіберстійкості дозволять українським банкам не лише підтримувати високу конкурентоспроможність, а й стати частиною глобальної інтелектуальної фінансової мережі. ■

БІБЛІОГРАФІЯ

1. Ситник Н. С., Назаркевич І. Б., Мицишин О. Я. Діджиталізація у фінансах: навч. посіб. Львів: Львів. нац. ун-т ім. Івана Франка, 2025. 287 с.
2. Binh M. X., Tuan N. H., Hai Ph., Le Hong D. An Overview of Digital Transformation in the Banking Sector through Bibliometric Analysis. *International Journal of Knowledge and Systems Science*. 2025. Vol. 16. Iss. 1. Art. 384591. DOI: <https://doi.org/10.4018/IJKSS.384591>
3. Miachon N. Mobile banking trends 2026 and beyond. *SBS Software*. 14.01.2026. URL: <https://sbs-software.com/insights/mobile-banking-trends-innovation/>
4. Огляд банківського сектору. Листопад 2025 року. Київ: Національний банк України, 2025. URL: https://bank.gov.ua/admin_uploads/article/Banking_Sector_Review_2025-11.pdf?v=16
5. Мирончук Р. Кількість успішних ідентифікацій через BankID НБУ зросла на 25%. *Мінфін*. 2026. URL: <https://minfin.com.ua/ua/2026/02/03/167492726/>
6. Mastercard study: 51% of Ukrainians are ready to entirely switch to digital banking. *Mastercard*. 05.04.2023. URL: <https://www.mastercard.com/news/eemea/en/newsroom/press-releases/en/2023/april/mastercard-study-51-of-ukrainians-are-ready-to-entirely-switch-to-digital-banking/>
7. Intelligent banking: A blueprint for creating value through AI-driven transformation. *KPMG*. 2025. URL: <https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/us-intelligent-banking-report-web-v2.pdf>
8. Беркаль М. Живі люди замість ШІ. Наскільки успішно сьогодні працюють чат-боти провідних українських банків. *Delo.ua*. 15 серпня 2023 р. URL: <https://delo.ua/banks/zivi-lyudi-zamist-si-naskilki-uspisno-syogodni-pracyuyut-cat-boti-providnix-ukrayinskix-bankiv-422545/>
9. Статистика кібератак на український бізнес у 2026 році: цифри, тренди та захист. *IT-Premium*. URL: <https://it-premium.com.ua/blog/statystyka-kiberatak-ukrainskyj-biznes-2026/>
10. А-Банк зазнав масштабної хакерської атаки. *Financial Club*. 2026. URL: <https://finclub.net/news/abank-zaznav-masshtabnoi-khakerskoi-ataky.html>
11. Наймасштабніші кібератаки на Україну (інфографіка). *Слово і Діло*. 24 березня 2025. URL: <https://www.slovoidilo.ua/2025/03/24/infografika/bezpeka/najmasshtabnishi-kiberataky-ukrayinu>
12. ПриватБанк успішно протистоїть 1,5 млн кібератак з початку війни. *Мінфін*. 2026. URL: <https://minfin.com.ua/ua/2026/02/27/169027662/>
13. У 2026 році у шістьох банках заплановані перевірки з питань інформаційної безпеки, кіберзахисту та кваліфікованих електронних довірчих послуг. *Національний банк України*. 30 грудня 2025. URL: <https://bank.gov.ua/ua/news/all/u-2026-rotsi-u-shistoh-bankah-zaplanovani-perevirki-z-pitan-informatsiynoi-bezpeki-kiberzahistu-ta-kvalifikovanih-elektronnih-dovirchih-poslug>

REFERENCES

- Berkal M. (2023, August 15). Zhyvi lyudi zamist ShI. Naskilky uspishno sohodni pratsiuiut chat-boty providnykh ukrainskykh bankiv [Real people instead of AI. How successfully the chat-bots of leading Ukrainian banks are working today]. *Delo.ua*. <https://delo.ua/banks/zivi-lyudi-zamist-si-naskilki-uspisno-syogodni-pracyuyut-cat-boti-providnix-ukrayinskix-bankiv-422545/>
- Binh M. X., Tuan N. H., Hai Ph. & Le Hong D. (2025). An Overview of Digital Transformation in the Banking Sector through Bibliometric Analysis. *International Journal of Knowledge and Systems Science*, 1(16). Art. 384591. <https://doi.org/10.4018/IJKSS.384591>
- Financial Club. (2026). A-Bank zaznav masshtabnoi khakerskoi ataky [A-Bank suffered a large-scale hacker attack]. <https://finclub.net/news/abank-zaznav-masshtabnoi-khakerskoi-ataky.html>
- IT-Premium. (2026). Statystyka kiberatak na ukrainskyj biznes u 2026 rotsi: tsyfry, trendy ta zakhyst [Statistics of cyber attacks on Ukrainian business in 2026: numbers, trends and protection]. <https://it-premium.com.ua/blog/statystyka-kiberatak-ukrainskyj-biznes-2026/>
- KPMG. (2025). *Intelligent banking: A blueprint for creating value through AI-driven transformation*. <https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/us-intelligent-banking-report-web-v2.pdf>
- Mastercard. (2023, April 5). *Mastercard study: 51% of Ukrainians are ready to entirely switch to digital banking*. <https://www.mastercard.com/news/eemea/en/newsroom/press-releases/en/2023/april/mastercard-study-51-of-ukrainians-are-ready-to-entirely-switch-to-digital-banking/>
- Miachon N. (2026, January 14). Mobile banking trends 2026 and beyond. *SBS Software*. <https://sbs-software.com/insights/mobile-banking-trends-innovation/>
- Minfin. (2026, February 27). *PryvatBank uspishno protystoit 1,5 mln kiberatak z pochatku viiny* [PrivatBank successfully resists 1.5 million cyber attacks since the start of the war]. <https://minfin.com.ua/ua/2026/02/27/169027662/>
- Myronchuk R. (2026, February 3). *Kilkist uspishnykh identyfikatsii cherez BankID NBU zroslo na 25%* [The number of successful identifications through BankID NBU increased by 25%]. *Minfin*. <https://minfin.com.ua/ua/2026/02/03/167492726/>
- Natsionalnyi bank Ukrainy. (2025, December 30). *U 2026 rotsi u shistokh bankakh zaplanovani perevirky z pytan informatsiinoi bezpeky, kiberzakhystu ta kvalifikovanykh elektronnykh dovirchych poslug* [In 2026, inspections on information security, cyber protection, and qualified electronic trust services are planned in six banks]. <https://bank.gov.ua/ua/news/all/u-2026-rotsi-u-shistoh-bankah-zaplanovani-perevirki-z-pitan-informatsiynoi-bezpeki-kiberzahistu-ta-kvalifikovanih-elektronnih-dovirchih-poslug>

Natsionalnyi bank Ukrainy. (2025). *Ohliad bankivskoho sektoru. Lystopad 2025 roku* [Banking Sector Review. November 2025]. https://bank.gov.ua/admin_uploads/article/Banking_Sector_Review_2025-11.pdf?v=16

Slovo i Dilo. (2025, March 24). *Naimasshtabnishi kiberataky na Ukrainu (infohrafika)* [The largest cyber attacks on Ukraine (infographic)]. <https://www.slovovidilo.ua/2025/03/24/infohrafika/bezpeka/naj-masshtabnishi-kiberataky-ukrayinu>

Sytnyk N. S., Nazarkevych I. B. & Myshchysyn O. Ya. (2025). *Didzhytalizatsiia u finansakh: navch. posib* [Digitalization in Finance: a study guide]. Lviv. nats. un-t im. Ivana Franka

Стаття надійшла до редакції / Received: 16.01.2026
 Статтю прийнято до публікації / Accepted: 30.01.2026
 Оприлюднено / Published: 31.03.2026

УДК 336.226:347.9

JEL: H24

DOI: <https://doi.org/10.32983/2222-4459-2026-2-282-289>

АКТУАЛЬНІ ПИТАННЯ ОПОДАТКУВАННЯ СУДОВОГО ЗБОРУ, ВІДШКОДОВАНОГО ОСОБІ ЗА РІШЕННЯМ СУДУ

©2026 **КЛУБАНЬ М. В., ВІТОВЩИК Т. С.**

УДК 336.226:347.9

JEL: H24

Клубань М. В., Вітовщик Т. С. Актуальні питання оподаткування судового збору, відшкодованого особі за рішенням суду

У статті здійснено комплексний науково-правовий аналіз правової природи судового збору, що відшкодовується фізичній особі за рішенням суду, крізь призму його можливого оподаткування податком на доходи фізичних осіб та військовим збором. Актуальність дослідження зумовлена наявністю сталої правової невизначеності та суперечливої правозастосовної практики, за якої компенсаційні за своєю суттю виплати податковими органами нерідко кваліфікуються як оподатковуваний дохід або «додаткове благо» платника податку. У межах дослідження проаналізовано норми Податкового кодексу України, що регулюють поняття доходу, додаткового блага та об'єкта оподаткування, а також норми цивільного, господарського й адміністративного процесуального законодавства, які визначають судовий збір як складову судових витрат і встановлюють механізм їх розподілу та відшкодування. Обґрунтовано, що судовий збір за своєю правовою природою є вимушеною майновою втратою, понесеною особою з метою реалізації конституційного права на судовий захист, а його подальше відшкодування має виключно компенсаторний характер і спрямоване на відновлення попереднього майнового стану сторони (*restitutio in integrum*). Окрему увагу приділено критичному аналізу позицій Державної податкової служби України, викладених у листах та індивідуальних податкових консультаціях, у яких відшкодований судовий збір віднесено до загального оподаткованого доходу фізичної особи. Доведено, що такі підходи не узгоджуються ні з економічною сутністю доходу як приросту активів, ні з цивільно-правовим розумінням збитків та їх відшкодування, а також створюють дискримінаційні наслідки залежно від джерела компенсації судових витрат. Значне місце у статті відведено аналізу актуальної судової практики, зокрема правових позицій Верховного Суду, який послідовно виходить з того, що компенсація судових витрат, у тому числі судового збору, не є доходом платника податку, оскільки не приводить до збільшення його майнової сфери, а отже, не формує об'єкта оподаткування ПДФО та військовим збором. За результатами дослідження сформульовано науково обґрунтований висновок про недопустимість фіскального тлумачення сум відшкодованого судового збору як доходу або додаткового блага. Запропоновано напрями вдосконалення податкового законодавства України шляхом уточнення відповідних норм з метою усунення неоднозначного їх тлумачення та забезпечення принципів правової визначеності, справедливості оподаткування й ефективного доступу до правосуддя.

Ключові слова: оподаткування судового збору, додаткове благо, податок на доходи фізичних осіб, військовий збір.

Бібл.: 18.

Клубань Марія Володимирівна – кандидат юридичних наук, доцент, доцент кафедри права та економіко-фінансової безпеки, Академія рекреаційних технологій та права (вул. Карбишева, 2, Луцьк, 43023, Україна)

E-mail: fmv2209@gmail.com

Вітовщик Тетяна Сергіївна – кандидат економічних наук, доцент кафедри права та економіко-фінансової безпеки, Академія рекреаційних технологій та права (вул. Карбишева, 2, Луцьк, 43023, Україна)

E-mail: Tetyana220@gmail.com

ORCID: <https://orcid.org/0009-0003-3825-7151>

UDC 336.226:347.9

JEL: H24

Kluban M. V., Vitovshchik T. S. The Current Issues in Taxation of Court Fees Reimbursed to an Individual by Court Decision

The article provides a comprehensive scientific and legal analysis of the legal nature of court fees reimbursed to an individual by court decision, through the lens of their potential taxation under personal income tax and military tax. The relevance of the study is due to the persistent legal uncertainty and contradictory law enforcement practice, where compensatory payments, by their nature, are often classified by tax authorities as taxable income or an «additional benefit» for the taxpayer. The study examines the provisions of the Tax Code of Ukraine regulating the concepts of income, additional benefit, and taxable object, as well as provisions of civil, commercial, and administrative procedural law that define court fees as part of court costs and establish the mechanism for their allocation