

М. В. Кочеров,
д. ю. н., професор кафедри публічного управління та адміністрування,
Державний університет "Київський авіаційний інститут"
ORCID ID: <https://orcid.org/0000-0001-8687-8604>

DOI: 10.32702/2306-6814.2025.16.271

ДЕРЖАВНЕ РЕГУЛЮВАННЯ БАНКІВСЬКОГО СЕКТОРА УКРАЇНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

М. Kocherov,
Doctor of Science of Law,
Professor of the Department of Public Management and Administration, The State University "Kyiv Aviation Institute"

STATE REGULATION OF THE BANKING SECTOR OF UKRAINE IN CONDITIONS OF DIGITAL TRANSFORMATION

У статті обґрунтовано актуальність дослідження державного регулювання банківського сектора України в умовах стрімкої цифрової трансформації, що радикально змінює традиційні підходи до управління фінансовою системою. Проаналізовано вплив інноваційних технологій, зокрема FinTech, RegTech, SupTech, штучного інтелекту (AI) та аналітики великих даних (Big Data), на модернізацію регуляторних механізмів, що мають бути адаптовані до нових викликів цифрової доби. Визначено, що стратегічні ініціативи Національного банку України, такі як розвиток відкритого банкінгу (open banking), впровадження регуляторних "пісочниць" (regulatory sandboxes) та формування національної цифрової інфраструктури (BankID, платформи "Трембіта" та "Дія"), виступають головними чинниками трансформації банківського регулювання, формування єдиної інформаційної екосистеми та підвищенні інклюзії. Особливу увагу приділено інтеграції національного регулювання з європейськими та міжнародними стандартами, зокрема щодо використання ISO 20022, впровадження електронної гривні та розвитку миттєвих платежів. Досліджено нормативно-правову базу, спрямовану на забезпечення кібербезпеки, управління інформаційними ризиками та підвищення прозорості банківського сектору. Узагальнено основні проблеми, серед яких вказано технологічну залежність від зовнішніх провайдерів (vendor lock-in), нерівномірність цифрової готовності банківських установ, посилення кіберризиків та ризику регуляторних "провалів". Наголошено на необхідності балансування між інноваційністю, кібербезпекою та цифровою інклюзією, впровадження уніфікованих стандартів кіберзахисту, а також посилення інституційного потенціалу регулятора для забезпечення ефективного нагляду. Підкреслено важливість системного, проактивного та ризик-орієнтованого підходу до регулювання банківського сектору, що сприятиме підвищенню стійкості фінансової системи України та мінімізації технологічних і інформаційних ризиків у цифрову епоху. Окреслено перспективи подальших досліджень у сфері гармонізації законодавства і розробки адаптивних інструментів регулювання, які враховують сучасні виклики технологічного розвитку.

The article substantiates the relevance of researching the state regulation of Ukraine's banking sector amid rapid digital transformation, which is radically changing traditional approaches to managing the financial system. The influence of innovative technologies — in particular FinTech, RegTech, SupTech, artificial intelligence (AI), and big data analytics — on the modernization of regulatory mechanisms is analyzed, emphasizing the need for their adaptation to the challenges of the digital era. It is identified that the strategic initiatives of the National Bank of Ukraine, such as the development of open banking, the implementation of regulatory sandboxes, and the establishment of national digital infrastructure (BankID, Trembita and Diia platforms), serve as key drivers of regulatory transformation, the formation of a unified information ecosystem, and the enhancement of financial inclusion. Particular attention is paid to the integration of national regulation with European and international standards, especially regarding the adoption of ISO 20022, the introduction of the electronic hryvnia, and the development of instant payments. The legal and regulatory framework aimed at ensuring cybersecurity, managing information risks, and increasing the transparency of the financial sector is examined. The main challenges are summarized, including technological dependence on external providers (vendor lock-in), uneven digital readiness of banking institutions, the intensification of cyber risks, and the threat of regulatory failures. The article emphasizes the need to balance innovation, cybersecurity, and digital inclusion; to implement unified cybersecurity standards; to develop interagency cooperation; and to strengthen the institutional capacity of the regulator to ensure effective supervision. The importance of a systemic, proactive, and risk-based approach to banking regulation is highlighted, as it contributes to enhancing the resilience of Ukraine's financial system and minimizing technological and informational risks in the digital age. Prospects for further research are outlined in the area of legal harmonization and the development of adaptive regulatory instruments that respond to the current challenges of technological development.

Ключові слова: державне регулювання, банківський сектор, цифрова трансформація, FinTech, RegTech, фінансова система, кібербезпека.

Key words: government regulation, banking sector, digital transformation, FinTech, RegTech, financial system, cybersecurity.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах повсюдної цифровізації відбувається суттєва зміна характеру відносин між державою та фінансовими інститутами. Використання новітніх технологій, таких як фінансові технології, великі дані (Big Data), штучний інтелект (AI), хмарні обчислення, а також впровадження автоматизованих цифрових платформ, створює передумови для суттєвої модернізації механізмів державного регулювання банківської діяльності. Водночас цифровізація актуалізує низку викликів, пов'язаних із кібербезпекою, технологічною нерівністю, інформаційними ризиками та потенційними ситуаціями, коли традиційні інструменти регуляторного впливу виявляються неефективними або неадекватними новим умовам.

Особливої актуальності набуває проблема забезпечення балансу між інноваційністю та стабільністю у процесі державного втручання в банківську сферу. З одного боку, цифрові інструменти сприяють підвищенню прозорості, ефективності нагляду та зниженню транзакційних витрат, з іншого, формують нові регуляторні виклики, які потребують оперативного і науково обгрунто-

ваного реагування. До прикладу, так звані регуляторні "пісочниці" (regulatory sandboxes), спеціальні тестові середовища, які створюються для апробації нових фінансових продуктів чи технологій під контролем регулятора, є важливим інструментом адаптації державної політики до інноваційних практик, однак їх широке застосування потребує чіткої методологічної бази та ризик-орієнтованого підходу.

Таким чином, проблема удосконалення державного регулювання банківського сектора в умовах цифрової трансформації безпосередньо пов'язана з необхідністю формування інтегрованої цифрової інфраструктури, гармонізації нормативного середовища з урахуванням європейських підходів, а також розробки нових моделей регуляторної взаємодії між державою та банками, здатних забезпечити стійкість фінансової системи в умовах швидких технологічних змін.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Останні дослідження зосереджуються на розвитку FinTech, RegTech, SupTech технологій та застосуванні штучного інтелекту у банківському секторі. Зокрема, А. Ковачевич, С. Раденкович та Д. Ніколіх вивчають взаємозв'язок штучного інтелекту і кібербезпеки [4], Ш. Бі

та В. Бао досліджують ефективність штучного інтелекту в управлінні кредитними ризиками [3]. Аналіз кіберризиків і вплив цифровізації на банківську діяльність представлено у працях М. Валіулліха, Дж. Хоссейна. та ін. [12] тощо. М. Іорґачова та О. Ковальова аналізують вплив цифрових технологій на фінансовий ринок України [8], Г. Інґрем Г. та П. Вора досліджують роль цифрової економіки в умовах воєнного стану [10; 11]. Національний банк України визначив основні напрями розвитку фінансового сектору через стратегічні документи, регулювання відкритого банкінгу та нормативні акти з кібербезпеки [1; 5; 6; 7; 15—17]. Ці розробки та документи формують науково-практичну базу для удосконалення державного регулювання банківської сфери в умовах цифрової трансформації.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Формулювання цілей статті (постановка завдання) — дослідження особливостей та напрямів державного регулювання банківського сектору України в умовах цифрової трансформації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

У відповідь на стрімке поширення цифрових технологій у банківській сфері Національний банк України (НБУ) визначив розвиток фінансових інновацій як один із пріоритетів реформування фінансового ринку. У 2020 році було схвалено Стратегію розвитку фінансових технологій в Україні до 2025 року, яка заклала концептуальну основу для формування національної FinTech-екосистеми. У документі передбачено цільове впровадження інструментів відкритого банкінгу (open banking), розвиток регуляторних (RegTech) та наглядових технологій (SupTech), а також створення умов для тестування інноваційних фінансових сервісів у форматі регуляторної "пісочниці": спеціального правового поля для пілотних проєктів, що перебувають під наглядом НБУ [1].

Стратегія орієнтується на гармонізацію національного регулювання з європейськими та міжнародними стандартами (зокрема PSD2, ISO 20022, концепція електронної гривні, розвиток миттєвих платежів тощо), що відповідає імперативам євроінтеграції [1; 2]. Ці новації забезпечують інтеграцію цифрових технологій у функціонування банківської системи, створюючи передумови для глибокої трансформації не лише платіжної інфраструктури, а й філософії державного регулювання.

Особливої уваги заслуговує впровадження технологій штучного інтелекту (AI) та аналітики великих даних (Big Data), які вже стали важливими інструментами в оцінці кредитних ризиків, ідентифікації шахрайства, оптимізації комплаєнс-функцій. Дослідження Shuochen Bi та Wenqing Bao (2024) підтверджує ефективність застосування AI у системах управління кредитним ризиком, зокрема в адаптивних скорингових моделях і прогнозуванні дефолтів [3]. Інше дослідження, проведене Ана Ковачевич та ін., акцентує увагу на взаємозв'язку між застосуванням AI у банках і ризиками інформаційної безпеки, що вимагає комплексної регуляторної відповіді [4].

Незважаючи на очевидні переваги цифрових технологій, актуалізується ризик надмірної залежності банків і регуляторів від BigTech-постачальників інфраструкту-

ри для AI-систем, що загрожує появою vendor lock-in — стану, коли суб'єкт фінансового ринку або навіть регулятор обмежений у виборі альтернатив через технічну чи контрактну прив'язку до конкретного постачальника. Це, у свою чергу, створює загрозу концентрації технологічних ризиків і послаблює регуляторну автономію.

Враховуючи ці ризики, НБУ 31 березня 2025 року презентував Зелену книгу з розвитку регуляторних технологій (RegTech Green Paper), яка містить дорожню карту інтеграції автоматизованих інструментів відповідності (compliance tools) у внутрішні системи банків. Документ передбачає впровадження SupTech-рішень, які дозволяють регулятору здійснювати моніторинг у реальному часі, та RegTech-технологій для самооцінки відповідності банківських установ вимогам у сфері протидії відмиванню доходів, перевірки клієнтів та забезпечення кібербезпеки [5].

Значущим правовим кроком цифрових змін стало ухвалення Закону України "Про платіжні послуги" у 2021 році (набрав чинності у серпні 2022 р.). Закон не лише розширив коло учасників фінансового ринку, включивши небанківських постачальників послуг платіжних установ (PI) і установ електронних грошей (EMI), але й створив передумови для функціонування open banking на основі дозволеного користувачем обміну платіжними й фінансовими даними з третіми сторонами через стандартизовані API [6].

У травні 2025 року НБУ опублікував проєкт Положення про відкритий банкінг, набуття чинності якого датоване 1 серпня 2025 року [7]. Документ визначає організаційно-технічні вимоги до учасників open banking та структурує процеси взаємодії між банками, провайдерами платіжних послуг і споживачами.

Таким чином, трансформація регуляторної політики у банківському секторі включає низку основних складових:

- визначення та ліцензування нових суб'єктів ринку: платіжних установ (PI) і установ електронних грошей (EMI), що потребує адаптації нормативної бази;
- уніфікацію стандартів звітності та обміну (впровадження ISO 20022 як базового формату фінансових повідомлень);
- пілотування інституційних технологічних моделей, включаючи регуляторні пісочниці, як механізм апробації інновацій під контролем держави.

Вищезазначені ініціативи свідчать про системну трансформацію української моделі банківського регулювання у бік технологічної відкритості, інституційної адаптивності та орієнтації на ризик-орієнтований підхід. Водночас, ці процеси потребують належного методологічного супроводу, зокрема формування критеріїв оцінки ефективності регуляторних інновацій та механізмів їх правового закріплення. При цьому головним викликом залишається забезпечення технологічного суверенітету регулятора, збереження контролю над критичною цифровою інфраструктурою і запобігання надмірній залежності від зовнішніх постачальників технологій.

НБУ активно будує цифрову інфраструктуру для взаємодії регулятора з фінансовим сектором. Серед основних елементів є система BankID НБУ, що дозволяє здійснювати електронну ідентифікацію громадян у банківських та державних системах. У 2024 році BankID

обробив понад 87,7 млн успішних ідентифікацій у порівнянні з 42,9 млн у 2023 році, що свідчить про стрімке зростання цифрової взаємодії [8]. Ця система є вирішальним інструментом цифрової співпраці з клієнтами, забезпечує швидкість та зручність доступу до фінансових сервісів як споживачів, так і бізнес-клієнтів.

У 2023 році було реалізовано перехід на нове покоління Електронної платіжної системи НБУ [9], що працює відповідно до міжнародного стандарту ISO 20022 та підтримує цілодобові instant-платежі. Це забезпечує значне зниження транзакційних витрат, підвищення фінансової інклюзії та інтеграцію з європейською платіжною інфраструктурою. Автоматизовані звітні модулі дозволяють НБУ в реальному часі отримувати дані про ризики, ліквідність, комплаєнс завдяки SupTech-рішенням [11]. У комплексі це забезпечує гнучкість та ефективність регуляторного надзору.

Українські державні цифрові платформи формують єдину інформаційну екосистему. Зокрема, Trembita — це міждержавний обмін даними, подібний до естонської X-Road, що дозволяє безпечно обмінюватися державними реєстрами між установами [10]. Це сприяє підвищенню оперативності перевірок, інтеграції банківських даних у державні сервіси та скороченню паперового документообігу.

Крім того, платформа Дія забезпечує доступ населення до більш ніж 130 державних послуг в електронному форматі, включно з цифровими документами і взаємодією з фінансовими сервісами через API, що значно спрощує комунікацію між громадянами, державою та фінансовими інституціями, актуалізуючи роль цифрових каналів у регуляторній взаємодії.

Огляд кіберзагроз у банківському секторі (2025) показує, що найпоширенішими загрозами залишаються фішинг, шкідливе програмне забезпечення, програми-вимагачі та несанкціонований доступ. Дослідники встановили, що поширення таких ризиків суттєво стримує розвиток цифрового банкінгу [12]. Водночас рішення, засновані на штучному інтелекті, блокчейн-технологіях, біометричній ідентифікації та багатофакторній автентифікації, демонструють ефективність у зменшенні ризиків, проте вимагають чітко сформульованих регуляторних підходів до забезпечення безпеки та постійного моніторингу в режимі реального часу.

Вивчаючи стійкість цифрової економіки під час воєнного стану, науковці підкреслюють, що законодавчі норми відіграють вирішальну роль (ймовірність стійкості зростає в 2.65 раза), а кібербезпека і fintech-технології, також суттєво підсилюють витривалість систем (OR = 1.90 та 1.52 відповідно) [13].

Таким чином, цифрова інфраструктура НБУ і держави у цілому є фундаментальною передумовою для сучасного, ефективного та ризик-орієнтованого регулювання банківської сфери. Системи BankID, ISO 20022-сумісна платіжна інфраструктура, API-рішення open banking, Trembita, а також інтеграція в єдиний державний портал Дія створюють умови для безперебійної, прозорої взаємодії між регулятором, банками та споживачами. Водночас, дослідження підтверджують: рівень кіберризиків залишається вагомим обмеженням, що акцентує потребу в потужних SupTech-механізмах та безперервному моніторингу. При цьому значущість

аналізу ризиків і викликів, що супроводжують модернізацію регуляторних механізмів банківського сектора, стрімко зростає. Попри очевидні переваги впровадження цифрових рішень, таких як автоматизовані звітності, API-платформи, елементи штучного інтелекту, посилюються загрози, пов'язані з кібербезпекою, регуляторними "провалами" та нерівномірною цифровою адаптацією банків. Однією з основних проблем є забезпечення кіберстійкості, адже здатність фінансової інституції ефективно виявляти, запобігати й оперативно реагувати на кіберінциденти є критично важливою для стабільності всієї системи [14].

В Україні вже запроваджено нормативну основу щодо управління інформаційною безпекою в банківській системі: так, постановою Правління НБУ № 4 від 16.01.2021 затверджено Положення, яке встановлює механізми контролю за дотриманням банками вимог кібербезпеки, самооцінки, зовнішнього аудиту та перевірок [15]. Це спрямовано на підвищення прозорості та відповідальності банківських установ за стан своєї інформаційної безпеки. Постанова № 178 від 12.08.22 [16] деталізує вимоги до організаційної моделі кіберзахисту, передбачає обов'язкове впровадження банками систем управління інформаційною безпекою, налагодження моніторингу інцидентів, захисту критичних елементів інфраструктури, а також чітко визначає обов'язки керівництва банку щодо управління кіберризиками. Це створює підґрунтя для стандартизації підходів до захисту від кібератак та гармонізації внутрішніх політик банків з кращими міжнародними практиками. Постанова № 24 від 25.02.25 [17] оновлює чинні акти НБУ, фокусуючись на розширенні процедур з управління кіберризиками, уточненні вимог до захищеності інформаційних систем та зміцненні механізмів реагування на кіберінциденти.

Загалом, наявність цих нормативних актів свідчить про системний підхід регулятора до забезпечення кіберстійкості фінансового сектору. Водночас, ефективність їх реалізації значною мірою залежить від внутрішньої спроможності банків впроваджувати відповідні політики та забезпечувати достатній рівень технічної і кадрової готовності до сучасних загроз.

Наукові дослідження вказують на критичне зростання кількості кібератак у період 2022—2024 років, водночас фіксуючи дефіцит кваліфікованого персоналу та відсутність ефективного міжвідомчої комунікації [18]. Висновок очевидний: розрив між темпами цифровізації та рівнем безпекового забезпечення може створювати системні загрози.

Ще одним важливим викликом є нормативна неузгодженість. Вчені доводять, що технологічні інновації в сфері Fintech і Regtech часто випереджають можливості традиційного регуляторного реагування [19].

Цей дисбаланс добре ілюструється українською ситуацією: попри прийняття Закону України "Про платіжні послуги" ще у 2021 році, лише в 2025 році НБУ оприлюднив проєкт регламенту щодо впровадження open banking. Таке зволікання гальмує реалізацію інноваційних моделей цифрової взаємодії та знижує ефективність регуляторного контролю.

Особливої уваги потребує проблема нерівномірного доступу банків до цифрових технологій. Великі системно важливі банки мають змогу впроваджувати

Таблиця 1. Напрями державного регулювання банківського сектора України в умовах цифрових трансформаційних змін

Напрямок трансформації	Заходи державного впливу	Очікувані результати (ризик)
Фінансові інновації (FinTech)	Стратегія розвитку фінтех до 2025 року Закон «Про платіжні послуги» Впровадження open banking	Розширення доступу до фінансових послуг Поява нових суб'єктів ринку (PI, EMI) Інтенсифікація викликів кібербезпеки
RegTech і SupTech	RegTech Green Paper (2025) Автоматизовані інструменти комплаєнсу Інтеграція моніторингових рішень у реальному часі	Підвищення ефективності нагляду Прискорення реагування на порушення Ризики технологічної залежності від IT-провайдерів (vendor lock-in)
Штучний інтелект та Big Data	Використання AI у скорингу та виявленні шахрайства Аналітика кредитних ризиків	Оптимізація фінансових рішень Ризики порушення конфіденційності даних Потреба в адаптивному регулюванні
Регуляторні пісочниці	Тестування інноваційних сервісів під наглядом НБУ Оцінка ризиків у контрольованому середовищі	Гнучке регулювання для інновацій Виявлення прогалин у законодавстві Необхідність прозорих критеріїв допуску та оцінки результатів
Цифрова інфраструктура	Впровадження системи BankID Платіжна система ISO 20022 Інтеграція з «Дія» та системою «Трембіта»	Зниження транзакційних витрат Підвищення прозорості й інклюзії Уразливість до технічних збоїв та кіберзагроз
Кібербезпека	Постанова НБУ № 95 (2021) Постанова НБУ № 178 (2024) Постанова НБУ № 4 (2024) Постанова НБУ № 24 (2024) Політики кіберстійкості, ISMS, MFA	Посилення захисту критичних систем Уніфікація стандартів кіберзахисту Посилення відповідальності керівництва банків Дефіцит кваліфікованих фахівців
Нормативна адаптація	Проекти регламентів НБУ щодо технологій Законодавче врегулювання електронних сервісів та хмарних рішень	Підвищення нормативної відповідності до нових технологій Загроза відставання регулювання Регуляторні «провали»
Цифрова нерівність між банками	Компенсаторні та інституційні механізми підтримки	Ризик сегментації банківського ринку Посилення цифрового розриву Ускладнення виконання нагляду на єдиних засадах
Цифрова інклюзія і системна стійкість	Підвищення цифрової грамотності персоналу Централізовані сервіси НБУ Актуалізація нормативного забезпечення кіберстійкості	Зниження бар'єрів доступу до інновацій Підвищення адаптивності сектора до кризових ситуацій Розбудова єдиної цифрової екосистеми банківської взаємодії

Джерело: складено автором.

складні IT-рішення, натомість малі та середні установи відчувають брак ресурсів для подібних інвестицій. Це створює ризик сегментованості банківського ринку за рівнем цифрової зрілості, а також ускладнює уніфіковану реалізацію наглядових процедур. У останніх дослідженнях акцентується на необхідності впровадження компенсаторних механізмів: централізованих хмарних сервісів, навчальних програм для персоналу, інтеграції менш потужних банків до цифрових платформ регулятора за спрощеними протоколами [20].

Узагальнення напрямів державного регулювання банківського сектора України в умовах цифрових трансформаційних змін представлено у таблиці 1.

Таким чином, цифрова трансформація банківського сектора потребує не лише технологічного оновлення фінансових установ, а й послідовного посилення ролі держави у формуванні адаптивної системи регулювання. Сучасні виклики вимагають від державного регулятора оновлення нормативної бази, розвитку інституційного потенціалу та комплексного управління цифрови-

ми ризиками. Ефективне державне регулювання в цій сфері має забезпечити баланс між впровадженням інновацій, гарантованим рівнем кібербезпеки та дотриманням принципів цифрової інклюзії. Йдеться про впровадження уніфікованих вимог до кіберзахисту, обов'язковості функціонування систем управління інформаційною безпекою, розбудову механізмів міжвідомчої взаємодії між банками, регулятором та правоохоронними органами. За таких умов цифрові інновації можуть бути інтегровані у фінансову систему як стабілізуючий чинник, а не як джерело нових системних ризиків.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Вищезазначене дає підстави дійти висновку, що сучасна регуляторна політика функціонування банківського сектору набула чітко окресленого стратегічного вектора, зорієнтованого на комплексне управління ризиками цифрового середовища. Затвердження нових нормативно-правових актів засвідчує послідовність дій регулятора у створенні єдиної системи вимог до банків щодо захисту інформаційних активів, побудови внутрішньої політики безперервності кіберзахисту, визначення об'єктів критичної інфраструктури та формування захищених цифрових каналів взаємодії. Особливої ваги набуває обов'язковість організації системи управління інформаційною безпекою, що передбачає ідентифікацію, аналіз, оцінювання та моніторинг кіберризиків у динаміці. Запровадження систематичного аудиту, тестування на проникнення та моніторингу інцидентів у режимі реального часу створює передумови для гнучкого і проактивного регулювання, як того вимагають сучасні виклики технологічного розвитку.

Література:

1. Стратегія розвитку фінансових технологій (FinTech) в Україні до 2025 року. Національний банк України. 2020. URL: <https://bank.gov.ua/en/about/develop-strategy/fintech2025>
2. Стратегія розвитку фінансового сектору України до 2025 року. Національний банк України. 2021. URL: <https://bank.gov.ua/ua/news/all/strategiya-rozvitku-financevogo-sektoru-ukrayini-do-2025-roku-7686>
3. Shuochen Bi, Wenqing Bao. Innovative Application of Artificial Intelligence Technology in Bank Credit Risk Management. 2024. URL: <https://arxiv.org/abs/2404.18183>
4. Ana Kovacevic, Sonja D. Radenkovic, Dragana Nikolic. Artificial intelligence and cybersecurity in banking sector: opportunities and risks. 2024. URL: <https://arxiv.org/abs/2412.04495>
5. Зелена книга з розвитку регуляторних технологій на фінансовому ринку України. 2025. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/Zelena_knyga_2025_fin.pdf
6. Про платіжні послуги: закон України. 2023. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text>
7. Про затвердження Положення про відкритий банкінг в Україні: постанова Національного банку України від 25.07.2025 № 80. URL: <https://ips.liga-zakon.net/document/PB25112>

8. Iorgachova, Maria; Kovalova, Olena. Financial technologies in the development of banking activities in Ukraine's financial market, Economic Forum, Lutsk National Technical University. Lutsk, Ukraine, 2025. Vol. 15, Iss. 1, pp. 8-24. URL: <https://e-forum.com.ua/en/journals/tom-15-1-2025/finansovi-tehnologiyi-u-rozvitku-bankivskoyi-diyalnosti-na-finansovomu-rinku-ukrayini>

9. Про впровадження суптех (SupTech) та регтех (RegTech). Національний банк України. 2020. URL: <https://bank.gov.ua/ua/supervision/suptech-regtech>

10. George Ingram and Priya Vora. Ukraine: Digital government is central to resilience. URL: <https://www.brookings.edu/articles/ukraine-digital-government-is-central-to-resilience>

11. George Ingram and Priya Vora. Ukraine: Digital resilience in a time of war. URL: <https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/>

12. Md. Waliullah, Md Zahin Hossain George etc. Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. 2025. URL: <https://arxiv.org/abs/2503.22710>

13. Yuliia Pereguda, Svitlana Stender etc. Ukraine's digital economy under martial law: innovative approaches and legal context. International Journal of Economics and Financial Issues, 2025, 15(1), 431—440. URL: <https://econjournals.com/index.php/ijefi/article/view/17585>

14. Cyber resilience oversight expectations for financial market infrastructures. 2018. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

15. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг: постанова Правління НБУ від 16.01.25. № 4. URL: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>

16. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України: постанова Правління НБУ від 12.08.22 № 178. URL: <https://zakon.rada.gov.ua/laws/show/v0178500-22#Text>

17. Про затвердження Змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту: постанова Правління НБУ від 25.02.25 № 24. URL: <https://zakon.rada.gov.ua/laws/show/v0024500-25#Text>

18. Krasnobayev, Victor et al. Economic and cyber security: Collective monograph. Kharkiv. 2023. URL: <https://www.econstor.eu/handle/10419/302598>

19. Yiannis Anagnostopoulos. Fintech and Regtech: Impact on Regulators and Banks. Journal of Economics and Business. 2018. URL: https://www.researchgate.net/publication/326542210_Fintech_and_Regtech_Impact_on_Regulators_and_Banks

20. Сундук, Т. Ф., Бабенко-Левада, В. Г., Скорба, О. А., Чорновол, А. О. Щодо розвитку цифрових технологій у фінансовому секторі (український ключ). Академічні візії, 2023. (17), 1-7. URL: <https://zenodo.org/records/7774205>

References:

1. National Bank of Ukraine (2020), "Strategy for the Development of Financial Technologies (FinTech) in Ukraine until 2025", Available at: <https://bank.gov.ua/en/about/develop-strategy/fintech2025> (Accessed: 15 January 2025).
2. National Bank of Ukraine (2021), "Strategy for the Development of the Financial Sector of Ukraine until 2025", Available at: <https://bank.gov.ua/ua/news/all/strategiya-rozvitku-finansovogo-sektoru-ukrayini-do-2025-roku-7686> (Accessed: 04 March 2025).
3. Bi, S. and Bao, W. (2024), "Innovative Application of Artificial Intelligence Technology in Bank Credit Risk Management", Available at: <https://arxiv.org/abs/2404.18183> (Accessed: 07 May 2025).
4. Kovacevic, A., Radenkovic, S.D. and Nikolic, D. (2024), "Artificial Intelligence and Cybersecurity in Banking Sector: Opportunities and Risks", Available at: <https://arxiv.org/abs/2412.04495> (Accessed: 16 April 2025).
5. National Bank of Ukraine (2025), "Green Paper on the Development of Regulatory Technologies in the Financial Market of Ukraine", Available at: https://bank.gov.ua/admin_uploads/article/Zelena_knyga_2025_fin.pdf (Accessed: 17 June 2025).
6. Verkhovna Rada of Ukraine (2023), The Law of Ukraine "On Payment Services", Available at: <https://zakon.rada.gov.ua/laws/show/1591-20#Text> (Accessed: 03 February 2025).
7. National Bank of Ukraine (2025), Resolution "On Approval of the Regulation on Open Banking in Ukraine", Available at: <https://ips.ligazakon.net/document/PB25112> (Accessed: 09 May 2025).
8. Iorgachova, M. and Kovalova, O. (2025), "Financial Technologies in the Development of Banking Activities in Ukraine's Financial Market", Economic Forum, Lutsk National Technical University, Vol. 15, no. 1, pp. 8—24, Available at: <https://e-forum.com.ua/en/journals/tom-15-1-2025/finansovi-tehnologiyi-u-rozvitku-bankivskoyi-diyalnosti-na-finansovomu-rinku-ukrayini> (Accessed: 06 April 2025).
9. National Bank of Ukraine (2020), "On Implementation of SupTech and RegTech", Available at: <https://bank.gov.ua/ua/supervision/suptech-regtech> (Accessed: 28 May 2025).
10. Ingram, G. and Vora, P. (2024), "Ukraine: Digital Government is Central to Resilience", Available at: <https://www.brookings.edu/articles/ukraine-digital-government-is-central-to-resilience> (Accessed: 19 June 2025).
11. Ingram, G. and Vora, P. (2024), "Ukraine: Digital Resilience in a Time of War", Available at: <https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/> (Accessed: 12 February 2025).
12. Waliullah, M. and Hossain, M.Z. (2025), "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review", Available at: <https://arxiv.org/abs/2503.22710> (Accessed: 12 February 2025).
13. Pereguda, Y. and Stender, S. (2025), "Ukraine's Digital Economy under Martial Law: Innovative Approaches and Legal Context", International Journal of Economics and Financial Issues, Vol. 15, No. 1, pp. 431—440, Available at: <https://econjournals.com/index.php/ijefi/article/view/17585> (Accessed: 21 May 2025).

14. European Central Bank (2018), "Cyber Resilience Oversight Expectations for Financial Market Infrastructures", Available at: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (Accessed: 06 May 2025).

15. National Bank of Ukraine (2021), Resolution "Regulation on Control over Compliance by Banks with Legislation on Information Security, Cybersecurity and Electronic Trust Services", Available at: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text> (Accessed: 09 April 2025).

16. National Bank of Ukraine (2022), Resolution "Regulation on the Organization of Cybersecurity in the Banking System of Ukraine and Amendments to the Regulation on Identification of Critical Infrastructure Objects", Available at: <https://zakon.rada.gov.ua/laws/show/v0178500-22#Text> (Accessed: 19 April 2025).

17. National Bank of Ukraine (2025), Resolution "On Amendments to Some Regulatory Acts of the National Bank of Ukraine Regarding Information Security and Cyber Protection", Available at: <https://zakon.rada.gov.ua/laws/show/v0024500-25#Text> (Accessed: 27 March 2025).

18. Krasnobayev, V. (2023), Economic and Cyber Security: Collective Monograph, Kharkiv, Ukraine, Available at: <https://www.econstor.eu/handle/10419/302598> (Accessed: 07 March 2025).

19. Anagnostopoulos, Y. (2018), "Fintech and Regtech: Impact on Regulators and Banks", Journal of Economics and Business, Available at: https://www.researchgate.net/publication/326542210_Fintech_and_Regtech_Impact_on_Regulators_and_Banks (Accessed: 11 June 2025).

20. Sunduk, T.F., Babenko-Levada, V.H., Skorba, O.A. and Chornovol, A.O. (2023), "On the Development of Digital Technologies in the Financial Sector (Ukrainian Key)", Academic Visions, vol. 17, pp. 1—7, Available at: <https://zenodo.org/records/7774205> (Accessed: 17 June 2025).

Стаття надійшла до редакції 01.08.2025 р.

<https://nayka.com.ua>

Електронне фахове видання

ДЕРЖАВНЕ УПРАВЛІННЯ
удосконалення та розвиток

Виходить 12 разів на рік

включено до переліку наукових фахових видань України
з питань **ДЕРЖАВНОГО УПРАВЛІННЯ**
(Категорія «Б»)

Наказ Міністерства освіти і науки України
від 28.12.2019 №1643

Спеціальність 281

e-mail: economy_2008@ukr.net

viber: +38 050 3820663