РОЗВИТОК ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES

УДК 336.71:004.056
doi: https://doi.org/10.15330/apred.2.22.286-301

Кохан І.В.[1], Криховецька З.М.[2], Мацьків В.В.[3]

ІННОВАЦІЙНІ БАНКІВСЬКІ ТЕХНОЛОГІЇ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ БАНКІВСЬКОЇ БЕЗПЕКИ В УМОВАХ КІБЕРЗАГРОЗ

Карпатський національний університет імені Василя Стефаника,
кафедра фінансів,
вул. Шевченка, 57, Івано-Франківськ,
76018, Україна,
тел.: 0963560132

[1]e-mail: iryna.kokhan@cnu.edu.ua
ORCID: https://orcid.org/0000-0002-9262-5723

[2]e-mail: zoriana.krykhovetska@cnu.edu.ua
ORCID: https://orcid.org/0000-0002-0028-1960

[3]e-mail: volodymyr.matskiv@cnu.edu.ua
ORCID: https://orcid.org/0000-0003-3031-7060

Анотація. Стаття спрямована на дослідження теоретичних та прикладних засад використання інноваційних банківських технологій у системі забезпечення банківської безпеки в умовах посилення кіберзагроз.

Обґрунтовано, що активна цифрова трансформація банківської діяльності, розвиток дистанційних каналів обслуговування, мобільного та інтернет-банкінгу, електронних платежів, відкритого банкінгу й сучасних інформаційно-комунікаційних технологій, поряд із підвищенням ефективності фінансових операцій, зумовлюють появу нових кіберризиків та посилюють вимоги до формування комплексної системи банківської безпеки. Доведено необхідність переходу від переважно реактивного реагування на кіберінциденти до проактивної моделі управління кіберризиками, заснованої на принципах превентивності, адаптивності, безперервності, комплексності та постійного моніторингу цифрового середовища.

Систематизовано основні напрями впровадження інноваційних технологій у банківській сфері, зокрема цифровізацію бек-офісних процесів, розвиток електронних платіжних технологій, використання хмарних сервісів, технологій штучного інтелекту та машинного навчання, біометричних методів ідентифікації, систем електронної ідентифікації, мобільного та інтернет-банкінгу, QR-платежів і блокчейн-технологій. Визначено, що зазначені технології створюють додаткові можливості для автоматизації процесів виявлення аномальної активності, прогнозування кіберзагроз, захисту інформаційних ресурсів, підвищення надійності фінансових операцій та забезпечення безперервності банківської діяльності.

Запропоновано концептуальну модель механізму забезпечення кіберстійкості банку в структурі забезпечення банківської безпеки, яка передбачає формування концепції кіберстійкості та її реалізацію через взаємопов'язані системи аналізу й прогнозування кіберзагроз, оцінювання їхнього впливу, розроблення кіберстратегії, визначення цілей, рівня толерантності та індикаторів кіберстійкості, вибору методів управління кіберризиками, формування механізмів забезпечення, моніторингу, контролю, тестування, аудиту, адаптації та відновлення після кіберінцидентів. Особливу увагу приділено комплексному оцінюванню рівня

кіберстійкості банків на основі якісних і кількісних показників, що характеризують технічні, інформаційні, управлінські та організаційні параметри її захищеності.

Обґрунтовано доцільність створення спеціалізованого Центру кіберстійкості як ключового організаційного елемента стратегічного управління кіберризиками, що забезпечує інтеграцію процесів кібербезпеки, управління ризиками, контролю якості IT-інфраструктури та підтримання безперервності бізнес-процесів. Доведено, що впровадження запропонованої моделі сприятиме своєчасному прогнозуванню, виявленню, попередженню та нейтралізації кіберзагроз, підвищенню ефективності управління кіберризиками, мінімізації фінансових і репутаційних втрат, забезпеченню стабільності функціонування банківських установ та зміцненню банківської безпеки в умовах цифрової трансформації фінансового сектору.

Ключові слова: банківська безпека, банк, банківська система, кібербезпека, кіберзахист, кіберстійкість банку, інноваційні банківські технології, цифрова трансформація, кіберризики, штучний інтелект.

Kokhan I.V.[1], Krykhovetska Z.M.[2], Matskiv V.V.[3]

INNOVATIVE BANKING TECHNOLOGIES IN THE SYSTEM OF ENSURING BANKING SECURITY UNDER CYBER THREATS

Vasyl Stefanyk Carpathian National University
Department of Finance,
Shevchenka Str., 57, Ivano-Frankivsk,
76018, Ukraine,
tel.: +380 96 356 01 32

[1]e-mail: iryna.kokhan@cnu.edu.ua
ORCID: https://orcid.org/0000-0002-9262-5723

[2]e-mail: zoriana.krykhovetska@cnu.edu.ua
ORCID: https://orcid.org/0000-0002-0028-1960

[3]e-mail: volodymyr.matskiv@cnu.edu.ua
ORCID: https://orcid.org/0000-0003-3031-7060

Abstract. The article examines the theoretical and applied foundations of using innovative banking technologies within the system of ensuring banking security under increasing cyber threats. It substantiates that the active digital transformation of banking activities, the development of remote service channels, mobile and internet banking, electronic payments, open banking, and modern information and communication technologies, while improving the efficiency of financial transactions, also generate new cyber risks and increase the requirements for establishing a comprehensive banking security system. The need to move from a predominantly reactive response to cyber incidents towards a proactive model of cyber risk management based on the principles of prevention, adaptability, continuity, comprehensiveness, and continuous monitoring of the digital environment is substantiated.

The main directions of implementing innovative technologies in the banking sector are systematized, including the digitalization of back-office processes, the development of electronic payment technologies, the use of cloud services, artificial intelligence and machine learning technologies, biometric identification methods, electronic identification systems, mobile and internet banking, QR payments, and blockchain technologies. It is determined that these technologies create additional opportunities for automating the processes of detecting anomalous activity, forecasting cyber threats, protecting information resources, improving the reliability of financial transactions, and ensuring the continuity of banking operations.

A conceptual model of the mechanism for ensuring bank cyber resilience within the banking security framework is proposed. The model provides for the development of a cyber resilience concept and its implementation through interconnected systems of cyber threat analysis and forecasting, impact assessment, cyber strategy development, determination of objectives, risk tolerance levels and

cyber resilience indicators, selection of cyber risk management methods, development of supporting mechanisms, monitoring, control, testing, auditing, adaptation, and recovery following cyber incidents. Particular attention is paid to the comprehensive assessment of a banking institution's level of cyber resilience based on qualitative and quantitative indicators characterizing the technical, informational, managerial, and organizational parameters of its security.

The expediency of establishing a specialized Cyber Resilience Center as a key organizational element of strategic cyber risk management is substantiated. Such a center ensures the integration of cybersecurity processes, risk management, IT infrastructure quality control, and business continuity management. It is proved that the implementation of the proposed model will facilitate the timely forecasting, detection, prevention, and neutralization of cyber threats, improve the effectiveness of cyber risk management, minimize financial and reputational losses, ensure the stable functioning of banking institutions, and strengthen banking security in the context of the digital transformation of the financial sector.

Keywords: banking security, bank, banking system, cybersecurity, cyber protection, bank cyber resilience; innovative banking technologies; digital transformation; cyber risks; artificial intelligence.

Вступ. Сучасний етап розвитку банківського сектору характеризується стрімким проникненням цифрових технологій у всі сфери діяльності фінансових установ. Автоматизація внутрішніх процесів, поширення дистанційного обслуговування, розвиток мобільних застосунків, інтернет-банкінгу та цифрових платіжних сервісів істотно трансформують традиційну модель функціонування банків. Поряд із підвищенням оперативності фінансових операцій, розширенням спектра послуг і покращенням клієнтського досвіду цифрова трансформація формує новий комплекс загроз, пов’язаних із зростанням технологічної залежності банків та розширенням їх цифрової поверхні атаки. За таких умов питання захисту інформаційних ресурсів, фінансових активів і критично важливої банківської інфраструктури набувають стратегічного значення для забезпечення стабільності окремих банків і фінансової системи загалом.

Розвиток цифрового фінансового середовища супроводжується трансформацією характеру кіберзагроз. Сучасні кібератаки відзначаються високим рівнем складності, цілеспрямованістю та здатністю одночасно впливати на значну кількість інформаційних систем і користувачів. Фішингові кампанії, методи соціальної інженерії, шкідливе програмне забезпечення, DDoS-атаки, несанкціонований доступ до інформаційних ресурсів і різноманітні форми цифрового шахрайства створюють суттєві ризики для безперервності банківської діяльності. Додатковими чинниками розширення кіберризиків виступають розвиток Open Banking, інтеграція цифрових платформ, застосування штучного інтелекту та зростання масштабів обміну даними між різними учасниками фінансового ринку. Це актуалізує необхідність перегляду традиційних підходів до забезпечення банківської безпеки та формування більш гнучких і адаптивних систем кіберзахисту.

Особливої ваги зазначена проблематика набуває для України в умовах воєнного стану та функціонування національної економіки в середовищі постійних гібридних загроз. Повномасштабна військова агресія російської федерації супроводжується посиленням кібернетичного впливу на об’єкти критичної інфраструктури, державні інформаційні ресурси, платіжну інфраструктуру та фінансові установи. У таких обставинах безпека банківського сектору виходить за межі внутрішнього корпоративного завдання та перетворюється на важливу складову економічної й національної безпеки держави. Це зумовлює потребу в удосконаленні механізмів виявлення та нейтралізації кіберінцидентів, розвитку систем моніторингу, посиленні регуляторного впливу та забезпеченні скоординованої взаємодії банківських установ із суб’єктами національної системи кіберзахисту.

Водночас процес цифровізації доцільно розглядати не лише як джерело нових вразливостей, а і як важливий ресурс посилення банківської безпеки. Інноваційні технології створюють передумови для переходу від переважно реактивної моделі протидії кіберзагрозам до проактивного управління ризиками, коли банк заздалегідь виявляє потенційні ризики, прогнозує можливі атаки та вживає заходів для їх попередження. Застосування штучного інтелекту та алгоритмів машинного навчання дає змогу оперативно виявляти аномалії та прогнозувати потенційно небезпечні події; блокчейн-технології сприяють підвищенню цілісності та прозорості інформаційних потоків; біометрична ідентифікація й багатофакторна автентифікація забезпечують додатковий рівень захисту доступу до фінансових сервісів і персональних даних. Таким чином, інноваційні банківські технології поступово трансформуються з інструменту підвищення операційної ефективності у важливий елемент формування кіберстійкості та забезпечення комплексної банківської безпеки.

Проблематика різних аспектів банківської безпеки протягом останніх років знайшла відображення у наукових працях таких дослідників, як Коваленко В., Фімяр С., Сімаков С., Кирєєва І., Коробцова Д., Сидорович О., Буковський М. та інших [1–5]. Значний внесок у розвиток наукових підходів до вивчення впливу банківських інновацій і цифрової трансформації на банківську безпеку зробили Бондарук Т., Бондарук О., Пшик Б., Колодізєв О., Береговий В., Денисенко В., Прощаликіна А., Гаврилюк Ю. та інші [6–9]. Сучасні наукові підходи підтверджують необхідність розгляду банківських інновацій не лише з позиції їхнього економічного та сервісного ефекту, а й у контексті їх впливу на рівень захищеності та кіберстійкості банків.

Водночас, попри значний обсяг досліджень, присвячених окремо питанням безпеки банківських установ та розвитку банківських інновацій, взаємозв’язок між технологічною модернізацією банків і формуванням сучасних механізмів забезпечення їхньої безпеки ще не отримав достатнього комплексного висвітлення. Таким чином, актуальність дослідження інноваційних банківських технологій у системі забезпечення банківської безпеки визначається необхідністю пошуку нових підходів до протидії кіберзагрозам в умовах поглиблення цифрової трансформації банківського сектору. Комплексне дослідження можливостей сучасних технологій, механізмів управління кіберризиками та інструментів формування кіберстійкості має важливе значення для підвищення надійності банківських установ, забезпечення безперервності їх діяльності, збереження довіри клієнтів і зміцнення стабільності банківської системи як складової економічної безпеки держави.

Постановка завдання. Метою статті є обґрунтування ролі інноваційних банківських технологій у системі забезпечення банківської безпеки в умовах посилення кіберзагроз, розроблення концептуальної моделі механізму забезпечення кіберстійкості банку, визначення її структурних і функціональних складових, основних інструментів реалізації та підходів до оцінювання рівня кіберстійкості. Методологічною основою дослідження стали системний, комплексний, ризик-орієнтований та процесний підходи. У процесі дослідження використано методи аналізу і синтезу – для узагальнення теоретичних підходів до забезпечення банківської безпеки, управління кіберризиками та визначення ролі інноваційних технологій у підвищенні кіберстійкості банків; системно-структурний метод – для визначення основних складових механізму забезпечення кіберстійкості банку; метод логічного моделювання – для розроблення концептуальної моделі та встановлення взаємозв’язків між її структурними й функціональними елементами; порівняльний метод – для узагальнення міжнародних підходів і стандартів у сфері кібербезпеки та кіберстійкості фінансових установ; методи узагальнення та класифікації – для систематизації інноваційних банківських технологій

і методів управління кіберризиками; графічний метод – для візуалізації запропонованої моделі механізму забезпечення кіберстійкості банку.

Результати. Формування належного рівня банківської безпеки у сучасних умовах дедалі більше залежить від рівня їх технологічного розвитку. Традиційні інструменти ризик-менеджменту вже не можуть повною мірою забезпечити захист банку без інтеграції сучасних цифрових рішень. Використання інформаційно-комунікаційних технологій, цифрових платформ, мережевих систем та інтелектуальних алгоритмів обробки даних сприяє прискоренню банківських операцій, підвищенню їх точності та розвитку нових моделей обслуговування клієнтів. Разом із тим розширення цифрового середовища функціонування банків супроводжується збільшенням кількості потенційних точок кібервразливості. Унаслідок цього складовими сучасної системи банківської безпеки стають питання кіберзахисту, протидії кіберзлочинності та забезпечення стійкості інформаційної інфраструктури.

Подальше поширення цифрових сервісів істотно трансформує характер взаємодії між банківською установою та її клієнтами. Значна частина фінансових операцій переміщується до цифрового простору, де доступ до послуг забезпечується через інтернет-платформи, мобільні застосунки та інші дистанційні канали. Автоматизація банківських процесів дає можливість оптимізувати операційні витрати, скоротити час проведення транзакцій і персоналізувати фінансові послуги. Саме тому розвиток мобільного та інтернет-банкінгу, електронних платіжних інструментів, POS-інфраструктури та інших цифрових сервісів є важливим напрямом підвищення конкурентоспроможності банків. Водночас масштабування таких технологій потребує відповідного посилення механізмів захисту цифрової інфраструктури та даних користувачів.

У міру поглиблення цифровізації банківська безпека набуває комплексного характеру та поєднує фінансову стійкість, інформаційну захищеність і технологічну надійність. Тому оцінювання рівня безпеки банківської установи доцільно здійснювати не лише за традиційними фінансовими показниками, а й із урахуванням параметрів, що характеризують її здатність протидіяти кіберзагрозам. Запропонована система індикаторів дозволяє комплексно оцінити організаційну готовність банку, рівень захищеності його цифрової інфраструктури, масштаби використання дистанційних технологій та спроможність своєчасно виявляти й нейтралізувати кіберінциденти (табл. 1):

Таблиця 1

Система індикаторів оцінювання банківської безпеки в умовах кіберзагроз

Table 1

A system of indicators for assessing banking security under cyber threats

Індикатор	Зміст та аналітична характеристика
Інституційна спроможність щодо управління кіберризиками	Характеризує наявність у структурі банку спеціалізованих підрозділів або відповідальних функціональних напрямів, що здійснюють ідентифікацію, оцінювання, моніторинг і координацію заходів із мінімізації кіберризиків. Відображає рівень організаційної готовності банку до протидії цифровим загрозам та інтеграцію кіберризиків у загальну систему управління ризиками.
Масштаб і технологічна складність цифрової інфраструктури	Відображає кількість і рівень розвитку банкоматів, POS-терміналів, платіжних пристроїв та інших технічних елементів цифрової екосистеми банку. Зростання кількості підключених пристроїв розширює можливості обслуговування клієнтів, але водночас збільшує потенційну поверхню для здійснення кібератак.

Продовження табл.1

Рівень розвитку дистанційного банківського обслуговування	Характеризує ступінь використання інтернет-банкінгу, мобільних застосунків та інших цифрових каналів взаємодії з клієнтами. Дозволяє оцінити рівень цифрової трансформації банку та одночасно визначити масштаби потенційних ризиків, пов'язаних із несанкціонованим доступом і компрометацією даних.
Інтенсивність використання мобільних банківських технологій	Визначається масштабами застосування клієнтами мобільних додатків для здійснення платежів, переказів та інших банківських операцій. Показник характеризує рівень інтеграції мобільних технологій у бізнес-модель банку та залежність банківських сервісів від безпеки мобільного цифрового середовища.
Частка активних користувачів цифрових каналів	Відображає питому вагу клієнтів, які регулярно використовують онлайн-сервіси банку. Високе значення показника свідчить про рівень цифрової активності та довіри клієнтів, але водночас посилює необхідність захисту персональних даних, облікових записів і фінансових операцій від шахрайських дій.
Рівень комплексного захисту інформаційних ресурсів	Характеризує ступінь впровадження технічних і програмних засобів забезпечення конфіденційності, цілісності та доступності банківської інформації. Передбачає використання систем криптографічного захисту, міжмережевих екранів, антивірусних засобів, технологій резервного копіювання та інших механізмів захисту цифрових активів.
Автоматизація виявлення та реагування на кіберінциденти	Відображає рівень використання систем централізованого моніторингу подій інформаційної безпеки, засобів аналізу аномальної активності та автоматизованих інструментів реагування. Застосування таких технологій сприяє скороченню часу виявлення кіберінцидентів і зменшенню потенційного масштабу їх наслідків.
Захищеність цифрової взаємодії та міжбанківських комунікацій	Характеризує рівень безпеки інформаційного обміну між банком, платіжними системами та іншими учасниками фінансового ринку. Оцінюється з урахуванням використання захищених каналів зв'язку, криптографічних технологій, безпечних API та інших інструментів захисту міжсистемної взаємодії.
Інтеграція технологій штучного інтелекту в систему кіберзахисту	Відображає рівень застосування алгоритмів штучного інтелекту та машинного навчання для аналізу великих масивів даних, виявлення нетипових операцій, прогнозування кіберзагроз і підтримки прийняття рішень щодо реагування на інциденти.
Надійність архітектури зберігання та обробки банківських даних	Характеризує рівень організації інформаційних потоків і використання сучасних моделей управління базами даних, зокрема архітектури «клієнт–сервер». Відображає здатність банківської інформаційної системи забезпечувати контрольований доступ до даних, стабільність їх обробки, резервування та зниження ризиків втрати або пошкодження інформації.

Розроблено авторами на основі джерел [10,11,13,15,16,18].

Дослідження теоретичних положень і практичних підходів до забезпечення банківської безпеки свідчить про доцільність розмежування відповідних інструментів за джерелом та рівнем їх застосування. У цьому контексті систему забезпечення банківської безпеки можна умовно структурувати на внутрішній і зовнішній контури. Основою такого поділу є подвійна природа функціонування банківської установи.

З одного боку, банк є самостійним учасником фінансового ринку, який приймає управлінські рішення, формує власну систему ризик-менеджменту, визначає напрями розвитку та створює внутрішні механізми захисту своїх фінансових і інформаційних ресурсів. Саме на рівні окремої банківської установи реалізуються заходи щодо підтримання ліквідності, платоспроможності, операційної надійності та протидії

внутрішнім і зовнішнім загрозам. З іншого боку, діяльність банків здійснюється в межах загальнодержавної системи регулювання, у якій уповноважені органи встановлюють обов'язкові вимоги, здійснюють банківський нагляд, визначають регуляторні обмеження та застосовують інструменти впливу, спрямовані на підтримання стабільності фінансового сектору. Отже, рівень безпеки окремого банку формується під впливом як внутрішніх управлінських рішень, так і зовнішнього інституційно-регуляторного середовища.

Особливого значення технологічні інновації набувають у системі забезпечення банківської безпеки. Їх використання дозволяє автоматизувати контроль за інформаційними потоками, оперативніше виявляти потенційні загрози, знижувати ймовірність шахрайських операцій та забезпечувати безперервність критично важливих банківських процесів. Тому в умовах поширення цифрових технологій інноваційний розвиток доцільно розглядати як один із напрямів зміцнення кіберстійкості банків. Основні технологічні напрями, що мають найбільш суттєвий вплив на рівень захищеності банківської діяльності, можна представити таким чином:

1) Цифрова трансформація внутрішніх операційних процесів. Автоматизація цих процесів дає змогу зменшити частку ручної роботи, прискорити обробку інформації, знизити операційні витрати та підвищити точність виконання процедур. Водночас цифрові системи контролю сприяють дотриманню регуляторних вимог і підвищують надійність внутрішнього управління.

2) Удосконалення цифрових платіжних інструментів. Цифровий формат транзакцій забезпечує можливість фіксації та подальшого аналізу операцій, що створює додаткові можливості для контролю за рухом коштів. Аналіз параметрів платежів дозволяє оперативніше виявляти нетипову активність, ідентифікувати потенційно шахрайські дії та застосовувати відповідні обмежувальні заходи.

3) Застосування хмарної інфраструктури. Хмарні рішення розширюють можливості банків щодо зберігання, оброблення та резервування значних обсягів інформації. Використання спеціалізованої цифрової інфраструктури сприяє гнучкішому управлінню інформаційними ресурсами та створює умови для масштабування банківських систем.

4) Використання штучного інтелекту та інтелектуальних цифрових сервісів. Технології штучного інтелекту застосовуються як для автоматизації комунікації з клієнтами, так і для аналітичної обробки значних масивів інформації.

5) Розвиток P2P-моделей фінансування. Peer-to-Peer-платформи забезпечують можливість прямої взаємодії між сторонами, які мають потребу в залученні та наданні фінансових ресурсів. Така модель зменшує кількість традиційних посередницьких ланок і створює альтернативні канали доступу до фінансування.

6) Біометрична верифікація користувачів. Одним із перспективних напрямів посилення захисту доступу до банківських послуг є використання унікальних фізіологічних або поведінкових характеристик людини. У поєднанні з іншими механізмами автентифікації біометричні технології сприяють підвищенню рівня захисту персональної та фінансової інформації.

7) Електронна ідентифікація на основі BankID. Системи дистанційної електронної ідентифікації створюють можливість підтвердження особи користувача під час отримання цифрових послуг без необхідності особистого відвідування установи. BankID забезпечує організований обмін необхідними ідентифікаційними даними між учасниками системи із застосуванням визначених механізмів захисту інформації. Використання такого підходу сприяє зменшенню ризиків неправомірного використання персональних даних та створює більш зручні умови для доступу до банківських і інших цифрових сервісів.

8) Розвиток мобільного та веббанкінгу. Мобільні застосунки й вебплатформи перетворилися на один з основних каналів взаємодії банків із клієнтами. Вони забезпечують постійний доступ до рахунків, можливість контролювати рух коштів і здійснювати широкий спектр операцій у режимі реального часу. Водночас безпечне функціонування таких сервісів потребує застосування багаторівневих процедур перевірки користувачів, зокрема поєднання паролів, одноразових кодів, біометричних параметрів та інших факторів автентифікації.

9) Використання QR-технологій у платіжних операціях. QR-коди стали одним із доступних інструментів ініціювання безготівкових розрахунків. Їх застосування дозволяє швидко передавати параметри платежу та здійснювати операцію за допомогою мобільного пристрою. Такий спосіб розрахунків спрощує взаємодію між платником і отримувачем коштів та сприяє подальшому розвитку цифрових платіжних сервісів. Водночас безпека таких операцій значною мірою залежить від захищеності платіжної інфраструктури, достовірності сформованих кодів і належної автентифікації користувачів.

10) Використання технології блокчейн. Перспективним напрямом розвитку цифрової інфраструктури є застосування технологій розподіленого реєстру. Блокчейн забезпечує послідовне фіксування операцій у взаємопов'язаній структурі записів, що ускладнює непомітне внесення змін до вже сформованої інформації. Поєднання розподіленого зберігання даних і криптографічних механізмів може сприяти підвищенню контролю за цілісністю інформації та простежуваністю окремих операцій. Це створює потенційні можливості для зниження окремих операційних ризиків і підвищення надійності цифрової взаємодії [7, 8, 9, 13,17].

У цьому контексті одним із пріоритетних напрямів діяльності банківських установ є формування цілісної системи кіберзахисту, здатної забезпечувати своєчасне виявлення, попередження та нейтралізацію цифрових загроз. Важливими складовими такої системи є регулярне оновлення програмно-технічних засобів захисту, розвиток компетентностей персоналу у сфері кібербезпеки, постійний моніторинг інформаційного середовища та розроблення алгоритмів дій у разі виникнення кіберінцидентів. Поєднання технологічного розвитку із належним рівнем захисту інформаційних ресурсів створює передумови для підтримання стабільної роботи банку, збереження довіри клієнтів і забезпечення надійності фінансових операцій у цифровому середовищі [13].

Кіберризики, що виникають у фінансовій сфері, мають комплексний характер і здатні впливати не лише на діяльність окремої банківської установи, а й на стабільність усієї фінансової системи. Саме тому управління такими ризиками не повинно обмежуватися реагуванням на вже здійснені атаки. Воно має передбачати систематичне оцінювання потенційних загроз, прогнозування можливих сценаріїв їх розвитку, упровадження превентивних заходів та постійне підвищення рівня кіберстійкості [10] .

Система кіберзахисту банківської системи України формується за багаторівневим принципом, у межах якого важливе місце посідає Національний банк України. НБУ виконує функції секторального органу у сфері кіберзахисту банківської системи, бере участь у забезпеченні захисту критичної інфраструктури фінансового сектору та координує розвиток відповідних організаційних і регуляторних механізмів. Внутрішня структура центрального банку передбачає функціонування спеціалізованих підрозділів, діяльність яких спрямована на захист критичної інфраструктури та розвиток системи кібербезпеки банківського сектору.

Нормативну основу організації цих процесів формують вимоги Національного банку України щодо побудови та функціонування систем кіберзахисту. Зокрема, важливе значення має постанова Правління НБУ від 12 серпня 2022 року № 178, якою

визначено основні вимоги до організації кіберзахисту, функціонування відповідних систем і процедур, а також підходи до взаємодії суб'єктів банківської системи [18].

Важливою складовою сучасної системи протидії кіберзагрозам є оперативний обмін інформацією про виявлені інциденти, уразливості та потенційні способи здійснення атак. Для забезпечення такого інформаційного обміну використовується спеціалізована платформа MISP-NBU Центру кіберзахисту НБУ, створена на основі міжнародного програмного рішення MISP та адаптована до потреб українського кіберсередовища. Її функціонування забезпечує можливість поширення технічної інформації про індикатори компрометації, виявлені кіберзагрози та рекомендації щодо їх попередження і нейтралізації.

Значення такого інформаційного середовища полягає у формуванні єдиного простору взаємодії між фінансовими установами та спеціалізованими структурами, відповідальними за реагування на кіберінциденти. Зокрема, взаємодія із CERT-UA та іншими суб'єктами національної системи кібербезпеки сприяє оперативнішому поширенню інформації про актуальні загрози та координації заходів реагування.

Окремим елементом інституційного забезпечення кібербезпеки банківської системи є Центр реагування на кіберінциденти FinCERT при НБУ. Його діяльність пов'язана з аналізом поточної ситуації у сфері кіберзагроз, поширенням попереджувальної інформації, організацією обміну даними щодо кіберінцидентів та наданням методичної підтримки фінансовим установам. Функціонування таких координаційних центрів дає можливість перейти від ізольованого реагування окремих банків до формування спільної системи протидії кіберзагрозам [11].

Водночас забезпечення кіберстійкості банківської системи потребує тісної взаємодії з іншими державними інституціями. Важливу роль у цьому процесі відіграють підрозділи Національної поліції України, відповідальні за протидію кіберзлочинності, а також структури Державної служби спеціального зв'язку та захисту інформації України, діяльність яких спрямована на реагування на кіберінциденти, захист державних інформаційних ресурсів та розвиток загальнонаціональної системи кібербезпеки.

Особливого значення в умовах зростання транскордонних кіберзагроз набуває міжнародна взаємодія. Обмін досвідом, використання міжнародних практик, залучення технічної та експертної підтримки сприяють посиленню спроможності українського фінансового сектору протидіяти складним кібератакам. Зокрема, співробітництво Національного банку України з міжнародними партнерами створює можливості для розвитку інституційної спроможності Центру кіберзахисту, упровадження сучасних підходів до управління кіберризиками та вдосконалення системи інформаційного обміну щодо актуальних загроз [14].

Таким чином, кіберризики доцільно розглядати як одну із системних загроз стабільності банківської системи. Їх мінімізація потребує поєднання технологічної модернізації, безперервного моніторингу цифрового середовища, розвитку спеціалізованих центрів реагування, ефективної міжвідомчої координації та розширення міжнародного співробітництва. За такого підходу кіберстійкість стає не окремим напрямом діяльності банку, а важливою складовою його загальної системи безпеки.

Банківський сектор посідає стратегічне місце у забезпеченні стабільного функціонування національної економіки. Банки забезпечують рух фінансових ресурсів, здійснюють посередництво між власниками капіталу та його споживачами, підтримують функціонування платіжної системи, сприяють кредитуванню економіки та реалізації інвестиційних процесів. Саме тому порушення стабільності банківської системи може мати масштабні наслідки для економічної та національної безпеки

держави. У цьому контексті банківські установи та відповідна фінансова інфраструктура розглядаються як важливі елементи критичної інфраструктури, безперебійність функціонування яких має стратегічне значення [16].

Подальший розвиток цифрової економіки та поширення технологій Індустрії 4.0 формують принципово нове середовище функціонування банків. Активне використання штучного інтелекту, хмарних і розподілених обчислень, Інтернету речей, технологій аналізу великих даних, блокчейну та інших цифрових рішень сприяє модернізації банківських процесів. Водночас технологічне ускладнення інформаційної інфраструктури супроводжується появою нових векторів атак і збільшенням кількості потенційних загроз. Унаслідок цього кіберзагрози характеризуються високою динамічністю та постійно трансформуються відповідно до розвитку цифрових технологій [12].

Міжнародний досвід свідчить, що питання кіберстійкості фінансових установ поступово переходить до категорії ключових напрямів фінансового регулювання. Значну увагу цій проблематиці приділяє Європейський центральний банк, який розробив систему рекомендацій щодо нагляду за кіберстійкістю учасників фінансової інфраструктури.

Зокрема, документ Cyber Resilience Oversight Expectations визначає основні підходи до оцінювання рівня кіберзахисту та формування внутрішніх механізмів управління кіберризиками [15]. Використання міжнародних стандартів і рекомендацій сприяє уніфікації підходів до оцінювання кіберстійкості та формуванню спільних принципів забезпечення безперервності функціонування фінансової інфраструктури.

Практичне оцінювання готовності фінансових установ до протидії складним кібератакам передбачає застосування спеціальних методик тестування. Одним із таких підходів є методологія Threat Intelligence-based Ethical Red Teaming (TIBER-EU), розроблена для моделювання реалістичних сценаріїв кібернетичних атак на критичну фінансову інфраструктуру [13]. Контрольоване моделювання дій потенційного зловмисника дає можливість перевірити ефективність наявних механізмів захисту, оцінити швидкість виявлення загроз і визначити спроможність банку відновлювати свою діяльність після реалізації кіберінциденту.

За таких умов кіберстійкість банку доцільно трактувати як комплексну характеристику її здатності підтримувати стабільне функціонування в умовах реалізації кіберзагроз. Вона має подвійний характер. З одного боку, кіберстійкість є об'єктом управління та регуляторного контролю, що передбачає формування відповідних політик, процедур, систем контролю та розподілу відповідальності. З іншого боку, вона відображає внутрішню спроможність банку забезпечувати цілісність власних процесів, захищати критичні інформаційні ресурси та підтримувати операційну діяльність навіть за умов деструктивного зовнішнього впливу.

Саме тому параметри кіберстійкості мають бути інтегровані до загальної системи стратегічного управління банком. Їх доцільно враховувати під час визначення стратегічних цілей, оцінювання рівня ризиків, формування інвестиційної політики у сфері цифрових технологій та встановлення показників ефективності діяльності. Такий підхід дозволяє розглядати кібербезпеку не як відокремлену технічну функцію, а як один із чинників довгострокової фінансової та операційної стійкості банківської установи.

Оцінювання рівня кіберстійкості передбачає використання не лише кількісних, а й якісних характеристик. До останніх належать рівень сформованості внутрішніх політик, наявність процедур управління кіберризиками, ефективність організаційної структури, рівень підготовки персоналу та здатність відповідних підрозділів

координувати дії у разі виникнення кіберінциденту. Такий підхід дозволяє визначити фактичну готовність банку до функціонування в умовах цифрових загроз.

Особливої актуальності комплексне оцінювання набуває в умовах поширення складних і багатовекторних кібератак. DDoS-атаки, фішингові кампанії, використання програм-вимагачів та атаки через цифрові ланцюги постачання можуть одночасно впливати на різні елементи інформаційної інфраструктури. Тому важливим є не лише наявність окремих технічних засобів захисту, а й узгодженість усіх процесів, пов'язаних із виявленням, аналізом, локалізацією, нейтралізацією наслідків та відновленням функціонування банківських систем.

Узагальнюючи результати проведеного дослідження, запропоновано авторську модель механізму забезпечення кіберстійкості банку як складової системи банківської безпеки, що представлена на рис. 1.

Запропонований механізм формування та підтримання кіберстійкості банку створює основу для системного дослідження цифрового середовища її функціонування. Його застосування дає змогу своєчасно виявляти наявні та потенційні кіберзагрози, визначати найбільш уразливі елементи інформаційної інфраструктури, оцінювати ймовірні наслідки реалізації кіберризиків і прогнозувати виникнення нових типів кіберінцидентів. Водночас механізм забезпечує взаємоузгоджене використання превентивних, адаптаційних і відновлювальних заходів, спрямованих на збереження функціональної спроможності банку та мінімізацію негативних наслідків кібератак.

Важливою передумовою результативного функціонування системи кіберстійкості є належне організаційне забезпечення. Воно передбачає чіткий розподіл повноважень, відповідальності та функціональних завдань між усіма учасниками процесу кіберзахисту, управління цифровими ризиками й підтримання безперервності банківської діяльності. При цьому організаційна модель не може бути універсальною для всіх фінансових установ, оскільки її структура має враховувати масштаби банку, специфіку його операцій, рівень цифрової трансформації, архітектуру інформаційних систем, обсяг клієнтських сервісів та ресурсні можливості у сфері кібербезпеки і ризик-менеджменту.

На основі проведеного дослідження запропоновано формування спеціалізованого Центру кіберстійкості банку**,** який доцільно розглядати як координаційний орган стратегічного управління процесами протидії кіберризикам. До його діяльності мають бути залучені представники структурних підрозділів, відповідальних за інформаційну безпеку, управління кіберризиками, стабільність функціонування IT-систем, безперервність бізнес-процесів та відновлення операційної діяльності. Такий підхід забезпечує узгодження інтересів і дій бізнесових, технологічних та операційних підрозділів, формуючи єдиний контур управління кіберстійкістю.

Функціонування Центру кіберстійкості передбачає розроблення системи показників оцінювання результативності, зокрема спеціалізованих індикаторів і KPI, визначення критеріїв допустимого рівня кіберризику, організацію постійного моніторингу цифрового середовища та координацію заходів реагування на кіберінциденти. Це дозволяє забезпечити своєчасне виявлення внутрішніх і зовнішніх загроз, оцінювання їхнього потенційного впливу, вибір адекватних інструментів протидії та оперативне відновлення критично важливих процесів. Отже, кіберстійкість банку формується внаслідок взаємодії організаційно-управлінських, технологічних, інформаційних і методичних складових.

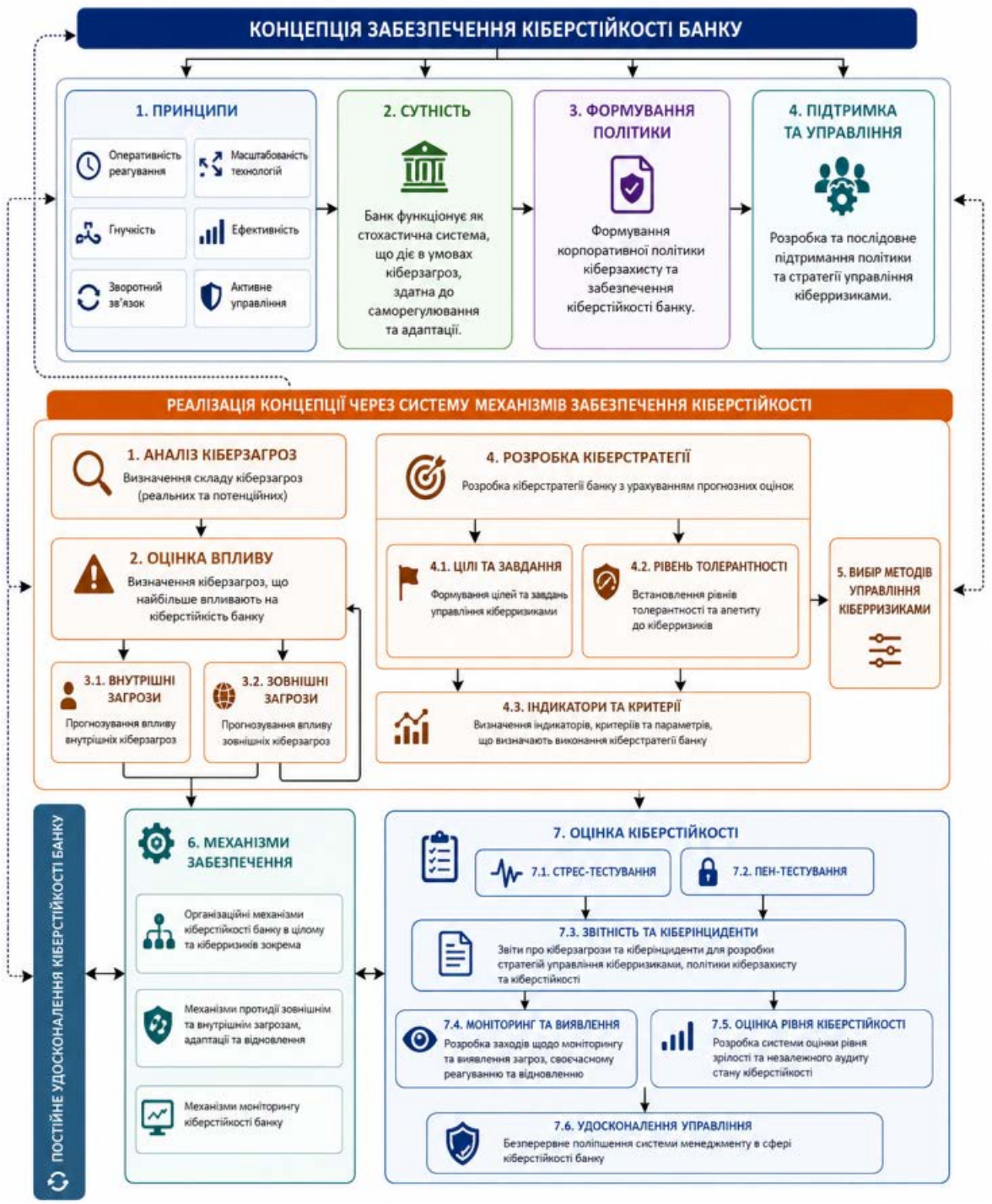

Рис. 1. Модель механізму забезпечення кіберстійкості банку в структурі забезпечення банківської безпеки

Fig.1. A model of the mechanism for ensuring a bank's cybersecurity within the framework of banking security

Розроблено авторами

Оцінювання рівня кіберстійкості банку доцільно здійснювати у двох площинах. Перша передбачає якісну характеристику**,** що відображає спроможність банку зберігати безперервність своєї діяльності, адаптуватися до динамічних кіберзагроз та підтримувати належний рівень функціонування за умов виникнення кіберінцидентів. Друга ґрунтується на використанні системи оціночних параметрів**,** до складу якої

входять якісні та кількісні індикатори технічного, інформаційного, організаційного, управлінського й операційного характеру. Сукупність таких показників дозволяє комплексно визначати стан захищеності банку та рівень практичної реалізації заходів із забезпечення його кіберстійкості.

Розроблена модель передбачає послідовне формування концептуальних засад забезпечення кіберстійкості та їх практичну реалізацію через взаємопов'язані процедури оцінювання, моніторингу, контролю, аудиту, адаптації й відновлення. У центрі цієї системи знаходиться Центр кіберстійкості**,** який виконує координаційну функцію та забезпечує стратегічне узгодження рішень у сфері управління кіберризиками з іншими напрямами діяльності банку.

Таким чином, підтримання належного рівня кіберстійкості є однією з визначальних умов стабільного функціонування банківських установ у середовищі, де цифрові ризики постійно змінюються, ускладнюються та набувають системного характеру. Досягнення цієї мети залежить не лише від використання сучасних засобів технічного захисту, а й від побудови ефективної системи управління, яка забезпечує координацію відповідальних структурних підрозділів, своєчасність прийняття рішень і безперервність ключових банківських процесів.

Практичне впровадження запропонованого механізму дає можливість об'єднати управління кіберризиками, інформаційною безпекою, розвитком і надійністю IT-інфраструктури та забезпеченням безперервності діяльності в межах єдиної процесно-орієнтованої системи. Така інтеграція сприятиме підвищенню якості управлінських рішень, удосконаленню процедур виявлення й локалізації кіберінцидентів, скороченню часу реагування та зменшенню можливих фінансових і операційних втрат.

Висновки. В умовах активної цифрової трансформації фінансового сектору, розвитку дистанційних каналів банківського обслуговування, поширення інноваційних технологій та постійного зростання масштабів і складності кіберзагроз забезпечення стабільного функціонування банківських установ потребує переходу від фрагментарного реагування на окремі кіберінциденти до формування комплексної системи забезпечення банківської безпеки та кіберстійкості. Така система має ґрунтуватися на принципах превентивності, адаптивності, комплексності, безперервності, ризик-орієнтованого управління, технологічної модернізації та постійного моніторингу, що забезпечує своєчасне виявлення кіберзагроз, прогнозування їх можливих наслідків і прийняття обґрунтованих управлінських рішень.

Інноваційні банківські технології виступають не лише чинником цифрової трансформації та підвищення ефективності банківської діяльності, а й важливим інструментом зміцнення системи банківської безпеки. Використання цифрових технологій, електронних платіжних систем, хмарних сервісів, штучного інтелекту, машинного навчання, біометричної ідентифікації, систем електронної ідентифікації, мобільного та інтернет-банкінгу, QR-платежів і блокчейн-технологій створює додаткові можливості для автоматизації процесів виявлення аномальної активності, прогнозування кіберзагроз, захисту інформаційних ресурсів, запобігання шахрайству та забезпечення безперервності фінансових операцій.

Центральним елементом запропонованого механізму виступає циклічний процес забезпечення кіберстійкості, який охоплює ідентифікацію та аналіз кіберзагроз, оцінювання їх потенційного впливу на діяльність банку, прогнозування ризиків, розроблення кіберстратегії, визначення цілей і допустимого рівня ризику, вибір методів управління кіберризиками, реалізацію захисних заходів, постійний моніторинг, контроль, тестування, аудит, адаптацію та відновлення після кіберінцидентів. Саме безперервність такого циклу забезпечує здатність банківської установи оперативно

адаптуватися до зміни цифрового середовища, мінімізувати негативні наслідки кібератак та підтримувати стабільність критично важливих бізнес-процесів.

Запропонована концептуальна модель механізму забезпечення кіберстійкості банку формує сучасний підхід до управління банківською безпекою, в основі якого лежить інтеграція інноваційних технологій, ризик-орієнтованого управління, безперервного моніторингу та організаційної взаємодії. Її практична реалізація сприятиме своєчасному прогнозуванню, виявленню, попередженню та нейтралізації кіберзагроз, підвищенню ефективності управління кіберризиками, мінімізації фінансових, операційних і репутаційних втрат, забезпеченню безперервності функціонування банківських установ та зміцненню стійкості банківської системи в умовах цифрової трансформації та посилення кіберзагроз.

1. Коваленко, В. Фінансова безпека банків в умовах воєнного стану. *Фінансовий простір*. 2023. №4(48). С. 81-93. URL: https://doi.org/10.30970/fp.4(48).2022.819394 (дата звернення: 15.06.2026)
2. Фімяр, С., Сімаков, С. Теоретичні основи забезпечення економічної безпеки діяльності банківських установ. *Таврійський науковий вісник. Серія: Економіка*. 2024. №21. С. 127-132. URL: https://doi.org/10.32782/2708-0366/2024.21.13 (дата звернення: 15.06.2026)
3. Кирєєва І. В., Коробцова Д. В. Заходи забезпечення контролю та безпеки у сфері банківської діяльності в умовах дії правового режиму воєнного стану. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція.* 2025. Вип. 73. С. 27-30. DOI https://doi.org/10.32782/2307-1745.2025.73.5 (дата звернення: 15.06.2026)
4. Сидорович О. Ю., Буковський М. М. Чинники фінансової стабільності банківської системи України як індикатор економічної безпеки держави. *Фінансовий простір*. 2025. № 3. С. 101-111. DOI: https://doi.org/10.30970/fp.3(57).2025.101110111 (дата звернення: 15.06.2026)
5. Криховецька З.М., Кохан І.В. Фінансова безпека банківських установ: теоретичні засади та управління в сучасних умовах. *Актуальні питання в сучасній науці.* 2026. № 4(46). С. 280-291. https://doi.org/10.52058/2786-6300-2026-4(46)-280-291 (дата звернення: 15.06.2026).
6. Бондарук Т. Г., Бондарук О. С. Управлінський та інформаційно-аналітичний аспекти розвитку цифрових банківських продуктів і технологій у контексті забезпечення економічної безпеки банків. *Статистика України*. 2025. № 4. С. 79–90. Doi: 10.31767/su.4(111)2025.04.08 (дата звернення: 15.06.2026)
7. Пшик Б. І. Вплив цифровізації на фінансову стабільність банківської системи та економічну безпеку держави. *Фінансовий простір*. 2025. № 3. С. 20-30. DOI: https://doi.org/10.30970/fp.3(57).2025.202930 (дата звернення: 15.06.2026)
8. Колодізєв О. М., Береговий В. О. Фінансова безпека банків в умовах воєнного стану: вплив диджитал-інструментів та інновацій. *Бізнес Інформ*. 2024. № 9. С. 335-341. DOI: https://doi.org/10.32983/2222-4459-2024-9-335-341 (дата звернення: 15.06.2026)
9. Денисенко В. О., Прощаликіна А. М., Гаврилюк Ю. М. Цифровізація банківської системи України: виклики та можливості для фінансової безпеки. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2025. № 9(1). С. 43–48. DOI: 10.25313/2520-2294-2025-9-11401 (дата звернення: 15.06.2026)
10. Хомишин І., Гавц О. Забезпечення кібербезпеки у фінансовому секторі: правовий та технологічний аспекти. *Електронне наукове видання «Науковий вісник Ужгородського національного університету». Серія: Право*. 2023. Т. 10, № 40. С. 170–178. URL: https://doi.org/10.23939/law2023.40.170 (дата звернення: 10.06.2026)
11. DDOS-атаки, що здійснювалися на українські банки. *НАБУ*. URL: https://nabu.ua/ua/ddos-ataki-shcho-zdiysnyuvalisya-na-ukrayinski-banki-vidbito.html (дата звернення: 10.06.2026).
12. Річний звіт системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Опер. центр реагування на кіберінциденти Держ. центру кіберзах. Держ. служби спец. зв'язку та зах. інформації. 2024. 24 с. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 15.06.2026).
13. Фінтех Інсайдер. Кібербезпека як ключовий фінтех-тренд року: що варто знати про загрози та захист. URL: https://fintechinsider.com.ua/kiberbezpeka-yak-klyuchovyj-finteh-trend-roku-shho-varto-znaty-pro-zagrozy-ta-zahyst/(дата звернення: 10.06.2026)
14. Апацький В. В. Ukrainian banks in the conditions of military risks, cyber threats, and uncertainty. *Journal of Strategic Economic Research*. 2026. № 2. P. 8–20. https://doi.org/10.30857/2786-5398.2026.2.1 (дата звернення: 15.06.2026)

15. Aamir M., Zaidi S. M. A. Clustering based semi-supervised machine learning for DDoS attack classification. *IEEE Access.* 2019. Vol. 7. P. 436–446.
16. Souri A., Hosseini R. A state-of-the-art survey of malware detection approaches using data mining techniques. *Computers & Security.* 2020. Vol. 93. DOI: https://doi.org/10.1186/s13673-018-0125-x. (дата звернення: 15.06.2026)
17. Кохан І.В., Криховецька З.М., Копчук А. Ю. Стратегічне управління цифровою трансформацією банківських установ. *Наукові інновації та передові технології.* 2026. №2(54). С.3603-3615 DOI: https://doi.org/10.52058/2786-5274-2026-2(54)-3603-3615 (дата звернення: 15.06.2026)
18. Постанова Правління Національного банку України від 12 серпня 2022 року № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України». URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text (дата звернення: 10.06.2026)

References

1. Kovalenko, V. "Financial security of banks under the conditions of martial law." *Finansovyi Prostir*, no.4(48), 2023, pp. 81-93, https://doi.org/10.30970/fp.4(48).2022.819394
2. Fimyar, S., & S. Simakov. "Theoretical foundations of ensuring the economic security of banking institutions." *Taurida Scientific Herald. Series: Economics*, no. 21, 2024, pp. 127-132. https://doi.org/10.32782/2708-0366/2024.21.13
3. Kyrieieva, I. V., & D. V. Korobtsova. "Measures to Ensure Control and Security in the Banking Sector under the Legal Regime of Martial Law." *Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence*, no. 73, 2025, pp. 27–30, https://doi.org/10.32782/2307-1745.2025.73.5
4. Sydorovych, O. Yu., & M. M. Bukovskyi. "Factors of Financial Stability of the Banking System of Ukraine as an Indicator of the Economic Security of the State." *Financial Space*, no. 3, 2025, pp. 101–111, https://doi.org/10.30970/fp.3(57).2025.101110111
5. Kokhan, I. V., and Z. M. Krykhovetska. "Financial Security of Banking Institutions: Theoretical Foundations and Management in Modern Conditions." *Topical Issues in Modern Science*, no. 4(46), 2026, pp. 280–291, https://doi.org/10.52058/2786-6300-2026-4(46)-280-291
6. Bondaruk, T. H., & O. S. Bondaruk. "Managerial and Information-Analytical Aspects of the Development of Digital Banking Products and Technologies in the Context of Ensuring the Economic Security of Banks." *Statistics of Ukraine*, no. 4, 2025, pp. 79–90, https://doi.org/10.31767/su.4(111)2025.04.08
7. Pshyk, B. I. "The Impact of Digitalization on the Financial Stability of the Banking System and the Economic Security of the State." *Financial Space*, no. 3, 2025, pp. 20–30, https://doi.org/10.30970/fp.3(57).2025.202930
8. Kolodiziev, O. M., & V. O. Berehovyi. "Financial Security of Banks under Martial Law: The Impact of Digital Tools and Innovations." *Business Inform*, no. 9, 2024, pp. 335–341, https://doi.org/10.32983/2222-4459-2024-9-335-341
9. Denysenko, V. O., A. M. Proshchalykina, & Yu. M. Havryliuk. "Digitalization of the Banking System of Ukraine: Challenges and Opportunities for Financial Security." *International Scientific Journal "Internauka". Series: Economic Sciences*, no. 9(1), 2025, pp. 43–48, https://doi.org/10.25313/2520-2294-2025-9-11401
10. Khomyshyn, I., and O. Havts. "Ensuring Cybersecurity in the Financial Sector: Legal and Technological Aspects." *Electronic Scientific Publication «Scientific Bulletin of Uzhhorod National University». Series: Law*, vol. 10, no. 40, 2023, pp. 170–178, https://doi.org/10.23939/law2023.40.170.
11. "DDoS Attacks Carried Out Against Ukrainian Banks." *NABU*, nabu.ua/ua/ddos-ataki-shcho-zdiysnyuvalisya-na-ukrayinski-banki-vidbito.html. Accessed 10 June 2026.
12. Annual Report of the Vulnerability Detection and Cyber Incident and Cyberattack Response System. Operational Center for Cyber Incident Response of the State Cyber Protection Center of the State Service of Special Communications and Information Protection of Ukraine, 2024, 24 p., scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006. Accessed 15 June 2026
13. "Cybersecurity as a Key FinTech Trend of the Year: What You Should Know About Threats and Protection," *Fintech Insider*, fintechinsider.com.ua/kiberbezpeka-yak-klyuchovyj-finteh-trend-roku-shho-varto-znaty-pro-zagrozy-ta-zahyst/. Accessed 10 June 2026.
14. Apatskyi, V. V. "Ukrainian Banks in the Conditions of Military Risks, Cyber Threats, and Uncertainty." *Journal of Strategic Economic Research*, no. 2, 2026, pp. 8–20, https://doi.org/10.30857/2786-5398.2026.2.1.
15. Aamir, M., and S. M. A. Zaidi. "Clustering-Based Semi-Supervised Machine Learning for DDoS Attack Classification." *IEEE Access*, vol. 7, 2019, pp. 436–446.
16. Souri, A., and R. Hosseini. "A State-of-the-Art Survey of Malware Detection Approaches Using Data Mining Techniques." *Computers & Security*, vol. 93, 2020, https://doi.org/10.1186/s13673-018-0125-x.

17. Kokhan, I. V., Z. M. Krykhovetska, & A. Yu. Kopchuk. “Strategic Management of Digital Transformation of Banking Institutions.” *Scientific Innovations and Advanced Technologies*, no. 2(54), 2026, pp. 3603–3615, https://doi.org/10.52058/2786-5274-2026-2(54)-3603-3615
18. On Approval of the Regulation on the Organization of Cyber Protection in the Banking System of Ukraine and Amendments to the Regulation on Determining Critical Infrastructure Objects in the Banking System of Ukraine. Resolution of the Board of the National Bank of Ukraine No. 178 of 12 August 2022. https://zakon.rada.gov.ua/laws/show/v0178500-22#Text Accessed 10 June 2026.

Дата подання: 29.07.2026
Дата прийняття до друку:15.08.2026