Фінанси, банківська справа, страхування та фондовий ринок

УДК 336.71:004.8

DOI https://doi.org/10.5281/zenodo.20677037

Ефект масштабування цифрових ризиків у банківському секторі: виклики BigTech-концентрації та штучного інтелекту

Вовченко Оксана Сергіївна

кандидат економічних наук, доцент, доцент кафедри фінансів, банківського бізнесу та оподаткування, Національний університет «Полтавська політехніка імені Юрія Кондратюка», проспект Віталія Грицаєнка, 24, м. Полтава, 36011, Україна

https://orcid.org/0000-0001-8065-0529

Прийнято: 18.05.2026 | Опубліковано: 30.05.2026

Анотація: *Стаття присвячена дослідженню теоретичних та практичних аспектів виникнення й поширення ефекту швидкого масштабування цифрових ризиків у сучасному банківському секторі, а також визначення системних викликів, зумовлених концентрацією ринку навколо BigTech-провайдерів та стрімким упровадженням технологій штучного інтелекту, з метою розробки проактивних інструментів забезпечення фінансової стабільності.*

У дослідженні використано комплекс загальнонаукових та спеціальних методів, зокрема: методи системно-структурного та порівняльного аналізу – для вивчення природи трансформації фінансових криз; статистико-економічний та трендовий аналіз даних Національного банку України – для оцінювання динаміки безготівкових розрахунків; інструменти економіко-

математичного моделювання та індексного аналізу – для декомпозиції інтегральних показників системної кіберврразливості; метод логічного узагальнення – для формування висновків і рекомендацій щодо вдосконалення регуляторної політики.

У результаті проведених досліджень з'ясовано нелінійну природу цифрових загроз у фінансовому секторі та ідентифіковано феномен «банківського спринту». Проаналізовано динаміку операцій із платіжними картками в Україні за 2023–2025 роки, що підтвердило критичну залежність національної економіки від стійкості цифрових каналів зв'язку. Визначено структуру системної кіберврразливості через взаємодію ворожого, технологічного та фінансового компонентів у моделі SCyMoN. Побудовано профіль операційних ризиків ключових постачальників ІКТ-послуг та доведено наявність високого рівня спільної динаміки уразливостей постачальників і комерційних банків. Виокремлено нові загрози промислового використання генеративного штучного інтелекту кіберзлочинцями й оцінено досвід упровадження проактивних data-driven моделей управління ризиками, європейських стандартів регулювання та функціонування вітчизняної автономної мережі POWER BANKING.

Доведено, що нейтралізація ефекту швидкого масштабування цифрових ризиків вимагає відмови від реактивних підходів на користь динамічного моніторингу операційної стійкості. Обґрунтовано необхідність консолідації зусиль регуляторів і банків за трьома стратегічними напрямами: гармонізація національних нормативних актів із європейським законодавством, розгортання проактивних систем машинного навчання для виявлення аномалій та розширення автономних інфраструктур подвійного призначення для протидії інфраструктурним шокам.

ISSN: 2786-9431

Ключові слова: *цифрова трансформація, фінансова стабільність, кібервразливість, банківський спринт, ІКТ-аутсорсинг, регуляторна пісочниця, операційна стійкість.*

The scaling effect of digital risks in the banking sector: challenges of BigTech-concentration and artificial intelligence

Oksana Vovchenko
Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Finance, Banking and Taxation,
National University «Yuri Kondratyuk Poltava Polytechnic», Vitaliia Hrytsaienka Avenue, 24, Poltava, 36011, Ukraine
https://orcid.org/0000-0001-8065-0529

Abstract: *The purpose of this article is a comprehensive study of the theoretical and practical aspects of the emergence and deployment of the rapid scaling effect of digital risks in the modern banking sector, as well as the identification of systemic challenges caused by market concentration around BigTech providers and the rapid implementation of artificial intelligence technologies, to develop proactive tools for ensuring financial stability.*

The study utilized a set of general scientific and special methods, including: methods of systemic-structural and comparative analysis – to study the nature of financial crises transformation; statistical-economic and trend analysis of the National Bank of Ukraine data – to assess the dynamics of cashless payments; tools of economic-mathematical modeling and index analysis – for the decomposition of integral indicators of systemic cyber vulnerability; the method of logical generalization – to form conclusions and recommendations for improving regulatory policy.

The non-linear nature of digital threats in the financial environment is investigated and the phenomenon of "bank sprint" is identified, which significantly reduces the time lag of depositors' reaction due to the use of mobile applications and coordination of panic moods in social networks. The dynamics of payment card transactions in Ukraine for 2023–2025 are analyzed, which confirmed the critical dependence of the national economy on the stability of digital communication channels. The structure of systemic cyber vulnerability is determined through the interaction of adversary, technological, and financial components in the SCyMoN model. The operational risk profile of key third-party ICT service providers (Microsoft, Google, Cisco, Apple, SAP, Salesforce) was constructed, proving a high level of co-movement between the vulnerabilities of providers and commercial banks. New threats of industrial use of generative artificial intelligence by cybercriminals are highlighted and the experience of implementing proactive data-driven risk management models, European regulatory standards, and the functioning of the domestic autonomous network POWER BANKING was evaluated.

It is proved that neutralizing the effect of rapid scaling of digital risks requires abandoning reactive approaches in favor of dynamic monitoring of operational resilience. The necessity of consolidating the efforts of regulators and banks in three strategic areas is substantiated: harmonization of national regulations with European legislation, deployment of proactive machine learning systems to detect anomalies, and expanding autonomous infrastructures of dual (physical and virtual) purpose to counter structural shocks.

Keywords: *digital transformation, financial stability, cyber vulnerability, bank sprint, ICT-outsourcing, regulatory sandbox, operational resilience.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. Глибока модернізація фінансових послуг, автоматизація операцій, упровадження систем штучного інтелекту,

інструментів роботи з великими даними, хмарних сервісів та блокчейн-технологій складають основу сучасної цифрової трансформації банківського сектору. Перехід фінансового сектору у віртуальну площину, що характеризується поширенням фінтех-рішень та необанків, створює широкі можливості для підвищення операційної ефективності, оптимізації витрат і покращення клієнтського досвіду. Водночас стрімка діджиталізація породжує системні виклики, які безпосередньо загрожують фінансовій стабільності та безпеці інформаційних ресурсів, потенційно гальмуючи і прогрес у досягненні глобальних цілей сталого розвитку. Нерівномірність доступу до новітніх технологій поглиблює цифровий розрив між різними соціальними групами та регіонами, що вступає в суперечність із засадами інклюзивного зростання.

Окрім цього, критична залежність банківських установ від стабільності інформаційної інфраструктури створює умови, за яких технічні збої, регуляторна невизначеність або цілеспрямовані кібератаки здатні паралізувати значну частину національної економіки. Зазначені загрози набувають особливої гостроти в умовах ведення активних бойових дій та гібридного протистояння, коли об’єкти фінансової інфраструктури стають мішенями для координованих атак. За таких обставин упровадження адаптивного ризик-орієнтованого підходу, стає необхідною передумовою для забезпечення стабільності фінансової системи на макроекономічному рівні та сталого розвитку держави в умовах глобальних геополітичних та цифрових трансформацій. Постановка проблеми в загальному вигляді включає в себе визначення ключових аспектів теми дослідження, їх важливість та необхідність детального розгляду.

Аналіз останніх досліджень і публікацій. Проблема забезпечення кіберстійкості та фінансової безпеки банківського сектору в умовах технологічних трансформацій стала об’єктом підвищеного інтересу як української, так і світової наукової спільноти.

У науковому дискурсі останніх років чітко виокремилися кілька ключових підходів до дослідження цієї проблематики. Важливий внесок у вивчення макроекономічних аспектів цифрової трансформації та їхнього взаємозв'язку з кібербезпекою здійснили А. Кузьор, Т. Васильєва, О. Кузьменко [1]. На основі розрахунку коефіцієнтів варіації та побудови регресійних рівнянь автори довели наявність стійкого взаємозв'язку між процесами діджиталізації та національною системою кіберзахисту. Вони обґрунтували, що рівень економічного розвитку країни безпосередньо залежить від її спроможності протидіяти загрозам у кіберпросторі, використовуючи для оцінки такі інтегральні інструменти, як індекс національної кібербезпеки та Basel AML Index. Проте їхні дослідження зосереджені переважно на загальнодержавному рівні й не розкривають внутрішньобанківських механізмів трансформації кібератак у кризи ліквідності та платоспроможності.

У контексті забезпечення сталого розвитку та безпечного функціонування цифрового середовища значний інтерес становить робота Н. Барченко, В. Лубчака та Т. Лаврик [2]. Науковці запропонували систему індикаторів для оцінки здатності суспільства та бізнес-структур протистояти цифровим загрозам у процесі досягнення глобальних цілей сталого розвитку. Їхні висновки підкреслюють важливість превентивного управління технологічними процесами, хоча специфіка функціонування платіжних систем комерційних банків у цих роботах практично не деталізується.

Аналізом безпосереднього впливу новітніх інструментів цифрової економіки на безпеку фінансових інституцій займалися А. Кудінова, О. Маслій [3]. Дослідники виявили, що ігнорування ризиків, пов'язаних з неконтрольованим розвитком крипторинку, новими формами електронних платіжних сервісів та швидким поширенням дезінформації у медіапросторі, створює суттєві загрози для фінансової стабільності держави. Специфіка

кібернетичної та економічної безпеки підприємств та фінансових установ в умовах кризових явищ та воєнного стану отримала свій розвиток у серії публікацій під керівництвом С. Онищенко [4]. Автори детально структурували виклики та загрози для національних інтересів, спричинені пандемією та бойовими діями, наголошуючи на необхідності формування гнучких адаптивних стратегій захисту критичної інфраструктури. Проте механізми взаємозв'язку між технологічними збоями сторонніх ІКТ-провайдерів та системним ризиком ліквідності на міжбанківському ринку потребують окремого, більш детального аналітичного моделювання.

Юридичні, організаційні та управлінські засади протидії кіберзагрозам у банківській сфері України були предметом прискіпливої уваги І. Хомишин та О. Гавц [5]. Вчені концептуалізували поняття кібератак як форми сучасного кібертероризму та обґрунтував нагальну потребу переорієнтації банківського ризик-менеджменту від реактивного підходу («розслідування скоєних кіберзлочинів») до проактивної превентивної парадигми («запобігання кібер-ризикам»). Питання нормативно-правового забезпечення цієї сфери у контексті євроінтеграційних прагнень України також ґрунтовно досліджували А. М. Клочко, Н. В. Волченко, вказавши на слабкі місця у законодавчому полі та базових мережевих протоколах (зокрема, фундаментальні вразливості протоколу TCP/IP) [6].

Проблематика оцінки індикаторів фінансової безпеки безпосередньо банківських установ в умовах діджиталізації отримала належне теоретичне та прикладне розкриття у праці Теслюк С., Матвійчук Н. та Левчук А. [7]. Автори систематизували інноваційні прояви діяльності банків та виділили ключові показники безпеки, серед яких: рівень поширеності мобільного та інтернет-банкінгу, щільність мережі POS-терміналів та банкоматів, використання систем BankID та засобів централізованого виявлення несанкціонованих проникнень. Поряд із цим, М. Тимоць здійснила ґрунтовний аналіз перспектив

та трендів вітчизняного цифрового банкінгу, вказавши на стрімке витіснення класичних форм обслуговування необанками [8].

Процеси цифровізації супроводжуються виникненням нових джерел загроз, які детально досліджує також О. Плесюк [9]. Автори вказує на зростання частоти прояву цифрових ризиків у 2024–2025 роках та наголошує, що через відсутність інтегрованих систем ризик-менеджменту на вітчизняних підприємствах посилюється деструктивний вплив технологічних чинників. Важливо відзначити позицію А. Аберніхіної щодо необхідності впровадження ризик-орієнтованої системи управління як інтегрованої стратегічної функції, що охоплює виявлення, оцінку, моніторинг і використання ризиків на всіх рівнях з урахуванням архітектури ризиків цифрової економіки (мікро-, мезо- та макрорівень) і відповідних цифрових інструментів управління [10].

Зарубіжні автори, зокрема Hacker P., Kasirzadeh A [11], Baker S. [12], акцентують увагу на технічній складовій захисту фінансових установ, обґрунтовуючи ефективність інтегрованих систем шифрування, біометричної аутентифікації та проведення регулярних стрес-тестів з використанням сучасних методик.

Виділення невирішених раніше частин загальної проблеми. Більшість існуючих досліджень фокусуються на локальних інструментах кіберзахисту окремої банківської установи або на аналізі традиційних фінансових ризиків (кредитного, ринкового, ліквідності). Проте поза увагою дослідників часто залишається ефект швидкого масштабування ризиків, який виникає через спільні технологічні точки вразливості та залежність банківського сектору від хмарних сервісів обмеженого кола ІКТ-постачальників. Потребує глибшого вивчення також механізм взаємодії автономних ШІ-агентів із наявним програмним забезпеченням банків та оцінка ефективності нових інструментів проактивного реагування регуляторів на загрози «банківського спринту».

Формулювання цілей статті (постановка завдання). Основними цілями дослідження є обґрунтування нелінійної природи та механізмів масштабування цифрових ризиків у банківській сфері, проведення аналізу динаміки безготівкових операцій в Україні як індикатора цифрової залежності системи, оцінювання профілю операційних ризиків BigTech-концентрації на основі системних індексів вразливості, дослідження впливу сучасного штучного інтелекту на безпекове середовище, а також визначення ключових проактивних та інфраструктурних напрямів протидії цим загрозам для забезпечення довгострокового сталого розвитку.

Виклад основного матеріалу дослідження. Головна небезпека сучасних цифрових загроз у банківській сфері полягає в ефекті їхнього швидкого масштабування [11]. На відміну від традиційних банківських ризиків, які зазвичай поширюються лінійно і мають локалізований характер, цифрові ризики мають нелінійну природу, здатність до накопичення та мінливі вектори прояву. Ефект швидкого масштабування означає, що технологічний збій або порушення безпеки на рівні однієї платформи, сервісу чи постачальника інфраструктури здатні миттєво поширитися на тисячі асоційованих користувачів та контрагентів, викликаючи масштабні руйнування в межах усієї фінансової екосистеми. Реальним прикладом реалізації цього ефекту є трансформація природи фінансових криз під впливом діджиталізації, що проявилося у виникненні явища «банківського спринту» [13]. Якщо класична паніка депонентів і вилучення вкладів у двадцятому столітті тривали днями чи тижнями, як це спостерігалося під час банкрутства Continental Illinois у 1984 році, то за умов цифрової синхронізації інформації через соціальні мережі цей процес скоротився до хвилин. Досвід краху Silicon Valley Bank у 2023 році продемонстрував, що клієнти за допомогою мобільних додатків та систем миттєвих платежів здатні вивести мільярдні обсяги ліквідності за лічені години, унеможливлюючи своєчасне втручання

регулятора для стабілізації ситуації. Штучний інтелект та великі мовні моделі додатково посилюють цей ефект, провокуючи цифровий, коли алгоритми автоматично поширюють панічні настрої та координують поведінку вкладників на цифрових платформах.

Сучасний стан розвитку фінансового сектору України свідчить про глибоку інтеграцію цифрових розрахунків у повсякденне життя населення та бізнесу. Незважаючи на воєнні виклики та періодичні обмеження енергопостачання, загальна тенденція до переходу до безготівкового обігу залишається стійкою та позитивною. Динаміка операцій із платіжними картками за період 2023–2025 років наочно ілюструє витіснення готівкових розрахунків безготівковими альтернативами.

Таблиця 1

Динаміка та структура операцій з платіжними картками в Україні протягом 2023-2025 років

Показник	2023 рік	2024 рік	2025 рік
Загальна кількість операцій, млн шт.	7 912,5	7 944,7	9 512,3
Безготівкові операції, млн шт.	7 397,2	7 482,4	9 083,5
Безготівкові операції, %	93,5	94,2	95,5
Отримання готівки, млн шт.	515,3	462,7	428,8
Отримання готівки, %	6,5	5,8	4,5
Загальна сума операцій, млрд грн	6 140,8	5 919,7	7 157,2
Безготівкові операції, млрд грн	3 991,5	3 818,1	4 684,3
Безготівкові операції, %	65,0	64,8	65,4
Отримання готівки, млрд грн	2 149,3	2 101,5	2 472,9
Отримання готівки, %	35,0	35,5	34,6

Джерело: розраховано автором за даними [14]

Аналіз статистики свідчить, що платіжна інфраструктура України забезпечує безперебійне та стале обслуговування безготівкових операцій з платіжними картками, що дає змогу зберігати високий рівень довіри українців до безготівкових розрахунків. Дані НБУ відображають зростання частки безготівкових транзакцій за кількістю до 95,5% та за сумою до 65,4% у 2025 році, при цьому загальна сума безготівкових операцій досягла майже 4,68 трлн

грн. Важливим складником цієї екосистеми є державні сервіси ідентифікації, зокрема Система BankID НБУ, у якій кількість успішних верифікацій у 2025 році зросла на 25% порівняно з 2024 роком, досягнувши 109,4 млн операцій. Це вказує на те, що фінансова система України майже повністю залежить від стійкості цифрових каналів.

Зворотним боком такої стрімкої діджиталізації є масштабування загрози кібератак. Фінансові установи традиційно є головною мішенню для кіберзлочинців через високу концентрацію ліквідних грошей та персональних даних. Статистика свідчить, що фінансові установи піддаються атакам у середньому в 300 разів частіше, ніж підприємства інших галузей, лише протягом 2025 року на платформі обміну інформацією про актуальні кіберзагрози MISP-NBU, до якої підключено 60 банків та ключові небанківські фінансові установи, було надіслано 340 повідомлень про кіберінциденти та індикатори кіберзагроз [15]. Згідно з дослідженнями Міжнародного валютного фонду, за останні 20 років у фінансовому секторі зафіксовано понад 20 000 кібератак, які спричинили операційні втрати на суму близько 12 млрд доларів США. Протягом десятирічного періоду частка кіберінцидентів у фінансовому секторі зросла з 6% до 13% від загальної кількості подій у світі. Аналіз структури цих атак показує, що 54% інцидентів носять експлуатаційний характер, спрямований на сервери додатків та кінцеві хости, тоді як 46% є деструктивними заходами, націленими на зупинку операційної діяльності [16].

Варто відзначити, що для ефективного управління ризиками швидкого масштабування розробляються кількісні інструменти оцінювання. Федеральний резервний банк Нью-Йорка запропонував комплексну модель моніторингу системної кібервразливості (System Cyber Vulnerability, SCV), реалізовану в індексі SCyMoN [12]. Цей індекс дозволяє відслідковувати рівень загрози для фінансової стабільності в динаміці.

Теоретична модель визначає, що системна кібервразливість фінансової

системи формується під впливом взаємодії трьох модульних компонентів:

$$SCV_t = f(A_t, T_t, F_t)$$

Кожен із зазначених компонентів відображає окремий аспект системного ризику та розраховується за унікальною процедурою на основі різнорідних даних.

Ворожий компонент (A_t) відображає загрози зовнішнього середовища, концентруючись на активності зловмисників, появі нових методів кібератак, частоті використання шкідливого програмного забезпечення та геополітичних чинниках. Зростання геополітичної напруженості та комерціалізація кіберзлочинних угруповань є головними рушійними силами цього показника.

Технологічний компонент (T_t) оцінює рівень захищеності безпосередньо фінансових інститутів, аналізуючи слабкі місця у шифруванні, використання застарілих систем, ризикову внутрішню поведінку персоналу та загальну чутливість внутрішньої інфраструктури безпеки до шкідливого коду.

Фінансовий компонент (F_t) визначає системний ризик кіберзагроз, виходячи з рівня операційної та фінансової взаємопов'язаності банківського сектору. Зокрема, цей показник моделює ефект доміно (зараження) на міжбанківському ринку, вимірюючи потенційний дефіцит ліквідності внаслідок реалізації кредитного ризику та ризику концентрації спільних активів у разі кібератаки.

Особливе місце у поширенні системних загроз належить ризикам концентрації сторонніх постачальників послуг ІКТ. Сучасні банки все частіше передають критичні операційні функції (хмарні обчислення, аналітику даних, платіжний процесинг) на аутсорсинг [17]. Це призводить до виникнення спільних точок системного ризику, коли технологічний збій у одного провайдера паралізує діяльність значної частини фінансового сектору. Емпіричний аналіз фінансового сектору підтвердив високий рівень коруху (спільної динаміки) уразливостей постачальників послуг та комерційних

банків: коефіцієнт кореляції між ними становить 0,488 [12]. Системна значущість BigTech-компаній прямо залежить від сукупного обсягу активів їхніх клієнтів у банківському секторі. При цьому спостерігається екстремальна концентрація операційного ризику навколо обмеженого кола глобальних брендів, де частка окремих гравців є домінуючою (табл. 2).

Таблиця 2

Профіль операційних ризиків BigTech-провайдерів у структурі індексу вразливості фінансових установ

Ранг (місце) в індексі вразливості	Сторонній постачальник ІКТ-послуг (BigTech)	Характер системного та операційного ризику для банківського сектору
1	Microsoft	Ризик системної компрометації базового системного ПЗ та хмарних екосистем бізнес-додатків; критична концентрація вразливостей типу CVE.
2	Google	Ризик уразливості хмарної інфраструктури (IaaS/PaaS), архітектури відкритих API та безпеки мобільних операційних платформ.
3	Cisco	Ризик відмови або дестабілізації базової мережевої інфраструктури; загрози несанкціонованого перехоплення та маршрутизації міжбанківського трафіку.
4	Apple	Ризик експлуатації вразливостей кінцевих точок доступу та компрометації каналів мобільного банкінгу користувачів.
5–6	SAP / Salesforce	Ризик порушення безперервності критичних бізнес-процесів через уразливості в архітектурі ERP та CRM-систем (операційні та клієнтські бази даних).

Джерело: сформовано автором за матеріалами [12]

Наведене ранжування відображає, що успішна реалізація хоча б однієї вразливості типу CVE на рівні інфраструктури Microsoft чи Cisco здатна спричинити миттєвий системний збій у сотнях банків в усьому світі, підтверджуючи загрозу глобального масштабування цифрових ризиків.

Розвиток технологій штучного інтелекту кардинально змінює ландшафт фінансової безпеки, виступаючи одночасно інструментом захисту та чинником підвищення системних загроз. Протягом останніх років виникли

нові канали поширення ризиків, зумовлені інтеграцією ШІ-агентів у критичні інфраструктури. У 2026 році використання ШІ кіберзлочинцями набуло промислових масштабів. Зловмисники використовують генеративний ШІ для створення реалістичних deepfake-матеріалів (аудіо та відео) з метою імітації голосу та зовнішності топ-менеджерів банків для ініціювання фіктивних платіжних інструкцій, а також клієнтів – з метою проходження віддаленої верифікації у банківських онлайн-системах. Окрім того, автономні ШІ-агенти використовуються для автоматичного пошуку слабких місць у коді застарілих банківських систем, які до цього часу використовують понад 90% фінансових компаній у розвинених країнах [18].

Уповільнити ефект швидкого масштабування цифрових ризиків виключно реактивними заходами неможливо, що вимагає переходу до проактивних data-driven моделей управління [19]. Центральне місце в цьому процесі належить інструментам інтегрального оцінювання, зокрема індексу цифрових ризиків (Digital Risk Index), який розраховується на основі поєднання класичних фінансових метрик Базельського комітету з нефінансовими даними [20]. Використання технологій машинного навчання та обробки природної мови дозволяє щоденно аналізувати величезні масиви альтернативної інформації — від новинних стрічок до настроїв споживачів у соціальних мережах, формуючи індекси ділових настроїв та сигнали раннього попередження про погіршення фінансового стану контрагентів. Це дозволяє інвесторам та кредиторам виявляти приховані ризики та загрози ліквідності за кілька місяців до публічного прояву кризи.

З метою гармонізації підходів до забезпечення цифрової стійкості у глобальному масштабі, регулятори впроваджують вимоги щодо створення контрольованих експериментальних майданчиків — регуляторних «пісочниць» [21]. Вони дозволяють банкам спільно з фінтех-компаніями тестувати інноваційні технологічні рішення та алгоритми ШІ під наглядом

регуляторів, мінімізуючи ризики для ширшого ринку та формуючи чіткі критерії безпечного виходу продуктів у промислову експлуатацію.

Паралельно відбувається удосконалення нормативних стандартів кібербезпеки на національному рівні. Національний банк України здійснює масштабну реформу регулювання цифрової стійкості, наближаючи національні стандарти до європейських вимог DORA, NIS2, GDPR та AI Act. Ключовим нормативним документом у цій сфері стало Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту [22]. Цей документ поширюється на небанківські фінансові установи, платіжні сервіси, онлайн-кредиторів та страховиків, вимагаючи від них побудови комплексних систем захисту, ідентичних стандартам ISO/IEC 27001 та європейському регламенту DORA. Додатково регулятор ухвалив Постанову [23], яка запровадила жорсткі вимоги до посиленої автентифікації користувачів на платіжному ринку для зниження рівня кібершахрайства. Нагляд за дотриманням цих вимог здійснюється НБУ на основі ризик-орієнтованого підходу через проведення планових виїзних перевірок та IT-аудитів.

Унікальним досягненням українського фінансового сектору в питанні забезпечення безперервності операційної діяльності в умовах безпрецедентних фізичних та інфраструктурних шоків стало створення мережі POWER BANKING. Ця ініціатива об’єднала близько 2400 банківських відділень по всій території країни, які оснащені альтернативними джерелами енергопостачання, резервними супутниковими каналами зв’язку та посиленими системами фізичної та цифрової безпеки. Створення такої автономної інфраструктури дозволило банківській системі безперебійно функціонувати навіть у періоди тривалих блекаутів, викликаних воєнними атаками на енергетичну систему. Цей досвід довів, що поєднання віртуальної кіберстійкості з фізичною та енергетичною автономністю є критично

важливим інструментом протидії масштабним системним ризикам у сучасну цифрову епоху.

Висновки. Отже, аналіз ефекту швидкого масштабування цифрових ризиків у банківському секторі дозволяє сформулювати кілька висновків. Перехід до цифрових моделей обслуговування суттєво змінив природу системного ризику, перетворивши його з лінійного та локалізованого на каскадний, миттєвий та транскордонний. Скорочення часового лагу реакції депонентів через використання цифрових каналів та вплив соціальних мереж призвело до появи явища «банківського спринту», що вимагає докорінної зміни наглядової парадигми від статичних коефіцієнтів ліквідності до динамічного управління операційною стійкістю.

Моделювання системного кіберризику за допомогою інтегральних індексів, таких як SCyMoN та Digital Risk Index, наочно ілюструє небезпеку надмірної концентрації технологічних залежностей навколо обмеженого кола глобальних IT-провайдерів, де технічний збій або порушення безпеки одного з ключових вузлів здатні паралізувати всю банківську систему. Розвиток технологій штучного інтелекту додатково загострив ці загрози через автоматизацію кібератак, появу складних мультиагентних систем та виникнення нових векторів фінансового шахрайства.

Для протидії ефекту швидкого масштабування цифрових ризиків необхідна консолідація зусиль регуляторів та фінансових установ мінімум у трьох напрямах:

– впровадження жорстких стандартів цифрової стійкості, гармонізованих із європейськими регламентами та вітчизняними постановами регулятора;

– перехід до проактивних data-driven моделей оцінювання ризиків із використанням штучного інтелекту для виявлення аномалій та аналізу настроїв контрагентів на ранніх етапах;

– створення автономних резервних інфраструктур, аналогічних мережі POWER BANKING, здатних забезпечити безперервність фінансового посередництва в умовах екстремальних інфраструктурних шоків.

Лише за умови інтеграції технічних засобів кіберзахисту, адаптивного регулювання та підвищення цифрової грамотності населення фінансовий сектор зможе нейтралізувати загрози масштабування ризиків та реалізувати потенціал цифровізації для забезпечення довгострокового сталого розвитку.

Список використаних джерел

1. Kuzior A., Vasylieva T., Kuzmenko O., Koibichuk V., Brożek P. Global digital convergence: impact of cybersecurity, business transparency, economic transformation, and AML efficiency. *Journal of Open Innovation: Technology, Market, and Complexity.* 2022. Vol. 8, No. 4. P. 195. DOI: https://doi.org/10.3390/joitmc8040195

2. Барченко Н., Лубчак В., Лаврик Т. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. *Кібербезпека: освіта, наука, техніка.* 2022. Вип. 2(18). С. 73–85. DOI: https://doi.org/10.28925/2663-4023.2022.18.7385

3. Kudinova A., Maslii O., Smokvina V., Tsyhanenko K. The impact of digitalization on the financial institutions' economic security in the face of growing cyber threats. *Financial and Credit Activity: Problems of Theory and Practice*. 2025. Vol. 4, No. 63. P. 466-483. DOI: https://doi.org/10.55643/fcaptp.4.63.2025.4790

4. Social and economic security: threats and strengthening targets : monograph / Onyshchenko S., Maslii O., Hlusko A., Yanko A., Cherviak A. Warszawa : E-SCIENCE SPACE, 2023. 203 p.

5. Khomyshyn I., Havts O. Cyber security of the banking sector of Ukraine: concepts, problems and experience of foreign countries. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*. 2023. Vol. 10, No. 4(40), pp. 170-

178. https://doi.org/10.23939/law2023.40.170

6. Клочко А.М., Волченко Н.В. Економіко-правові засади банківської безпеки в умовах посилення євроінтеграційних процесів в Україні. *Юридичний бюлетень : науковий журнал*. 2021. № 18. URL: http://www.lawbulletin.oduvs.od.ua/arkhiv.

7. Теслюк С. А., Матвійчук Н. М., Левчук А. О. Фінансова безпека банківських установ в умовах цифровізації. *Економіка та суспільство.* 2024. Вип. 60. DOI: 10.32782/2524-0072/2024-60-117.8.

8. Тимоць М.В. Аналіз трендів та перспектив цифрового банкінгу в Україні. *International Science Journal of Management, Economics & Finance.* 2025. Issue 4(5). P. 23-32. URL: http://repository.ukd.edu.ua/xmlui/handle/123456789/2119

9. Плесюк О. Цифрові ризики в управлінні розвитком підприємства. *Bulletin of Sumy National Agrarian University*. 2025. No. 3 (103). P. 65–70. DOI: https://doi.org/10.32782/bsnau.2025.3.10

10. Аберніхіна І. Ризик-орієнтоване управління в контексті цифрової економіки: сутність, цілі, інструменти. *Цифрова економіка та економічна безпека.* 2025. № 3 (18). С. 214–221. DOI: https://doi.org/10.32782/dees.18-32

11. Hacker P., Kasirzadeh A., Edwards L. AI, digital platforms, and the new systemic risk. arXiv preprint arXiv:2509.17878. 2025. DOI: https://doi.org/10.48550/arXiv.2509.17878

12. Baker Steven D., Lee Michael Junho. Systemic cyber risk. *Federal Reserve Bank of New York Staff Reports.* 2026. No. 1186. https://doi.org/10.59576/sr.1186

13. Юр О., Ходакевич С. Цифровізація та нові ризики: як технології змінюють природу фінансових криз. *Економічний простір*. 2026. № 209. С. 339–345. DOI: https://doi.org/10.30838/EP.209.339-345

14. Операції з платіжними картками у 2025 році: більшість –

безготівкові. Національний банк України. 2026. URL: https://bank.gov.ua/ua/news/all/operatsiyi-z-platijnimi-kartkami-u-2025-rotsi-bilshist--bezgotivkovi (дата звернення: 18.04.2026).

15. Огляд національної системи кібербезпеки України 2025. Аналітичне дослідження. Національний координаційний центр кібербезпеки при РНБО України. 2025. URL: https://www.rnbo.gov.ua/ua/Diialnist/7559.html (дата звернення: 18.04.2026).

16. Khiaonarong T., Zheng S. The rise of cyber events and digital fraud in the financial sector. *IMF Working Papers.* 2026. Vol. 2026, Issue 062. 36 p. DOI: https://doi.org/10.5089/9798229043557.001

17. ШІ змінює фінансову сферу: як банки використовують нові технології. Асоціації українських банків. 2025. URL: https://aub.org.ua/shi-zminiuie-finansovu-sferu-iak-banky-vykorystovuiut-novi-tekhnolohii/ (дата звернення: 18.04.2026).

18. Yerra P. V. Agentic AI framework for automating legacy core-banking operations and regulatory reporting pipelines. *Journal of Information Systems Engineering and Management.* 2025. Vol. 10, No. 2. DOI: https://doi.org/10.52783/jisem.v10i2.13924

19. Вовченко О.С. Цифрова трансформація системи фінансового менеджменту підприємств: концептуальна архітектура та імплементація data-driven інструментарію. *Грааль науки.* 2025. № 60. С. 302-306. DOI 10.36074/grail-of-science.26.12.2025.031

20. Кмитюк Т. О., Білик Т. В., Качан О. П. Ризик-орієнтований підхід у формуванні сталого розвитку національної економіки в умовах цифрової трансформації. *Вісник Хмельницького національного університету. Економічні науки.* 2025 р. № 348 (6). С. 577-583. https://doi.org/10.31891/2307-5740-2025-348-6-83.

21. Теслюк С., Шевчук Р. Розвиток фінансових технологій: загрози та

можливості для банків. *Економічний часопис Волинського національного університету імені Лесі Українки.* 2025 р. № 3 (43). С. 133–139. https://doi.org/10.29038/2786-4618-2025-03-133-139.

22. Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг. Постанова Правління Національного банку України від 09 грудня 2025 року № 143. URL: https://zakon.rada.gov.ua/laws/show/v0143500-25#Text (дата звернення: 18.04.2026).

23. Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку. Постанова Правління Національного банку України від 03 травня 2023 року № 58. URL: https://zakon.rada.gov.ua/laws/show/v0058500-23#n11 (дата звернення: 18.04.2026).