УДК 336.71:005.334
DOI:10.32782/2415-8240-2026-109-2-280-295

УПРАВЛІННЯ ЦИФРОВОЮ ОПЕРАЦІЙНОЮ СТІЙКІСТЮ КОМЕРЦІЙНИХ БАНКІВ В УМОВАХ КАСКАДНИХ ІНФРАСТРУКТУРНИХ ПОРУШЕНЬ

MANAGEMENT OF DIGITAL OPERATIONAL RESILIENCE OF COMMERCIAL BANKS UNDER CASCADING INFRASTRUCTURE DISRUPTIONS

Дубініна Марина Вікторівна,
доктор економічних наук, професор,
завідувач кафедри обліку і оподаткування
Миколаївський національний аграрний університет
ORCID: https://orcid.org/0000-0002-3993-0622

Maryna Dubinina,
Mykolayiv National Agrarian University

У статті розвинуто теоретико-методичні положення управління цифровою операційною стійкістю комерційних банків в умовах каскадних інфраструктурних порушень. Метою дослідження є обґрунтування механізму поширення інфраструктурного збою через систему критичних залежностей та визначення управлінських засобів підтримання і відновлення банківських операцій. Методичний базис поєднує описову статистику, динамічний, структурний і порівняльний аналіз, контент-аналіз та причинно-наслідкове узагальнення. За даними 2020–2025 рр. встановлено зростання операційної значущості окремих банківських установ на тлі скорочення їх кількості та збільшення масштабів діяльності. Результати опитування банків щодо перебоїв електропостачання підтвердили неоднорідність операційних наслідків інфраструктурного шоку. Виокремлено критичні цифрові та інфраструктурні залежності, обґрунтовано механізм каскадного поширення порушень і визначено напрями резервування, сценарного тестування та відновлення критичних операцій.

Ключові слова: безпекоорієнтоване управління; управління комерційними банками; управління ризиками; сценарне тестування; критичні операції; інфраструктурні залежності; безперервність діяльності.

The article develops theoretical and methodological provisions for managing the digital operational resilience of commercial banks under cascading infrastructure disruptions. The relevance of the study is determined by the growing dependence of banking operations on energy supply, telecommunications, data centres, payment and processing infrastructure, software, cloud environments, and external technology

providers. The purpose of the research is to substantiate the mechanism by which an infrastructure disruption propagates through critical digital dependencies and to determine management mechanisms for maintaining and restoring critical banking operations. The methodological framework combines descriptive statistics, dynamic, structural and comparative analysis, content analysis of regulatory and analytical documents, causal analysis, and structural-functional modelling. The empirical context covers the Ukrainian banking sector in 2020–2025, while 2026 data are used only to reflect current regulatory and technological developments. The analysis shows that a reduction in the number of operating banks was accompanied by an expansion in sector assets, funding, lending, and financial results, increasing the operational significance of individual institutions. Survey data on additional operating losses caused by power outages demonstrate substantial heterogeneity in banks' exposure to infrastructure shocks. The study structures critical dependencies into energy, telecommunications, computing, payment and processing, software, cloud, and third-party service components and distinguishes technological dependence from counterparty dependence. A causal mechanism of cascading disruption is substantiated, according to which a primary failure may propagate through interconnected resources to critical operations and generate operational, financial, and reputational consequences. The proposed approach integrates identification of critical operations, dependency mapping, reserve mechanisms, scenario testing, and recovery procedures within security-oriented bank management. The practical significance lies in supporting business continuity planning, third-party assessment, testing of reserve readiness, and prioritisation of operational recovery.

Key words: security-oriented management; commercial bank management; risk management; scenario testing; critical operations; infrastructure dependencies; business continuity.

Вступ. Цифровізація банківської діяльності змінює організацію операційних процесів і посилює залежність комерційних банків від інформаційно-комунікаційних систем, дата-центрів, телекомунікаційних мереж, енергетичної інфраструктури, платіжних сервісів та зовнішніх технологічних постачальників. Розширення дистанційного обслуговування, автоматизація операцій і використання хмарних технологій підвищують доступність банківських послуг, однак водночас збільшують кількість взаємозв'язків, від яких залежить виконання критичних операцій [1; 2].

За умов воєнних дій така залежність набуває особливого значення. Пошкодження енергетичної та телекомунікаційної інфраструктури, перебої електропостачання, кібератаки й обмеження доступу до технологічних ресурсів можуть діяти одночасно та посилювати наслідки одне одного. Для банку це означає необхідність не лише технічного резервування, а й оперативного перерозподілу ресурсів, підтримання автономності підрозділів і збереження безперервності критичних операцій. Практика 2022–2025 рр. засвідчила поступове посилення таких механізмів, зокрема через розвиток мережі POWER BANKING та резервних каналів функціонування [3-8].

Специфіка інфраструктурного порушення полягає у здатності поширюватися за межі первинного збою. Втрата електроживлення, телекомунікаційного каналу, дата-центру або зовнішнього технологічного сервісу може обмежити доступ до інформаційних систем, проведення платежів і дистанційне обслуговування, а надалі спричинити операційні, фінансові та репутаційні наслідки. За таких умов предметом управлінської уваги стає не окремий ресурс, а сукупність залежностей, що забезпечує виконання банківської операції.

Принципи операційної стійкості орієнтують банки на визначення критичних операцій, ресурсів їх забезпечення, взаємозалежностей та здатності до відновлення [1]. Зростання ролі зовнішніх постачальників додає до цього необхідність оцінювати концентрацію критичних сервісів і можливість їх заміщення [2].

Попередні дослідження автора були зосереджені на ідентифікації та калібруванні нефінансових загроз у системі забезпечення фінансової надійності комерційних банків [9]. Наступним етапом є дослідження не стільки джерела загрози, скільки здатності банку зберігати критичні операції за умов її реалізації. У цьому контексті цифрова операційна стійкість розглядається як складова безпекоорієнтованого управління, що поєднує виявлення критичних залежностей, локалізацію поширення порушення та відновлення операційної діяльності.

Огляд літератури. Дослідження банківської стійкості дедалі більше поєднують проблематику фінансової стабільності, операційного ризику, цифрової трансформації, кібербезпеки та безперервності діяльності. Це відповідає зміні самої природи банківських операцій: їх результативність залежить не лише від фінансових параметрів, а й від доступності технологічних та інфраструктурних ресурсів.

Зміни ризикового середовища банків України розкрито у працях І. Вахович, І. Боярко, О. Заруцької, В. Фесенко, Л. Слободи та О. Середи [10], які простежують вплив масштабних зовнішніх шоків на фінансову стабільність і виокремлюють етапи опірності та адаптації. О. Агрес і О. Садура [11], О. Еркес, О. Калита та Т. Сундук [12] акцентують увагу на функціонуванні банківської системи в умовах війни та напрямах її пристосування до тривалих обмежень. У сукупності ці дослідження дають підстави розглядати стійкість як динамічну властивість банківської системи, що виявляється у здатності змінювати організаційно-функціональні параметри без втрати базових функцій.

Регуляторний аспект представлено у дослідженнях І. Бакало [13], М. Балицької та А. Ткаченко [14]. Стрес-тестування використовується для оцінювання чутливості банків до несприятливих сценаріїв, а практика Національного банку України засвідчує посилення превентивного нагляду й раннього реагування. Водночас переважна орієнтація такого інструментарію на фінансові параметри залишає поза межами оцінювання частину цифрових та інфраструктурних залежностей, через які первинний збій може вплинути на виконання окремої операції.

Операційні ризики платіжних систем систематизовано В. Міщенком, С. Науменковою та С. Міщенком [15], які виокремлюють інформаційні, технологічні, організаційні та кібернетичні джерела втрат. Безпековий аспект банківського менеджменту розвинуто М. Пінтохою [16]. У попередній праці М. Дубініної та О. Боднар [9] обґрунтовано трансмісійний характер нефінансових загроз і виокремлено операційно-технологічні та воєнно-безпекові складові. Для подальшого розвитку цього положення важливим є встановлення того, як конкретне порушення проходить через систему ресурсних залежностей і змінює функціональність банківської операції.

У зарубіжних працях переважає дослідження цифрової трансформації та кіберризику. Y. Azura, M. Azad та Y. Ahmed [17] поєднують ідентифікацію загроз, оцінювання вразливостей і заходи реагування в управлінні онлайн-банкінгом. E. Bruno, F. Pistolesi та E. Teti [18] обґрунтовують взаємозв'язок кібербезпекової політики з операційним ризиком, N. Türegün [19] розглядає кіберризик як супровідний результат цифрової трансформації, а D. Cumming, M. Nguyen, A.Pham та A. Samarasinghe [20] аналізують стабільність банківської системи у зв'язку з інституційними умовами протидії кіберзлочинності. Спільною рисою цих підходів є перенесення цифрового ризику з суто технічної площини у сферу банківського управління.

Окремий напрям формують дослідження операційної та кіберстійкості. N. Abidi, L. Gambacorta, C. Kok, I. Miquel-Flores, L. Madio та A. Partida [21] на матеріалах кіберстрес-тестування показують значення взаємозалежностей і можливість поширення порушення за межі окремої установи. Принципи Basel Committee on Banking Supervision [1] акцентують на критичних операціях, взаємозалежностях, безперервності діяльності та сценарному тестуванні. Принципи управління ризиками третіх сторін [2] доповнюють цей підхід оцінюванням критичності зовнішніх сервісів, концентрації постачальників та можливостей їх заміщення.

Цифрову операційну стійкість комерційного банку доцільно трактувати як спроможність управлінської та технологічної систем зберігати виконання критичних операцій у межах допустимого часу та масштабу порушення, адаптувати конфігурацію ресурсів і забезпечувати їх відновлення. На відміну від кіберстійкості, таке трактування охоплює також енергетичні, телекомунікаційні, обчислювальні, програмні та організаційні залежності.

Теоретичні засади дослідження взаємозалежності критичних інфраструктур сформовано у праці S. Rinaldi, J. Peerenboom та T. Kelly, які обґрунтували взаємозв'язок фізичних, інформаційних та організаційних залежностей і можливість поширення порушень між інфраструктурними системами [22]. Розвиток нормативного забезпечення цифрової операційної стійкості фінансового сектору відображено в Регламенті ЄС 2022/2554 (DORA), який передбачає комплексний підхід до управління ризиками інформаційно-комунікаційних технологій, операційної стійкості та ризиками третіх сторін [23]. Водночас особливості каскадного поширення інфраструктурних порушень

у діяльності комерційних банків потребують подальшого дослідження з урахуванням взаємозалежності критичних операцій і ресурсів їх забезпечення.

Огляд наукових праць показує, що фінансова стійкість, операційний ризик, кібербезпека, безперервність діяльності та зовнішні технологічні залежності мають розвинений методичний інструментарій, однак здебільшого аналізуються окремо. Менш дослідженим залишається причинно-наслідковий зв'язок між первинним інфраструктурним порушенням, зміною доступності пов'язаних ресурсів, деградацією критичної операції та управлінською реакцією банку. Цей розрив визначає потребу у підході, за якого критичні операції, інфраструктурні залежності, резервування та відновлення розглядаються як взаємопов'язані елементи управління цифровою операційною стійкістю. Такий ракурс дає можливість перейти від опису окремих ризиків до дослідження логіки поширення порушення та меж його локалізації.

Метою статті є розвиток теоретико-методичних засад управління цифровою операційною стійкістю комерційних банків шляхом обґрунтування механізму каскадного поширення інфраструктурних порушень, структуризації критичних залежностей і визначення механізмів підтримання та відновлення критичних банківських операцій.

Для досягнення поставленої мети визначено такі завдання: дослідити структурні зміни банківського сектору України у 2020–2025 рр.; систематизувати критичні цифрові та інфраструктурні залежності банківських операцій; обґрунтувати причинно-наслідковий механізм каскадного поширення інфраструктурних порушень; визначити управлінські засоби підтримання безперервності та відновлення критичних банківських операцій.

Методика досліджень. Методичний базис поєднує кількісний і якісний підходи та ґрунтується на матеріалах Національного банку України, Європейського центрального банку і Basel Committee on Banking Supervision [1-8; 21]. Для оцінювання динаміки банківського сектору використано дані за 2020–2025 рр., опрацьовані методами описової статистики, динамічного, структурного та порівняльного аналізу; матеріали 2026 р. залучено лише для характеристики актуальних регуляторних і технологічних змін. Окремо систематизовано результати опитування банків щодо додаткових операційних втрат унаслідок перебоїв електропостачання [3]. Контент-аналіз регуляторних і аналітичних матеріалів застосовано для виокремлення критичних цифрових та інфраструктурних залежностей, а логічне узагальнення, причинно-наслідковий аналіз і структурно-функціональне моделювання використано для обґрунтування механізму каскадного поширення порушень та визначення напрямів резервування, локалізації й відновлення критичних операцій.

Інструменти генеративного штучного інтелекту не використовувалися для формування наукових ідей, розроблення методології дослідження, збирання, оброблення або інтерпретації даних. ChatGPT використовувався для мовного редагування окремих фрагментів авторського рукопису та підготовки редакційних пропозицій. Відповідальність за науковий зміст, достовірність результатів і висновки дослідження несе автор.

Результати досліджень. Упродовж 2020–2025 рр. банківський сектор зазнав помітних структурних змін. Кількість діючих банків скоротилася з 73 до 60 [7], тоді як масштаби діяльності зростали. За таких умов на одну установу припадає більший обсяг активів, операцій та клієнтських потоків, а отже, підвищується значення безперервності її функціонування для клієнтів і платіжної інфраструктури.

Переломним став 2022 р., коли воєнні, енергетичні та технологічні обмеження одночасно вплинули на банківську систему. Попри масштаб зовнішнього шоку, сектор зберіг функціональність, а у наступні роки відновив кредитну активність і нарощування активів. У 2025 р. чисті активи збільшилися на 17,2 %, а чисті кредити бізнесу та населенню — приблизно на третину [7].

Фінансові показники не вимірюють цифрову операційну стійкість безпосередньо, але характеризують масштаб операцій, безперервність яких має бути забезпечена. Тому їх динаміка використовується як контекст для подальшого аналізу інфраструктурних залежностей і резервних механізмів.

Основні зміни параметрів банківського сектору за 2020–2025 рр. систематизовано у табл. 1.

Таблиця 1. Динаміка основних показників банківського сектору у 2020-2025 рр.

Показники	Роки						2025 р. у % до 2020 р.
	2020	2021	2022	2023	2024	2025	
Кількість діючих банків, од.	73	71	67	63	61	60	82,2
Чисті активи, млрд грн	1 823	2 053	2 352	2 945	3 415	4 001	219,5
Чисті кредити суб'єктам господарювання, млрд грн	432	540	529	511	589	774	179,2
Чисті кредити фізичним особам, млрд грн	149	200	134	160	222	297	199,3
Кошти суб'єктів господарювання, млрд грн	681	800	943	1 322	1 564	1 808	265,5
Кошти фізичних осіб, млрд грн	682	727	933	1 084	1 216	1 407	206,3
Чистий прибуток, млрд грн	39,7	77,4	21,9	83,0	90,9	126,8	319,4

Джерело: сформовано автором за даними Національного банку України [7].

Дані табл. 1 відображають асиметричну трансформацію банківського сектору. За скорочення кількості діючих банків на 17,8 % чисті активи зросли у 2,2 раза. У розрахунку на одну установу їх обсяг збільшився приблизно з 25,0 млрд грн у 2020 р. до 66,7 млрд грн у 2025 р. Це характеризує збільшення фінансового масштабу діяльності в розрахунку на один банк та актуалізує необхідність забезпечення безперервності критичних банківських операцій.

Найбільш різка зміна окремих показників припала на 2022 р. Чистий прибуток зменшився до 21,9 млрд грн проти 77,4 млрд грн у 2021 р., а чисті кредити фізичним особам – з 200 до 134 млрд грн. Водночас кошти суб'єктів господарювання та населення продовжували зростати [7]. Поєднання цих

тенденцій характеризує різну швидкість адаптації окремих складових банківської діяльності та пріоритетність збереження ліквідності й виконання платіжних зобов'язань.

У подальшому ключові фінансові параметри відновилися. У 2025 р. обсяг чистих кредитів суб'єктам господарювання перевищив рівень 2020 р. на 79,2%, фізичним особам – на 99,3%, коштів суб'єктів господарювання – на 165,5%, коштів населення – на 106,3%. Чистий прибуток був у 3,2 раза вищим за показник 2020 р. [7]. Проте така динаміка відображає результат адаптації, а не ті інфраструктурні умови, завдяки яким банківські операції залишалися доступними.

Однією з найбільш наочних таких умов є енергетичне забезпечення. Перебої електропостачання одночасно впливають на роботу відділень, серверного обладнання, каналів зв'язку, дистанційного обслуговування та платіжної інфраструктури. Результати опитування банків, проведеного Національним банком України у 2022 р., засвідчили значну диференціацію додаткових операційних втрат [3]. Їх розподіл наведено на рис. 1.

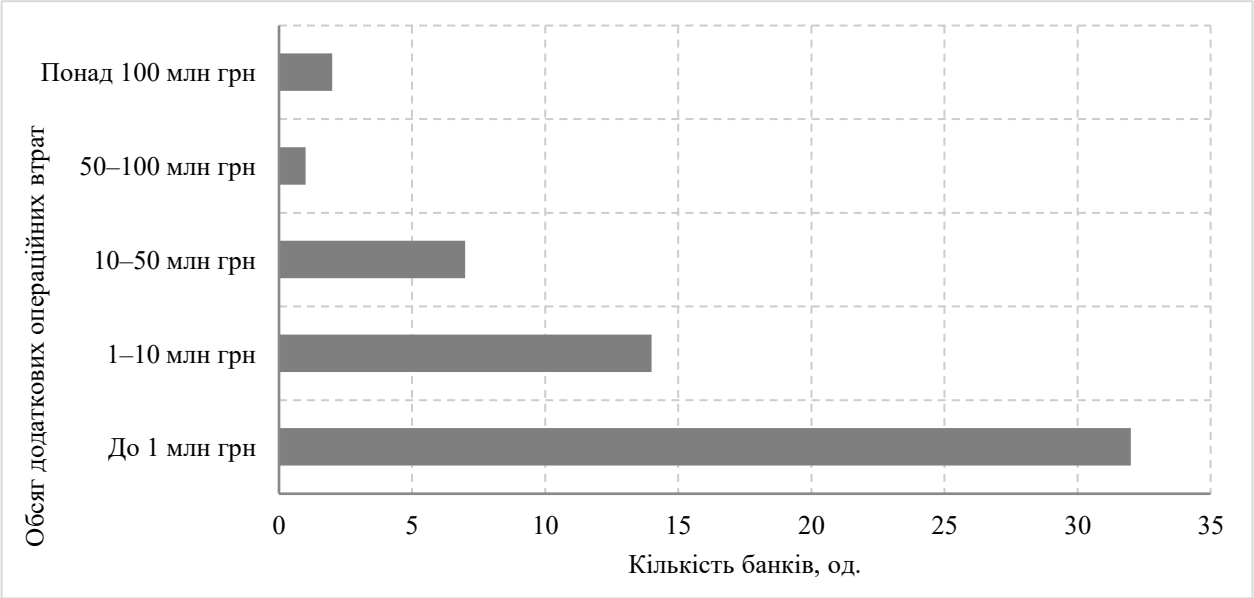


Рисунок 1. – Розподіл банків за обсягом очікуваних додаткових операційних збитків унаслідок перебоїв електропостачання, 2022 р.
Джерело: побудовано автором за результатами опитування банків, оприлюдненими Національним банком України [3].

За результатами опитування Національного банку України, проведеного у 2022 р., розподіл 56 банків за розміром очікуваних додаткових операційних збитків унаслідок перебоїв електропостачання засвідчив суттєву неоднорідність їхньої вразливості до енергетичних порушень [3]. Найбільшу групу становили банки з втратами до 1 млн грн, водночас окремі установи повідомляли про втрати понад 100 млн грн [3]. Агрегований характер даних не дає змоги кількісно визначити внесок масштабу банку, територіального розміщення або рівня резервування, однак сам розподіл підтверджує різну чутливість установ до однакового типу інфраструктурного порушення.

Енергетичне забезпечення у цьому випадку виступає не ізольованим технічним ресурсом, а умовою функціонування кількох пов'язаних процесів. Втрата електроживлення може одночасно обмежити роботу відділення, банкоматної мережі, серверного обладнання та каналів дистанційного обслуговування. Саме через таку взаємозалежність локальний збій набуває каскадного характеру.

Реакцією банківського сектору стало розширення автономного електроживлення, резервних каналів зв'язку та мережі відділень, здатних працювати за тривалих перебоїв. POWER BANKING інституціоналізувала частину цих рішень на рівні сектору [4; 8]. Проте резервування одного ресурсу не забезпечує безперервності операції, якщо недоступним залишається інший критичний елемент.

Це визначає необхідність розглядати резервування у зв'язку з усією сукупністю ресурсів, від яких залежить конкретна операція. Основні цифрові та інфраструктурні залежності, характер можливого порушення та відповідні механізми забезпечення стійкості наведено у табл. 2.

Таблиця 2. Критичні цифрові та інфраструктурні залежності комерційного банку в системі забезпечення операційної стійкості

Критична залежність	Характер потенційного порушення	Банківські операції під впливом	Механізми забезпечення операційної стійкості
1	2	3	4
Енергетична інфраструктура	знеструмлення, пошкодження енергетичних мереж, нестабільність електропостачання	робота відділень, банкоматів, серверного обладнання, процесингових систем	резервні джерела живлення, системи безперебійного живлення, автономізація критичних підрозділів, пріоритизація критичних навантажень
Телекомуні-каційна інфраструктура	пошкодження каналів зв'язку, відмова оператора, перевантаження мереж	дистанційне банківське обслуговування, авторизація платежів, передавання даних між підрозділами	дублювання каналів зв'язку, використання альтернативних операторів, резервні маршрути передавання даних
Дата-центри та серверна інфраструктура	фізичне пошкодження, технічний збій, недоступність основного майданчика	оброблення та зберігання даних, функціонування основних банківських інформаційних систем	географічне резервування, резервні майданчики, дублювання та синхронізація даних, процедури аварійного відновлення
Платіжна та процесингова інфраструктура	збій процесингового центру, порушення взаємодії з платіжними системами, технічна недоступність окремих сервісів	карткові операції, перекази, еквайринг, міжбанківські розрахунки	резервування процесингових потужностей, альтернативні маршрути оброблення операцій, процедури безперервності платежів

продовження таблиці 1

1	2	3	4
Зовнішні постачальники критичних технологічних послуг	недоступність постачальника, порушення умов надання послуг, концентрація критичних функцій у одного контрагента	супровід інформаційних систем, технічна підтримка, процесингові та інші передані зовнішнім виконавцям функції	оцінювання концентрації залежності, альтернативні постачальники, договірні вимоги щодо безперервності та відновлення
Хмарна інфраструктура та зовнішні цифрові платформи	обмеження доступу, технічний збій, втрата зв'язку із сервісом або недоступність технологічного середовища	зберігання й оброблення даних, аналітичні сервіси, клієнтські цифрові послуги	резервне копіювання, розподілене зберігання даних, географічне розосередження та альтернативні технологічні середовища
Критичне програмне забезпечення	помилки оновлення, відмова програмного комплексу, кібератака	основні банківські інформаційні системи, дистанційні канали, внутрішні облікові та контрольні системи	резервні версії програмного забезпечення, тестове середовище, сегментація систем, процедури оперативного відновлення

Джерело: сформовано автором на основі матеріалів НБУ [3; 4; 8], Європейського центрального банку [21] та Базельського комітету з банківського нагляду [1; 2].

Дані табл. 2 показують, що критичні залежності відрізняються не лише джерелом порушення, а й можливістю заміщення та характером управлінської реакції. Найбільш небезпечними є ситуації, коли один ресурс забезпечує кілька операцій або коли його швидке дублювання неможливе. У таких випадках стійкість визначається не формальною наявністю резерву, а його здатністю фактично перебрати функцію критичного елемента.

Концентрація функцій у межах одного дата-центру, оператора зв'язку чи постачальника технологічного сервісу утворює точки підвищеної залежності. Їх значення визначається тривалістю можливої недоступності, наявністю альтернативи та часом, необхідним для перемикання або відновлення. Тому географічне розосередження, функціональна взаємозамінність і попередньо відпрацьовані процедури відновлення мають оцінюватися у взаємозв'язку.

Окремого розмежування потребують зовнішні постачальники та хмарна інфраструктура. У першому випадку управлінська увага зосереджується на концентрації контрагента, умовах надання послуг і можливості заміни постачальника. У другому критичною є доступність технологічного середовища, резервування даних і можливість переходу на альтернативний майданчик. Таке розмежування уточнює характер контролю зовнішніх залежностей [2].

Взаємодія зазначених залежностей формує послідовність, у межах якої первинний інфраструктурний збій переходить у обмеження критичного ресурсу, порушення цифрової залежності, деградацію банківської операції та вторинні наслідки. Механізм такого поширення і відповідне управлінське реагування наведено на рис. 2.



Рисунок 2. – Механізм каскадного поширення інфраструктурних порушень у системі цифрової операційної стійкості комерційного банку
Джерело: сформовано автором на основі матеріалів НБУ [3], Європейського центрального банку [21] та Базельського комітету з банківського нагляду [1; 2].

Рис. 2 відображає внутрішню логіку каскадного порушення: первинний збій стає системним не сам по собі, а через залежності, що поєднують інфраструктурні ресурси з критичними операціями. Відповідно, управління стійкістю має починатися з визначення операції та ресурсів, без яких її виконання стає неможливим або суттєво обмежується.

Практичну реалізацію зазначеного механізму можна простежити на прикладі порушення електропостачання. За недостатньої автономності критичних технологічних ресурсів первинний енергетичний збій може спричинити недоступність телекомунікаційного обладнання, обмежити взаємодію з процесинговими системами та призвести до затримки виконання платіжних операцій. Подальше поширення порушення залежить від конфігурації резервних ресурсів, наявності альтернативних каналів зв'язку та готовності процедур відновлення. За таких умов результативність управлінського реагування визначається здатністю банку локалізувати порушення та забезпечити відновлення критичних операцій.

Функціональна архітектоніка цифрової операційної стійкості ґрунтується на взаємодії превентивної, компенсаційної та відновлювальної складових. Перша орієнтована на визначення критичних операцій і ресурсів; друга забезпечує підтримання функціональності за рахунок резервування, дублювання та заміщення; третя пов'язана з поверненням процесів до

прийнятного режиму після порушення. Їх узгодженість визначає перехід від локального реагування на інцидент до системного забезпечення безперервності діяльності.

Пріоритетність резервування та відновлення доцільно визначати з урахуванням наслідків припинення операції, її залежності від інфраструктурних ресурсів і допустимої тривалості недоступності. За такого підходу предметом оцінювання стає не лише ймовірність інциденту, а й межа, в якій деградація функціональності ще не призводить до неприйнятних наслідків для клієнтів, платіжної інфраструктури та інших учасників фінансової системи [1; 2].

Резервний механізм має управлінську цінність лише за умови фактичної готовності до використання. Тому наявність альтернативного каналу, резервного майданчика чи дублюючого сервісу потребує перевірки доступності, сумісності, пропускної спроможності та часу активації. Сценарне тестування дає можливість виявити приховані залежності до настання реального порушення та скоригувати процедури безперервності. Передавання технологічної функції зовнішньому постачальнику не передає йому відповідальність банку за безперервність критичної операції. Відповідно, оцінювання критичності послуги, концентрації залежності, умов відновлення та можливості заміни постачальника має бути складовою договірних і контрольних процедур [2].

У межах безпекоорієнтованого управління зазначений підхід поєднує ідентифікацію критичних операцій із визначенням інфраструктурних залежностей, сценарним тестуванням, резервуванням ресурсів та процедурами відновлення. Це дає змогу пов’язати джерело порушення з характером його поширення, визначити потенційні точки втрати функціональності та встановити пріоритетність управлінського реагування.

Одержані результати узгоджуються з висновками N. Abidi та співавторів [21] щодо значення технологічних взаємозалежностей у поширенні операційних порушень та положеннями Базельського комітету з банківського нагляду [1] стосовно визначення критичних операцій і забезпечення їх безперервності. Відмінність запропонованого підходу полягає в розгляді каскадного поширення порушень через сукупність цифрових та інфраструктурних залежностей, включаючи енергетичні й телекомунікаційні ресурси, та визначенні відповідних засобів управлінського реагування.

Обмеження дослідження пов’язані з використанням агрегованих показників банківського сектору та результатів опитування НБУ 2022 р., які не відображають індивідуальних характеристик операційної стійкості окремих банків у наступні періоди. Запропонований механізм має концептуальний характер і потребує подальшої емпіричної перевірки на рівні критичних банківських операцій із використанням даних про тривалість порушень, резервування ресурсів та відновлення функціональності.

Висновки. Проведене дослідження засвідчило, що скорочення кількості діючих банків у 2020–2025 рр. супроводжувалося зростанням масштабів їх діяльності, що посилило операційну значущість окремих установ і вимоги до безперервності критичних операцій. Встановлено, що інфраструктурні

порушення мають каскадний характер і поширюються через взаємопов'язані енергетичні, телекомунікаційні, обчислювальні, платіжні, програмні та зовнішні сервісні залежності. Наукова новизна полягає в обґрунтуванні причинно-наслідкового механізму такого поширення та його інтеграції у систему безпекоорієнтованого управління комерційними банками. Практичне значення одержаних результатів визначається можливістю їх використання під час формування планів безперервності діяльності, сценарного тестування, оцінювання готовності резервних ресурсів і зовнішніх постачальників. Подальші дослідження доцільно спрямувати на мікрорівневе оцінювання цифрової операційної стійкості окремих банків з урахуванням допустимого часу порушення, швидкості відновлення та замінності критичних ресурсів.

Внесок авторів. *Автор повністю провів дослідження, написав і відредагував текст.*

Фінансування. *Автор заявляє, що дослідження виконано без зовнішнього фінансування.*

Конфлікт інтересів. *Автор заявляє про відсутність конфлікту інтересів*.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Basel Committee on Banking Supervision. *Principles for operational resilience*. Basel : Bank for International Settlements, 2021. 12 p. URL: https://www.bis.org/publications/202103-guidelines-principles-operational-resilience (accessed: 28.09.2026).

2. Basel Committee on Banking Supervision. *Principles for the sound management of third-party risk*. Basel : Bank for International Settlements, 2025. 22 p. URL: https://www.bis.org/publications/202512-guidelines-principles-sound-management-third-party-risk (accessed: 28.09.2026).

3. Національний банк України. *Звіт про фінансову стабільність. Грудень 2022 року*. Київ : Національний банк України, 2022. URL: https://bank.gov.ua/admin_uploads/article/FSR_2022-H2.pdf?v=4 (дата звернення: 28.09.2026).

4. Національний банк України. *Річний звіт 2022*. Київ : Національний банк України, 2023. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2022.pdf (дата звернення: 28.09.2026).

5. Національний банк України. *Звіт про фінансову стабільність*. *Червень 2025 року*. Київ : Національний банк України, 2025. URL: https://bank.gov.ua/admin_uploads/article/FSR_2025-H1.pdf (дата звернення: 28.09.2026).

6. Національний банк України. *Звіт про фінансову стабільність. Грудень 2025 року*. Київ : Національний банк України, 2025. URL: https://bank.gov.ua/admin_uploads/article/FSR_2025-H2.pdf (дата звернення: 28.09.2026).

7. Національний банк України. *Огляд банківського сектору. Лютий 2026 року*. Київ : Національний банк України, 2026. URL:

https://bank.gov.ua/admin_uploads/article/Banking_Sector_Review_2026-02.pdf?v=16 (дата звернення: 28.09.2026).

8. Національний банк України. *POWER BANKING : об'єднана мережа відділень банків України*. URL: https://power.bank.gov.ua/ (дата звернення: 28.09.2026).

9. Дубініна М. В., Боднар О. А. Ідентифікація та калібрування нефінансових загроз у системі забезпечення фінансової надійності комерційних банків. *Modern Economics*. 2026. № 58. С. 107–120. DOI: https://doi.org/10.31521/modecon.V58(2026)-14.

10. Вахович І., Боярко І., Заруцька О., Фесенко В., Слобода Л., Середа О. Трансформація банківських ризиків і їхній вплив на фінансову стабільність: ідентифікація та сучасні виклики. *Фінансово-кредитна діяльність: проблеми теорії і практики*. 2026. Т. 4, № 69. С. 25–40. DOI: https://doi.org/10.55643/fcaptp.4.69.2026.5301 (дата звернення: 28.09.2026).

11. Агрес О. Г., Садура О. Б. Стан банківської системи України в умовах війни: проблеми стабільності та стратегічні орієнтири розвитку. *Регіональна економіка*. 2025. № 2(116). С. 73–82. DOI: https://doi.org/10.36818/1562-0905-2025-2-7 (дата звернення: 28.09.2026).

12. Еркес О., Калита О., Сундук Т. Банківська система України в умовах війни. *Scientia Fructuosa*. 2022. Т. 144, № 4. С. 122–133. DOI: https://doi.org/10.31617/1.2022(144)09 (дата звернення: 28.09.2026).

13. Бакало І. І. Стрес-тестування банківської системи України: інструменти, сценарії та результати в умовах війни. *Наукові записки Національного університету «Острозька академія». Серія «Економіка»*. 2025. № 37(65). С. 37–42. DOI: https://doi.org/10.25264/2311-5149-2025-37(65)-37-42 (дата звернення: 28.09.2026).

14. Балицька М. В., Ткаченко А. П. Досвід Національного банку України у забезпеченні стійкості банківської системи в умовах сучасних викликів. *Економіка та суспільство*. 2025. № 72. DOI: https://doi.org/10.32782/2524-0072/2025-72-132 (дата звернення: 30.09.2026).

15. Міщенко В. І., Науменкова С. В., Міщенко С. В. Управління операційними ризиками в платіжних системах. *Економічний простір*. 2023. № 183. С. 79–87. DOI: https://doi.org/10.32782/2224-6282/183-13 (дата звернення: 28.09.2026).

16. Пінтоха М. М. Стратегічні цілі діяльності банків України: безпековий аспект держави під час дії воєнного стану. *Український економічний часопис*. 2024. № 7. С. 81–84. DOI: https://doi.org/10.32782/2786-8273/2024-7-13 (дата звернення: 30.09.2026).

17. Azura Y. T. Y., Azad M. A., Ahmed Y. An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*. 2025. Vol. 9. P. 85–104. DOI: https://doi.org/10.1007/s42786-025-00056-3 (дата звернення: 30.09.2026).

18. Bruno E., Pistolesi F., Teti E. Cybersecurity policy, ESG and operational risk: a virtuous relationship to improve banks' performance. *International Review of*

Economics & Finance. 2025. Vol. 99. Art. 104053. DOI: https://doi.org/10.1016/j.iref.2025.104053 (дата звернення: 28.09.2026).

19. Türegün N. Digital transformation and cybersecurity risks. *International Journal of Accounting Information Systems*. 2025. Vol. 56. Art. 100749. DOI: https://doi.org/10.1016/j.accinf.2025.100749 (дата звернення: 28.09.2026).

20. Cumming D., Nguyen M., Pham A. V., Samarasinghe A. Banking system stability: a global analysis of cybercrime laws. *Journal of International Business Studies*. 2026. Vol. 57. P. 356–380. DOI: https://doi.org/10.1057/s41267-025-00838-3 (дата звернення: 30.09.2026).

21. Abidi N., Gambacorta L., Kok C., Miquel-Flores I., Madio L., Partida A. Disciplining digital risk: evidence from cyber stress tests. *ECB Working Paper Series*. 2026. No. 3222. Frankfurt am Main : European Central Bank. URL: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3222~27c5b77e07.en.pdf (дата звернення: 28.09.2026).

22. Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. 2001. Vol. 21, No. 6. P. 11–25. DOI: https://doi.org/10.1109/37.969131 (дата звернення: 28.09.2026).

23. European Parliament and Council of the European Union. Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector. *Official Journal of the European Union*. 2022. L 333. P. 1–79. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (дата звернення: 28.09.2026).

REFERENCES

1. Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Basel: Bank for International Settlements, 12 p. Available at: https://www.bis.org/publications/202103-guidelines-principles-operational-resilience (accessed September 28, 2026).

2. Basel Committee on Banking Supervision. (2025). Principles for the sound management of third-party risk. Basel: Bank for International Settlements, 22 p. Available at: https://www.bis.org/publications/202512-guidelines-principles-sound-management-third-party-risk (accessed September 28, 2026).

3. National Bank of Ukraine. (2022). Zvit pro finansovu stabilnist. Hruden 2022 roku [Financial Stability Report. December 2022]. Kyiv: National Bank of Ukraine. Available at: https://bank.gov.ua/admin_uploads/article/FSR_2022-H2.pdf?v=4 (accessed September 28, 2026) [in Ukrainian].

4. National Bank of Ukraine. (2023). Richnyi zvit 2022 [Annual Report 2022]. Kyiv: National Bank of Ukraine. Available at: https://bank.gov.ua/admin_uploads/article/annual_report_2022.pdf (accessed September 28, 2026) [in Ukrainian].

5. National Bank of Ukraine. (2025). Zvit pro finansovu stabilnist. Cherven 2025 roku [Financial Stability Report. June 2025]. Kyiv: National Bank of Ukraine. Available at: https://bank.gov.ua/admin_uploads/article/FSR_2025-H1.pdf (accessed September 28, 2026) [in Ukrainian].

6. National Bank of Ukraine. (2025). Zvit pro finansovu stabilnist. Hruden 2025 roku [Financial Stability Report. December 2025]. Kyiv: National Bank of Ukraine. Available at: https://bank.gov.ua/admin_uploads/article/FSR_2025-H2.pdf (accessed September 28, 2026) [in Ukrainian].

7. National Bank of Ukraine. (2026). Ohliad bankivskoho sektoru. Liutyi 2026 roku [Banking Sector Review. February 2026]. Kyiv: National Bank of Ukraine. Available at: https://bank.gov.ua/admin_uploads/article/Banking_Sector_Review_2026-02.pdf?v=16 (accessed September 28, 2026) [in Ukrainian].

8. National Bank of Ukraine. (n.d.). POWER BANKING: obiednana merezha viddilen bankiv Ukrainy [POWER BANKING: A united network of branches of Ukrainian banks]. Available at: https://power.bank.gov.ua/ (accessed September 28, 2026) [in Ukrainian].

9. Dubinina M. V., & Bodnar O. A. (2026). Identyfikatsiia ta kalibruvannia nefinansovykh zahroz u systemi zabezpechennia finansovoi nadiinosti komertsiinykh bankiv [Identification and calibration of non-financial threats in the system of ensuring the financial reliability of commercial banks]. Modern Economics, no. 58, pp. 107–120. DOI: https://doi.org/10.31521/modecon.V58(2026)-14 [in Ukrainian].

10. Vakhovych I., Boiarko I., Zarutska O., Fesenko V., Sloboda L., & Sereda O. (2026). Transformatsiia bankivskykh ryzykiv i yikhnii vplyv na finansovu stabilnist: identyfikatsiia ta suchasni vyklyky [Transformation of banking risks and their impact on financial stability: Identification and current challenges]. Finansovo-kredytna diialnist: problemy teorii i praktyky, vol. 4, no. 69, pp. 25–40. DOI: https://doi.org/10.55643/fcaptp.4.69.2026.5301 (accessed September 28, 2026) [in Ukrainian].

11. Ahres O. H., & Sadura O. B. (2025). Stan bankivskoi systemy Ukrainy v umovakh viiny: problemy stabilnosti ta stratehichni oriientyry rozvytku [The state of Ukraine's banking system in wartime: Stability problems and strategic development guidelines]. Rehionalna ekonomika, no. 2(116), pp. 73–82. DOI: https://doi.org/10.36818/1562-0905-2025-2-7 (accessed September 28, 2026) [in Ukrainian].

12. Erkes O., Kalyta O., & Sunduk T. (2022). Bankivska systema Ukrainy v umovakh viiny [Ukraine's banking system in wartime]. Scientia Fructuosa, vol. 144, no. 4, pp. 122–133. DOI: https://doi.org/10.31617/1.2022(144)09 (accessed September 28, 2026) [in Ukrainian].

13. Bakalo I. I. (2025). Stres-testuvannia bankivskoi systemy Ukrainy: instrumenty, stsenarii ta rezultaty v umovakh viiny [Stress testing of Ukraine's banking system: Tools, scenarios and results in wartime]. Naukovi zapysky Natsionalnoho universytetu "Ostrozka akademiia". Seriia "Ekonomika", no. 37(65), pp. 37–42. DOI: https://doi.org/10.25264/2311-5149-2025-37(65)-37-42 (accessed September 28, 2026) [in Ukrainian].

14. Balytska M. V., & Tkachenko A. P. (2025). Dosvid Natsionalnoho banku Ukrainy u zabezpechenni stiikosti bankivskoi systemy v umovakh suchasnykh vyklykiv [The experience of the National Bank of Ukraine in ensuring the resilience

of the banking system amid current challenges]. Ekonomika ta suspilstvo, no. 72. DOI: https://doi.org/10.32782/2524-0072/2025-72-132 (accessed September 30, 2026) [in Ukrainian].

15. Mishchenko V. I., Naumenkova S. V., & Mishchenko S. V. (2023). Upravlinnia operatsiinymy ryzykamy v platizhnykh systemakh [Operational risk management in payment systems]. Ekonomichnyi prostir, no. 183, pp. 79–87. DOI: https://doi.org/10.32782/2224-6282/183-13 (accessed September 28, 2026) [in Ukrainian].

16. Pintokha M. M. (2024). Stratehichni tsili diialnosti bankiv Ukrainy: bezpekovyi aspekt derzhavy pid chas dii voiennoho stanu [Strategic goals of Ukrainian banks' activities: The security aspect of the state under martial law]. Ukrainskyi ekonomichnyi chasopys, no. 7, pp. 81–84. DOI: https://doi.org/10.32782/2786-8273/2024-7-13 (accessed September 30, 2026) [in Ukrainian].

17. Azura Y. T. Y., Azad M. A., & Ahmed Y. (2025). An integrated cyber security risk management framework for online banking systems. Journal of Banking and Financial Technology, vol. 9, pp. 85–104. DOI: https://doi.org/10.1007/s42786-025-00056-3 (accessed September 30, 2026).

18. Bruno E., Pistolesi F., & Teti E. (2025). Cybersecurity policy, ESG and operational risk: A virtuous relationship to improve banks' performance. International Review of Economics & Finance, vol. 99, art. 104053. DOI: https://doi.org/10.1016/j.iref.2025.104053 (accessed September 28, 2026).

19. Türegün N. (2025). Digital transformation and cybersecurity risks. International Journal of Accounting Information Systems, vol. 56, art. 100749. DOI: https://doi.org/10.1016/j.accinf.2025.100749 (accessed September 28, 2026).

20. Cumming D., Nguyen M., Pham A. V., & Samarasinghe A. (2026). Banking system stability: A global analysis of cybercrime laws. Journal of International Business Studies, vol. 57, pp. 356–380. DOI: https://doi.org/10.1057/s41267-025-00838-3 (accessed September 30, 2026).

21. Abidi N., Gambacorta L., Kok C., Miquel-Flores I., Madio L., & Partida A. (2026). Disciplining digital risk: Evidence from cyber stress tests. ECB Working Paper Series, no. 3222. Frankfurt am Main: European Central Bank. Available at: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3222~27c5b77e07.en.pdf (accessed September 28, 2026).

22. Rinaldi S. M., Peerenboom J. P., & Kelly T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11–25. DOI: https://doi.org/10.1109/37.969131 (accessed September 28, 2026).

23. European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector. Official Journal of the European Union, L 333, pp. 1–79. Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (accessed September 28, 2026).