Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2026. № 5.
ISSN 2307-2105

DOI: http://doi.org/10.32702/2307-2105.2026.5.244
УДК 336.71:004

О. В. Прокоф'єва,
к. е. н., доцент кафедри страхування, банківської справи та ризик-менеджменту, Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID ID: https://orcid.org/0009-0005-3715-3558
В. Б. Білорус,
студент 2 курсу ОС «Магістр» спеціальності 072 «Фінанси, банківська справа, страхування та фондовий ринок»,
Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID ID: https://orcid.org/0009-0007-8996-1316

АДАПТАЦІЯ ДО ОПЕРАЦІЙНИХ РИЗИКІВ У БАНКАХ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ: ВПЛИВ КІБЕРЗАГРОЗ ТА ЕНЕРГЕТИЧНОЇ КРИЗИ

O. Prokofieva,
PhD in Economics, Associate Professor of the Department of Insurance, Banking and Risk Management, Taras Shevchenko National University of Kyiv
V. Bilorus,
Master's Student, Specialty 072 «Finance, Banking, Insurance and Stock Market», Taras Shevchenko National University of Kyiv

ADAPTATION TO OPERATIONAL RISKS IN UKRAINIAN BANKS UNDER MARTIAL LAW: THE IMPACT OF CYBER THREATS AND THE ENERGY CRISIS

У статті досліджено трансформацію системи управління операційними ризиками банків України в умовах воєнного стану (2022-2026 рр.). Встановлено, що повномасштабне вторгнення сформувало якісно нове ризикове середовище, в якому традиційні управлінські моделі виявилися структурно недостатніми. Визначено два ключові системні вектори загроз: кіберризики - масштабні DDoS-атаки, фішингові кампанії, що імітували повідомлення НБУ та держорганів, і спроби горизонтального переміщення в мережах фінансових установ - та ризики хронічної нестабільності електропостачання, які суттєво порушили функціонування платіжних систем, IT-інфраструктури та каналів дистанційного обслуговування. Проаналізовано адаптаційні практики банків: розгортання резервних джерел живлення та систем накопичення енергії, міграцію критичних сервісів до розподілених хмарних дата-центрів, перегляд планів безперервності діяльності та застосування принципів архітектури нульової довіри (ZTA). Розглянуто регуляторну відповідь НБУ, зокрема оновлення порядку розрахунку капіталу на покриття операційного ризику відповідно до стандартів ЄС та впровадження платформи MISP-НБУ для обміну індикаторами кіберзагроз між учасниками фінансового сектору. Узагальнено досвід BNP Paribas і Banco Santander у контексті виконання вимог DORA як орієнтирів для євроінтеграції вітчизняного ризик-менеджменту. За результатами дослідження обґрунтовано необхідність формування інтегрованої моделі управління операційною стійкістю, що об'єднує кібер-, енергетичні та організаційні ризики в єдину аналітичну систему.

This paper examines the transformation of operational risk management in Ukrainian banks under martial law conditions covering the period from 2022 to 2026. The full-scale Russian invasion created a qualitatively distinct risk environment in which traditional operational risk models - designed for stable operating conditions - proved structurally insufficient against concurrent, sustained, and mutually reinforcing threats.

Two principal systemic threat vectors are identified and analysed. The first encompasses cyber risks: large-scale DDoS attacks targeting payment infrastructure and online banking platforms, phishing campaigns that deliberately impersonated the National Bank of Ukraine and state authorities to exploit heightened public anxiety, and sophisticated intrusion attempts relying on lateral network movement within financial institutions. The second vector involves chronic energy supply disruptions resulting from systematic strikes against Ukraine's energy infrastructure. Unlike the brief, isolated outages addressed by standard business continuity plans, the prolonged and recurring blackouts of the wartime period disrupted payment systems, ATM networks, and remote service channels, while simultaneously degrading the operational capacity of information security monitoring and incident response functions - a compounding effect that transformed energy risk into a systemic feature of the banking sector's risk profile.

The study analyses the adaptive responses of Ukrainian banks, including: deployment of backup power systems and battery storage units, accelerated migration of critical workloads to geographically distributed cloud data centers, multi-scenario revision of business continuity plans to incorporate extended blackout modelling, and implementation of Zero Trust Architecture (ZTA) principles to limit the impact of network compromise. The regulatory response of the National Bank of Ukraine is assessed, with particular attention to the January 2026 update aligning operational risk capital requirements with EU Basel III standards - eliminating the internal loss multiplier in line with European practice - and the rollout of the MISP-NBU platform for structured sharing of cyber threat indicators across the financial sector. The operational risk governance approaches of BNP Paribas under DORA and Banco Santander's holistic risk control model are examined as reference frameworks for Ukraine's ongoing regulatory convergence with European standards.

The central finding is that cyber threats and energy instability have ceased to function as isolated operational incidents and must be managed as persistent, integrated components of banks risk profiles. On this basis, the paper formulates

recommendations for strengthening cyber resilience, energy autonomy of critical IT infrastructure, and business continuity planning, with relevance for bank management, the NBU, and policymakers engaged in wartime and post-war financial sector governance.

Ключові слова: *операційні ризики, кіберзагрози, енергетична криза, операційна стійкість, безперервність банківської діяльності.*

Keywords: *operational risks, cyber threats, energy crisis, operational resilience, continuity of banking operations.*

Постановка проблеми. Повномасштабне вторгнення рф у 2022 році кардинально змінило операційне середовище банківського сектору України, спричинивши різке зростання операційних ризиків. Постійні ракетні обстріли, тривалі відключення електроенергії, релокація персоналу та безпрецедентна інтенсивність кібератак змусили банки терміново переглядати системи управління ризиками. Традиційні моделі, орієнтовані на стабільні умови, виявилися неефективними перед новими системними загрозами фізичного та цифрового характеру.

Актуальність проблеми зумовлена критичною роллю банків у забезпеченні фінансової стабільності держави: будь-які значні порушення їхньої діяльності здатні паралізувати платіжну систему, кредитування та виконання державних фінансових функцій. Операційні ризики набули нових форм - від тривалих блекаутів і втрати доступу до ІТ-систем до кібершантажу, дезінформаційних атак та логістичних обмежень.

Незважаючи на суттєві регуляторні зміни НБУ та впровадження планів безперервності бізнесу, низка питань залишається недостатньо дослідженою: ефективність кіберзахисту в умовах воєнного часу, оптимальні моделі резервування критичної інфраструктури, адаптивні процедури реагування на довготривалі енергетичні перебої, а також інтеграція кібер-, ІТ-, кадрових та фізичних ризиків в єдину систему управління. Тому пошук

напрямів адаптації ризик-менеджменту банків до сучасних викликів воєнного стану є надзвичайно актуальним завданням, вирішення якого сприятиме зміцненню операційної надійності та безперервності функціонування банківського сектору України.

Аналіз останніх досліджень і публікацій. Проблематика управління операційними ризиками банків та забезпечення їх стійкості у кризових умовах висвітлюється у працях О. Чумак, Д. Третяк, П. Душейко, Ю. Коломієць, В. Кочорби, де проаналізовано трансформацію ризик-профілю банків та особливості функціювання систем ризик-менеджменту у період воєнних загроз. У навчально-методичному посібнику О. Кібік, О. Слободянюк та Л. Кузнецової систематизовано підходи до класифікації та оцінювання операційних ризиків, що становить важливу теоретичну основу для сучасних досліджень. Окремі аспекти впливу кіберзагроз і цифровізації на операційну стійкість банків висвітлені в роботах І. Гончаренко, О. Грабчук, С. Оніщенка, Т. Болгар, Г. Кришталь та інших авторів, які підкреслюють зростання ролі інформаційної безпеки у воєнний період. У зарубіжному досліджені (Aminul et al., 2024) репутаційні та операційні ризики розглядаються у контексті медіа-впливу та цифрових факторів, що формує додаткове аналітичне підґрунтя.

Невирішені частини загальної проблеми. Високий рівень операційних ризиків, кіберзагроз та енергетичної нестабільності є ключовою особливістю поточного стану банківської системи в Україні. Однак наукові методи їх інтегрованого управління не були достатньо розроблені. Відповідно до цього можна підкреслити такі проблеми:

1) відсутність комплексної моделі інтегрованого управління операційними ризиками, яка б охоплювала одночасно кіберзагрози, технічні збої, перебої енергопостачання та ризики безперервності діяльності банків.

2) недостатній рівень адаптивності існуючих систем ризик-менеджменту до тривалих енергетичних криз, що ускладнює підтримання роботи критичних ІТ-сервісів, платіжних систем та каналів зв’язку.

3) низький ступінь практичної готовності банків до реалізації планів безперервності діяльності, оскільки більшість із них орієнтовані на короткострокові збої, а не на затяжні системні кризи.

Мета статті - дослідження трансформації системи управління операційними ризиками в банках України в умовах воєнного стану з особливим акцентом на адаптацію до кіберзагроз та енергетичної кризи у 2022-2026 рр., а також розробка практичних рекомендацій щодо забезпечення безперервності банківської діяльності в екстремальних умовах.

Об'єкт дослідження - управління операційними ризиками у банках України.

Предмет дослідження - інструменти та організаційні механізми адаптації банків до операційних ризиків, спричинених кіберзагрозами, технічними збоями та енергетичною нестабільністю в умовах воєнного стану.

Для досягнення сформованої мети дослідження було визначено перелік таких **завдань**:

- Систематизувати операційні ризики, що актуалізувалися в банківському секторі під час воєнного стану.
- Охарактеризувати вплив кіберзагроз та енергетичної кризи на безперервність діяльності банків.
- Проаналізувати сучасні підходи до управління операційними ризиками та визначити їхні обмеження.
- Обґрунтувати напрями вдосконалення інтегрованої моделі управління операційною стійкістю банків.
- Розробити практичні рекомендації щодо посилення кіберзахисту та стійкості ІТ-інфраструктури у банках України.

Розв'язання поставлених завдань зумовило застосування таких **методів дослідження:**

Системний підхід - комплексна оцінки взаємозв'язку між операційними, технологічними ризиками та безпековими ризиками, а також

для обґрунтування інтегрованої моделі управління операційною стійкістю банків.

Порівняльний аналіз - порівняння антикризових практик банків України з підходами міжнародних фінансових інституцій в частині кіберзахисту та забезпечення безперервності бізнесу.

Метод структурно-функціонального аналізу - оцінка внутрішньої архітектури систем управління ризиками, роль ІТ-інфраструктури, резервних каналів та хмарних сервісів.

Метод узагальнення та синтезу - формулювання практичних рекомендацій щодо посилення управління операційними ризиками в умовах воєнного стану.

Огляд літератури. Кібік О., Слободянюк О. та Кузнєцова Л. системно пояснюють еволюцію підходів до управління ризиками. Крім того, вони наголошують на важливості інтегрованих інформаційних системах управління та системах для виявлення та моніторингу операційних ризиків. Висновки з праці: операційний ризик є складною категорією, яка охоплює безліч технологічних, організаційних та людських факторів; акцент робиться на створенні адаптивних механізмів контролю.

Коломієць Ю., Кочорба В. аналізують кредитні та операційні ризики в умовах підвищеної чутливості. Висновки з їх роботи: постійні атаки збільшують операційні збої та залежність від технологічної надійності банків; цифровізація банківських процесів збільшує ризик можливих кібератак.

Панаско О. М., Сагун А. В., Гавриш О. С., Гончаренко І. Г., Кльоба Л. у своїх роботах про кіберризики в банківському секторі підкреслюють зростання кіберзагроз. Висновки з роботи: відстеження та розуміння трендів кіберзагроз сприяють ефективному управлінню кіберризиками; кіберзагрози є основним драйвером операційних ризиків, оскільки існує дефіцит механізмів мінімізації репутаційних та технологічних втрат.

Виклад основного матеріалу дослідження. У рамках дослідження ризик-менеджменту банківських установ операційний ризик розглядається як фундаментальна категорія, що об'єднує різноманітні загрози, пов'язані з функціонуванням внутрішніх процесів, помилками персоналу, станом інформаційних систем та впливом зовнішніх чинників. Відповідно до вимог Базель III, цей вид ризику визначається як загроза збитків через недоліки в організаційних процедурах, технологічних рішеннях або внаслідок зовнішніх подій, що зумовлює його високий рівень комплексності та прогностичних складностей [18].

Одним із ключових елементів системи управління операційним ризиком є наявність чітко визначених нормативних положень, правил, процедур та організаційної структури, що забезпечує розподіл повноважень і відповідальності між окремими підрозділами та уповноваженими особами. Не менш важливим компонентом виступає механізм регулярного інформування вищого керівництва про стан управління операційним ризиком. Крім того, необхідне встановлення чітких правил обміну інформацією між підрозділами банку, а також між учасниками платіжної системи. Суттєве значення мають також відповідні технологічні засоби, процедури та комплекс методів і інструментів, призначених для ідентифікації, оцінки, контролю, управління та моніторингу операційних ризиків [20].

Доцільно розглянути особливості нормативно-правової бази управління операційним ризиком банку з позиції її ієрархічної структури, що поділяється на три основні рівні:

- метарівень (зовнішній міжнародний рівень) - охоплює міжнародну регуляторну базу та рекомендації, зокрема принципи Базельського комітету з банківського нагляду (зокрема, принципи належного управління операційним ризиком), стандарти Базель II/III щодо розрахунку капіталу на покриття операційного ризику та інші глобальні

рекомендації щодо управління операційними ризиками в банківському секторі [18];

- макрорівень (національний рівень) - включає внутрішню регуляторну базу Національного банку України, а також закони України, які прямо чи опосередковано регулюють відносини у сфері управління операційним ризиком (зокрема, положення про організацію системи управління ризиками в банках України та банківських групах, вимоги до розрахунку мінімального розміру операційного ризику тощо) [1, 2, 3].
- мікрорівень (внутрішньобанківський рівень) - складається з внутрішньої документації банку, включаючи інструкції, положення, політики та регламенти, що регулюють управління операційним ризиком з урахуванням специфіки діяльності, масштабів, структури та особливостей конкретної банківської установи.

Такий ієрархічний підхід до нормативного регулювання забезпечує узгодженість між глобальними стандартами, національними вимогами та індивідуальними особливостями банку, сприяючи формуванню комплексної та ефективної системи управління операційним ризиком.

Національний банк затвердив зміни до Положення про порядок визначення банками України мінімального розміру операційного ризику, врахувавши оновлення в Європейському Союзі з 01 січня 2025 року підходу до визначення банками вимог до капіталу на покриття мінімального розміру операційного ризику. Запроваджений у ЄС підхід не передбачає застосування внутрішнього мультиплікатора збитків, тому й був вилучений із Положення. Це означає, що розрахунковий розмір операційного ризику для покриття капіталом і надалі не залежатиме від історичного розміру збитків від подій операційного ризику банків, як це передбачалося від запровадження відповідних вимог [4].

Також у змінах до Положення передбачено диференціацію граничного коефіцієнта зважування. Наприкінці 2025 року він набував значень від 0,12 до

0,18 залежно від розміру компонента бізнес індикатора. Компонент бізнес індикатора відображає розмір діяльності банку та відповідно розмір експозиції до операційного ризику. Він розраховується як сукупний розмір чистих процентних доходів, доходу у вигляді дивідендів, комісійних доходів, інших операційних доходів, результату переоцінки від операцій купівлі-продажу активів / зобов'язань. Оскільки майже для всіх банків коефіцієнт зважування набуватиме значення 0,12, запровадження оновлених вимог знизить потреби в капіталі для покриття операційного ризику [4].

Операційні ризики банківського сектору України в умовах воєнного стану зазнали суттєвої структурної трансформації, що обумовлено комплексною дією енергетичних, кібернетичних та організаційних загроз. Вплив цих факторів має системний характер, оскільки стосується практично всіх ключових бізнес-процесів банку - від функціонування ІТ-інфраструктури та процесингових центрів до внутрішніх контрольних процедур і роботи персоналу. В умовах постійної зовнішньої нестабільності рівень операційного ризику перестав залежати лише від внутрішньої організації процесів і дедалі більше формується під впливом факторів, на які банки не можуть безпосередньо впливати [10].

Нижче узагальнено наведено категорії ризиків, які у свою чергу мають ключові типи та конкретні прояви з урахуванням сучасних подій (див. табл. 1).

Таблиця 1. Операційні ризики банків України в умовах воєнного стану

Категорія ризику / Джерело	**Основний тип ризику**	**Конкретні прояви / Складові ризику**
Зовнішні фактори (воєнне середовище)	Ризики безперервності діяльності	- Енергетична нестабільність та блекаути - Руйнування або пошкодження фізичної інфраструктури (відділення, банкомати) - Системні перебої в роботі мобільного зв'язку та інтернет-провайдингу
Гібридні загрози (кібербезпека)	Кіберризики	- Масовані DDoS-атаки на платіжні та онлайн-сервіси - Цілеспрямовані фішингові та соціально-інженерні атаки на персонал - Спроби несанкціонованого доступу до критичних інформаційних систем - Ризики компрометації даних та порушення роботи процесингових центрів
Внутрішні фактори (організаційні)	Ризики людського фактору	- Кадрові втрати, мобілізація та вимушена релокація співробітників - Підвищений рівень стресу та психоемоційного виснаження персоналу - Зростання ймовірності операційних помилок у критичних процесах (розрахунки, валютний контроль тощо)
Технічні фактори (ресурсні обмеження)	Технологічні ризики	- Фізична недоступність критичного обладнання або серверів - Ненадійність або обмежена пропускна здатність резервних каналів зв'язку - Прискорене зношення IT-інфраструктури через експлуатацію в нештатних режимах
Операційні потоки (взаємодія з клієнтами)	Ризики, пов'язані з обслуговуванням клієнтів	- Нестабільність і структурні зрушення попиту на банківські продукти - Екстремальні пікові навантаження на контакт-центри та онлайн-канали обслуговування

Джерело: складено автором на основі [6, 10]

З таблиці 1 чітко видно, що за період воєнного стану в Україні для банків значно збільшилися прояви різних категорій ризиків. Серед усіх загроз найбільш відчутним став ризик порушення операційної безперервності, що тісно пов'язаний зі станом енергетичної інфраструктури країни. Системні відключення електроенергії взимку з початку війни призвели до суттєвої нестабільності в роботі платіжних систем, відділень та мереж банкоматів. На пікові періоди блекаутів припадали спади функціональності банкоматів, коливання навантаження на цифрові сервіси та відстрочення в обробці

окремих транзакцій. Така ситуація зумовила необхідність у посиленні резервних потужностей, збільшенні мережі автономних точок обслуговування та активному впровадженні альтернативних каналів комунікації, зокрема супутникового зв'язку. Емпіричні дані підтверджують, що фінансові установи, які завчасно проінвестували в розвиток резервних джерел енергії та перехід на хмарні рішення, продемонстрували вищу адаптивність і зазнали менших операційних збитків [11].

Паралельно з енергетичними викликами спостерігалося різке зростання рівня кіберзагроз, інтенсивність яких демонструвала чітку кореляцію з динамікою бойових дій на території України (рис. 1).

Рис. 1 Основні сучасні кіберзагрози для банків і фінансових установ

Джерело: складено автором на основі [8, 9]

Фінансовий сектор залишався однією з пріоритетних цілей кіберагресії, зазнаючи масованих розподілених атак типу DDoS на системи дистанційного банкінгу, спроб несанкціонованого проникнення в інформаційні системи, а також цілеспрямованого розповсюдження шкідливого програмного забезпечення [16]. Характерною рисою цього періоду стало домінування складних багаторівневих кібератак, що поєднували компрометацію облікових записів співробітників через соціальну інженерію з подальшим горизонтальним переміщенням у мережах установ. Значно зросла кількість фішингових кампаній, які імітували офіційні повідомлення державних органів, Національного банку України, гуманітарних організацій або програм підтримки населення, що суттєво ускладнювало їх своєчасне виявлення [8].

Ескалація складних кібератак спричинила значне зростання відтермінованих операційних втрат, що виникають через порушення цілісності інформаційних систем, несанкціонований доступ до конфіденційних даних та необхідність тривалої відновлювальної роботи IT-інфраструктури. У багатьох випадках шкода від шкідливої активності не призводила до миттєвого припинення банківських операцій, однак створювала підґрунтя для подальших фінансових, регуляторних та репутаційних втрат. Це, у свою чергу, ускладнювало своєчасну ідентифікацію та оцінку таких ризиків у межах традиційних методів управління операційними ризиками [9].

На тлі воєнного стану кіберзагрози перестали розглядатися виключно як частина технологічного ризику. Замість цього вони набути системного характеру, суттєво впливаючи на безперервність ключових банківських процесів. Збої у роботі систем дистанційного банкінгу, процесингових центрів і внутрішніх платіжних платформ стали причиною не тільки прямих операційних втрат, але й значних репутаційних збитків, які підривали довіру клієнтів і посилювали загрози для стабільності фінансової системи [13].

Особливо гостро проблема управління кіберризиками виявляється у поєднанні з фізичними та енергетичними обмеженнями. Тривалі перебої з електропостачанням і порушення в роботі телекомунікаційної інфраструктури значно знижували функціональність систем моніторингу інформаційної безпеки, ускладнювали оперативність реагування на інциденти та створювали проблеми із забезпеченням резервного відновлення даних. Унаслідок цього кібератаки дедалі частіше трансформувалися у складні операційні кризи, які виходили за межі стандартних сценаріїв управління ризиками [7].

У зв’язку з такими викликами постає нагальне завдання перегляду підходів до керування операційними ризиками на основі принципів операційної стійкості та інтегрованого управління ризиками. Практика міжнародних регуляторних установ та органів нагляду свідчить про

ефективність створення уніфікованих аналітичних концептуальних рамок для менеджменту ризиків. Це передбачає інтеграцію кіберризиків, ризиків безперервності діяльності та технологічних загроз з використанням інструментів сценарного аналізу і механізмів раннього попередження.

Для кращого розуміння основних проявів операційних ризиків та підходів до їх аналізу і управління варто проаналізувати окремі приклади з практики міжнародних банків. Вони демонструють актуальні виклики, з якими стикаються фінансові установи в умовах кризи.

Таблиця 2. Досвід зарубіжних банків в управлінні операційними ризиками

Тип операційного ризику	Приклад реалізації	Ключові підходи до управління
Кіберризики	2022 р. - Flagstar Bank: витік персональних даних клієнтів унаслідок атаки програм-вимагачів	Постійний моніторинг даних, навчання персоналу кібербезпеці, плани реагування на кібератаки, стрес-тестування, перевірка аудиту
Технологічні ризики	2023 р. - Bank of Ireland: збій ІТ-систем, що призвів до перевищення клієнтських лімітів	Резервування ІТ-систем, регулярне тестування ПЗ, відновлення даних
Регуляторні (комплаєнс) ризики	2023 р. - Wells Fargo: штраф регулятора за порушення вимог фінансового нагляду	Автоматизація комплаєнс-контролю, внутрішні аудити, удосконалення політик та стратегій банку
Ризики людського фактору	2023 р. - Silicon Valley Bank: управлінські помилки в умовах кризового навантаження	Підвищення кваліфікації, дисциплінарні заходи, автоматизовані механізми контролю та звітності
Макроекономічні та геополітичні ризики	2023 р. - HSBC: втрати внаслідок валютної нестабільності в регіонах присутності	Диверсифікація портфелів банку, стрес-тестування, сценарний аналіз

Джерело: складено на основі [7]

Вищезгадані приклади показують, що операційні ризики в банківському секторі не виникають ізольовано, а пов’язані з технологічними збоями, помилками управління, регуляторними обмеженнями та макроекономічною нестабільністю. Досвід іноземних банків свідчить про необхідний перехід від фрагментованого управління окремими видами ризиків до інтегрованої моделі операційної стабільності, яка об’єднує

операційні, кібернетичні та регуляторні ризики в єдину систему управління ризиками. Отримані знання можуть бути застосовані на практиці в українських банках, ризики яких під час воєнного стану посилюються іншими факторами, такими як енергетична нестабільність, фізичні загрози та обмежений доступ до інфраструктурних ресурсів.

З активною інтеграцією банківської системи України в європейську банківську систему, вивчення та адаптація управління операційними ризиками, яке застосовують деякі європейські банки, набуває більшої уваги. Фінансові установи, зокрема банки в Європі все частіше застосовують різні методи для подолання операційних ризиків, зосереджуючись на посиленні стійкості до операційних загроз та захисті від кібератак. Ось деякі з цих заходів, що застосовуються провідними банками.

- BNP Paribas працює над дотриманням Закону про цифрову операційну стійкість (DORA), який спрямований на підвищення цифрової стійкості. Банк створює внутрішні рамки управління ризиками в сфері ІКТ - ідентифікує, оцінює та зменшує ризики, а також ефективно реагує на такі інциденти. Особлива увага приділяється узгодженню та гармонізації стратегій управління ризиками третіх сторін та запровадженню узгодженого дотримання європейських регуляторних стандартів щодо цифрової стійкості [19].
- Ще одним цікавим прикладом може бути Banco Santander. Існує кілька ризиків та їх рішень, які він реалізує за допомогою цілісної моделі управління операційними ризиками, зосереджуючись різними способами на постійній ідентифікації, оцінці, моніторингу та зменшенні загроз, включаючи кіберзагрози, шахрайство та технологічні збої. Банк використовує офіційну базу внутрішніх подій операційного ризику, самооцінку ризиків та контроль (RCSA), які у свою чергу організовані та реалізуються за принципами «Захист - Виявлення - Реагування - Запобігання шахрайству». Такий підхід не тільки зменшує

ймовірність збитків, але й підвищує загальну стійкість бізнес-процесів [17].

Впровадження цих стратегій відображає зміну парадигми в європейській банківській сфері від традиційного реактивного управління операційними ризиками до проактивної стратегії операційної стійкості. Такі практики, включаючи інтеграцію принципів DORA, тестування сценаріїв, посилений нагляд за третіми сторонами та постійне вдосконалення систем раннього виявлення загроз, можуть слугувати важливими орієнтирами для зміцнення національної системи управління операційними ризиками в контексті гармонізації з європейськими стандартами.

Слід ще зазначити, що для підвищення кіберстійкості, важливо зміцнити гарантії навколо критично важливих IT-систем за допомогою сегментації мережі, обмежень привілеїв доступу та застосування принципів архітектури нульової довіри (ZTA). Ця стратегія ефективно зменшує ризик, пов’язаний із горизонтальним переміщенням зловмисників у мережі банку, а також зменшує потенційний вплив операційних збоїв у випадках, коли певні компоненти інфраструктури скомпрометовані [9].

Для посилення координації дій у сфері кіберзахисту, а також централізованого обміну інформацією між установами, що працюють у фінансовій галузі, Національний банк України розробив спеціальну інформаційну платформу для збору, обробки, зберігання та поширення даних про інциденти інформаційної безпеки. Для роботи в контексті функцій Центру кіберзахисту при НБУ створено платформу MISP-НБУ, що слугує механізмом захоплення та обміну інформацією про кіберзагрози між банками та іншими зацікавленими сторонами. На основі відкритої міжнародної платформи MISP спроектовано та налаштовано платформу MISP-NBU під умови фінансової системи України. MISP-UA, як гармонізована версія, враховує національну специфіку того, як організації організовують кіберзахист всередині країни, сприяє систематичному обміну інформацією між фахівцями з моніторингу, аналізу, реагування на кіберінциденти. У

відповідних випадках його застосування дає змогу поєднувати аналітичний потенціал команд для протидії загрозам, забезпечення безпеки інформаційних систем фінансових установ та груп реагування на кіберінциденти, до складу яких входять спеціалізовані підрозділи Державної служби спеціального звязку та захисту інформації України, зокрема структури CERT [15].

Своєчасне оприлюднення технічних даних, індикаторів компромісу та інформації про тактику, прийоми та процедури дій зловмисників відкриває перспективу для спільного аналізу ризиків, швидкого виявлення нових загроз та потенційного впливу їх загрози на важливі інформаційні системи банків. Завдяки платформі MISP-UA вона заохочує інтерактивних учасників реагувати на кіберінциденти активніше взаємодіяти на ще вищому рівні. Також це скорочує час реагування на кіберзагрози у фінансовому секторі та допомагає створити більшу готовність банків до можливих кібератак. MISP-UA стане важливим інституційним інструментом для зміцнення національної кібербезпеки, об’єднуючи дії, спрямовані урядом, приватним сектором та іншими організаціями для протидії сучасним кіберзагрозам [15].

Повертаючись до іншого вагомого ризику, внаслідок того, що Україна постійно страждає від масштабних атак на свою енергетичну інфраструктуру, відбувається постійне зростання операційних ризиків для банківського сектору в період воєнного стану. Перебої в електропостачанні, особливо системні та тривалі, призвели до порушення стабільності критично важливих банківських бізнес-процесів, таких як робота наземних банківських платіжних систем, обробка платежів, мережі банкоматів і відділень, а також обслуговування клієнтів через дистанційні канали [11].

Банківська діяльність, пов’язана з ризиками відключення електроенергії, виходить за межі фізичної недоступності інфраструктури через ненадійні телекомунікації, порушений доступ до резервних центрів обробки даних та банківські структурні підрозділи з поганою координацією між функціями банку. Таким чином, ймовірність операційних збоїв, затримок платежів та погіршення якості банківських послуг буде ще більше

збільшуватися і може бути вищою навіть за наявності офіційних планів забезпечення безперебійної діяльності.

Унікальною характеристикою енергетичної кризи у воєнний час є її тривалий і повторюваний характер, що різко відрізняється від короткочасних аварійних відключень електроенергії, які зазвичай займають чільне місце у стандартних планах реагування банків. У таких випадках накопичується операційний ризик, оскільки тривалі відключення електроенергії спричиняють швидший знос резервного обладнання, більше навантаження на автономні джерела живлення та частіші технічні збої у важливих ІТ-системах [11].

Разом з тим, поняття, що стало дуже близьким для суспільства «блекаут», а точніше ризики, пов’язані з ним тісно поєднані з людським фактором, оскільки тривала робота в умовах недостатніх ресурсів, тиску та ненадійних комунікацій збільшує ймовірність операційних помилок персоналу та ускладнює дотримання процесів внутрішнього контролю.

Як результат, енергетична криза в період воєнного стану трансформувала «блекаут-ризики» з допоміжного фактора операційної нестабільності в системну особливість ризик-профілю українських банків. Це вимагає перегляду традиційних підходів управління операційними ризиками з акцентом на забезпеченні тривалої автономності критичної інфраструктури, підвищенні надійності надлишкових ІТ-рішень та інтеграції енергетичних ризиків у моделі оцінки операційної стійкості.

Одним із способів забезпечення безперервності роботи та надійності в надзвичайних ситуаціях є використання автономних генераторів і накопичувачів електроенергії як резервних копій. Ця інфраструктура може підтримувати виконання основних видів діяльності після довгострокових відключень електроенергії, таких як використання основних серверів, каналів зв’язку та систем обробки.

Українські банки також переходять на більш розподілені дата-центри і хмарні сервіси, які забезпечують резервування інформаційних систем на

іншому рівні, а саме по географічно розподіленим центрам обробки даних. Хмарні платформи дозволяють важливим ІТ-сервісам продовжувати функціонувати навіть під час аварійних відключень електроенергії та довготривалих блекаутів, адже вони розміщуються в кількох центрах обробки даних з автономними лініями живлення [11].

Іншим критичним аспектом адаптації є переробка внутрішніх планів безперервності банківської діяльності, відповідно до специфіки енергетичної кризи. Це передбачає формалізацію алгоритмів реагування на різні сценарії ризику відключення електроенергії, альтернативні комунікаційні коридори, характеристику основних функцій, а також навчання та симуляційні вправи з розробки сценарію відключення електроенергії. Що стосується технічних рішень, то активно впроваджуються системи моніторингу енергоспоживання та інтелектуального контролера потужності, що приводить до оптимізації розподілу енергоресурсів на більш пріоритетні та критичні елементи ІТ-інфраструктури. Це зменшує залежність від незалежних джерел енергії та покращує їх ефективність щодо низьких рівнів енергозабезпечення.

Результати 2023 року показали: банківська система в період війни довела свою інституційну спроможність і має довіру людей. Приріст коштів відбувся у 43 банках, відплив - лише у 21 банківській установі та серед тих, хто втратив ліцензію на ведення банківського бізнесу. Серед лідерів із залучення коштів фізичних осіб - ПриватБанк, Ощадбанк, Універсал (Моно) банк, ПУМБ, Укрсиббанк, Укрексімбанк, Сенс банк, Аккордбанк, А-банк, «Південний».

Бізнес працює у найскладніших умовах. Якщо раніше матеріальні резерви доцільно було тримати у складських запасах, то в реаліях війни при постійному бомбардуванні складських приміщень збільшилися залишки у грошових коштах на банківських рахунках [14].

Також доцільно буде вказати події, в яких банки беруть активну участь в рамках спільного меморандуму про готовність фінансувати відновлення енергетичної інфраструктури. Банки долучилися до реалізації проєктів

розбудови, реконструкції та відновлення генерації потужністю 1,373 ГВт. Найбільші обсяги фінансування в цьому напрямі надано на розбудову СЕС, газових і гідро/біо/вітрових установок. Крім генерації, банки фінансують проєкти зі зберігання електроенергії (створення систем накопичення, придбання інверторів та акумуляторів тощо), теплопостачання, модернізацію теплообладнання. Потужність за цими проєктами становить 556 МВт. Надані раніше кредити поволі погашаються частково або повністю, тож валовий портфель «енергетичних» кредитів юридичним особам станом на 01 лютого 2026 року становив 24,2 млрд грн, фізичним особам - 2,1 млрд грн. [5, 12].

Висновки і перспективи подальших досліджень. В умовах воєнного стану операційні ризики українських банків суттєво змінилися і набули досить складного характеру. На їх розвиток впливає поєднання кіберзагроз, енергетичної нестабільності та організаційних обмежень, що значно ускладнює підтримку банківських операцій. Не дивно, що зосередження уваги на окремих інцидентах або короткострокових порушеннях, які зазвичай вважаються традиційним підходом до управління операційними ризиками, не є ефективним для банків, які перебувають у кризовому стані. Енергетична криза перетворила ризики відключень електроенергії на системний елемент операційної нестабільності в банках, впливаючи на платіжні системи, IT-інфраструктуру та канали дистанційного обслуговування. Важливість кіберризику зросла через підвищену роль кіберзагроз, які у воєнний час вже не є просто технологічним ризиком, а стають значними фінансовими втратами та втратами через репутаційний ризик. Це вимагає більш повної інтеграції управління кіберризиками в загальну систему управління операційними ризиками банків. Тим самим було підтверджено потенціал для вдосконалення планів безперервності банків для охоплення багатосценарного підходу: врахування довгострокових сценаріїв відключення, комбінованих кібер- та фізичних загроз, а також обмеження ресурсів.

Головним результатом дослідження є формулювання важливості розробки інтегрованої моделі управління операційною стійкістю для

інтеграції управління операційними, кібер- та енергетичними ризиками в єдину аналітичну перспективу та активний регулятор. Перспективи майбутніх досліджень включають встановлення і аналіз кількісних методів оцінювання операційної стійкості банків за відсутності або обмеженості історичних даних та дослідження впливу європейських регуляторних стандартів у сфері цифрової операційної стійкості на трансформацію українського банківського сектору.

Література

1. Про внесення змін до Положення про порядок визначення банками України мінімального розміру операційного ризику : Постанова НБУ від 19.12.2025 № 149. URL: https://ips.ligazakon.net/document/MN030933?an=3
2. Про затвердження Змін до деяких нормативно-правових актів Національного банку України : Постанова НБУ від 22.01.2026 № 9. URL: https://zakon.rada.gov.ua/laws/show/v0009500-26#n2
3. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : Постанова НБУ від 11.06.2018 № 64. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text
4. Оновлено порядок оцінки банками та банківськими групами операційного ризику. Національний банк України URL: https://bank.gov.ua/ua/news/all/onovleno-poryadok-otsinki-bankami-ta-bankivskimi-grupami-operatsiynogo-riziku
5. Банки забезпечили фінансування енергетичних проєктів на 36,6 млрд грн. Національний банк України. URL: https://bank.gov.ua/ua/news/all/banki-zabezpechili-finansuvannya-energetichnih-proyektiv-na-366mlrdgrn
6. Абрамова А. Тенденції розвитку та особливості управління операційними ризиками комерційних банків. Науковий вісник Полісся. 2021. Вип. 2 (23). С. 93-104.

7. Гончар К. О., Гогуленко Н. О. Міжнародний та вітчизняний досвід управління операційним ризиком банку. Науковий вісник Одеського національного економічного університету. 2024. Вип. 5-6 (318-319). С. 39-46.

8. Гончаренко І. Г. Кіберзагрози фінансового сектора в умовах війни. Економіка та суспільство. 2023. Вип. 50. 6 с.

9. Кльоба Л., Кльоба Т. Кіберзагрози банківського сектора в умовах воєнного стану в Україні. Financial and Credit Activity: Problems of Theory and Practice. 2022. Вип. 5 (46). С. 19-28.

10. 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.

11. Лісовий А. В., Андрух О. В. Енергетична безпека України: виклики війни та перспективи відновлення економічного потенціалу. Український економічний часопис. 2025. Вип. 8. С. 40-43.

12. Аналітичні матеріали щодо стабільності енергосистеми України. НЕК «Укренерго». URL: https://ua.energy/category/analityka/

13. Панаско О. М., Сагун А. В., Гавриш О. С. Аналіз трендів кіберзагроз як важливий етап управління ризиками фінансового сектору. Сучасний захист інформації. 2025. Вип. 2 (62). С. 98-106.

14. Рейтинг життєздатності банків - 2024. Перевірка на витривалість. Mind. URL: https://mind.ua/publications/20269589-rejting-zhittezdatnosti-bankiv-2024-perevirka-na-vitrivalist

15. Роз'яснення CERT-UA: платформа MISP, що це, як підключатися та які переваги. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/roz-yasnennya-cert-ua-platforma-misp-sho-ce-yak-pidklyuchatisya-ta-yaki-perevagi

16. Сучасні кіберзагрози для фінансових установ та ефективні методи їх захисту. IT Specialist. URL: https://my-itspecialist.com/modern-cyber-threats-to-financial-institutions-and-effective-methods-of-their-protection

17. Banco Santander. Operating risk disclosure. URL: https://www.santander.com/content/dam/santander-com/en/contenido-paginas/landing-pages/banco-santander-hong-kong-branch/do-operational-risk-disclosure-en.pdf

18. Basel Committee on Banking Supervision. Operational Risk: Supervisory Guidelines for the Advanced Measurement Approaches. Basel : BIS, 2011. URL: https://www.bis.org/publ/bcbs196.pdf

19. BNP Paribas. DORA - Digital Operational Resilience Act: regulation memo. URL: https://securities.cib.bnpparibas/dora-regulation-eu/

20. Clark B., Ebrahim A. Risk shifting and regulatory arbitrage: Evidence from operational risk. Journal of Financial Stability. 2022. Vol. 58. P. 100965.

References

1. National Bank of Ukraine (2025), “On amendments to the Regulation on the procedure for determining the minimum amount of operational risk by banks of Ukraine”, available at: https://ips.ligazakon.net/document/MN030933?an=3 (Accessed 10 May 2026).

2. National Bank of Ukraine (2026), Resolution “On Approval of Amendments to Certain Regulatory Acts of the National Bank of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/v0009500-26#n2 (Accessed 10 May 2026).

3. National Bank of Ukraine (2018), Resolution “On approval of the Regulation on the organization of the risk management system in banks of Ukraine and banking groups”, available at: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text (Accessed 10 May 2026).

4. National Bank of Ukraine (2021), “Updated procedure for assessing operational risk by banks and banking groups”, available at: https://bank.gov.ua/ua/news/all/onovleno-poryadok-otsinki-bankami-ta-bankivskimi-grupami-operatsiynogo-riziku (Accessed 10 May 2026).

5. National Bank of Ukraine (2026), “Banks provided financing for energy projects worth UAH 36.6 billion”, available at: https://bank.gov.ua/ua/news/all/banki-zabezpechili-finansuvannya-energetichnih-proyektiv-na-366mlrdgrn (Accessed 10 May 2026).

6. Abramova, A. (2021), “Development trends and features of operational risk management of commercial banks”, Naukovyj visnyk Polissia, vol. 2 (23), pp. 93-104.

7. Honchar, K. O. and Hohulenko, N. O. (2024), “International and domestic experience in managing bank operational risk”, Naukovyj visnyk Odes'koho natsional'noho ekonomichnoho universytetu, vol. 5-6 (318-319), pp. 39-46.

8. Honcharenko, I. (2023), “Cyber threats of the financial sector in the conditions of war”, *Ekonomika ta suspilstvo,* vol. 50.

9. Kl'oba, L. and Kl'oba, T. (2022), “Cyber threats to the banking sector under martial law in Ukraine”, Financial and Credit Activity: Problems of Theory and Practice, vol. 5 (46), pp. 19-28.

10. Kolodiziev, O. M. and Berehovyj, V. O. (2024), “Financial security of banks under martial law: the impact of digital tools and innovations”, Biznes Inform, vol. 9, pp. 335-341.

11. Lisovyj, A. V. and Andrukh, O. V. (2025), “Energy security of Ukraine: challenges of war and prospects for restoring economic potential”, Ukrains'kyj ekonomichnyj chasopys, vol. 8, pp. 40-43.

12. NEK «Ukrenerho» (2026), “Analytical materials on the stability of the energy system of Ukraine”, available at: https://ua.energy/category/analityka/ (Accessed 10 May 2026).

13. Panasko, O. M., Sahun, A. V. and Havrysh, O. S. (2025), “Analysis of cyber threat trends as an important stage of financial sector risk management”, Suchasnyj zakhyst informatsii, vol. 2 (62), pp. 98-106.

14. Mind (2024), “Bank viability rating - 2024. Endurance test”, available at: https://mind.ua/publications/20269589-rejting-zhittezdatnosti-bankiv-2024-perevirka-na-vitrivalist (Accessed 10 May 2026).

15. State Service of Special Communications and Information Protection of Ukraine (2025), “CERT-UA Explains MISP: Enhancing Ukraine's Cyber Resilience Through Automated Threat Intelligence Sharing”, available at: https://cip.gov.ua/ua/news/roz-yasnennya-cert-ua-platforma-misp-sho-ce-yak-pidklyuchatisya-ta-yaki-perevagi (Accessed 10 May 2026).

16. IT Specialist (2026), “Modern cyber threats to financial institutions and effective methods of their protection”, available at: https://my-itspecialist.com/modern-cyber-threats-to-financial-institutions-and-effective-methods-of-their-protection (Accessed 10 May 2026).

17. Banco Santander (2026), “Operating risk disclosure”, available at: https://www.santander.com/content/dam/santander-com/en/contenido-paginas/landing-pages/banco-santander-hong-kong-branch/do-operational-risk-disclosure-en.pdf (Accessed 10 May 2026).

18. Basel Committee on Banking Supervision (2011), “Operational Risk: Supervisory Guidelines for the Advanced Measurement Approaches”, available at: https://www.bis.org/publ/bcbs196.pdf (Accessed 10 May 2026).

19. BNP Paribas. (2026), “DORA - Digital Operational Resilience Act: regulation memo”, available at: https://securities.cib.bnpparibas/dora-regulation-eu/ (Accessed 10 May 2026).

20. Clark, B. and Ebrahim, A. (2022), “Risk shifting and regulatory arbitrage: Evidence from operational risk”, Journal of Financial Stability. Vol. 58. pp. 100965.

Отримано редакцією журналу / Received: 15.05.26

Прорецензовано / Revised: 22.05.26

Дата публікації / Published: 26.05.26