DOI: https://doi.org/10.32782/ecovis/2025-4-9
УДК 336.71:004](477)

Харабара Віолетта Миколаївна
кандидат економічних наук, доцент кафедри фінансів і кредиту,
Чернівецький національний університет імені Юрія Федьковича
ORCID: https://orcid.org/0000-0002-8555-6440

Мінічев Олександр Володимирович
аспірант,
Чернівецький національний університет імені Юрія Федьковича
ORCID: https://orcid.org/0009-0008-3936-8036

КІБЕРБЕЗПЕКА ЯК СТРАТЕГІЧНИЙ РЕСУРС РИНКОВОГО ПОЗИЦІОНУВАННЯ БАНКІВ У ЦИФРОВІЙ ЕКОНОМІЦІ

У статті обґрунтовано трактування кібербезпеки як стратегічного ресурсу, що безпосередньо впливає на ринкове позиціонування банків у цифровій економіці. Показано, що за глибокої цифровізації послуг, домінування дистанційних каналів і загострення кіберзагроз кіберстійкість виходить за межі технічної функції та стає інструментом стратегічного управління, який формує довіру, репутаційний і моральний капітал банку. Узагальнення досліджень України й зарубіжжя та аналіз підходів ЄС доводять: якість управління кіберризиками є чинником конкурентної диференціації. Кібербезпеку інтерпретовано як інтегрований ресурс (технологічний, організаційний, регуляторний, поведінковий), що підтримує стале позиціонування в умовах турбулентності та воєнних загроз. Запропоновано включати показники кіберстійкості до BSC банку та визначено напрями подальших досліджень.

Ключові слова: банк, ринкове позиціонування, кібербезпека, цифрова економіка, стратегічний менеджмент, кіберризики, довіра клієнтів, цифрова операційна стійкість.

Violetta Kharabara
PhD in Economics,
Associate Professor of the Department of Finance and Credit,
Yuriy Fedkovych Chernivtsi National University

Oleksandr Minichev
Postgraduate Student,
Yuriy Fedkovych Chernivtsi National University

CYBERSECURITY AS A STRATEGIC RESOURCE FOR BANKS' MARKET POSITIONING IN THE DIGITAL ECONOMY

The article substantiates the interpretation of cybersecurity as a strategic resource that directly influences banks' market positioning in the digital economy. It shows that as banking services migrate to digital and remote channels and cyberthreats intensify, cyber resilience extends beyond operational protection to strategic governance, shaping trust, reputational and moral capital. The study synthesizes recent scholarship on cybersecurity in the banking sectors of Ukraine and other countries and analyses contemporary EU regulatory approaches to digital operational resilience and cyber risk governance. The findings confirm that the quality of cyber risk management is becoming a material driver of competitive differentiation: mature governance, disciplined risk assessment, resilient architectures, transparent incident handling, and controlled third-party dependencies increase perceived reliability and support customer retention. In wartime conditions the strategic value of cyber resilience increases further because attacks target payment infrastructure, customer data, and service continuity; therefore, resilience must be treated as a strategic capability and a reputational safeguard. Cybersecurity is conceptualized as an integrated strategic resource combining technological controls, organizational processes, regulatory alignment and behavioural factors, which collectively determine a bank's ability to sustain secure operations and maintain stable market positioning under high turbulence. The author proposes a logic for embedding cyber resilience indicators into the bank's Balanced Scorecard by linking measurable cyber metrics to strategic objectives across customer, internal process, learning and growth, and financial perspectives. The paper argues for using indicator clusters such as governance maturity, vulnerability management speed, detection and response performance (e.g., time to detect and time to recover), continuity of critical services, third-party risk control, and staff awareness. Practical implications include prioritizing resilience investments, strengthening accountability and training, improving disclosure and communication to protect trust, and aligning cyber strategy with digital

transformation goals. Directions for further research are outlined for developing sector-specific indicator systems and empirically evaluating how cyber resilience affects positioning in different banking models.

Keywords: bank, market positioning, cybersecurity, digital economy, strategic management, cyber risks, customer trust, digital operational resilience.

Постановка проблеми. Прискорена цифровізація банківської діяльності, розширення спектра віддалених каналів, впровадження відкритого банкінгу та фінтех-рішень докорінно змінюють логіку конкурентної боротьби у банківському секторі. Класичні параметри ринкового позиціонування, такі як широта продуктового ряду, цінова політика чи географія мережі відділень, поступово втрачають вирішальне значення порівняно з якістю цифрового досвіду клієнта, рівнем захисту даних та стабільністю функціонування цифрових сервісів. У таких умовах кібербезпека перестає сприйматися як «технічна функція ІТ-підрозділу» і набуває рис стратегічного ресурсу, що визначає здатність банку утримувати та розширювати цільові сегменти ринку.

Для України ця проблема є особливо загостреною внаслідок поєднання кількох чинників. По-перше, банківська система країни проходить складну трансформацію під впливом війни, що супроводжується зростанням інтенсивності та складності кібератак на фінансову інфраструктуру [2, с. 70–81]. По-друге, відбувається прискорений перехід клієнтів до безготівкових та дистанційних операцій, що збільшує залежність бізнес-моделей банків від стійкості цифрових каналів. По-третє, поглиблюється інтеграція України до європейського фінансового простору, що зумовлює потребу адаптації до підходів ЄС у сфері цифрової операційної стійкості, зокрема до вимог Регламенту (ЄС) 2022/2554 (DORA) [6, с. 1–4]. У цих умовах постає завдання теоретичного обґрунтування кібербезпеки як ресурсу ринкового позиціонування банків та уточнення її місця у системі стратегічного менеджменту.

Аналіз останніх досліджень і публікацій. Сучасні дослідження, присвячені кібербезпеці банківської сфери України, концентруються переважно на питаннях ідентифікації загроз, аналізу нормативно-правового забезпечення та описі організаційних механізмів протидії кібератакам. Зокрема, у роботі І. Хомишин та О. Гавц систематизовано основні види кіберзагроз для банківського сектору України, а також підкреслено недостатність наявних механізмів правового регулювання та інституційної взаємодії у сфері кіберзахисту [1, с. 170–178]. Автори акцентують на фрагментарності підходів до управління кіберризиками і водночас окреслюють необхідність їх інтеграції в загальну систему економічної безпеки банків.

У праці Н. Ситник та І. Половчак цифровізацію та кібербезпеку розглянуто вже безпосередньо в контексті фінансової безпеки банків в умовах війни [2, с. 70–81]. Доведено, що різке зростання частки безготівкових розрахунків, розширення спектра онлайн-операцій та активізація ворожих кібератак створюють якісно нову конфігурацію ризиків, у якій кіберзагрози стають одним з ключових детермінантів фінансової стійкості. Автори роблять висновок, що без системного підходу до кібербезпеки неможливо забезпечити прийнятний рівень загальної фінансової безпеки банків, однак питання ринкового позиціонування в цих роботах майже не артикулюється.

Міжнародні дослідження демонструють перехід до розуміння кібербезпеки як чинника ефективності та конкурентоспроможності банківських установ. У емпіричному дослідженні D. Elsayed, T. Ismail та E. Ahmed на основі вибірки банків країн MENA (країни Близького сходу і Північної Африки) показано, що рівень розкриття інформації про заходи кібербезпеки позитивно корелює з фінансовими показниками банків, зокрема з рентабельністю активів і капіталу [3, с. 1–15]. Відзначено також модераційну роль інституцій корпоративного управління, що свідчить про стратегічний характер кіберризиків і їхній вплив на інвесторське та стейкхолдерське сприйняття.

У роботі W. Gaviyau та J. Godi сучасні трансформації банківського сектору описано через призму глибинних технологічних зрушень, зокрема масового впровадження фінтех-рішень та цифрових платформ [4, с. 1–27]. Автори підкреслюють, що цифрова трансформація радикально змінює структуру витрат, джерела створення вартості та конфігурацію конкурентних переваг банків. Водночас питання кібербезпеки у цій роботі розглядається передусім як структурний компонент ризик-менеджменту, а не як самостійний ресурс ринкового позиціонування.

Аспект взаємозв'язку між сприйняттям кібербезпеки та поведінкою клієнтів банків детально аналізується у дослідженні A. AlHares, Z. Zaerinajad та M. Al Bahr, присвяченому поінформованості клієнтів банків країн ОЕСР щодо кібербезпеки [5, с. 371–381]. Результати емпіричного опитування засвідчують, що суб'єктивне відчуття захищеності цифрових банківських сервісів суттєво впливає на рівень задоволеності, довіри та готовності надалі користуватися продуктами конкретного банку. Цей висновок прямо пов'язує кібербезпеку з формуванням довіри та, відповідно, із позиціонуванням банку в очах клієнта.

Нарешті, новітні європейські регуляторні ініціативи, зокрема Регламент (ЄС) 2022/2554 про цифрову операційну стійкість фінансового сектору (DORA), формалізують підхід до кібербезпеки як до комплексу вимог до ІСТ-ризик-менеджменту, інцидент-менеджменту, тестування стійкості та управління ризиками третіх сторін [6, с. 1–4]. У сфері захисту критичної банківської інфраструктури укра-

їнські дослідники акцентують на необхідності багаторівневого підходу, що охоплює платіжні системи, канали передавання фінансових даних, бази даних клієнтів та системи онлайн-банкінгу, причому будь-які порушення в цій інфраструктурі прямо загрожують фінансовій стабільності та довірі до банківської системи [7, с. 96–106].

Загалом сучасний науковий дискурс фіксує перехід від вузького технічного розуміння кібербезпеки до більш інтегральних підходів, пов'язаних із фінансовою стійкістю, регуляторними вимогами та поведінкою клієнтів. Водночас недостатньо розкритим залишається питання її інтерпретації саме як стратегічного ресурсу ринкового позиціонування банку, що визначає потребу в подальшій теоретичній розробці цієї проблеми.

Метою статті є теоретичне обґрунтування кібербезпеки як стратегічного ресурсу ринкового позиціонування банків у цифровій економіці та конкретизація механізмів її інтеграції в систему стратегічного менеджменту банківської установи. Досягнення поставленої мети передбачає уточнення змісту поняття «кібербезпека банку» в контексті ринкового позиціонування, розкриття логіки трансформації кібербезпеки з операційної функції в стратегічний ресурс, а також виокремлення ключових вимірів, за якими кіберстійкість впливає на конкурентне становище банку на ринку.

Виклад основного матеріалу дослідження. Цифрова трансформація банківської діяльності приводить до зміни структури ресурсів, які забезпечують конкурентні переваги. Якщо в традиційній моделі банківського бізнесу ключовими ресурсами були капітал, мережа відділень і доступ до дешевих пасивів, то в цифровій економіці дедалі більшої ваги набувають нематеріальні активи, пов'язані з даними, алгоритмами, репутацією та довірою клієнтів. Кібербезпека в цій конфігурації постає як механізм захисту саме нематеріальних активів, передусім персональних і фінансових даних клієнтів, алгоритмів ризик-менеджменту та бренду банку. Порушення кібербезпеки одразу трансформується в репутаційні втрати, відтік клієнтів, підвищення вартості ресурсів та регуляторні санкції, що безпосередньо змінює ринкове позиціонування банку в бік погіршення.

З урахуванням цього доцільно інтерпретувати кібербезпеку не лише як набір технологічних рішень або процедур відповідності, а як інтегрований стратегічний ресурс, що поєднує технологічний, організаційний, регуляторний та поведінковий виміри. Технологічний вимір пов'язаний із архітектурою інформаційних систем, використанням сучасних засобів захисту, впровадженням систем моніторингу, виявлення аномалій та реагування на інциденти. Організаційний вимір полягає у вбудуванні управління кіберризиками в загальну систему корпоративного управління, ролі спеціалізованих комітетів і функції CRO, що підтверджують результати емпіричних досліджень щодо впливу інституцій корпоративного управління на зв'язок між розкриттям інформації про кібербезпеку та ефективністю банку [3, с. 1–15].

Регуляторний вимір проявляється у відповідності діяльності банку вимогам національного та наднаціонального законодавства. Впровадження Регламенту (ЄС) 2022/2554 інституціоналізує підхід, за яким цифрова операційна стійкість трактується як необхідна умова фінансової стабільності, а не як факультативна внутрішня політика [6, с. 1–4]. Для українських банків, що працюють у режимі інтеграції до європейського фінансового простору, це означає необхідність випереджального наближення внутрішніх стандартів до вимог DORA, зокрема щодо управління ризиками зовнішніх постачальників ІСТ-послуг, тестування операційної стійкості та налагодження процедур повідомлення про інциденти.

Поведінковий вимір кібербезпеки безпосередньо пов'язаний зі сприйняттям клієнтами рівня захищеності цифрових сервісів та прозорості комунікації банку щодо управління кіберризиками. Дослідження поведінки клієнтів у країнах ОЕСР показують, що їхня поінформованість про загрози та оцінка ефективності заходів кібербезпеки є важливими детермінантами задоволеності та довіри [5, с. 371–381]. Для банку це означає, що комунікація про кібербезпеку повинна розглядатися як елемент маркетингової стратегії та інструмент формування ринкового позиціонування, а не лише як вимога регуляторної звітності.

Розглядаючи кібербезпеку як стратегічний ресурс ринкового позиціонування, доцільно звернути увагу на її вплив на структуру ціннісної пропозиції банку. У сегменті роздрібного банкінгу, де продукти різних установ є високозамінними, а цінова конкуренція часто обмежена регуляторно, ключовими диференціаторами стають якість цифрових сервісів, швидкість та зручність операцій, а також суб'єктивне відчуття безпеки при використанні мобільних застосунків і онлайн-банкінгу [1, с. 170–178; 2, с. 70–81]. Банк, який послідовно демонструє високий рівень кіберстійкості, прозоро інформує клієнтів про заходи захисту та коректно поводиться у випадках інцидентів, формує більш стійке ринкове позиціонування як інституція з підвищеним рівнем довіри.

Особливе значення кібербезпека набуває в контексті захисту критичної банківської інфраструктури. Українські дослідження показують, що в умовах війни банки опиняються під тиском одночасних загроз, пов'язаних із фізичним ураженням об'єктів інфраструктури, збоєм енергопостачання та кібератаками на платіжні системи, канали передачі фінансових даних і системи онлайн-банкінгу [7, с. 96–106]. У таких умовах забезпечення безперервності функціонування основних критичних систем стає частиною не лише операційної, а й комунікаційної стратегії банку: здатність підтримувати роботу ключових сервісів під час криз прямо перетворюється на еле-

мент позиціонування як «стійкої» інституції, спроможної забезпечити клієнтам доступ до коштів незалежно від зовнішніх шоків.

З огляду на наведені аргументи доцільно розглядати кібербезпеку як компонент системи стратегічного менеджменту банку, інтегрований у ключові управлінські контури. На рівні корпоративного управління це означає закріплення відповідальності за кіберстійкість на рівні наглядової ради, створення профільних комітетів, визначення ролі CRO як суб'єкта стратегічного управління ризиками, а не суто операційного менеджера [3, с. 8–12]. На рівні стратегічного планування кібербезпека має відображатися в цільових орієнтирах та ключових показниках ефективності, що характеризують допустимий рівень інцидентів, швидкість реагування на них, результати тестувань стійкості, а також рівень довіри клієнтів до цифрових продуктів.

Для практичної реалізації такого підходу доцільно включати показники, пов'язані з кібербезпекою, до системи збалансованих показників банку. У фінансовому вимірі це можуть бути індикатори, що відображають прямі та непрямі втрати від кіберінцидентів, вплив інцидентів на вартість фондування та на структуру доходів. У клієнтському вимірі логічно відстежувати зміну NPS, рівня задоволеності та частки активних користувачів цифрових сервісів після інцидентів, а також реакцію клієнтів на комунікацію щодо заходів кібербезпеки [5, с. 374–378]. У внутрішньому процесному вимірі ключовими стають показники покриття критичних систем регулярним тестуванням, тривалість вікна виявлення та реагування на інциденти, а також повнота інвентаризації активів і постачальників ICT-послуг відповідно до логіки DORA [6, с. 2–4]. Нарешті, у вимірі навчання й розвитку важливими є показники рівня цифрової та кіберграмотності персоналу, регулярності тренінгів і навчальних симуляцій.

У дискурсі ринкового позиціонування важливо також підкреслити морально-етичний вимір кібербезпеки. Клієнти, довіряючи банку свої персональні та фінансові дані, фактично делегують йому відповідальність за збереження частини свого приватного простору. Виконання банком цієї відповідальності підтримує його моральний та репутаційний капітал, тоді як невиконання – у формі витоків даних, маніпуляції інформацією чи непрозорої реакції на інциденти – веде до його стрімкої девальвації. У такій інтерпретації кібербезпека стає не лише технічною, а й моральною категорією, що визначає ступінь відповідності практик банку очікуванням суспільства щодо чесності, прозорості та турботи про клієнта. Це безпосередньо вписується в концепцію ринкового позиціонування, де банк може бути віднесений до категорії «етично відповідальних» або, навпаки, «ризикових» інституцій.

Для українських банків, що працюють в умовах війни та високої загальної турбулентності, інтеграція кібербезпеки у стратегічне позиціонування набуває додаткового змісту. З одного боку, вона стає інструментом підтримання функціональної безперервності та стабільності у кризових умовах [2, с. 70–81; 7, с. 96–106]. З іншого – створює передумови для посилення довіри з боку як внутрішніх, так і зовнішніх стейкхолдерів, включно з міжнародними партнерами, які дедалі більше орієнтуються на відповідність банку європейським стандартам цифрової операційної стійкості [6, с. 1–4]. У довгостроковій перспективі банки, які раніше та системніше інтегрують вимоги DORA та споріднених актів у свою бізнес-модель, отримують кращі стартові позиції для участі в транскордонних фінансових сервісах і партнерствах.

Висновки. Проведений аналіз дає підстави стверджувати, що в умовах цифрової економіки кібербезпека набуває статусу ключового стратегічного ресурсу ринкового позиціонування банків. Технологічна трансформація банківського бізнесу, зростання ролі нематеріальних активів, інтенсифікація цифрової взаємодії з клієнтами та загострення кіберзагроз зумовлюють перехід від переважно операційного до стратегічного розуміння кібербезпеки. Вона не зводиться до технічної функції або формальної регуляторної відповідності, а виступає інтегрованим ресурсом, що визначає здатність банку підтримувати стабільне ринкове позиціонування, формувати довіру, репутаційний і моральний капітал, а також забезпечувати фінансову й цифрову стійкість в умовах турбулентності та воєнних загроз.

Узагальнення сучасних досліджень підтверджує, що вплив кібербезпеки на ринкове позиціонування проявляється щонайменше у трьох взаємопов'язаних вимірах. По-перше, через фінансові результати та інвесторську привабливість, оскільки рівень кіберзрілості і якість розкриття релевантної інформації знижують інформаційну асиметрію, підсилюють керованість ризиків і позитивно відображаються на сприйнятті банку з боку стейкхолдерів. По-друге, через поведінку клієнтів у цифрових каналах: відчуття захищеності сервісів, прогнозованість реагування на інциденти та безперервність критичних послуг прямо впливають на лояльність, утримання клієнтської бази й готовність користуватися віддаленими продуктами. По-третє, через відповідність сучасним регуляторним стандартам цифрової операційної стійкості, що перетворюється на необхідну умову конкурентоспроможності та інтеграції у європейський фінансовий простір, а також на маркер якості корпоративного управління.

Аргументовано, що стратегічна інтеграція кібербезпеки має бути закріплена у корпоративному управлінні, стратегічному плануванні та системі збалансованих показників. Доцільним є перехід від трактування кібербезпеки як «центру витрат» до її розуміння як інвестиції у довгострокову стійкість позиціонування: через зниження втрат від інцидентів, підвищення надійності цифрових продуктів, посилення довіри і репутації, а також формування стійких

конкурентних переваг у середовищі цифрової конкуренції. Включення показників кіберстійкості до BSC має забезпечувати причинно-наслідковий зв'язок між кіберризиками, якістю процесів, клієнтською довірою та фінансовими результатами.

Перспективи подальших досліджень пов'язані з кількісною операціоналізацією індикаторів кіберстійкості в системі стратегічного управління банком, побудовою моделей оцінювання впливу кіберінцидентів на ринкову вартість, довіру й брендовий/моральний капітал, а також розробленням методичних підходів до порівняльного аналізу ринкового позиціонування банків із різним рівнем інтеграції вимог цифрової операційної стійкості та воєнних ризиків.

СПИСОК ЛІТЕРАТУРИ

1. Хомишин І., Гавц О. Кібербезпека банківської сфери України: поняття, проблеми та досвід зарубіжних держав. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки.* 2023. Т. 10, № 4(40). С. 170–178. DOI: https://doi.org/10.23939/law2023.40.170
2. Ситник Н. С., Половчак І. Р. Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни. *Галицький економічний вісник.* 2024. Т. 89, № 4. С. 70–81. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2024.04.070
3. Elsayed D. H., Ismail T. H., Ahmed E. A. The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal.* 2024. Vol. 10, Is. 1. P. 1–15. DOI: https://doi.org/10.1186/s43093-024-00402-9
4. Gaviyau W., Godi J. Banking Sector Transformation: Disruptions, Challenges and Opportunities. *FinTech.* 2025. Vol. 4, Is. 3. Art. 48. DOI: https://doi.org/10.3390/fintech4030048
5. AlHares A., Zaerinajad Z., Al Bahr M. Customer awareness and cyber security in the Organisation for Economic Co-operation and Development countries. *Corporate & Business Strategy Review.* 2024. Vol. 5, Is. 1 (Special Issue). P. 371–381. DOI: https://doi.org/10.22495/cbsrv5i1siart11
6. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. *Official Journal of the European Union.* 2022. L 333. P. 1–76. https://eur-lex.europa.eu/eli/reg/2022/2554/oj
7. Дорогий Я. Ю., Цуркан В. В., Бердиченко І. О. Захист критичної інфраструктури банківської сфери України. Цифрові технології у відновленні економіки та інфраструктури України: матеріали І міжнар. наук.-практ. конф., 13 листоп. 2024 р., Київ. Київ: Державне агентство відновлення та розвитку інфраструктури України, 2024. С. 96–106. DOI https://doi.org/10.5281/zenodo.14704594

REFERENCES

1. Khomyshyn I. & Havts O. (2023). Kiberbezpeka bankivskoi sfery Ukrainy: poniattia, problemy ta dosvid zarubizhnykh derzhav [Cybersecurity of Ukraine's banking sector: concept, problems and foreign experience]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Yurydychni nauky,* Vol. 10, No. 4(40), pp. 170–178. DOI: https://doi.org/10.23939/law2023.40.170
2. Sytnyk N. S. & Polovchak I. R. (2024). Tsyfrovizatsiia ta kiberbezpeka u zabezpechenni finansovoi bezpeky bankiv v umovakh viiny [Digitalization and cybersecurity in ensuring banks' financial security under war]. *Halytskyi ekonomichnyi visnyk,* Vol. 89, No. 4, pp. 70–81. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2024.04.070
3. Elsayed D. H., Ismail T. H. & Ahmed E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. *Future Business Journal,* Vol. 10, Is. 1, pp. 1–15. DOI: https://doi.org/10.1186/s43093-024-00402-9
4. Gaviyau W. & Godi J. (2025). Banking sector transformation: Disruptions, challenges and opportunities. *FinTech,* Vol. 4, Is. 3, Art. 48. DOI: https://doi.org/10.3390/fintech4030048
5. AlHares A., Zaerinajad Z. & Al Bahr M. (2024). Customer awareness and cyber security in the Organisation for Economic Co-operation and Development countries. *Corporate & Business Strategy Review,* Vol. 5, Is. 1 (Special Issue), pp. 371–381. DOI: https://doi.org/10.22495/cbsrv5i1siart11
6. European Parliament and Council. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. *Official Journal of the European Union,* L 333, pp. 1–76. Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
7. Dorohyi Ya. Yu., Tsurkan V. V. & Berdychenko I. O. (2024). Zakhyst krytychnoi infrastruktury bankivskoi sfery Ukrainy [Protection of critical infrastructure of the banking sector of Ukraine]. *Tsyfrovi tekhnolohii u vidnovlenni ekonomiky ta infrastruktury Ukrainy: Materialy I mizhnarodnoi naukovo-praktychnoi konferentsii* (Kyiv, November 13, 2024) (pp. 96–106). Kyiv: Derzhavne ahentstvo vidnovlennia ta rozvytku infrastruktury Ukrainy. DOI: https://doi.org/10.5281/zenodo.14704594

Стаття надійшла: 12.11.2025
Стаття прийнята: 03.12.2025
Стаття опублікована: 26.12.2025