DOI: https://doi.org/10.32782/2524-0072/2026-88-1

УДК 336.71:004.056

КІБЕРРИЗИКИ ЯК ФАКТОР ДЕСТАБІЛІЗАЦІЇ ФІНАНСОВОЇ СИСТЕМИ КРАЇНИ

CYBER RISKS AS A DESTABILIZATION FACTOR OF THE COUNTRY'S FINANCIAL SYSTEM

Азаров Євгеній Сергійович
аспірант,
Сумський державний університет
ORCID: https://orcid.org/0009-0004-3459-7260

Azarov Yevhenii
Sumy State University

Виконано в рамках НДР «Моделювання механізмів протидії організованій та транснаціональній кіберзлочинності у воєнний та післявоєнний часи» (реєстраційний номер 0124U000550). У статті досліджено теоретико-практичні аспекти впливу кібернетичних ризиків на стабільність фінансової системи країни в умовах тотальної цифровізації економіки. На основі проведеного бібліометричного аналізу наукових публікацій із застосуванням інструментарію VOSviewer доведено стрімке зростання інтересу дослідників до проблематики фінансової кібербезпеки та макропруденційного регулювання. Уточнено сутність поняття «кіберризик» з позиції фінансової науки, виділено його специфічні ознаки: швидкоплинність, асиметричність, здатність до системного зараження та латентність. Запропоновано комплексну класифікацію кіберризиків за джерелами виникнення, об'єктами посягання та характером фінансових наслідків з наведенням ретроспективних прикладів масштабних інцидентів. Розроблено структурно-логічну схему, яка демонструє трансмісійний механізм конвертації кіберризиків у традиційні фінансові загрози (ризик ліквідності, репутаційний, ринковий). Обґрунтовано, що кіберризики виступають ендогенним фактором дестабілізації макроекономічної ситуації, що потребує інтеграції новітніх інструментів управління, зокрема розвитку ринку Cyber Insurance.

Ключові слова: кіберризик, фінансова система, дестабілізація, бібліометричний аналіз, інформаційна безпека, кіберстійкість, страхування кіберризиків, VOSviewer, макропруденційне регулювання.

The rapid digitalization of the global economy and implementation of innovative financial technologies have transformed the financial sector. While providing unprecedented efficiency, this shift has catalyzed critical vulnerabilities through sophisticated cyber threats. The relevance of this research is dictated by the urgent need to conceptualize cyber risks not merely as isolated IT failures, but as profound systemic threats capable of causing macroeconomic destabilization. The purpose of this article is to conduct a theoretical and methodological assessment of cyber risks as a destabilization factor within the financial system, including a bibliometric analysis, systematization of their characteristics, and determination of their structural place in national security. To achieve this goal, a methodology incorporating bibliometric analysis of scientific databases (utilizing VOSviewer) was applied to identify global research trends. Methods of systemic analysis, synthesis, modeling, and classification were utilized to deconstruct the economic concept of cyber risk and map its transmission mechanisms. The research indicates an exponential increase in academic interest in financial cyber resilience, shifting from technical defense to macroeconomic prudential regulation. The study refines the economic definition of cyber risk, emphasizing its systemic nature, extreme velocity, asymmetry, and contagion potential across interconnected networks. A multidimensional classification of cyber risks is proposed, categorizing them by sources, targets, and financial consequences. A key outcome is the development of a structural scheme that conceptualizes the place of cyber risks in the financial system, illustrating how localized incidents trigger systemic liquidity constraints and insolvency. The practical value lies in providing regulators with a foundation for integrating cyber risk metrics into management frameworks. The proposed models serve as a baseline for developing targeted stress-testing and designing specialized cyber insurance mechanisms to mitigate the consequences of attacks on critical infrastructure, enhancing overall resilience.

Keywords: cyber risk, financial system, destabilization, bibliometric analysis, information security, cyber resilience, cyber risk insurance, macroprudential regulation, liquidity risk.

Постановка проблеми. Трансформація глобального економічного простору під впливом форсованої цифровізації зумовила появу нових категорій загроз для національних економік. Фінансовий сектор, будучи кровоносною системою будь-якої держави, традиційно виступає піонером у впровадженні інноваційних технологій, алгоритмічного трейдингу, хмарних обчислень та систем відкритого банкінгу (Open Banking). Проте такий безпрецедентно високий рівень технологічної інтеграції робить фінансові інститути найбільш вразливими до зловмисних дій у кіберпросторі.

За даними звіту Всесвітнього економічного форуму (Global Cybersecurity Outlook 2026), кіберінциденти вже давно не розглядаються виключно як локальні проблеми IT-відділів; вони визнані однією з ключових загроз для безперервності бізнесу та системної макроекономічної стабільності. Більше того, фокус уваги вищого керівництва фінансових установ зміщується з класичних програм-вимагачів на складніші форми кібершахрайства із використанням штучного інтелекту [1, с. 14]. Сучасні кібератаки здатні не лише призвести до прямих фінансових втрат окремого банку, але й спровокувати ефект доміно, підриваючи довіру до всієї фінансової системи країни. Враховуючи, що середня вартість ліквідації наслідків витоку даних у фінансовому секторі у 2026 році досягла позначки у 6,4 млн доларів США [2, с. 3], питання глибинної ідентифікації, оцінки та концептуального управління кіберризиками набуває критичної ваги для забезпечення національної безпеки.

Аналіз останніх досліджень і публікацій. Проблематика впливу кібернетичних загроз на економічну безпеку активно досліджується в академічному середовищі. Фундаментальні аспекти глобальної кібербезпеки та формування кіберсуверенних держав розглядаються у працях Р. Алгулієва та Б. Набієва. Вплив кіберризиків на державний та фінансовий сектори, питання національної кіберстійкості та розробки політик управління ризиками висвітлено у глобальних звітах Міжнародного союзу електрозв'язку (Global Cybersecurity Index 2024), де запроваджено п'ятирівневу модель оцінки кіберготовності країн – від тих, що лише розбудовують потенціал (Tier 5), до еталонних держав (Tier 1) [3, с. 5]. Аналітичні матеріали компанії Cisco (Cybersecurity Readiness Index 2025) підтверджують, що лише 4% організацій досягли зрілого рівня готовності до відбиття сучасних кіберзагроз [4, с. 2].

Серед вітчизняних науковців вагомий внесок у дослідження фінансової безпеки в умовах цифровізації та управління специфічними ризиками зробили І. В. Тютюник, А. О. Ярова [5, с. 115] та інші дослідники, які наголошують на необхідності інтеграції показників кібербезпеки до загальної системи ризик-менеджменту фінансових установ.

Виділення невирішених частин загальної проблеми. Незважаючи на значний емпіричний масив публікацій, переважна більшість досліджень продовжує фокусуватися на технологічній, програмно-апаратній складовій кіберзахисту. Натомість у фінансовій науці гостро відчувається брак комплексних праць, які б аналізували кіберризик саме як самостійну макроекономічну категорію та ендогенний фактор дестабілізації. Залишаються недостатньо розкритими питання деталізованої класифікації кіберризиків з огляду на специфіку їх трансмісії у класичні банківські ризики, а також відсутня загальноприйнята структурно-логічна схема, що описує механізм системного зараження фінансового ринку внаслідок кібератак.

Формулювання цілей статті (постановка завдання). Метою даного дослідження є комплексне теоретико-методологічне обґрунтування сутності кіберризиків як ключового фактора дестабілізації фінансової системи країни. Для досягнення поставленої мети визначено такі наукові завдання:

1. Провести розширений бібліометричний аналіз наукових публікацій для виявлення глобальних трендів у дослідженні фінансової кібербезпеки.
2. Уточнити економічну природу поняття «кіберризик» та виокремити його специфічні ознаки.
3. Розробити багатокритеріальну класифікацію кіберризиків з урахуванням особливостей їх реалізації у фінансовій сфері.
4. Побудувати структурно-логічну схему трансмісії кіберризиків, яка наочно демонструє механізм переростання технологічних інцидентів у системні фінансові кризи.

Виклад основного матеріалу дослідження. Еволюція наукової думки щодо ролі кіберризиків у функціонуванні фінансового сектору вимагає застосування сучасного інструментарію аналізу баз даних. Нами було проведено бібліометричний аналіз за допомогою наукометричної бази Scopus (аналізований період: 2018–2026 рр.). Пошуковий запит за дескрипторами “cyber risk” AND “financial system” дозволив виявити стійкий експонен-

ційний тренд зростання кількості публікацій. Побудова мапи термінів (co-occurrence analysis) за допомогою програмного комплексу VOSviewer дозволила візуалізувати внутрішню структуру цього наукового дискурсу. Аналіз щільності зв'язків (Total link strength) засвідчив формування трьох потужних дослідницьких кластерів.

Перший (найбільший) кластер формують дослідження макропруденційного регулювання. Центральними вузлами тут виступають дескриптори systemic risk, financial stability, central banks, contagion effect. Це доводить, що академічна спільнота остаточно визнала здатність кіберризиків генерувати макроекономічні шоки. Другий кластер концентрується навколо технологічних детермінант вразливості (fintech, ransomware, decentralized finance, supply chain attack). Третій кластер охоплює інструментарій нівелювання загроз (risk management, cyber insurance, operational resilience). Отже, результати просторового моделювання у VOSviewer неспростовно доводять: кіберризик вийшов за вузькі межі прикладної інформатики.

З огляду на вищезазначене, виникає потреба в уточненні термінологічного апарату. Традиційно Базельський комітет з банківського нагляду розглядав проблеми IT-безпеки як підвид операційного ризику. Однак у сучасних умовах такий підхід є редукціоністським. Ми пропонуємо визначати *кіберризик фінансової системи* як імовірність настання прямих або непрямих фінансових, репутаційних та регуляторних втрат, а також каскадного порушення безперервності функціонування фінансових ринків унаслідок збоїв, компрометації, деструктивного втручання або використання вразливостей в інформаційно-телекомунікаційних екосистемах.

Проведене дослідження дозволило виокремити низку специфічних ознак кіберризиків, які унеможливлюють їх управління за допомогою класичних фінансових моделей (VaR, стрес-тестування кредитного портфеля):

1. *Гіпершвидкоплинність реалізації.* Якщо криза ліквідності чи погіршення кредитного портфеля формуються тижнями або місяцями, дозволяючи регулятору застосувати превентивні заходи, то деструктивна кібератака (наприклад, вірус-шифрувальник) здатна повністю паралізувати операційну діяльність банку за лічені хвилини.

2. *Радикальна асиметричність ресурсів.* Для здійснення атаки на системно важливий банк зловмисникам не потрібні капітали, співмірні з бюджетами на захист. Поширення моделі Ransomware-as-a-Service (RaaS) знизило поріг входу для кіберзлочинців, зробивши загрози масовими та децентралізованими.

3. *Екстериторіальність та системна контагіозність.* Високий ступінь взаємопов'язаності учасників фінансового ринку (кореспондентські рахунки, системи клірингу, платіжні шлюзи) призводить до того, що інфікування одного, навіть незначного, елемента мережі створює загрозу для всієї екосистеми, ігноруючи національні юрисдикції.

4. *Глибока латентність.* Кіберінциденти класу Advanced Persistent Threats (APT) здатні місяцями перебувати в інфраструктурі банку у «сплячому» режимі. Зловмисники можуть непомітно вивчати алгоритми транзакцій, щоб у критичний момент завдати максимальної фінансової шкоди.

Для системного розуміння структури загроз нами розроблено розширену багатокритеріальну класифікацію кіберризиків фінансової системи (Таблиця 1).

Розкриваючи практичний аспект Таблиці 1, варто звернутися до історичних прецедентів, які підтверджують масштабність наслідків. Показовим прикладом екзогенного ризику ланцюга поставок є інцидент грудня 2025 року з криптовалютним гаманцем Trust Wallet. Зловмисники скомпрометували розширення для браузера через викрадений API-ключ, що призвело до миттєвої крадіжки активів на суму близько 7 мільйонів доларів США [7, с. 1]. Іншим красномовним прикладом реалізації ризику доступності з колосальними макроекономічними наслідками стала атака вірусу-вимагача на Міністерство фінансів та критичні урядові установи Коста-Рики у 2022 році. Держава була змушена оголосити надзвичайний стан, оскільки податкова та митна системи були паралізовані, що зупинило зовнішньоторговельні операції країни та призвело до багатомільйонних втрат бюджету [7, с. 2].

Розуміння руйнівної природи цих ризиків вимагає концептуалізації їхнього місця в загальній архітектурі фінансової системи. Процес переходу суто технічного збою у площину фінансової катастрофи ми називаємо «трансмісією кіберризику». Розроблена нами структурно-логічна схема наочно демонструє цей механізм (Таблиця 2).

Аналіз схеми, наведеної у Таблиці 2, дозволяє зробити фундаментальний висно-

Таблиця 1

Комплексна класифікація кіберризиків фінансової системи країни

Класифікаційна ознака	Види кіберризиків	Змістовна характеристика та прояви у фінансовому секторі
За джерелом виникнення	Екзогенні (зовнішні)	Спрямовані атаки хакерських синдикатів, кібершпигунство, DDoS-атаки на сервери інтернет-банкінгу. Окремо виділяються ризики ланцюга поставок (Supply chain attacks), коли злам відбувається через вразливості стороннього програмного забезпечення підрядників банку.
	Ендогенні (внутрішні)	Ненавмисні помилки персоналу фінансових установ (перехід за фішинговими посиланнями), свідомий інсайдерський витік банківської таємниці, некоректні налаштування архітектури хмарних баз даних.
За об'єктом посягання (Тріада CIA)	Ризики конфіденційності	Викрадення баз даних клієнтів (PII), компрометація алгоритмів високочастотного трейдингу, витік стратегічних інвестиційних планів установи. За даними SentinelOne, 78% інцидентів у фінансовому секторі пов'язані саме з викраденням облікових даних [2].
	Ризики цілісності	Несанкціонована зміна записів у банківських реєстрах, підміна реквізитів транзакцій у системі SWIFT, маніпуляції з балансами рахунків.
	Ризики доступності	Блокування доступу клієнтів до рахунків через програми-вимагачі (Ransomware), зупинка роботи банкоматних мереж та платіжних терміналів (PoS).
За характером фінансових наслідків	Прямі економічні втрати	Безпосереднє викрадення фіатних коштів або криптовалют з гаманців бірж, виплата викупу кіберзлочинцям, витрати на залучення forensic-експертів для розслідування інциденту [6, с. 14].
	Непрямі (опосередковані)	Штрафні санкції регуляторів за недотримання протоколів безпеки, відтік депозитів через втрату довіри клієнтів, падіння ринкової капіталізації банку, витрати на судові позови.

Джерело: сформовано автором

вок: кіберризик не існує в ізольованому вакуумі IT-департаменту. Він відіграє роль первинного каталізатора (тригера), який через високу технологічну щільність зв'язків миттєво мутує у найнебезпечніші види фінансових ризиків. Наприклад, якщо локальний інцидент виводить з ладу сервери банку, що належить до категорії системно важливих (Systemically Important Financial Institutions – SIFIs), неможливість цього банку виконати транзакції перед контрагентами протягом навіть однієї операційної доби спровокує гострий дефіцит ліквідності у десятках інших банків-партнерів. Таким чином, кіберінцидент ініціює руйнівний контагіозний ефект, здатний похитнути макроекономічну стабільність цілої держави.

Висновки. На основі проведеного комплексного дослідження можна зробити висновок, що в умовах глобальної цифрової економіки кіберризики еволюціонували з розряду інцидентних технічних збоїв у фундаментальну економічну загрозу найвищого рівня. Проведений із залученням інструментарію VOSviewer бібліометричний аналіз переконливо доводить зміщення світового наукового фокусу від парадигми суто технічного захисту до концепції макропруденційного розуміння кіберзагроз як фактора системної дестабілізації.

Запропонована в роботі деталізована класифікація кіберризиків та структурно-логічна схема їх трансмісії емпірично та теоретично доводять, що їхня головна небезпека полягає у здатності до миттєвої конвертації. Кіберінцидент виступає першопричиною, яка блискавично генерує критичні ризики ліквідності, масштабні ринкові коливання та непоправні репутаційні втрати, провокуючи ефект макроекономічного доміно (контагіозності). Наведені приклади (від атак на урядові мережі Коста-Рики до крадіжок у секторах децентра-

Таблиця 2

Структурно-логічна схема:
Трансмісійний механізм конвертації кіберризику у фінансовій системі

Тригер (Первинна кіберподія)	Уражений елемент фінансової інфраструктури	Конвертація у традиційний фінансовий ризик	Макроекономічний наслідок (Дестабілізація системи)
Масштабна DDoS-атака на сервери Центрального банку або платіжної системи	Розрахунково-клірингові центри, міжбанківські електронні платіжні системи.	**Ризик ліквідності.** Банки втрачають здатність проводити розрахунки за своїми зобов'язаннями та зобов'язаннями клієнтів.	Формування ланцюга неплатежів у реальному секторі економіки, зупинка міжбанківського ринку кредитування, касові розриви підприємств.
Успішна атака вірусу-вимагача (Ransomware) із шифруванням баз даних	Внутрішні автоматизовані банківські системи (АБС), реєстри заставного майна, кредитні досьє.	**Кредитний та Операційний ризики.** Установа фізично не може ідентифікувати боржників, стягувати відсотки за кредитами та оцінювати якість портфеля.	Стрімке знецінення активів банку, порушення нормативів адекватності капіталу, примусове введення тимчасової адміністрації, банкрутство.
Масовий витік (Data Breach) конфіденційної інформації VIP-клієнтів банку	Репутаційний капітал банку, лояльність клієнтської бази, інформаційний фон.	**Репутаційний ризик та Ризик відпливу капіталу (Bank run).**	Панічне масове зняття коштів з депозитних рахунків, що виснажує резерви банку; втрата довіри населення до всієї банківської системи держави.
Компрометація та злам алгоритмів високочастотного трейдингу на фондовій біржі	Біржові термінали, інституційні інвестори, брокерські системи.	**Ринковий ризик.** Штучне генерування хибних заявок на купівлю/продаж цінних паперів.	Миттєвий обвал котирувань акцій (Flash crash), дестабілізація фондового ринку, незворотні втрати пенсійних та інвестиційних фондів.

Джерело: сформовано автором

лізованих фінансів) засвідчують, що фінансові інститути стикаються з високоорганізованою, асиметричною загрозою, яка вимагає принципово нових підходів до ризик-менеджменту.

Дальші перспективи в цьому напрямку. Усвідомлення безпрецедентного масштабу та руйнівного потенціалу кіберзагроз безальтернативно вимагає від фінансових регуляторів переходу від реактивних (спрямованих на ліквідацію наслідків) до проактивних методів управління. Подальші наукові розвідки у цій площині доцільно зосередити на розробці інноваційних фінансових інструментів трансферу кіберризиків. Зокрема, критично важливим є теоретичне та практичне обґрунтування моделі розбудови вітчизняного ринку страхування кіберризиків (Cyber Insurance) для банківських установ та об'єктів критичної інфраструктури. Інтеграція механізмів страхового захисту дозволить не лише мінімізувати прямі фінансові втрати від можливих атак, але й стимулюватиме фінансові установи до підвищення базового рівня власної кібергігієни, що у підсумку зміцнить загальну макроекономічну кіберстійкість держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. World Economic Forum. Global Cybersecurity Outlook 2026. Geneva : WEF, 2026. 47 p. (дата звернення: 15.06.2026)

2. Key Cyber Security Statistics for 2026. SentinelOne, 2026. URL: https://www.sentinelone.com/cyber-security-statistics (дата звернення: 26.06.2026)

3. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. Geneva : ITU, 2024. 28 p. (дата звернення: 15.06.2026)

4. Cisco. Cybersecurity Readiness Index 2025. San Jose : Cisco Systems, 2025. 24 p. (дата звернення: 11.06.2026)

5. Тютюник І. В., Ярова А. О. Управління фінансовою безпекою в умовах цифровізації: виклики та новітні загрози. *Економіка і суспільство*. 2025. № 52. С. 112–118. (дата звернення: 09.06.2026)

6. Alguliyev R., Nabiyev B., Dashdamirova K. Comparative Analysis of Global Cybersecurity Indices in the Context of the Formation of Cyber Sovereign States. *17th International Conference on Application of Information and Communication Technologies (AICT)*. Baku, 2025. P. 1–6. (дата звернення: 15.06.2026)

7. Center for Strategic and International Studies (CSIS). Significant Cyber Events. Washington, D.C. : CSIS, 2026. 15 p. (дата звернення: 15.06.2026)

8. National Cyber Security Index 2026 / e-Governance Academy. Tallinn : eGA, 2026. URL: https://ncsi.ega.ee/ (дата звернення: 15.06.2026)

REFERENCES:

1. Alguliyev, R., Nabiyev, B., & Dashdamirova, K. (2025). Comparative Analysis of Global Cybersecurity Indices in the Context of the Formation of Cyber Sovereign States. *17th International Conference on Application of Information and Communication Technologies (AICT)*, 1–6. Baku. (accessed Juny 15, 2026)

2. Center for Strategic and International Studies (CSIS). (2026). *Significant Cyber Events*. Washington, D.C.: CSIS. (accessed Juny 15, 2026)

3. Cisco. (2025). *Cybersecurity Readiness Index 2025*. San Jose: Cisco Systems. (accessed Juny 11, 2026)

4. International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index 2024*. Geneva: ITU. (accessed Juny 15, 2026)

5. SentinelOne. (2026). *Key Cyber Security Statistics for 2026*. Retrieved June 26, 2026, from https://www.sentinelone.com/cyber-security-statistics. (accessed Juny 26, 2026)

6. Tiutiunyk, I. V., & Yarovyi, A. O. (2025). Upravlinnia finansovoiu bezpekoiu v umovakh tsyfrovizatsii: vyklyky ta novitni zahrozy [Management of financial security in the conditions of digitalization: challenges and latest threats]. *Ekonomika i suspilstvo [Economy and society]*, 52, 112–118. (accessed Juny 09, 2026)

7. World Economic Forum. (2026). *Global Cybersecurity Outlook 2026*. Geneva: WEF. (accessed Juny 15, 2026)

8. e-Governance Academy. (2026). National Cyber Security Index 2026. Tallinn: eGA. Retrieved July 14, 2026, from https://ncsi.ega.ee/ (accessed Juny 15, 2026)

Дата надходження статті: 26.06.2026
Дата прийняття статті до публікації: 03.08.2026
Дата публікації статті: 05.08.2026