DOI: https://doi.org/10.32782/2521-666X/2026-93-14
УДК 336.13.012.24:355.01

Гудзь О.Є.
доктор економічних наук, професор,
Державний податковий університет
ORCID: https://orcid.org/0000-0002-9982-7328
Правдюк Н.Л.
доктор економічних наук, професор,
Вінницький національний аграрний університет
ORCID: https://orcid.org/0000-0003-1157-2242

Gudz Olena
State Tax University
Pravdiuk Natalia
Vinnytsia National Agrarian University

РЕЗИЛ'ЄНТНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ ЗА ГЛОБАЛІЗАЦІЙНИХ ТА ЦИФРОВИХ ВИКЛИКІВ

INFORMATION SECURITY RESILIENCE OF FINANCIAL INSTITUTIONS TO GLOBALIZATION AND DIGITAL CHALLENGES

У статті досліджено наявний стан резил'єнтності інформаційної безпеки українських фінансових установ у воєнний період (2022–2025 рр.). Відмічено, що Україна перебуває на етапі становлення резил'єнтності, і зрівняно із США та ЄС, українські установи ще потребують масштабних інвестицій у кіберзахист, інтеграції міжнародних стандартів, адаптації систем відновлення й безперервності діяльності, розвитку культури інформаційної безпеки. Викрито сучасні глобалізаційні та цифрові виклики для інформаційної безпеки українських фінансових установ. Розкрито, що перед вітчизняними фінансовими установами постають комплексні завдання. Обґрунтовано пріоритетні напрями забезпечення резил'єнтності інформаційної безпеки фінансових установ, реалізація яких, сприятиме інтеграції у європейський простір та сформує основу для довгострокового розвитку й відновлення за глобалізаційних та цифрових викликів.

Ключові слова: *фінансові установи, інформаційна безпека, резил'єнтність, глобалізація, цифрові виклики.*

The article examines the current state of resilience in information security of Ukrainian financial institutions during the wartime period (2022–2025). It is noted that this state is characterized by the intensification of regulatory framework development and the gradual implementation of practical tools for resilient information protection. At the same time, although Ukraine has taken an important step by adopting new requirements for the information security of financial institutions, it remains at the stage of resilience formation. Compared to the United States and the European Union, where cyber resilience has become an integral part of financial policy, Ukrainian institutions still require substantial investments in cybersecurity, integration of international standards, adaptation of recovery and business continuity systems, and the development of an information security culture. The study reveals modern globalization and digital challenges for the information security of Ukrainian financial institutions, which lie in the combination of wartime cyber threats, global integration into the financial space, and rapid digitalization of financial services. This creates a high level of risk for their stability and customer trust. It is identified that Ukrainian financial institutions face dual pressure: globalization challenges demand compliance with international standards, while digital challenges open new channels for attacks. The article highlights that domestic financial institutions encounter complex tasks grouped into four strategic blocks: financial-organizational, technological, human resources and educational, and regulatory-legal. Priority directions for ensuring information security resilience are substantiated. Their implementation will enable Ukrainian financial institutions to combine economic stability with technological sustainability, protect financial assets from global cyber threats, promote integration into the European financial space, and form a foundation for long-term development and recovery in the post-war period under globalization and digital challenges.

Keywords: *financial institutions, information security, resilience, globalization, digital challenges.*

Постановка проблеми. У сучасних умовах глобалізації та цифрової трансформації фінансові установи опинилися в епіцентрі нових викликів, пов'язаних із забезпеченням інформаційної безпеки. Зростання масштабів транскордонних фінансових операцій, активне впровадження фінтех-рішень, мобільних додатків та онлайн-банкінгу створюють не лише нові можливості для розвитку, але й відкривають додаткові канали для інформаційного шпигунства, кібер інцидентів й кібератак. Водночас воєнні та кризові

© Гудзь О.Є., Правдюк Н.Л., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

реалії України актуалізують потребу у формуванні стійких та резил'єнтних механізмів захисту фінансових установ, здатних протистояти загрозам і швидко відновлювати функціонування після різних інформаційних атак та інцидентів. Таким чином, вважаємо, що розгляд резил'єнтності інформаційної безпеки фінансових установ за глобалізаційних та цифрових викликів є доцільним, адже постановка такої проблеми виходить за межі класичного підходу до інформаційного й кіберзахисту, акцентуючи увагу на здатності фінансових установ адаптуватися, витримувати навантаження та відновлюватися після кризових ситуацій. Окрім того, це має стратегічне значення для інтеграції України у європейський фінансовий простір, де установлені стандарти кіберрезил'єнтності. Тобто, вагоме теоретичне і практичне значення цієї проблеми полягає у формуванні напрямів, що мінімізують фінансові та репутаційні втрати, забезпечують безперервність критичних послуг та формують довіру населення й інвесторів до фінансових установ. Таким чином, означене підтверджує актуальність та стратегічну важливість представленого наукового доробку, оскільки поєднує резил'єнтність й економічну стабільність із технологічною стійкістю, створюючи основу для довгострокового розвитку фінансових установ України в умовах глобальних і цифрових викликів.

Аналіз останніх досліджень та публікацій. Останніми воєнними роками, проблема інформаційної безпеки фінансових установ привертає увагу багаточисельної аудиторії науковців, фінансових аналітиків та експертів. Доречно відмітити цікаві розвідки й пропозиції таких дослідників, як: А. Абрамова [1], В. Гречка, В. Островський, М. Білий [2], О. Григораш, В. Пугач [3], Ю. Неустроєв, Н. Згадова, Ю. Работін [4], М. Мельник [6], Н. Трусова, І. Чкан [7], M. Barr, A. Harris, L. Menand, W. Xu [8], F. Forcadell, E. Aracil, F. Úbeda, [9], T. Eisenbach, A. Kovner, M. Lee [10], J. Walker, M. Cooper [11] та інші. При цьому мало вивченими залишаються можливості й переваги резил'єнтності інформаційної безпеки фінансових установ, що вважаємо архіважливим, оскільки дослідження резил'єнтності інформаційної безпеки фінансових установ є необхідним у сучасних умовах глобалізації та цифровізації.

Метою статті є виявлення наявних тенденцій та проблем резил'єнтності інформаційної безпеки українських фінансових установ у воєнний період та обґрунтування пріоритетних напрямів забезпечення їх резил'єнтності інформаційної безпеки за глобалізаційних та цифрових викликів.

Виклад основного матеріалу. Агресивна війна росії «продовжує чинити руйнівний вплив не лише на інфраструктуру та бізнес-середовище, вона знизила рівень фінансової стійкості держави в цілому» [3]. У таких умовах «фінансові установи змушені організовувати свою діяльність в умовах невизначеності, непередбачуваності, загроз і небезпек, породжених умовами сучасного розвитку» [4].

Цікаво, що останнім часом, фінансові установи активізували цифровізацію своєї діяльності, і «саме цифрова трансформація забезпечує розширення їх можливостей, збереження клієнтської бази, покращення позицій на світових фінансових ринках, зменшення витрат, підвищення конкурентоспроможності тощо» [7]. Ключовими трендами цифровізації фінансових установ в Україні вважається «оптимізація віддаленої роботи працівників, зростання операцій онлайн, розширення й спрощення доступу до фінансових послуг, розвиток дистанційних комунікаційних каналів та ланцюгів продажу, протидія шахраям і хакерам, активне використання хмарних технологій та технологій штучного інтелекту, персоніфікація фінансових продуктів» [1; 8].

Водночас, цифровізація створює нові загрози й виклики для інформаційної безпеки фінансових установ, серед них: «кіберзлочинність (хакерські атаки, крадіжки даних, фішинг); цифрове шахрайство (використання підроблених документів, соціальна інженерія); внутрішні загрози (зловживання з боку персоналу, помилки в програмному забезпеченні)» [2]. Найбільш типовими кібератаками на фінансові установи є «конфіденційна чи банківська таємниця; фінансова інфраструктура; кошти клієнтів і установи; веб-сайти фінансових установ і регуляторів» [9]. Фактично, «кіберризики як результат цифрових атак, ризики функціональної моделі та ризики зараження і пошкодження персональних даних клієнтів й звітних даних фінансових установ демонструють тенденції до поширення» [10]. І саме, «тенденції до зростання кіберзлочинності зробили кібербезпеку ключовим питанням державної політики для регуляторних і наглядових органів, адже фінансові установи, стають все більш привабливою мішенню для кіберзлочинців» [7].

Переважно, академічна спільнота вважає, що «в умовах глобальної нестабільності дослідження динамічних соціально-економічних систем набуває все більшої актуальності, а особливо це стосується складних систем, які характеризуються нелінійною динамікою та непередбачуваними траєкторіями розвитку й взаємозв'язків» [6]. І, вагоме значення у цьому зрізі має резил'єнтність інформаційної безпеки фінансових установ за глобалізаційних та цифрових викликів.

«Резил'єнтність (resilience) є антиподом до крихкості (fragility), це поняття відображає здатність будь-якої системи, якій вдається виживати, до відновлення після шоків та адаптації до змінного середовища» [11]

Дослідивши наявний стан резил'єнтності інформаційної безпеки українських фінансових установ у 2022–2025 роках, доходимо переконання, що він характеризується активізацією формування регламентів, нормативного поля та поступового впровадження практичних інструментів резил'єнтного інформаційного захисту. Так, держава, відчутно посилила вимоги резил'єнтності до усіх вітчизняних фінансових установ, але рівень їх резил'єнтної зрілості, ще поступається установленим глобальним стандартам (зокрема: ISO/IEC 27001, NIST, DORA), де кіберрезил'єнтність, вже давно вплітається у стратегії фінансової стабільності.

У кінці 2025 року, Національний банк України посилив вимоги до резил'єнтності інформаційної безпеки для українських фінансових установ, ухваливши відповідне Положення [5], яке передбачає «обов'язкове впровадження адекватних систем моніторингу, управління кіберризиками, забезпечення захисту персональних даних клієнтів» [5]. Водночас, дослідження засвідчує, що переважно, вітчизняні фінансові установи лише почали формувати внутрішні політики резил'єнтності інформаційної безпеки, впроваджувати надійні системи інформаційного захисту, однак, наразі, відсутні ще комплексні моделі й механізми резил'єнтності, які забезпечують швидке відновлення після інцидентів та атак. До такого стану, додамо ще й існуючі інші гострі виклики, серед яких: воєнні ризики та часті кібератаки на критичну інфраструктуру; обмежені бюджети на інформаційну безпеку й кіберзахист; недостатня інтеграція міжнародних стандартів.

А, от зарубіжний досвід засвідчує, що фінансові установи США та ЄС активно впроваджують концепцію кібер резил'єнтності (cyber resilience), тобто забезпечують не лише захист, а й піклуються про здатність установи до швидкого відновлення й забезпечення стабільності. Так, у ЄС діє Digital Operational Resilience Act (DORA), що зобов'язує фінансові установи розробляти плани безперервності діяльності, тестувати системи на стійкість та звітувати про різноманітні атаки й інциденти. У США регулятори (SEC, Federal Reserve) вимагають від фінансових установ регулярних „stress tests" кіберзахисту щодо інвестицій та безпеки хмарних технологій. Цікаво, що МВФ у 2026 році систематизував „Good Practices in Cyber Risk Regulation" щодо комплексних рішень кіберризиків, оскільки вони можуть впливати на стабільність функціонування фінансових ринків. Тобто, переконуємось, що у провідних країнах, спостерігається доволі високий рівень резил'єнтної зрілості інформаційної безпеки. Фактично, вона інтегрована у загальні безпекові стратегії, забезпечуючи фінансову стабільність, при цьому, бюджети на інформаційну безпеку й кіберзахист зростають, а фінансові установи часто формують спеціалізовані підрозділи для захисту й реагування на різноманітні інциденти.

Таким чином, відмітимо, що хоча Україна й робила важливий крок, ухваливши нові вимоги до інформаційної безпеки фінансових установ, але перебуває на етапі становлення резил'єнтності, і зрівняно із США та ЄС, де кіберрезил'єнтність давно стала частиною фінансової політики, українські установи ще потребують масштабних інвестицій у кіберзахист, інтеграції міжнародних стандартів та адаптації систем відновлення й безперервності діяльності, що дозволить не лише захистити фінансові установи від атак, а й забезпечити їх стійкість та підвищити довіру у глобальному інформаційному середовищі.

Сучасні глобалізаційні та цифрові виклики для інформаційної безпеки українських фінансових установ полягають у поєднанні воєнних кіберзагроз, глобальної інтеграції у фінансовий простір та швидкої цифровізації фінансових послуг. Це створює високий рівень ризику для їх стабільності та довіри клієнтів. Так, глобалізація фінансових потоків збільшує ризики атак на міжнародні транзакції та системи SWIFT. Окрім того, зростає конкуренція, адже міжнародні фінтех-компанії виходять на український ринок, що підвищує вимоги до інформаційної безпеки та прозорості. Водночас, посилюються міжнародні кіберзагрози, почастішали атаки з боку глобальних хакерських угруповань, які тестують нові методи кіберзлочинності на українських фінансових установах.

Активна цифровізація фінансових послуг (розвиток онлайн-банкінгу, мобільних додатків, цифрових платформ) створює нові можливості й канали для інформаційних атак. Так, у 2025 році спостерігалось зростання кількості кіберінцидентів, збільшились атаки на фінансові установи (особливо на банки), через інсайдерську діяльність та фішингові кампанії. Використання нових інформаційних технологій (хмарні сервіси, блокчейн та штучний інтелект) потребують додаткових механізмів безпеки й захисту, а наявний низький рівень фінансової та цифрової грамотності клієнтів вітчизняних фінансових установ, робить їх вразливими до різноманітних шахрайських схем. Водночас, вагомо впливає воєнний чинник, адже кібератаки на критичну інфраструктуру (включно з фінансовими установами) залишаються системними, що підриває довіру до усієї фінансової системи.

Фактично, українські фінансові установи стикаються з подвійним тиском: глобалізаційні виклики вимагають відповідності міжнародним стандартам, а цифрові виклики створюють нові канали для атак. У порівнянні з провідними країнами, Україна перебуває на етапі становлення системи резил'єнтності,

що потребує: масштабних інвестицій у кіберзахист, інтеграції міжнародних стандартів, розвитку культури інформаційної безпеки серед персоналу та клієнтів. Це критично важливо для забезпечення резил'єнтності й стійкості фінансових установ України та їх інтеграції у глобальний інформаційний простір.

Таким чином, перед вітчизняними фінансовими установами постають комплексні завдання, які доцільно згрупувати у кілька стратегічних блоків:

фінансово-організаційний блок, у якому має передбачатися: інтеграція міжнародних стандартів кіберрезил'єнтності (ISO/IEC 27001, NIST, DORA) у внутрішні політики фінансових установ; формування безпекових бюджетів на кіберзахист як окремої статті витрат, а не допоміжного елемента; розробка планів безперервності діяльності (Business Continuity Plans) та різних гнучких сценаріїв відновлення після атак; формування спеціалізованих підрозділів з кіберризиків у фінансових установах. Очікуваним ефектом від реалізації цих завдань буде забезпечення системного управління резил'єнтністю інформаційної безпеки та зниження втрат;

технологічний блок, у якому має передбачатися: впровадження систем моніторингу та раннього виявлення атак (SIEM, SOC); розвиток хмарних рішень із підвищеним рівнем безпеки та резервне копіювання даних; тестування стійкості систем через регулярні «stress tests» та моделювання кризових сценаріїв; використання блокчейн- та AI-рішень для прозорого контролю транзакцій і прогнозування ризиків. Очікуваним ефектом від реалізації цих завдань буде забезпечення резил'єнтності й стійкості інформаційних систем і платформ та швидке їх відновлення;

кадровий та освітній блок, у якому має передбачатися: підвищення кваліфікації персоналу у сфері кібербезпеки та інформаційної резил'єнтності; розробка програм фінансової та цифрової грамотності для клієнтів, щоб зменшити ризики соціальної інженерії; формування культури кіберрезил'єнтності й усвідомлення, що інформаційна безпека є спільною відповідальністю. Очікуваним ефектом від реалізації цих завдань буде зниження помилок персоналу й клієнтів та підвищення довіри;

регуляторно-правовий блок, у якому має передбачатися: виконання нормативних вимог і регламентів щодо інформаційної безпеки і кіберзахисту; звітування про інциденти та прозорість комунікації з клієнтами та регуляторами; участь у міжнародних програмах кіберспівпраці для обміну досвідом і технологіями. Очікуваним ефектом від реалізації цих завдань буде підвищена транспарентність і прозорість та відповідність глобальним стандартам резил'єнтності.

Отже, метою щодо забезпечення резил'єнтності інформаційної безпеки для вітчизняних фінансових установ є перехід від реактивної моделі кіберзахисту до проактивної резил'єнтності, де безпека розглядається як стратегічний ресурс і конкурентна перевага.

При цьому, пріоритетними напрямами щодо досягнення цієї мети доцільно визначити:

інтеграція міжнародних стандартів кіберрезил'єнтності, гармонізація українських нормативів із європейськими для підвищення довіри іноземних інвесторів, що забезпечить відповідність глобальним практикам, зменшення регуляторних ризиків, інтеграцію у світовий інформаційний і фінансовий простір;

адаптація й розвиток систем моніторингу та реагування у фінансових установах, використання SIEM-систем для раннього виявлення атак, регулярні stress tests та моделювання кризових сценаріїв, що дозволить швидко виявляти інциденти, мінімізувати втрати, підвищити стійкість інформаційних систем і платформ;

забезпечення безперервності діяльності фінансових установ, використання хмарних рішень із резервним копіюванням даних, тестування здатності інформаційних систем і платформ відновлюватися після атак чи збоїв), що гарантуватиме безперервність критичних фінансових послуг навіть у кризових умовах;

впровадження інноваційних технологій (блокчейн-рішень для прозорого контролю транзакцій, AI/ML для прогнозування кіберризиків й автоматизації захисту, Zero Trust Architecture для мінімізації внутрішніх загроз), що підвищить рівень захисту, зменшить корупційні ризики, генеруватиме конкурентні переваги;

підвищення компетентності персоналу та безпекової культури (постійне навчання персоналу щодо кіберризиків та резил'єнтності, впровадження програм фінансової та цифрової грамотності, формування корпоративної культури кіберрезил'єнтності), що дасть змогу зменшити ризики соціальної інженерії, підвищити довіру клієнтів та резил'єнтність і стійкість фінансової установи.

Реалізація заходів за означеними напрямами забезпечення резил'єнтності інформаційної безпеки дозволить вітчизняним фінансовим установам поєднати економічну стабільність із технологічною стійкістю, забезпечить їх захист фінансових від глобальних кіберзагроз, сприятиме інтеграції у європейський простір та сформує основу для довгострокового розвитку й відновлення у пост воєнний період за глобалізаційних та цифрових викликів. Таким чином, констатуємо, що удосконалення інформаційної безпеки у контексті резил'єнтності – це не лише технічне завдання, а й стратегічний напрям

розвитку фінансових установ України, який забезпечить їх стійкість, відновлення, довіру та інтеграцію у глобальний цифровий простір.

Висновки. У статті виявлено наявні тенденції резил'єнтності інформаційної безпеки українських фінансових установ у воєнний період (2022–2025 рр.), відмічено, що вони характеризуються активізацією формування регламентів, нормативного поля та поступового впровадження практичних інструментів резил'єнтного інформаційного захисту. Водночас, зауважено, що хоча Україна й зробила важливий крок, ухваливши нові вимоги до інформаційної безпеки фінансових установ, але перебуває на етапі становлення резил'єнтності, і зрівняно із США та ЄС, де кіберрезил'єнтність стала частиною фінансової політики, українські установи ще потребують масштабних інвестицій у кіберзахист, інтеграції міжнародних стандартів, адаптації систем відновлення й безперервності діяльності, розвитку культури інформаційної безпеки. Викрито сучасні глобалізаційні та цифрові виклики для інформаційної безпеки українських фінансових установ, які полягають у поєднанні воєнних кіберзагроз, глобальної інтеграції у фінансовий простір та швидкої цифровізації фінансових послуг. Це створює високий рівень ризику для їх стабільності та довіри клієнтів. Виявлено, що українські фінансові установи стикаються з подвійним тиском: глобалізаційні виклики вимагають відповідності міжнародним стандартам, а цифрові виклики створюють нові канали для атак. Розкрито, що перед вітчизняними фінансовими установами постають комплексні завдання, які згруповано у чотири стратегічних блока (фінансово-організаційний блок технологічний блок кадровий та освітній блок регуляторно-правовий блок). Обґрунтовано пріоритетні напрями забезпечення резил'єнтності інформаційної безпеки, реалізація яких дозволить вітчизняним фінансовим установам поєднати економічну стабільність із технологічною стійкістю, забезпечить їх захист фінансових від глобальних кіберзагроз, сприятиме інтеграції у європейський простір та сформує основу для довгострокового розвитку й відновлення у пост воєнний період за глобалізаційних та цифрових викликів.

Список літератури:

1. Абрамова А. С. Система ризиків діяльності комерційних банків в умовах цифровізації. *Проблеми і перспективи економіки та управління.* 2021. № 4 (28). С. 186–193.

2. Гречка В., Островський В., Білий М. Розвиток системи фінансової безпеки банківських установ в умовах цифровізації. *Науковий вісник Полісся*. 2025. № 2 (29), С. 461–478. DOI: https://doi.org/10.25140/2410-9576-2024-2(29)-461-478

3. Григораш О., Пугач В. Фінансова стійкість України в умовах війни: реалії та перспективи. *Економіка та суспільство*. 2024 (65). DOI: https://doi.org/10.32782/2524-0072/2024-65-57

4. Неустроєв Ю. Г., Згадова Н. С., Работін Ю. А. Принципи безпеки фінансових установ в Україні. *Агросвіт.* 2021. № 3. с. 37–43. DOI: 10.32702/2306-6792.2021.3.37

5. *Постанова правління НБУ № 143 від 09 грудня 2025 року.* Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг. URL: https://bank.gov.ua/admin_uploads/law/09122025_143.pdf?v=15

6. *Резильєнтність ендогенного розвитку регіонів в умовах глобальних викликів та шоків:* монографія: НАН України. ДУ «Інститут регіональних досліджень імені М. І. Долішнього НАН України»; наук. редактор М.І. Мельник. Львів. 2024. 307 с.

7. Трусова Н. В., Чкан І. О Кіберзахист банківської системи України в умовах цифрових трансформацій. *Збірник наукових праць ТДАТУ ім. Д. Моторного (економічні науки).* № 1 (47), 2023. С. 151–163. DOI: https://doi.org/10.31388/2519-884X-2023-47-151-163

8. Barr, M.S., Harris, A., Menand, L., Xu, W. Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion. *Center on Finance, Law & Policy.* 2020. Pp. 1–28. URL: https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/cbotf-paper-3-future-payment-systems.pdf

9. Forcadell F. J., Aracil E., Úbeda, F. The Impact of Corporate Sustainability and Digitalization on International Banks' Performance. *Global Policy.* 2020. № 11 (S1). Pp. 18–27. DOI: https://doi.org/10.1111/1758-5899.12761

10. Eisenbach,T.M., Kovner A., Lee, M.J. Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics.* 2022. № 145 (3). Pp. 802–826.

11. Walker J., Cooper M. Genealogies of resilience. Security Dialogue. 2011. Vol. 42. No. 2. Pp. 143–160. DOI: https://doi.org/10.1177/0967010611399616

References:

1. Abramova A. S. (2021). Systema ryzykiv diialnosti komertsiinykh bankiv v umovakh tsyfrovizatsii [The system of risks of commercial banks in the context of digitalization]. *Problemy i perspektyvy ekonomiky ta upravlinnia.* № 4 (28). Pp. 186–193. (in Ukrainian)

2. Hrechka V., Ostrovskyi V. & Bilyi M. (2025) Rozvytok systemy finansovoi bezpeky bankivskykh ustanov v umovakh tsyfrovizatsii [Development of the financial security system of banking institutions in the context of digitalization]. *Naukovyi visnyk Polissia.* No. 2 (29), Pp. 461–478. DOI: https://doi.org/10.25140/2410-9576-2024-2(29)-461-478 (in Ukrainian)

3. Hryhorash O. & Puhach V. (2024) Finansova stiikist Ukrainy v umovakh viiny: realii ta perspektyvy [Financial stability of Ukraine in times of war: realities and prospects]. *Ekonomika ta suspilstvo*. No. (65). DOI: https://doi.org/10.32782/2524-0072/2024-65-57 (in Ukrainian)

4. Neustroiev Yu. H., Zghadova N. S. & Rabotin Yu. A. (2021) Pryntsypy bezpeky finansovykh ustanov v Ukraini [Security principles of financial institutions in Ukraine]. *Ahrosvit.* No. 3. Pp. 37–43. DOI: https://doi.org/10.32702/2306-6792.2021.3. (in Ukrainian)

5. *Postanova pravlinnia NBU № 143 vid 09 hrudnia 2025 roku.* Pro zatverdzhennia Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky ta kiberzakhystu nadavachamy finansovykh posluh [On approval of the Regulation on the organization of measures to ensure information security and cyber protection by financial service providers]. Available at: https://bank.gov.ua/admin_uploads/law/09122025_143.pdf?v=15 (in Ukrainian)

6. *Rezylientnist endohennoho rozvytku rehioniv v umovakh hlobalnykh vyklykiv ta shokiv* [Resilience of endogenous development of regions in the face of global challenges and shocks]: monohrafiia. (2024) NAN Ukrainy. DU "Instytut rehionalnykh doslidzhen imeni M. I. Dolishnoho NAN Ukrainy"; nauk. redaktor M.I. Melnyk. Lviv. 307 p. (in Ukrainian)

7. Trusova N. V. & Chkan I. O (2023) Kiberzakhyst bankivskoi systemy Ukrainy v umovakh tsyfrovykh transformatsii [Cyber defense of the banking system of Ukraine in the context of digital transformations]. *Zbirnyk naukovykh prats TDATU im. D. Motornoho (ekonomichni nauky).* No. 1 (47). C. 151–163. DOI: https://doi.org/10.31388/2519-884X-2023-47-151-163 (in Ukrainian)

8. Barr M. S., Harris A., Menand L., & Xu, W. (2020) Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion. *Center on Finance, Law & Policy.* Pp. 1–28. URL: https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/cbotf-paper-3-future-payment-systems.pdf

9. Forcadell F. J., Aracil E. & Úbeda F. (2020) The Impact of Corporate Sustainability and Digitalization on International Banks' Performance. *Global Policy.* No. 11 (S1), pp. 18–27. DOI: https://doi.org/10.1111/1758-5899.12761

10. Eisenbach T. M., Kovner A., & Lee M. J. (2022) Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics.* No. 145 (3). Pp. 802–826. DOI: https://doi.org/10.1016/j.jfineco.2021.10.007

11. Walker J., Cooper M (2011). Genealogies of resilience. *Security Dialogue.* Vol. 42. No. 2. Pp. 143–160. DOI: https://doi.org/10.1177/0967010611399616

Дата надходження статті: 15.01.2026
Дата прийняття статті: 04.02.2026
Дата публікації статті: 25.02.2026