

Юлія ТИМОШЕНКО¹,

кандидат економічних наук, директор департаменту реклами,
директор академії інновацій та бізнесу Європейського університету
ORCID ID: 0009-0005-2107-7634

¹ Європейський університет

Прийняття: 05/12/2025

Рецензія: 10/12/2025

Публікація: 30/12/2025

DOI: <https://doi.org/10.53920/ES-2025-4-16>

ФІНАНСОВІ РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ У ЦИФРОВІЙ ЕКОНОМІЦІ

JEL Класифікатор:
I23, I25, L26, G21, G22,
G32, Q02



This is an Open Access
article distributed
under the terms
of the [Creative Commons
CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/)

© Тимошенко Ю.,
2025

Стаття присвячена комплексному дослідженню фінансових ризиків та загроз економічній безпеці електронних платіжних систем у контексті динамічного розвитку цифрової економіки та зростання масштабів кіберзлочинності. У роботі обґрунтовано теоретико-методологічні підходи щодо аналізу природи фінансових ризиків, пов'язаних із функціонуванням систем, зокрема ризиків втрати коштів користувачів, операційних збоїв, порушення цілісності даних, інформаційних атак та репутаційних втрат. Виокремлено особливості взаємозв'язку між ризиком і загрозою в цифровому платіжному середовищі, наголошено на їх часовій та імовірнісній природі, а також на необхідності розмежування понять «ризик», «загроза» та «вразливість» у сучасному ризик-менеджменті.

Обґрунтовано, що сучасна система управління ризиками в електронних платіжних системах має базуватися на комплексному оцінюванні ймовірнісних моделей виникнення загроз, аналізі вразливостей ІТ-інфраструктури, змістовній класифікації ризиків і побудові багаторівневої системи захисту, яка містить процедури ідентифікації, автентифікації, авторизації та забезпечення цілісності даних. Розкрито ключові групи ризиків, виокремлені міжнародними регуляторами (ризиків ліквідності, кредитні, операційні, правові, інформаційні, репутаційні), та їх взаємодію в умовах інтенсивних цифрових трансакцій. Показано, що ефективне управління ризиками вимагає синергії технічних, організаційних і поведінкових механізмів,

розвитку системного моніторингу операцій, удосконалення стандартів кібербезпеки, підвищення фінансової грамотності користувачів та імплементації сучасних технологічних інструментів захисту.

Результати дослідження дозволяють узагальнити основні напрями посилення економічної безпеки електронних платіжних систем, серед яких провідне місце посідають: підвищення стійкості IT-інфраструктури, розвиток механізмів раннього виявлення інцидентів, гармонізація регуляторних вимог із міжнародними стандартами та впровадження інноваційних моделей управління ризиками. Подані аналітичні висновки можуть бути використані у практиці банківських установ, державних регуляторів і постачальників платіжних сервісів для розроблення стратегій підвищення безпеки та довіри у цифровому фінансовому середовищі.

Ключові слова: електронні платіжні системи, фінансові ризики, економічна безпека, цифрова економіка, ризик-менеджмент.

Yuliia TYMOSHENKO

FINANCIAL RISKS AND THREATS TO THE ECONOMIC SECURITY OF ELECTRONIC PAYMENT SYSTEMS IN THE DIGITAL ECONOMY

The article is devoted to a comprehensive study of financial risks and threats to the economic security of electronic payment systems in the context of the dynamic development of the digital economy and the growth of cybercrime. The paper substantiates theoretical and methodological approaches to analyzing the nature of financial risks associated with the functioning of systems, in particular, the risks of loss of users' funds, operational failures, data integrity breaches, information attacks, and reputational losses. The peculiarities of the relationship between risk and threat in the digital payment environment are highlighted, their temporal and probabilistic nature is emphasized, as well as the need to distinguish between the concepts of «risk», «threat», and «vulnerability» in modern risk management.

It is substantiated that the modern risk management system in electronic payment systems should be based on a comprehensive assessment of probabilistic models of threats, analysis of IT infrastructure vulnerabilities, meaningful classification of risks, and the development of a multi-level protection system that includes procedures for identification, authentication, authorization, and data integrity assurance. The key risk groups identified by international regulators (liquidity, credit, operational, legal, information, and reputational risks) and their interaction in the context of intensive digital transactions are revealed. It is shown that effective risk management requires the synergy of technical, organizational, and behavioral mechanisms, the development

of systematic monitoring of operations, the improvement of cybersecurity standards, the enhancement of users' financial literacy, and the implementation of modern technological protection tools.

The research results allow us to summarize the main directions for strengthening the economic security of electronic payment systems, among which the following occupy a leading place: increasing the stability of IT infrastructure, developing mechanisms for early detection of incidents, harmonizing regulatory requirements with international standards, and introducing innovative risk management models. The analytical conclusions presented can be used in the practice of banking institutions, state regulators, and payment service providers to develop strategies for enhancing security and trust in the digital financial environment.

Keywords: *electronic payment systems, financial risks, economic security, digital economy, risk management.*

Постановка проблеми. Стрімкий розвиток цифрової економіки, упровадження електронних платіжних сервісів та зростання частки безготівкових операцій докорінно змінюють архітектуру фінансових ринків і формують нові вимоги щодо системи економічної безпеки. В умовах зростання обсягів онлайн-транзакцій, активного використання платіжних карток та мобільних додатків істотно підвищується ймовірність реалізації фінансових ризиків, пов'язаних із кіберзагрозами, соціальною інженерією, технологічними збоями й недостатньою стійкістю інформаційних систем. Статистичні дані Національного банку України за 2022 – 2024 рр. підтверджують, що масштаби незаконних дій із використанням платіжних карток зростають як у частині фінансових втрат, так і у складності механізмів шахрайства, що прямо впливає на економічну безпеку держави, банківських установ, бізнесу та домогосподарств [1].

Незважаючи на актуальність проблеми, наукові підходи щодо аналізу фінансових ризиків електронних платіжних систем залишаються фрагментарними, а існуючі моделі ризик-менеджменту не повною мірою враховують специфіку цифрового середовища, уразливості IT-інфраструктури та поведінкові фактори користувачів. Неврегульованість окремих аспектів нормативного забезпечення платіжної безпеки, різний рівень технічної оснащеності учасників ринку, відсутність єдиної системи моніторингу та прогнозування ризиків поглиблюють проблему, створюючи передумови для зростання загроз економічній стабільності та довіри до фінансових інновацій.

У цьому контексті виникає необхідність у комплексному науковому дослідженні фінансових ризиків та загроз експлуатації електронних платіжних систем, визначенні їхньої природи, динаміки та каналів реалізації,

а також у розробленні методологічних підходів щодо їх мінімізації. Вирішення зазначеної проблеми сприятиме посиленню економічної безпеки на національному рівні та забезпеченню сталості розвитку цифрового фінансового сектору України.

Аналіз останніх досліджень і публікацій. Питання фінансово-економічної безпеки в умовах цифрової економіки, діджиталізації державних фінансів, розвитку електронних сервісів податкової адміністрації, стійкості бізнесу та трансформації ризик-менеджменту розглянуто у працях І. Надточій, І. Крамаренко, Н. Гришиної [2], А. Тимошенка [3, 4, 6], О. Васильчишина [5], А. Максименка [7], М. Артемчука [9], Н. Бобро [11 – 13], А. Крапа, С. Батаєва, В. Козуб, Н. Глевацької [12], С. Сафарлі, С. Колач, М. Живко, О. Волського [14]. У зазначених дослідженнях обґрунтовано теоретичні засади фінансової стабільності та економічної безпеки, проаналізовано вплив цифровізації, воєнних загроз і глобалізаційних процесів на фінансові ринки, інвестиційні стратегії та корпоративне управління, однак специфічні фінансові ризики електронних платіжних систем і механізми протидії несанкціонованим операціям досліджено фрагментарно, що зумовлює потребу в подальшій науковій розробці цієї проблематики.

Мета статті – здійснити комплексне наукове дослідження фінансових ризиків та загроз економічній безпеці електронних платіжних систем у цифровій економіці, виявити їх природу, динаміку та канали реалізації, проаналізувати тенденції несанкціонованих списань коштів у банківському секторі України у 2022 – 2024 рр., а також обґрунтувати концептуальні підходи й практичні рекомендації щодо удосконалення системи управління ризиками та підвищення рівня захищеності платіжної інфраструктури.

Виклад основного матеріалу дослідження. Проблематика аналізу та управління фінансовими ризиками у сфері електронних платіжних систем почала формуватися у вітчизняній економічній науці порівняно нещодавно й досі залишається недостатньо системно дослідженою. Сучасна цифрова економіка зумовлює появу нових форм невизначеності у фінансових транзакціях, що, у свою чергу, актуалізує потребу в оновленні методологічних підходів щодо виявлення, класифікації й оцінювання ризиків у платіжній інфраструктурі [2, С. 83].

У наукових джерелах, економічний ризик здебільшого пов'язується з категорією невизначеності, яка виникає у процесі управління соціально-економічними системами, адже саме невизначеність формує передумови для загрози втрат ресурсів, активів або очікуваних результатів. Незважаючи на широкий спектр підходів щодо тлумачення цих понять у сучасній економічній та юридичній літературі, дослідники сходяться на тому, що ри-

зик у фінансовій сфері завжди має імовірнісний характер та пов'язаний із можливістю відхилення фактичного результату від очікуваного [8, С. 546].

У контексті функціонування електронних платіжних систем (ЕПС) фінансовий ризик визначається як імовірність ненадходження або втрати очікуваного фінансового результату внаслідок дії зовнішніх чи внутрішніх загроз. Цей ризик характеризується складною структурою та різною інтенсивністю прояву для всіх учасників ЕПС – банків, торговців, постачальників платіжних послуг і безпосередніх користувачів. Як підкреслюють українські дослідники, цифровізація фінансових операцій створює нові канали уразливості, що підсилює потребу у формуванні комплексної системи фінансово-економічної безпеки [2, 3].

Суттєвого значення набувають ризики, пов'язані з порушенням нормативних вимог та недотриманням стандартів платіжної безпеки. Зокрема недосконалість внутрішніх процедур контролю, слабкі механізми аутентифікації або недостатня стійкість ІТ-інфраструктури підвищують ймовірність шахрайських втручань, що призводять до несанкціонованих списань коштів з рахунків користувачів. Такі випадки відображають не лише технічну вразливість ЕПС, а й загрозу для національної економічної безпеки, оскільки втрати клієнтів та бізнесу мають прямі фінансові наслідки для банківської системи [4].

Аналіз офіційних даних Національного банку України засвідчує, що несанкціоновані списання коштів, пов'язані з незаконними діями з використанням платіжних карток, формують одну з найбільш небезпечних груп ризиків електронних платіжних систем. Так, лише за останні 3 роки сума збитків від таких операцій зросла з 481 млн грн у 2022 році до 1,1 млрд грн у 2024 році, тобто більш ніж у 2,3 рази, а середня сума однієї незаконної транзакції збільшилася з приблизно 2,2 тис. грн до понад 4,2 тис. грн (табл. 1).

Таблиця 1. Динаміка несанкціонованих списань коштів (незаконних дій з платіжними картками) у банківському секторі України, 2022 – 2024 рр.

№	Показник	2022	2023	2024
1	Кількість незаконних операцій, тис.	218	272	270
2	Сума збитків, млн грн	481	833	1100
3	Середня сума однієї незаконної операції, грн	2 200	3 065	4 247
4	Середня сума незаконної операції в інтернеті, грн	2 408	3 150	4 761

Джерело: сформовано автором на підставі [1]

Дослідження динаміки несанкціонованих списань коштів у банківському секторі України за 2022 – 2024 рр. свідчить про суттєве посилення фінансових ризиків у сфері електронних платежів. Незважаючи на незначне зниження кількості шахрайських операцій у 2024 р. (–1% порівняно з 2023 р.), сума збитків продовжила стрімко зростати, досягнувши 1,1 млрд грн, що на 37% більше, ніж попереднього року. Водночас середня сума однієї незаконної операції збільшилася до 4 247 грн, а середня сума шахрайства в Інтернеті – до 4 761 грн, що демонструє зміщення акценту шахрайських схем у бік високовартісних онлайн-транзакцій. Загальна тенденція підтверджує підвищення складності та інтенсивності цифрових загроз, а також зростаючу ефективність методів соціальної інженерії, що вимагає посилення кіберзахисту та фінансової грамотності користувачів платіжних сервісів.

Подані статистичні дані щодо несанкціонованих списань коштів з рахунків підтверджують сталу тенденцію до зростання шахрайства у цифровому фінансовому середовищі, що безпосередньо формує високий рівень фінансових ризиків та призводить до втрати власних коштів користувачів платіжних сервісів. З огляду на це, у науковій літературі наголошується на багатовимірності поняття «ризик», яке набуває різного змістового наповнення залежно від галузевого контексту [8, С. 84]. У страхуванні під ризиком традиційно розуміють узагальнюючу категорію небажаних подій або міру можливих майбутніх негативних наслідків, тоді як в економічному та фінансовому дискурсі ризик тісно пов'язаний з невизначеністю щодо настання певної події та її потенційного впливу на стан економічного агента [7, С. 113].

У межах дослідження ризиків ЕПС, фінансовий ризик доцільно визначати як вимірювану та невимірювану ймовірність реалізації небажаної події, пов'язаного із втратою коштів користувачами системи внаслідок недостатнього рівня захисту ЕПС від протиправних або шахрайських дій третіх осіб. З наукової точки зору важливим є також поняття «ступінь ризику», яке відображає кількісну характеристику ймовірності та масштабів потенційних втрат, що набуває особливої значущості у процесі забезпечення економічної безпеки цифрових фінансових операцій [11, С. 57]. Висока варіативність і складність загроз визначають необхідність глибокого розуміння сутності фінансових ризиків для формування ефективної системи контролю й мінімізації збитків у платіжному середовищі.

З методологічної точки зору загроза розглядається як невід'ємний компонент ризику. Аналіз фінансових ризиків, таким чином, передбачає послідовне визначення ймовірності виникнення загрози для платіжної системи, оцінювання рівня її вразливості, а також дієвості механізмів внутрішнього контролю фінансових ризиків та захисту інформаційних активів [12, 13]. Сукупна оцінка цих компонентів дозволяє сформулювати комплексну

характеристику фінансового ризику та визначити рівень його впливу на стабільність ЕПС.

Фінансовий ризик та загроза в електронних платіжних системах є різними часовими стадіями прояву невизначеності. Обидва поняття суттєво визначають економічну поведінку користувачів і постачальників платіжних послуг, оскільки формують очікування щодо безпеки операцій, ймовірності втрати ресурсів та стабільності транзакційного середовища [10]. Виникнення ризиків ЕПС зумовлене структурою та обсягом транзакцій, числом учасників фінансової екосистеми, а також характером технологічних операцій, що виконуються у режимі реального часу.

Для ефективної оцінки ризиків електронних платіжних систем, міжнародна та вітчизняна практика передбачає виконання низки аналітичних процедур, серед яких:

- формування алгоритму класифікації ризиків відповідно до їх джерел і каналів реалізації;
- обчислення ймовірності настання кожного виду ризику з урахуванням історичних даних і поточних трендів;
- проведення кількісної та якісної оцінки потенційних збитків, включаючи визначення їхнього масштабу, повторюваності та каналів виникнення [2, 6, 13].

Виявлення та ідентифікація конкретних ризикових подій в електронних платіжних системах, належать до найбільш складних і відповідальних елементів сучасного ризик-менеджменту, оскільки саме на цьому етапі формується повноцінне розуміння природи загроз і масштабу їхнього впливу на фінансову стабільність системи. Для окремих категорій ризиків, зокрема ризиків підроблення електронних платіжних документів, накопичені статистичні дані дають можливість здійснювати ймовірнісну оцінку на основі історичних спостережень. Водночас важливо враховувати наявність «прихованої частини» ризикових подій, коли шахрайські дії не були ідентифіковані або не потрапили до офіційної звітності, що ускладнює точність оцінювання реального рівня загроз у цифровому платіжному середовищі [9, 14].

Необхідність системної класифікації ризиків ЕПС зумовлена потребами побудови ефективної системи управління фінансовими загрозами, яка враховує специфіку зовнішнього і внутрішнього середовища функціонування платіжних інструментів. У міжнародній практиці регулювання платіжних систем, зокрема у стандартах Європейського центрального банку та Європейського банківського органу, наголошується на ключовому значенні управління такими групами ризиків, як ризик ліквідності, операційний ризик, кредитний ризик та правовий ризик [15]. Ці види ризиків виникають унаслідок взаємодії між учасниками фінансової інфраструктури,

високої інтенсивності транзакцій, використання складних цифрових алгоритмів та необхідності забезпечення неперервності платіжного процесу.

В електронних платіжних системах також виокремлюють ризик доступності, пов'язаний із тимчасовою неможливістю проведення платежів через технічні збої або відмову інфраструктури, та ризик інформаційних систем, який охоплює вразливості програмно-технічних компонентів, процесинг-центрів та інтерфейсів клієнтського доступу. Значну увагу приділяють і адміністративному ризику, пов'язаному з помилками персоналу або недоліками внутрішніх процедур, та ризику варіації, що виникає внаслідок волатильності потоків ліквідності або тимчасових розривів між проведенням операції та її покриттям.

Окрему, надзвичайно важливу групу, становлять кримінально-фінансові ризики, що відображають поширення шахрайських схем, соціальної інженерії та цифрових атак на користувачів платіжних карток і онлайн-банкінгу. Так, за даними Національного банку України, у 2022 – 2024 рр. саме ця категорія ризиків демонструє найдинамічніше зростання, зокрема у сегменті операцій, проведених через Інтернет, частка яких у загальній сумі збитків у 2024 р. досягла 93% [1].

Узагальнюючи, основні ризики, притаманні електронним платіжним системам, охоплюють такі (рис. 1).

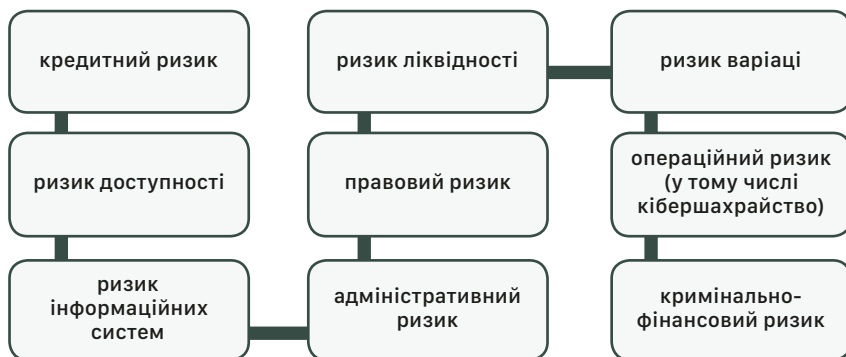


Рис. 1. Основні ризики під час здійснення фінансових операцій в електронних платіжних системах

Джерело: сформовано автором самостійно

Кожен із базових ризиків електронних платіжних систем має власний інструментарій управління, що зумовлено специфікою його змістових характеристик.

Основні загрози, причини їх виникнення та можливі способи зниження рівня небезпеки відображено на рис. 2.

<p>Загроза впливу шкідливих програм</p>	<ul style="list-style-type: none"> До таких програм належать різноманітні віруси, трояни і т.д. Метою їхнього впливу може бути збір конфіденційної інформації, блокування роботи програм, пошкодження або зупинка обладнання, здійснення несанкціонованих платіжних транзакцій. Зниження цієї загрози досягається використанням сучасних програмних засобів захисту.
<p>Загроза недостатнього рівня захищеності програмних продуктів</p>	<ul style="list-style-type: none"> Ця загроза зумовлена неможливістю відстеження дій кожного окремого користувача або співробітника ЕПС. За наявності комп'ютерної системи в організації складно й фінансово витратно налаштувати повноцінний контроль доступу. Через це неможливо повністю запобігти спробам малокомпетентних працівників вносити зміни у роботу програм (особисті налаштування, використання мереж у власних цілях, підключення до небезпечних каналів зв'язку), що підвищує вразливість системи.
<p>Загроза підбору пароля</p>	<ul style="list-style-type: none"> Ця загроза означає, що будь-яка система вразлива, оскільки має базовий захист у вигляді пароля. Пароль може бути підібраний, випадково розголошений або неправильно збережений користувачем.
<p>Загроза неправомірного використання інформації</p>	<ul style="list-style-type: none"> Загроза пов'язана з втратою конкурентних переваг через дії користувачів або конкурентів, що може призвести до порушення авторських прав або використання інформації в інших, невігідних для ЕПС, цілях. Фактично будь-яка інформація електронної організації, розміщена на сайті чи сторінці в мережі Інтернет, піддається впливу цієї загрози.
<p>Загроза втрати або зміни інформації</p>	<ul style="list-style-type: none"> Ця загроза має негативні наслідки як для продавця, так і для покупця, і пов'язана з інформацією, що зберігається на серверах. Будь-який учасник ЕПС володіє даними про своїх клієнтів, партнерів і конкурентів. Ця інформація може бути втрачена через технічні несправності (збої у сховищах, відсутність резервного копіювання, вихід з ладу основних та резервних носіїв даних).
<p>Загрози ідентифікації та автентифікації</p>	<ul style="list-style-type: none"> Можуть призвести до низки наслідків: відмови від здійснення операції, неправильного сприйняття даних, надання недостовірної інформації, шахрайства.
<p>Загроза втрати ділової репутації</p>	<ul style="list-style-type: none"> Зумовлена можливістю поширення неправдивої або викривленої інформації, яка здатна підірвати довіру користувачів до ЕПС.

Рис. 2. Потенційні загрози в електронних платіжних системах

Джерело: сформовано автором самостійно

Ефективна електронна платіжна система, відповідно до сучасних підходів, – це така система, яка забезпечує миттєве підтвердження операцій, безперешкодний обмін даними між учасниками без залучення третьої сторони, функціонування у захищеному транзакційному середовищі та гарантований рівень інформаційної та фінансової безпеки [2, 5]. Однак подібна модель є радше еталонною, ніж повністю досяжною, оскільки реальний стан цифрового фінансового середовища характеризується постійним зростанням кількості кібератак, ускладненням шахрайських схем та підвищенням технологічної вразливості користувачів і провайдерів платіжних послуг.

Міжнародний досвід підтверджує: шахрайські дії у сфері цифрових платежів дедалі частіше здійснюються організованими групами, які використовують методи соціальної інженерії, зараження комп'ютерних систем шкідливими програмами, компрометацію платіжних реквізитів та інші інструменти несанкціонованого доступу [6, С. 111]. Типовий алгоритм такої атаки містить кілька послідовних етапів:

- розвідка – визначення цілі, підбір технічних засобів впливу, створення шкідливого програмного забезпечення;
- інфікування та проникнення в ЕПС – завантаження небезпечних файлів або ініціювання фішингових переходів з метою пошуку слабких місць;
- закріплення у системі та приховування слідів – використання вразливостей для непомітного здійснення незаконних операцій протягом тривалого часу.

Наслідком таких дій є формування нових загроз, у тому числі репутаційних. Репутаційний ризик ЕПС виникає внаслідок поширення викривленої або недостовірної інформації, втрати довіри клієнтів, а також через затримку чи неякісне реагування на інциденти безпеки. Цей вид ризику складно ідентифікувати, оскільки він має непрямий характер і часто пов'язаний із низкою інших загроз – операційних, правових, інформаційних.

Забезпечення комплексної безпеки електронної платіжної системи передбачає функціонування кількох ключових рівнів захисту:

- ідентифікація;
- автентифікація;
- авторизація;
- рівень довіри між учасниками;
- гарантована цілісність даних;
- підтверджена платоспроможність і згода клієнта на транзакцію [4, 6].

Наявність цих рівнів не усуває загроз повністю, однак формує бар'єр, що суттєво знижує ймовірність реалізації ризиків.

У контексті дослідження економічної безпеки ЕПС під загрозою достільно розуміти наявність умов, за яких виникають події, що здатні дестабілізувати роботу системи та завдати фінансових втрат її учасникам. До основних таких випадків належать:

- розкриття конфіденційної інформації;
- порушення цілісності або коректності даних;
- відмова в обслуговуванні (DoS/DDoS), збій або блокування системи.

Кожен із цих інцидентів виступає окремою загрозою і здатен суттєво знизити рівень економічної безпеки платіжної системи.

Можна констатувати, що уразливість електронної платіжної системи, на сьогодні, визначається як потенційна можливість виникнення загрози, яка реалізується через слабкі місця технічної, організаційної або поведінкової природи. Зловмисник, здійснюючи атаку, використовує саме ці вразливості, що дозволяє вважати атаку фактичною реалізацією загрози. Таким чином, рівень економічної безпеки ЕПС є похідною від того, наскільки швидко система може виявляти та нейтралізувати власні вразливості, а також від ефективності функціонування її внутрішніх контрольних механізмів.

Висновки та пропозиції. Проведене дослідження дало можливість теоретично уточнити зміст категорій «фінансовий ризик», «загроза» та «уразливість» в контексті функціонування електронних платіжних систем, розмежувавши їх як різні часові стадії прояву невизначеності. Показано, що фінансові ризики ЕПС мають багатовимірний характер і охоплюють не лише класичні кредитний, ліквідний, операційний і правовий ризики, а й ризик доступності, ризик інформаційних систем, адміністративний, репутаційний та кримінально-фінансовий ризики. Визначено, що саме кримінально-фінансові ризики, пов'язані з шахрайством, соціальною інженерією та кіберзлочинністю, стають домінуючими у цифровому платіжному середовищі та найбільшою мірою впливають на економічну безпеку учасників ринку.

Емпіричний аналіз динаміки несанкціонованих списань коштів у банківському секторі України за 2022 – 2024 рр. засвідчив суттєве зростання фінансових втрат від незаконних дій з платіжними картками. Попри певну стабілізацію за кількістю шахрайських операцій, сума збитків у 2024 році, більш ніж удвічі перевищила показники 2022 року, а середній розмір однієї незаконної транзакції істотно зріс, особливо в сегменті інтернет-операцій. Це свідчить про еволюцію шахрайських схем у бік більш технологічно складних і високочастотних атак, що посилює вимоги щодо системного управління ризи-

ками, підвищення стійкості IT-інфраструктури та удосконалення процедур ідентифікації, автентифікації й авторизації користувачів.

З урахуванням отриманих результатів, доцільно посилити інституційні засади управління фінансовими ризиками ЕПС за допомогою: гармонізації національних стандартів платіжної безпеки з європейськими регуляторними підходами; удосконалення регуляторних вимог щодо моніторингу операцій та обов'язкової звітності про кіберінциденти; запровадження для постачальників платіжних послуг ризик-орієнтованих моделей комплаєнсу та регулярного стрес-тестування платіжної інфраструктури. На мікрорівні необхідно розширити використання багатofакторної автентифікації, систем поведінкової аналітики транзакцій, внутрішніх протоколів реагування на інциденти, а також продовжити масштабні освітні кампанії з підвищення фінансової та цифрової грамотності населення. Перспективним напрямом подальших досліджень є розробка інтегрованих моделей кількісної оцінки кримінально-фінансових ризиків ЕПС та оцінювання ефективності впроваджених інструментів кіберзахисту.

ЛІТЕРАТУРА

1. Національний банк України. Кількість випадків шахрайства з картками знизилась, збитки за ними – зросли. URL: <https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli> (дата звернення: 04.12.2025).
2. Надточій І., Крамаренко І., Гришина Н. Фінансово-економічна безпека в умовах цифрової економіки та суспільства: наукові засади, особливості управління та регулювання. *Український економічний часопис*. 2024. № 4. С. 83 – 88. DOI: 10.32782/2786-8273/2024-4-16.
3. Тимошенко А. Діджиталізація державних фінансів у контексті забезпечення економічної безпеки України. *Сталий розвиток економіки*. 2025. № 6(57). С. 44 – 51. DOI: 10.32782/2308-1988/2025-57-6.
4. Тимошенко А. Електронні сервіси податкової адміністрації як чинник прозорості та довіри бізнесу. *Економіка та суспільство*. 2025. № 79. DOI: 10.32782/2524-0072/2025-79-171.
5. Васильчишин О. Б. Фінансові злочини у банківській системі як загроза національній безпеці України. *Наука та освіта в умовах воєнного часу*. 2025. С. 74. DOI: 10.64076/ihrс250925.10.
6. Тимошенко А. О. Фінансова стійкість малих і середніх підприємств України в умовах невизначеності. *The Future of Science, Technology and Economy: Proceedings of the 3rd International Scientific and Practical Conference*. Sofia, Bulgaria, 29 – 31 October 2025. С. 108 – 112. DOI: 10.70286/isu-29.10.2025.001.

7. Максименко А. П. Вплив цифровізації на загрози економічній безпеці держави : дис. ... д-ра філософії : 051; 05. Полтава : Нац. ун-т ім. Юрія Кондратюка, 2025. 267 с.

8. Тимошенко Ю. Фінансова стабільність як ключова категорія економічної науки. *Бізнес-навігатор*. 2025. № 6(83). С. 544 – 549. DOI: 10.32782/business-navigator.83-88.

9. Артемчук М. Д. Оцінка впливу воєнних загроз на новітній ризик-менеджмент малого та середнього бізнесу. *Здобутки економіки: перспективи та інновації*. 2025. № 16. DOI: 10.5281/zenodo.14967604.

10. Тимошенко Ю. О. Концептуальні підходи до дослідження грошово-кредитної політики у сучасній економіці. *Здобутки економіки: перспективи та інновації*. 2025. № 23. DOI: 10.5281/zenodo.17557469.

11. Бобро Н. С. Сталий економічний розвиток в умовах цифрової трансформації. *Агросвіт*. 2024. № 1. С. 56 – 60. DOI: 10.32702/2306-6792.2024.1.56.

12. Krap A., Bataiev S., Bobro N., Kozub V., Hlevatska N. Examination of digital advancements: Their influence on contemporary corporate management methods and approaches. *Multidisciplinary Reviews*. 2024. Vol. 7. Article 2024spe026. DOI: 10.31893/multirev.2024spe026.

13. Бобро Н. С. Нові тренди в економіці: цифровізація та діджиталізація. *Наука і техніка сьогодні*. 2023. № 14(28). С. 160 – 167. DOI: 10.52058/2786-6025-2023-14(28)-160-167.

14. Safarli C., Kolach S., Zhyvko M., Volskyi O., Bobro N. The Impact of Globalization on the Formation and Implementation of International Investment Strategies. *Economic Affairs*. 2024. Vol. 69, No 3. С. 1415 – 1422. DOI: 10.46852/0424-2513.4.2024.25.

15. European Central Bank. ECB oversight framework for electronic payment instruments, schemes and arrangements (PISA). 2021. URL: https://www.ecb.europa.eu/paym/pdf/psd/ecb.pisa_oversight.en.pdf (дата звернення: 05.12.2025).

REFERENCES

1. Natsionalnyi Bank Ukrainy (2025) Kilkist випадків shakhraystva z kartkami znyzylasia, zbytky za nymy – zrosly [The number of card fraud cases decreased while losses increased]. Available at: <https://bank.gov.ua/ua/news/all/kilkist-vypadkiv-shahraystva-z-kartkami-znizylasya-zbitki-za-nimi--zrosly> (accessed 04 December 2025).

2. Nadtochii I., Kramarenko I., Hryshyna N. (2024) Finansovo-ekonomichna bezpeka v umovakh tsyfrovoy ekonomiky ta suspilstva: naukovi zasady, osoblyvosti upravlinnia ta rehuliuвання [Financial and economic security in the digital economy and society: scientific foundations, management features and regulation]. *Ukrainian Economic Journal*, No 4, Pp. 83 – 88. DOI: 10.32782/2786-8273/2024-4-16.

3. Tymoshenko A. (2025) Didzhitalizatsiia derzhavnykh finansiv u konteksti zabezpechennia ekonomichnoi bezpeky Ukrainy [Digitalization of public finance in the context of ensuring Ukraine's economic security]. *Stalyi Rozvytok Ekonomiky*, No 6(57), Pp. 44 – 51. DOI: 10.32782/2308-1988/2025-57-6.

4. Tymoshenko A. (2025) Elektronni servisy podatkovoi administratsii yak chynnyk prozorosti ta doviry biznesu [Electronic tax administration services as a factor of transparency and business trust]. *Ekonomika ta Suspiilstvo*, no. 79. DOI: 10.32782/2524-0072/2025-79-171.

5. Vasylychshyn O. B. (2025) Finansovi zlochyny u bankivskii systemi yak zahroza natsionalnii bezpetsi Ukrainy [Financial crimes in the banking system as a threat to Ukraine's national security]. *Nauka ta Osvita v Umovakh Voiennoho Chasu*, P. 74. DOI: 10.64076/ihrc250925.10.

6. Tymoshenko A. O. (2025) Finansova stiikist malykh i serednykh pidpriemstv Ukrainy v umovakh nevyznachenosti [Financial stability of small and medium-sized enterprises in Ukraine under uncertainty]. In: *The Future of Science, Technology and Economy: Proceedings of the 3rd International Scientific and Practical Conference* (Sofia, Bulgaria, 29 – 31 October 2025), Pp. 108 – 112. DOI: 10.70286/isu-29.10.2025.001.

7. Maksymenko A. P. (2025) Vplyv tsyfrovizatsii na zahrozy ekonomichnii bezpetsi derzhavy [Impact of digitalization on threats to the economic security of the state] (PhD Thesis), Poltava: National University named after Yuri Kondratyuk.

8. Tymoshenko Yu. (2025) Finansova stabilnist yak kliuchova katehoriia ekonomichnoi nauky [Financial stability as a key category of economic science]. *Business Navigator*, No 6(83), Pp. 544 – 549. DOI: 10.32782/business-navigator.83-88.

9. Artemchuk M. D. (2025) Otsinka vplyvu voiennykh zahroz na novitnii ryzyk-menedzhment maloho ta serednoho biznesu [Assessment of the impact of war-time threats on innovative risk management of small and medium-sized businesses]. *Zdobutky Ekonomiky: Perspektyvy ta Innovatsii*, No 16. DOI: 10.5281/zenodo.14967604.

10. Tymoshenko Yu. O. (2025) Kontseptualni pidkhody do doslidzhennia hroshovo-kredytnei polityky u suchasnii ekonomitsi [Conceptual approaches to the study of monetary policy in the modern economy]. *Zdobutky Ekonomiky: Perspektyvy ta Innovatsii*, No 23. DOI: 10.5281/zenodo.17557469.

11. Bobro N. S. (2024) Stalyi ekonomichnyi rozvytok v umovakh tsyfrovoy transformatsii [Sustainable economic development under digital transformation]. *Agrosvit*, No 1, Pp. 56 – 60. DOI: 10.32702/2306-6792.2024.1.56.

12. Krap A., Bataiev S., Bobro N., Kozub V., Hlevatska N. (2024) Examination of digital advancements: Their influence on contemporary corporate management methods and approaches. *Multidisciplinary Reviews*, vol. 7, article 2024spe026. DOI: 10.31893/multi-rev.2024spe026.

13. Bobro N. S. (2023) Novi trendy v ekonomitsi: tsyfrovyzatsiia ta didzhytalizatsiia [New trends in the economy: digitization and digitalization]. *Nauka i Tekhnika Sьогодni*, No 14(28), Pp. 160 – 167. DOI: 10.52058/2786-6025-2023-14(28)-160-167.

14. Safarli C., Kolach S., Zhyvko M., Volskyi O., Bobro N. (2024) The impact of globalization on the formation and implementation of international investment strategies. *Economic Affairs*, Vol. 69, No 3, Pp. 1415 – 1422. DOI: 10.46852/0424-2513.4.2024.25.

15. European Central Bank (2021) ECB oversight framework for electronic payment instruments, schemes and arrangements (PISA). Available at: https://www.ecb.europa.eu/paym/pdf/psd/ecb.pisa_oversight.en.pdf (accessed 05 December 2025).