ФІНАНСИ. БАНКІВСЬКА СПРАВА ТА СТРАХУВАННЯ

DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-233-247
УДК 336.717
JEL Classification: G21; E42; O33

Артем Валерійович Тарасенко
кандидат економічних наук, доцент,
докторант кафедри фінансів, банківської справи та страхування
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: avtarasenko88@gmail.com. **ORCID:** https://orcid.org/0000-0003-4395-3605

Артур Віталійович Жаворонок
Кандидат економічних наук, доцент, доцент кафедри фінансів і кредиту
Чернівецький національний університет імені Юрія Федьковича (Чернівці, Україна)
E-mail: artur.zhavoronok@ukr.net. **ORCID:** https://orcid.org/0000-0001-9274-8240

Володимир Костянтинович Суховецький
аспірант кафедри фінансів, банківської справи та страхування
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: moskalyura73@gmail.com. **ORCID:** https://orcid.org/0009-0007-7585-9505

БЕЗПЕКА ПЛАТЕЖІВ У ЦИФРОВІЙ ЕКОНОМІЦІ: ВИКЛИКИ ДЛЯ БАНКІВСЬКОГО КАРТКОВОГО БІЗНЕСУ

Анотація. *У статті здійснено систематизацію ключових ризиків, характерних для банківського карткового бізнесу в умовах цифрової трансформації, на основі багатофакторної класифікації. Особливу увагу приділено кіберризикам, які визначено як найбільш небезпечні через їхню високу динамічність, складність виявлення та потенційно значні фінансові наслідки. Обґрунтовано необхідність переорієнтації безпекової парадигми від реактивного реагування до проактивного моніторингу та запобігання загрозам шляхом впровадження інноваційних цифрових технологій. Розглянуто перспективи використання штучного інтелекту та машинного навчання, біометрії, хмарних обчислень і технології блокчейн у розвитку безпекової інфраструктури банківського карткового бізнесу. Доведено доцільність інтегрованої стратегії безпеки, що поєднує технічні, організаційні та регуляторні рішення. Виокремлено ключові показники оцінювання ефективності безпекових заходів. Проаналізовано значення стійкої платіжної інфраструктури й міжбанківської співпраці для підвищення кіберстійкості сектору.*

Ключові слова: *банківський картковий бізнес; цифрова економіка; ризики; кіберзагрози; інформаційна безпека; інноваційні технології; штучний інтелект; біометрія; блокчейн.*
Рис.: 2. Табл.: 1. Бібл.: 16.

Постановка проблеми. Стрімкий розвиток цифрових технологій і перехід до безготівкової економіки докорінно трансформували фінансову систему, відкривши нові можливості для ефективних та зручних платіжних рішень. У цьому контексті банківський картковий бізнес відіграє ключову роль, оскільки забезпечує щоденні фінансові операції як для фізичних осіб, так і для суб'єктів господарювання.

Проте зростання частки онлайн-платежів, розширення каналів доступу до платіжної інфраструктури та ускладнення технологічних рішень водночас призводять до підвищення рівня загроз інформаційній та фінансовій безпеці. Кібершахрайство, витік персональних даних, атаки на платіжні шлюзи, фішингові кампанії та експлуатація вразливостей у мобільних застосунках – усе це ставить під сумнів стійкість та надійність банківських карткових систем.

Ситуація ускладнюється ще й тим, що нові ризики з'являються швидше, ніж формуються ефективні механізми їх виявлення та нейтралізації. Банківські установи змушені постійно адаптуватися, впроваджувати складні технології захисту, дотримуватися міжнародних стандартів безпеки, зберігаючи при цьому довіру користувачів і ефективність своїх послуг.

У зв'язку з цим виникає потреба в комплексному дослідженні сучасного стану безпеки платежів у цифровій економіці, з фокусом на банківський картковий бізнес як на одну з найбільш вразливих, але критично важливих складових фінансової інфраструктури.

Аналіз останніх досліджень і публікацій. У світлі зростання популярності цифрових платіжних інструментів безпека фінансових операцій стає предметом посиленої уваги з боку науковців та практиків. Останні публікації висвітлюють спектр новітніх викликів, з якими стикається банківський картковий бізнес. Зокрема, окремі аспекти порушеної у статті проблеми досліджують Т. Гордєєва [8], Р. Квасницька [8], Н. Матвійчук [15], Л. Свістун [16], Є. Сопін [13], А. Степаник [14], С. Теслюк [15], І. Форкун [8], Ю. Худолій [16] та інші.

Виділення недосліджених частин загальної проблеми. Попри велику кількість досліджень, актуальними залишаються питання формування інтегрованих стратегій протидії шахрайству, оцінювання ефективності застосованих технологій безпеки та забезпечення стійкості банківського карткового бізнесу в умовах стрімкої цифровізації.

Мета статті – провести комплексний аналіз стану безпеки банківського карткового бізнесу в цифровій економіці, ідентифікувати основні ризики, оцінити новітні технології захисту та розробити рекомендації щодо формування інтегрованих стратегій протидії загрозам.

Виклад основного матеріалу. Банківський картковий бізнес відіграє ключову роль у формуванні сучасної платіжної інфраструктури, забезпечуючи мільйони щоденних транзакцій у фізичному та цифровому середовищах. Активне впровадження безготівкових розрахунків, мобільного банкінгу та електронної комерції суттєво підвищує ефективність фінансової взаємодії, але водночас генерує нові загрози та ризики, які потребують системного аналізу та управління.

Сучасна практика функціонування платіжних систем демонструє, що банківські карткові операції підпадають під вплив широкого спектра факторів ризику, серед яких кіберзлочинність, технічні збої, недосконаліть регуляторного середовища, людський фактор тощо. З огляду на це виникає необхідність у комплексному підході до ідентифікації, структурування та типологізації таких ризиків.

Класифікація ризиків дає змогу систематизувати наявні загрози, виявити взаємозв'язки між ними, оцінити потенційний вплив на функціонування карткових платіжних систем та сформувати основу для розробки превентивних заходів і механізмів реагування. Зважаючи на багатогранність та динамічність ризиків, доцільно враховувати не лише технічні аспекти безпеки, але й організаційні, правові, економічні, поведінкові й соціальні чинники.

У табл. 1 представлено узагальнену класифікацію ризиків банківського карткового бізнесу, розроблену з урахуванням сучасних викликів цифрової економіки.

Загальна класифікація ризиків банківського карткового бізнесу дає змогу сформувати уявлення про їхню багатогранність і різнорідність за джерелами виникнення, характером впливу та іншими системоутворювальними ознаками. Водночас особливого аналітичного значення набуває диференціація ризиків за функціональною природою, оскільки вона безпосередньо пов'язана з операційними процесами банку та впливає на побудову системи внутрішнього контролю, інформаційної безпеки та стратегічного планування. У цьому контексті доцільно виокремити класифікацію ризиків за функціональними напрямами, яка дозволяє більш точно ідентифікувати джерела загроз та механізми їх нейтралізації (рис. 1).

Таблиця 1

Класифікація ризиків банківського карткового бізнесу

Класифікаційна ознака	Види ризиків	Характеристика
1	2	3
За джерелом виникнення	Внутрішні	Формуються в межах самого банку й пов'язані з людським фактором (помилки персоналу, службові зловживання), неефективною внутрішньою системою контролю, конфліктом інтересів, неправильним налаштуванням IT-систем, інсайдерськими атаками тощо.
	Зовнішні	Виникають унаслідок впливу зовнішнього середовища: шахрайських дій, змін у законодавстві, нестабільності ринку або технічних збоїв у партнерських структурах.
За характером впливу	Прямі	Безпосередньо призводять до фінансових втрат, наприклад, у разі несанкціонованого списання коштів через розкриття інформації про реквізити платіжних карток.
	Непрямі	Проявляються опосередковано, зокрема у вигляді втрати репутації або довіри з боку клієнтів.
За тривалістю впливу	Короткострокові	Мають миттєвий або тимчасовий характер (наприклад, технічні збої при здійсненні транзакцій).
	Довгострокові	Впливають на стратегічні перспективи розвитку банку (зокрема, втрата конкурентоспроможності через недостатній рівень інноваційності).
За ступенем реалізованості	Потенційні	Існують як загроза, але ще не призвели до негативних наслідків.
	Фактичні	Вже реалізувались і спричинили фінансові втрати або інші ускладнення.
За рівнем контрольованості	Керовані	Можуть бути знижені або усунені шляхом запровадження відповідних процедур управління, технологій захисту, навчання персоналу тощо.
	Некеровані	Не піддаються прямому впливу з боку банку, але потребують розробки сценаріїв адаптації або перенесення ризику (наприклад, через страхування)

Закінчення таблиці 1

1	2	3
За об'єктом впливу	Ризики для банку	Охоплюють загрози, що безпосередньо впливають на фінансову стійкість, ділову репутацію та юридичну відповідальність банківської установи (зловживання службовим становищем, інформаційні витоки, недотримання регуляторних вимог тощо)
	Ризики для клієнта	Стосуються безпеки персональних і фінансових даних, можливості безперебійного доступу до платіжних сервісів, а також якості обслуговування. Зокрема, клієнти можуть зазнати фінансових втрат унаслідок шахрайських дій або технічних збоїв у системах.
	Ризики для партнерів	Виявляються у порушенні або ускладненні договірних відносин з міжнародними платіжними системами, процесинговими центрами, фінтех-компаніями та іншими учасниками екосистеми (затримка розрахунків, невиконання зобов'язань тощо).

***Джерело**: удосконалено авторами на основі [9; 11].*

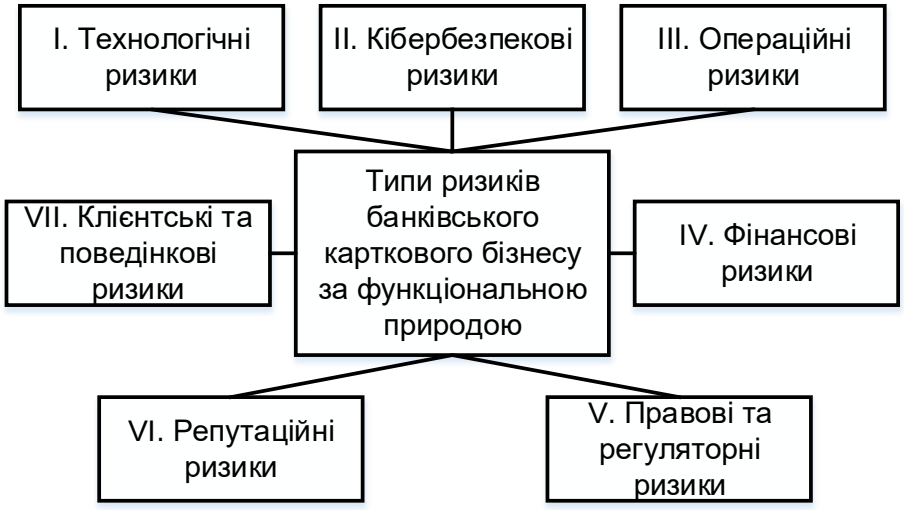

Рис. 1. Типи ризиків банківського карткового бізнесу за функціональною природою

***Джерело**: систематизовано авторами на основі [6; 7; 9; 11; 13; 14].*

Зростаюча залежність фінансових установ від складної цифрової інфраструктури зумовлює виникнення технологічних ризиків, що охоплюють збої в роботі апаратного забезпечення, нестабільність телекомунікаційних каналів, вразливості інформаційних систем, а також ризики втрати критичних даних через технічні або організаційні збої.

Вразливість банків до зовнішніх цифрових загроз посилює значущість кібербезпекових ризиків, які включають шахрайські дії (фішинг, скімінг, соціальна інженерія), несанкціоновані доступи, кібератаки, витоки персональних даних і недотримання міжнародних стандартів у сфері захисту інформації [6; 7].

Операційні ризики виникають переважно як наслідок внутрішніх помилок персоналу, неефективних процедур або неналежного контролю над аутсорсинговими процесами. Такі ризики загрожують як безперервності операційної діяльності, так і стабільності клієнтського обслуговування [9; 14].

У свою чергу, фінансові ризики проявляються як у формі прямого збитку внаслідок несанкціонованих транзакцій, так і у вигляді непрямих втрат, пов'язаних зі скороченням доходів через збої у функціонуванні сервісів, відтік клієнтів або зростання витрат на забезпечення безпеки. Значний вплив на ефективність карткових операцій чинять макрофінансові чинники, такі як валютні коливання та зміни регуляторних ставок.

Правові та регуляторні ризики зумовлені невідповідністю внутрішніх політик вимогам чинного законодавства, порушенням норм НБУ, директив ЄС (зокрема PSD2), стандартів PCI DSS або рекомендацій FATF. Окрім ризиків штрафних санкцій, банки також можуть зазнати судових позовів з боку клієнтів, партнерів або контролюючих органів. Не менш важливою є загроза правової невизначеності, яка виникає в умовах швидких змін нормативно-правової бази щодо цифрових фінансів [4].

Репутаційні ризики мають вторинний характер, однак можуть мати довготривалий вплив. Вони виникають у результаті широкого суспільного розголосу інцидентів, пов'язаних із порушенням безпеки, негативного інформаційного фону або партнерства з організаціями сумнівної репутації. Особливу увагу слід приділяти клієнтським та поведінковим ризикам, які формуються внаслідок низької цифрової грамотності користувачів, нехтування правилами кібергігієни, зловживання правами споживачів, а також недовіри до цифрових сервісів. Втрата довіри користувачів може мати прямі фінансові наслідки, а також стримувати впровадження інноваційних рішень у сфері платіжних технологій.

Таким чином, проаналізована класифікація ризиків у сфері банківського карткового бізнесу дозволяє систематизувати загрози, що виникають унаслідок як внутрішніх операційних чинників, так і зовнішніх. Проте варто зазначити, що характер і динаміка цих ризиків стрімко змінюються під впливом новітніх цифрових трансформацій. Саме технологічний прогрес формує нові підходи до управління ризиками, водночас породжуючи нові виклики.

Сучасний картковий банківський бізнес переживає глибоку трансформацію під впливом цифрових технологій. Традиційні моделі управління ризиками вже не гарантують належного рівня захисту в умовах зростаючої складності, динаміки та високотехнологічного характеру сучасних загроз. У відповідь на ці виклики фінансові установи впроваджують інноваційні рішення, які не лише посилюють здатність виявляти та запобігати шахрайству, а й забезпечують швидке реагування на інциденти безпеки. Серед ключових технологічних трендів варто виокремити застосування штучного інтелекту та машинного навчання, біометричної автентифі-

кації, хмарних рішень, а також технології блокчейн. Ці інструменти докорінно змінюють підходи до управління ризиками, формуючи нову парадигму безпеки в картковій індустрії.

Вагоме значення в оновленій архітектурі систем безпеки відіграють технології штучного інтелекту та машинного навчання, які суттєво розширюють можливості банків у сфері управління ризиками. Завдяки глибокому аналізу великих обсягів транзакційних даних ці інструменти дозволяють формувати точні та гнучкі моделі поведінки користувачів, що забезпечує оперативне виявлення нетипових дій. Інтелектуальні алгоритми здатні самостійно оновлюватися під впливом нових типів загроз, що дає змогу системам адаптуватися до змін без втручання людини. Такий підхід забезпечує перехід до моделі управління, що передбачає випереджальне виявлення загроз, значно підвищуючи ефективність захисту платіжної інфраструктури [1].

У контексті зростання загроз цифрового шахрайства дедалі важливішу роль у системах фінансової безпеки відіграють біометричні технології. Ідентифікація користувачів на основі фізіологічних ознак – відбитків пальців, розпізнавання обличчя або сканування райдужної оболонки ока – забезпечує підвищений рівень достовірності при доступі до платіжних сервісів. У банківських мобільних застосунках використання біометрії значно ускладнює несанкціонований доступ до персональних даних, що сприяє зниженню як операційних, так і шахрайських ризиків [5].

Стратегічним компонентом сучасних систем управління ризиками у фінансовому секторі виступає хмарна інфраструктура. Централізований доступ до великих обсягів даних дозволяє фінансовим установам швидко адаптувати аналітичні платформи до змін ринкового середовища без потреби у значних капіталовкладеннях в інфраструктуру. Хмарні рішення сприяють ефективному моніторингу транзакцій у реальному часі та злагодженій взаємодії структурних підрозділів банку. Це дає змогу вчасно виявляти підозрілі операції та реагувати на потенційні загрози.

У сфері карткових розрахунків впровадження блокчейн-технологій відкриває широкі перспективи для підвищення прозорості фінансових операцій та забезпечує надійний захист від змін у даних. Розподілена архітектура зберігання інформації забезпечує високий рівень довіри до транзакцій, оскільки будь-які модифікації автоматично реєструються і стають доступними для всіх учасників мережі. Такий підхід знижує ризик підробки операцій або несанкціонованого втручання в дані. Крім того, блокчейн може ефективно застосовуватись для верифікації контрагентів і як інструмент протидії легалізації доходів, отриманих злочинним шляхом [2].

Подальше посилення захисту платіжних систем в умовах цифровізації потребує не лише впровадження ізольованих інструментів, а й формування інтегрованої моделі безпеки, що поєднує технологічні, організаційні та регуляторні складові (рис. 2).

Запропонована інтегрована модель безпеки платіжних систем являє собою трирівневу та взаємопов'язану систему заходів, спрямованих на мінімізацію ризиків та забезпечення безпеки на всіх етапах здійснення платіжних операцій.

Рис. 2. Інтегрована модель безпеки платежів у цифровій економіці

***Джерело**: розроблено авторами на основі [3; 4; 10; 12].*

Рівень технологічних складових охоплює впровадження та підтримку сучасних технологічних рішень, спрямованих на захист інформації, запобігання кіберзагрозам та забезпечення безперебійного функціонування платіжної інфраструктури. Основні елементи включають [10]:

- криптографічні методи захисту, що передбачають використання надійного шифрування даних на всіх етапах їх передачі та зберігання. Наприклад, протоколи SSL/TLS для безпечного з'єднання, алгоритми симетричного (AES) та асиметричного (RSA) шифрування, цифрові сертифікати та хеш-функції;

- системи ідентифікації та автентифікації користувачів, які забезпечують надійне підтвердження особи при доступі до систем і виконанні транзакцій. До них належать багатофакторна автентифікація (MFA), біометричні технології (відбитки пальців, розпізнавання обличчя), токени та кваліфіковані електронні підписи;

- технології захисту мережевої інфраструктури, що включають впровадження міжмережевих екранів (firewalls), систем виявлення і запобігання вторгненням (IDS/IPS), а також логічну сегментацію мереж для ізоляції критичних зон і зменшення потенційного впливу атак;

- засоби захисту кінцевих пристроїв, що забезпечують безпеку комп'ютерів, мобільних пристроїв, платіжних терміналів (POS). До них належать антивірусне програмне забезпечення, системи управління доступом, а також шифрування даних на рівні пристрою;

- системи моніторингу та аналізу інформаційної безпеки, які базуються на використанні платформ SIEM (Security Information and Event Management) для централізованого збору, кореляції та аналізу подій безпеки, виявлення аномалій та оперативного реагування на інциденти в реальному часі;

- технології безпечної розробки програмного забезпечення, що включають інтеграцію практик Secure SDLC (Secure Software Development Life Cycle), зокрема статичного аналізу коду, тестування на вразливості, контролю змін, на всіх етапах створення платіжних застосунків для запобігання потенційним загрозам ще на етапі проєктування.

Рівень організаційних складових визначає систему внутрішніх правил, процесів і заходів, що забезпечують управління інформаційною безпекою на всіх етапах функціонування платіжних систем. Основні компоненти включають:

- політики та стандарти безпеки, що забезпечують формування єдиного нормативного середовища шляхом розробки, затвердження та впровадження чітких регламентів, інструкцій і протоколів дій у сфері захисту інформації;

- системи управління доступом, які передбачають реалізацію принципу найменших привілеїв, багаторівневу аутентифікацію та детальний контроль прав доступу до критичних систем, даних і ресурсів;

- підготовка та обізнаність персоналу, що реалізується через систематичне навчання, моделювання кіберзагроз, тестування на фішинг та інші тренінгові заходи з метою формування культури безпеки серед працівників;

- управління ризиками інформаційної безпеки, яке включає в себе процеси виявлення, оцінки, пріоритизації та мінімізації ризиків із застосуванням сучасних методологій та інструментів (наприклад, ISO/IEC 27005) [3];

- управління інцидентами безпеки, що базується на впровадженні структурованих планів реагування, включаючи швидке виявлення загроз, їх ізоляцію, усунення наслідків та аналіз інцидентів для запобігання повторенню [12];

- плани безперервності бізнесу, які гарантують збереження ключових функцій організації навіть у разі критичних порушень, з обов'язковим тестуванням і оновленням сценаріїв реагування;

- аудит та оцінка стану безпеки, що передбачають проведення внутрішніх і зовнішніх перевірок для виявлення недоліків, перевірки відповідності політикам та вдосконалення системи захисту на основі отриманих результатів.

Рівень регуляторних складових передбачає дотримання чинних норм, вимог і стандартів, встановлених як національним, так і міжнародним законодавством у сфері безпеки платіжної інфраструктури. Ключові напрями включають:

- виконання законодавчих вимог, що охоплює суворе дотримання нормативно-правових актів у сферах платіжних послуг, кібербезпеки, захисту персональних даних та критичної інфраструктури;

- сертифікація та відповідність стандартам, яка передбачає впровадження та підтримку міжнародно визнаних стандартів, зокрема PCI DSS, ISO/IEC 27001 та інших, що гарантують високий рівень інформаційної безпеки [3; 4];

- інституційна взаємодія з регуляторами, що включає активну комунікацію з центральними банками, кібербезпековими органами та профільними асоціаціями для обміну інформацією, запобігання загрозам та координації дій;

- оперативне звітування про інциденти, яке забезпечує своєчасне подання звітності про виявлені порушення та інциденти відповідно до встановлених процедур і строків;

- гнучкість і адаптивність до змін регуляторного середовища, що проявляється у постійному моніторингу нових вимог, змін до законодавства, а також у своєчасному оновленні політик і процедур компанії.

Впровадження інтегрованої моделі кібербезпеки, у якій ефективність кожного окремого елементу підсилюється завдяки взаємодії з іншими, дозволяє створити цілісну, взаємозалежну систему захисту платіжної інфраструктури. Такий підхід не лише забезпечує здатність оперативно реагувати на актуальні загрози, а й формує основу для проактивного протистояння новим викликам у сфері інформаційної безпеки. У результаті це сприяє підвищенню стійкості, стабільності та рівня довіри до банківського карткового бізнесу в умовах стрімкої цифровізації та зростаючих кіберризиків.

Надійний захист платіжних систем не обмежується лише впровадженням сучасних технологій. Важливо постійно перевіряти, наскільки ці рішення дійсно ефективні. Системне оцінювання заходів кібербезпеки дозволяє вчасно виявляти слабкі місця, покращувати стратегії захисту та приймати обґрунтовані управлінські рішення.

Для цього використовують кількісні та якісні показники, що дозволяють оцінити як технічну ефективність (здатність системи виявляти та зупиняти загрози), так і економічну доцільність (чи виправдовують витрати отримані результати).

До ключових показників ефективності належать:

- рівень виявлення шахрайських дій – скільки потенційно небезпечних операцій було успішно ідентифіковано та заблоковано;

- кількість помилкових спрацювань – як часто система помилково розпізнає безпечні транзакції як загрозливі;

- середній час реагування на інцидент – як швидко команда безпеки виявляє, аналізує та нейтралізує загрозу;

- співвідношення витрат на безпеку до збережених активів – наскільки ефективними є інвестиції в кіберзахист;

- рівень довіри користувачів – наскільки безпека системи впливає на лояльність клієнтів та їхнє відчуття захищеності.

Для глибшого аналізу ефективності використовуються аудити інформаційної безпеки, методи оцінювання ризиків та симульовані атаки, що дозволяють протестувати систему в умовах, наближених до реальних.

Важливу роль у цьому процесі відіграє залучення зовнішніх експертів, які проводять неупереджене оцінювання поточного стану безпеки. До таких методів належать: по-перше, моделювання цілеспрямованої атаки з метою виявлення вразливостей, які може використати реальний зловмисник, по-друге, комплексна перевірка, що включає технічні атаки та аналіз дій персоналу, щоб оцінити загальну стійкість системи. Такі перевірки дозволяють виявити приховані ризики, які можуть залишитися непоміченими під час стандартних внутрішніх аудитів.

У підсумку, регулярне оцінювання ефективності системи безпеки є не просто рекомендованим, а необхідним кроком для платіжних систем, що прагнуть бути стійкими до загроз. Це дозволяє оптимізувати витрати, підвищити рівень захисту й зберегти довіру клієнтів навіть у нестабільному цифровому середовищі.

Після оцінювання ефективності безпекових заходів наступним ключовим аспектом стає побудова стійкої інфраструктури, здатної забезпечити безперервне функціонування банківських карткових систем навіть у кризових умовах. Під стійкістю у цьому контексті розуміється здатність системи протистояти як зовнішнім (кібератаки, перебої в інфраструктурі), так і внутрішнім (збій програмного забезпечення, людські помилки) деструктивним факторам, при цьому гарантуючи цілісність та безпечність транзакцій, конфіденційність даних користувачів, доступність сервісів для клієнтів у режимі 24/7.

У добу цифрової трансформації та зростання залежності від електронних каналів обслуговування стійкість системи набуває вирішального значення для репутації, надійності та конкурентоспроможності банку. До основних компонентів забезпечення стійкості належать:

- плани безперервності бізнесу, які передбачають сценарії дій у випадку порушення критичних функцій банку;

- плани реагування на інциденти – чітко визначені кроки з локалізації, усунення та аналізу кіберінцидентів;

- резервування інфраструктури – використання дублюючих серверів, незалежних дата-центрів та альтернативних каналів зв’язку, які можуть бути активовані в разі відмови основних систем;

- засоби швидкого відновлення – технології та автоматизовані механізми повернення до стабільного стану після інциденту;

- адаптивні моделі безпеки, що дозволяють системі гнучко підлаштовуватись під динамічне загрозливе середовище, впроваджуючи оновлення політик, фільтрів та поведінкових механізмів у реальному часі.

Окрему увагу слід приділити галузевій співпраці. Банки, як елементи спільного фінансового простору, не можуть діяти ізольовано. Обмін інформацією про інциденти, спільні розслідування кіберзагроз, участь у міжбанківських ініціативах з кібербезпеки створюють колективну цифрову оборону, підвищуючи інституційну витривалість усієї банківської екосистеми.

У результаті, саме поєднання стратегічного планування, оперативного реагування, адаптивних технологій і міжорганізаційної координації формує нову парадигму забезпечення стійкості банківського карткового бізнесу. Такий підхід дозволяє ефективно функціонувати навіть в умовах кризи, залишаючись надійним партнером для мільйонів клієнтів.

Висновки і пропозиції. Банківський картковий бізнес у сучасних умовах цифрової економіки зазнає глибоких трансформацій, зумовлених активною інтеграцією фінансових технологій, зростанням обсягів безготівкових розрахунків та зміною поведінки споживачів. З одного боку, це відкриває нові можливості для оптимізації платіжних процесів, підвищення їхньої швидкості, зручності та доступності, а з іншого – суттєво ускладнює структуру ризиків, зокрема тих, що пов’язані з інформаційною та кібербезпекою.

У цьому контексті безпека платежів постає як критичний фактор стабільного функціонування банківського карткового бізнесу, який має розглядатися як багаторівнева та інтегрована система, що поєднує в собі не лише технічні засоби захисту (криптографічні протоколи, штучний інтелект, біометрію), а й ефективне управління ризиками, стандартизацію процесів, організаційну культуру кібергігієни та правове регулювання відповідно до міжнародних вимог.

Особливої актуальності набуває розробка та впровадження адаптивних стратегій управління ризиками, здатних динамічно реагувати на новітні загрози – від фішингових атак і зловживань у сфері соціальної інженерії до вразливостей у мобільних та хмарних платформах.

Крім того, формування платіжної безпеки в цифровій економіці неможливе без інвестування у цифрову грамотність користувачів, підвищення їхньої обізнаності щодо потенційних загроз, механізмів захисту даних та безпечної поведінки у платіжному середовищі.

З огляду на швидкі темпи розвитку фінтех-сектору, подальші наукові дослідження мають бути зосереджені на створенні кількісних моделей оцінювання ефективності систем захисту платіжних операцій; аналізі інституційної спроможності банків до впровадження інноваційних механізмів кібербезпеки; дослідженні асиметрії інформації між учасниками платіжного ринку як джерела нових ризиків; вивченні взаємодії цифрових платформ, платіжних сервісів та регуляторних органів у забезпеченні стійкості до кіберзагроз тощо.

Отже, безпека платежів у цифровій економіці вимагає системного, міждисциплінарного підходу та постійної адаптації до нових технологічних і поведінкових викликів, які постають перед банківським картковим бізнесом.

Список використаних джерел

1. Arizu A. AI vs. Traditional Risk Models: Why Machine Learning is the Future of Payment Security [Electronic resource] / A. Arizu // Argoz Consultants. – 2025. – Accessed mode: https://argozconsultants.com/blog/ai-the-future-of-payment-security.

2. Exploring the Future of Blockchain Technology in Securing Digital Transactions [Electronic resource]. – 2025. – Accessed mode: https://community.nasscom.in/communities/blockchain/exploring-future-blockchain-technology-securing-digital-transactions.

3. ISO/IEC 27005, NIST RMF. Що таке управління ризиками інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://surl.li/vunkln.

4. PCI DSS – міжнародні стандарти безпеки даних індустрії платіжних карток vs національне законодавство [Електронний ресурс] // Юридична газета. – 28 лютого 2024. – Режим доступу: https://yur-gazeta.com/publications/practice/bankivske-ta-finansove-pravo/pci-dss--mizhnarodni-standarti-bezpeki-danih-industriyi-platizhnih-kartok-vs-nacionalne-zakonodavstv.html.

5. Strobel A. Biometric payment cards: The next evolution in secure contactless transactions [Електронний ресурс]. – 2022. – Режим доступу: https://thepaypers.com/expert-opinion/biometric-payment-cards-the-next-evolution-in-secure-contactless-transactions.

6. Віннікова І. І. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними [Електронний ресурс] / І. І. Віннікова, С. В. Марчук // Східна Європа: економіка, бізнес та управління. – 2018. – № 5(16). – С. 110-114. – Режим доступу: https://www.easterneurope-ebm.in.ua/ journal/16_2018/21.pdf.

7. Зростання важливості кібербезпеки в платіжній індустрії [Електронний ресурс]. – Режим доступу: https://paysaxas.com/uk/zrostannya-vazhlyvosti-kiberbezpeky-v-platizhnij-industriyi.

8. Квасницька Р. Сучасні підходи забезпечення інформаційної безпеки платіжних систем та їх кіберзахисту [Електронний ресурс] / Р. Квасницька, І. Форкун, Т. Гордєєва // Вісник Хмельницького національного університету. – 2022. – № 5, т. 1. – С. 47-52. – Режим доступу: https://elar.khmnu.edu.ua/handle/123456789/12637.

9. Павленко Л. Д. Ризики банків України та організаційна система управління ними в умовах воєнного стану [Електронний ресурс] / Л. Д. Павленко, О. А. Криклій, О. В. Чумак // Інвестиції: практика та досвід. – 2024. – № 15. – С. 126-132. – Режим доступу: https://nayka.com.ua/index.php/investplan/article/view/3186/3222.

10. Пелюх О. І. Сучасні загрози інформаційно-комунікаційним системам та методи захисту від них [Електронний ресурс] / О. І. Пелюх, М. В. Єсіна, Д. Ю. Голубничий // Радіотехніка. – 2024. – № 216. – С. 46-56. – Режим доступу: http://rt.nure.ua/article/view/304698/296532.

11. Система ризик-менеджменту в банках: теоретичні та методологічні аспекти: монографія / за ред. В. В. Коваленко. – Одеса : ОНЕУ, 2017. – 304 с.

12. Система управління інцидентами та подіями [Електронний ресурс]. – Режим доступу: https://metinvest.digital/ua/page/959.

13. Сопін Є. Основні комплаєнс ризики надавача платіжних послуг в умовах цифрової економіки [Електронний ресурс] / Є. Сопін // Актуальні проблеми економіки. – 2019. – № 7 (217). – С. 142-157. – Режим доступу: https://eco-science.net/wp-content/uploads/2019/07/7_2019_142-157.pdf.

14. Степаник А. О. Управління операційним ризиком карткового бізнесу банку / А. О. Степаник // Економіка, менеджмент та аудит: сучасні проблеми, перспективи та напрями розвитку: Матеріали міжнародної науково-практичної конференції (Львів, 31 травня 2019 року) / ГО «Львівська економічна фундація». – Львів : ЛЕФ, 2019. – С. 130-132.

15. Теслюк С. Фінансова безпека банківських установ в умовах цифровізації [Електронний ресурс] / С. Теслюк, Н. Матвійчук, А. Левчук // Економіка та суспільство. – 2024. – № (60). – Режим доступу: https://economyandsociety.in.ua/index.php/journal/article/view/3646/3575.

16. Худолій Ю. Сучасні тенденції FinTech та їх вплив на безпеку банківських установ [Електронний ресурс] / Ю. Худолій, Л. Свістун // Економіка і регіон. – 2021. – № 3 (82). – С. 115-123. – Режим доступу: https://journals.nupp.edu.ua/eir/article/ view/2375/1844.

References

1. Arizu, A. (2025). AI vs. Traditional Risk Models: Why Machine Learning is the Future of Payment Security. Argoz Consultants. https://argozconsultants.com/blog/ai-the-future-of-payment-security.

2. Exploring the Future of Blockchain Technology in Securing Digital Transactions. (n.d.). https://community.nasscom.in/communities/blockchain/exploring-future-blockchain-technology-securing-digital-transactions.

3. ISO/IEC 27005, NIST RMF. What is Information Security Risk Management? [ISO/IEC 27005, NIST RMF. Shcho take upravlinnia ryzykamy informatsiinoi bezpeky]. (n.d.). https://surl.li/vunkln.

4. PCI DSS – mizhnarodni standarty bezpeky danykh industrii platizhnykh kartok vs natsionalne zakonodavstvo [PCI DSS – International Payment Card Industry Data Security Standards vs National Legislation]. (February 28, 2024). *Yurydychna hazeta – Legal newspaper.* https://yur-gazeta.com/publications/practice/bankivske-ta-finansove-pravo/pci-dss--mizhnarodni-standarti-bezpeki-danih-industriyi-platizhnih-kartok-vs-nacionalne-zakonodavstv.html.

5. Strobel, A. (2022). *Biometric payment cards: The next evolution in secure contactless transactions*. https://thepaypers.com/expert-opinion/biometric-payment-cards-the-next-evolution-in-secure-contactless-transactions.

6. Vinnikova, I. I., & Marchuk, S. V. (2018). Kiber-ryzyky yak odyn iz vydiv suchasnykh ryzykiv u diialnosti maloho ta serednoho biznesu ta upravlinnia nymy [Cyber Risks as One of the Modern Types of Risks in Small and Medium Business and Their Management]. *Skhidna Yevropa: ekonomika, biznes ta upravlinnia – Eastern Europe: Economy, Business and Management, 5*(16), 110–114. https://www.easterneurope-ebm.in.ua/journal/16_2018/21.pdf.

7. Zrostannia vazhlyvosti kiberbezpeky v platizhnii industrii [Growing Importance of Cybersecurity in the Payment Industry]. (2024). https://paysaxas.com/uk/zrostannya-vazhlyvosti-kiberbezpeky-v-platizhnij-industriyi.

8. Kvasnytska, R., Forkun, I., & Hordiieva, T. (2022). Suchasni pidkhody zabezpechennia informatsiinoi bezpeky platizhnykh system ta yikh kiberzakhystu [Modern Approaches to Ensuring Information Security of Payment Systems and Their Cyber Protection]. *Visnyk Khmelnytskoho Natsionalnoho Universytetu – Bulletin of Khmelnytskyi National University, 5*(1), 47–52. https://elar.khmnu.edu.ua/handle/ 123456789/12637.

9. Pavlenko, L. D., Krykliy, O. A., & Chumak, O. V. (2024). Ryzyky bankiv Ukrainy ta orhanizatsiina systema upravlinnia nymy v umovakh voiennoho stanu [Risks of Ukrainian Banks and the Organizational System for Their Management Under Martial Law]. *Investytsii: praktyka ta dosvid – Investments: Practice and Experience, 15*, 126–132. https://nayka.com.ua/index.php/investplan/article/view/3186/3222

10. Peliukh, O. I., Yesina, M. V., & Holubnychyi, D. Yu. (2024). Suchasni zahrozy informatsiino-komunikatsiinym systemam ta metody zakhystu vid nykh [Modern Threats to Information and Communication Systems and Methods of Protection]. *Radiotekhnika – Radiotechnics, 216*, 46–56. http://rt.nure.ua/article/view/304698/296532.

11. Kovalenko, V. V. (2017). *Systema ryzyk-menedzhmentu v bankakh: teoretychni ta metodolohichni aspekty [Risk Management System in Banks: Theoretical and Methodological Aspects]*. ONEU.

12. Systema upravlinnia intsydentamy ta podiiamy [Incident and Event Management System]. (n.d.). https://metinvest.digital/ua/page/959.

13. Sopin, Ye. (2019). Osnovni komplaiens ryzyky nadavacha platizhnykh posluh v umovakh tsyfrovoi ekonomiky [Key Compliance Risks of Payment Service Providers in the Digital Economy]. *Aktualni problemy ekonomiky – Actual Problems of Economics, 7*(217), 142–157. https://eco-science.net/wp-content/uploads/2019/07/ 7_2019_142-157.pdf.

14. Stepanyk, A. O. (2019). Upravlinnia operatsiinym ryzykom kartkovoho biznesu banku [Operational Risk Management of Bank Card Business]. In *Economy, Management and Audit: Current Problems, Prospects and Directions of Development: Proceedings of the International Scientific and Practical Conference* (Lviv, May 31, 2019) (pp. 130–132). Lviv Economic Foundation.

15. Tesliuk, S., Matviichuk, N., & Levchuk, A. (2024). Finansova bezpeka bankivskykh ustanov v umovakh tsyfrovizatsii [Financial Security of Banking Institutions in the Context of Digitalization]. *Ekonomika ta suspilstvo – Economy and Society,* (60). https://economyandsociety.in.ua/index.php/journal/article/view/3646/3575.

16. Khudolii, Yu., & Svistun, L. (2021). Suchasni tendentsii FinTech ta yikh vplyv na bezpeku bankivskykh ustanov [Modern FinTech Trends and Their Impact on the Security of Banking Institutions]. *Ekonomika i rehion – Economy and Region, 3*(82), 115–123. https://journals.nupp.edu.ua/eir/article/view/2375/1844

Отримано 21.05.2025

UDC 336.717
JEL Classification: G21; E42; O33

Artem Tarasenko

PhD in Economics, Doctoral Student of the Department of Finance, Banking and Insurance
Chernihiv National University of Technology (Chernihiv, Ukraine)
E-mail: avtarasenko88@gmail.com. **ORCID:** https://orcid.org/0000-0003-4395-3605

Artur Zhavoronok

PhD in Economics, Associate Professor, Associate Professor
of the Department of Public, Corporate Finance and Financial Intermediation
Yuriy Fedkovych Chernivtsi National University (Chernivtsi, Ukraine)
E-mail: artur.zhavoronok@ukr.net. **ORCID:** https://orcid.org/0000-0001-9274-8240

Volodymyr Suhovetskyy

PhD Student of the Department of Finance, Banking and Insurance
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: moskalyura73@gmail.com. **ORCID:** https://orcid.org/0009-0007-7585-9505

PAYMENT SECURITY IN THE DIGITAL ECONOMY: CHALLENGES FOR THE BANKING CARD BUSINESS

Abstract. *The article systematizes the main risks inherent in the bank card business based on a multifactor classification. It is established that cyber risks are the most dangerous in the context of digital transformation, as they are characterized by high dynamics, detection complexity, and significant potential damage. The necessity of*

shifting the focus in the security system from reactive incident response to proactive monitoring and threat prevention through the implementation of modern digital technologies is substantiated.

Promising directions for innovative security enhancement are identified, with the most effective being: the use of artificial intelligence and machine learning algorithms for user behavior analysis, anomaly detection, and real-time fraud prevention; biometric authentication, which significantly reduces the risk of unauthorized access to accounts and personal data; the use of cloud platforms, which provide centralized management, scalability of security mechanisms, and rapid updates of protection tools; blockchain technology, which enhances the transparency, reliability, and immutability of transactions and promotes the creation of decentralized verification systems.

The necessity of forming an integrated information security strategy that combines technical, organizational, and regulatory tools is justified. The article highlights approaches to assessing the effectiveness of implemented measures and identifies the key security performance indicators: fraud detection rate; number of false positives; average incident response time; ratio of security costs to preserved assets; and the level of user trust.

Particular attention is paid to the importance of a resilient payment infrastructure capable of ensuring the continuity of banking operations even under crisis conditions. Emphasis is placed on the significance of industry-wide cooperation as a factor in enhancing the digital resilience of the financial sector.

Key words: *banking card business; digital economy; risks; cyber threats; information security; innovative technologies; artificial intelligence; biometrics; blockchain.*

Fig.: 2. Table: 1. References: 16.

Бібліографічний опис для цитування:

Тарасенко А. В., Жаворонок А. В., Суховецький В. К. Безпека платежів у цифровій економіці: виклики для банківського карткового бізнесу. *Науковий вісник Полісся*. 2025. № 1(30). С. 233-247. DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-233-247.