УДК 336.71:004.056.5
DOI: https://doi.org/10.30838/EP.207.18-24

Козій Н.С.
кандидат економічних наук
Державний податковий університет
Koziy Natalia
PhD in Economic Sc.
State Tax University
https://orcid.org/0000-0001-8230-2974

Семенова О.В.
Державний податковий університет
Semenova Oleksandra
State Tax University
https://orcid.org/0009-0002-7504-7906

Герман Я.І.
Державний податковий університет
Herman Yana
State Tax University
https://orcid.org/0009-0002-5377-5953

БЕЗПЕКА ЦИФРОВИХ ПЛАТІЖНИХ СЕРВІСІВ У БАНКІВСЬКОМУ СЕКТОРІ: ВИКЛИКИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

У статті проаналізовано сучасний стан безпеки цифрових платіжних сервісів у банківському секторі України. Визначено основні загрози кібербезпеці, серед яких фішингові атаки, витік персональних даних, DDoS-атаки та шахрайські операції з платіжними картками. Окреслено тенденції зростання частки безготівкових операцій і кількості користувачів мобільного банкінгу, що підвищує значущість надійного захисту електронних транзакцій. Обґрунтовано необхідність комплексного підходу до кіберзахисту банків, який поєднує технічні, правові та організаційні заходи. Запропоновано шляхи вдосконалення безпеки цифрових платіжних систем: запровадження багатофакторної автентифікації, моніторинг транзакцій на основі аналітики великих даних, адаптація міжнародних стандартів безпеки та підвищення цифрової грамотності клієнтів.

Ключові слова: *цифрові платіжні сервіси, банківський сектор, кібербезпека, безготівкові операції, фінансові технології.*

SECURITY OF DIGITAL PAYMENT SERVICES IN THE BANKING SECTOR: CHALLENGES AND WAYS FOR IMPROVEMENT

This article investigates the current state of digital payment service security in the Ukrainian banking sector, focusing on the challenges, threats, and potential methods for enhancement. The study identifies key cybersecurity risks, including phishing attacks, data breaches, DDoS attacks, malware, insider threats, API vulnerabilities, and fraudulent operations with payment cards. The analysis emphasizes the rapid growth of cashless transactions, the increase in payment cards issued, and the rising number of mobile banking users, highlighting the critical importance of reliable and resilient protection for electronic financial operations. The research examines the necessity of a comprehensive cybersecurity approach, which integrates technical solutions, organizational measures, legal regulations, and managerial practices. Technical improvements include the use of multi-factor authentication, encryption, secure communication channels, AI-driven transaction monitoring, machine learning for anomaly detection, timely software patching, and resilient IT infrastructure with geographically distributed backup centers. Organizational measures focus on staff training, access control policies, regular internal audits, and security governance to reduce human errors and enhance operational stability. Legal and regulatory measures ensure compliance with national and international standards, including ISO 27001, and facilitate coordination among banks, regulators, and technology providers. The study presents practical examples of cyber incidents in Ukraine from 2022 to 2024, demonstrating how phishing, DDoS attacks, malware, and

ISSN друкованої версії: 2224-6282
ISSN електронної версії: 2224-6290

social engineering have targeted major banks, resulting in compromised accounts, service disruptions, and data leaks. The article concludes that strengthening digital payment security is essential for maintaining financial stability, building customer trust, and ensuring the continuity of banking operations under crisis or wartime conditions. Proactive strategies combining technological innovation, regulatory alignment, organizational readiness, and client education are crucial for minimizing risks, enhancing cyber resilience, and ensuring the sustainable development of digital banking services in Ukraine.

Keywords: *digital payment services, banking sector, cybersecurity, cashless transactions, financial technologies.*

JEL classification: *G21, G28, E42.*

Постановка проблеми. У сучасних умовах стрімкої цифровізації фінансового сектору питання безпеки цифрових платіжних сервісів набуває особливої значущості. Банківські установи дедалі активніше впроваджують інноваційні технології — мобільні додатки, інтернет-банкінг, безконтактні платежі, системи миттєвих переказів — що підвищує зручність та швидкість фінансових операцій, але водночас створює нові ризики кіберзагроз. Зростання кількості кібератак, фішингових схем, витоку даних та шахрайських операцій вимагає від банків посилення систем захисту інформації, удосконалення механізмів аутентифікації клієнтів та впровадження міжнародних стандартів безпеки. Саме тому дослідження проблем безпеки цифрових платіжних сервісів є актуальним і має важливе практичне значення для забезпечення стабільності банківської системи та довіри користувачів до електронних фінансових інструментів.

Аналіз останніх досліджень та публікацій. Проблематика безпеки цифрових платіжних сервісів відображено у працях багатьох вітчизняних та зарубіжних науковців, які досліджують вплив цифровізації на стабільність банківської системи, захист даних і довіру клієнтів. Зокрема, у своїх роботах питання інформаційної безпеки, кіберзагроз і цифрових ризиків у фінансовому секторі розглядають такі науковці, як Гончаренко А.В., Гордєєва Т., Данік Н., Квасницька Р., Криклій О.А., Мельник О.В., Павленко Л.Д., Пелюх О.І., Торлопов А., Форкун І., та інші. Їхні праці зосереджені на аналізі механізмів кіберзахисту, впровадженні інноваційних технологій у платіжних системах, а також на формуванні нормативної бази для забезпечення безпеки цифрових фінансових послуг.

Водночас, потребують подальшого вивчення питання удосконалення систем моніторингу транзакцій, розвитку національної політики кіберзахисту банків та адаптації міжнародних стандартів безпеки до українських реалій.

Мета статті полягає у дослідженні основних викликів безпеки цифрових платіжних сервісів у банківському секторі України під час війни та визначення практичних шляхів їх вдосконалення з урахуванням сучасних технологій та кризових умов. Для досягнення мети застосовано аналітичний, системний та порівняльний методи дослідження.

Виклад основних результатів дослідження. Цифровізація банківських послуг у сучасному світі є ключовим чинником розвитку фінансового сектору. В Україні процес діджиталізації значно прискорився в умовах війни, коли безконтактні та дистанційні платіжні сервіси стали життєво необхідними для забезпечення фінансової стабільності населення та бізнесу. Водночас війна створила нові виклики для безпеки платіжних сервісів, підвищивши ризики кіберзлочинності, кібератак на фінансову інфраструктуру та спроби шахрайства.

Сутність безпеки цифрових платіжних сервісів розкривається через погляди та трактування різних науковців, які визначають основні принципи захисту фінансових даних та транзакцій.

Гончаренко А.В. визначає безпеку цифрових платіжних сервісів як комплекс організаційних, технічних та правових заходів, що спрямовані на захист фінансових транзакцій і персональних даних користувачів від несанкціонованого доступу, шахрайства та кібератак [2, с. 36].

Науковці Данік Н., Торлопов А. розглядають безпеку цифрових платіжних сервісів як сукупність технологічних та управлінських заходів, які забезпечують надійність електронних транзакцій, запобігають шахрайству та кіберзлочинам, а також гарантують права користувачів фінансових послуг [2, с. 101].

Автори Квасницька Р., Форкун І., Гордєєва Т. визначають безпеку цифрових платіжних систем як здатність платіжної інфраструктури підтримувати стабільну роботу, захищати дані клієнтів та відповідати нормативно-правовим вимогам у цифровому середовищі [3, с. 48].

Національний банк України визначає безпеку цифрових платіжних послуг як забезпечення конфіденційності, цілісності, доступності та автентичності інформації та платіжних операцій у банківських системах [5].

У міжнародній практиці Basel Committee on Banking Supervision, безпека цифрових платіжних сервісів трактується як здатність інформаційної системи банку протистояти кіберзагрозам, підтримувати стабільність і безперервність фінансових операцій та мінімізувати ризики втрат для клієнтів і самої установи [13].

Узагальнивши наведені трактування вище, безпека цифрових платіжних сервісів — це комплекс технічних, організаційних, правових та управлінських заходів, спрямованих на захист фінансових транзакцій і персональних даних користувачів, забезпечення надійності та стійкості платіжної інфраструктури, підтримку конфіденційності, цілісності, доступності й автентичності інформації, а також протидію кіберзагрозам і мінімізацію ризиків для клієнтів і банківських установ.

Цифрові платіжні сервіси в банківському секторі являють собою комплекс електронних інструментів і технологій, що забезпечують проведення фінансових

операцій без використання готівки. Вони включають онлайн-банкінг, мобільні додатки, електронні платіжні системи, карткові розрахунки, а також інтегровані фінтех-рішення для здійснення транскордонних платежів. Основними характеристиками цифрових платіжних сервісів є швидкість, доступність у режимі 24/7, автоматизація процесів та інтеграція з іншими фінансовими та нефінансовими платформами [4, с. 112].

У банківській практиці цифрові платіжні сервіси забезпечують ефективність обробки транзакцій, зменшення операційних витрат, підвищення якості обслуговування клієнтів та розширення спектру фінансових послуг. При цьому розвиток цифрових сервісів супроводжується підвищеними вимогами до безпеки, захисту персональних даних, кіберзахисту та відповідності законодавчим і нормативним стандартам. Системи цифрових платежів у банківському секторі відіграють ключову роль у формуванні довіри клієнтів, забезпеченні фінансової стабільності та інтеграції банківських послуг у глобальну цифрову економіку.

Безпека цифрових платіжних сервісів у банківському секторі охоплює комплекс заходів, спрямованих на захист фінансових операцій, інформаційних систем та персональних даних клієнтів у процесі електронних розрахунків. Вона включає технічні рішення, організаційні механізми та правові регламентації, що забезпечують конфіденційність, цілісність, доступність та автентичність інформації. У банківському секторі безпека цифрових платежів передбачає:

1) технічний аспект, який охоплює використання криптографії, багатофакторної автентифікації, шифрування даних, захищених каналів передачі інформації та сучасних систем моніторингу транзакцій для виявлення шахрайських операцій у режимі реального часу;

2) організаційний аспект, що включає політики безпеки банку, процедури управління доступом, навчання персоналу, контроль за дотриманням правил роботи з платіжними системами та регулярний аудит внутрішніх процесів [7, с. 131];

3) правовий аспект, який передбачає відповідність банківських цифрових систем нормативним актам, законодавству про платіжні послуги та захист персональних даних, а також дотримання міжнародних стандартів кібербезпеки та фінансової стабільності [11, с. 49].

В умовах сучасної цифровізації та розвитку фінтех-технологій безпека цифрових платіжних сервісів стає критичною для підтримки довіри клієнтів, стабільності банківської системи та забезпечення безперервності фінансових операцій навіть у кризових або воєнних умовах. Ефективна система безпеки дозволяє протидіяти кіберзагрозам, мінімізувати фінансові ризики та забезпечити надійність та стійкість банківської інфраструктури.

Цифрові платіжні сервіси (інтернет-банкінг, мобільні додатки, безконтактні платежі, електронні гаманці та системи на кшталт BankID) стали ключовим елементом банківського сектору України в умовах воєнного стану та прискореної діджиталізації. За останні роки спостерігається істотне зростання частки безготівкових операцій та кількості платіжних карток у банківському секторі (рис. 1), що відображає прискорену цифровізацію фінансових послуг. Водночас активізація цифрових розрахунків супроводжується збільшенням кіберзагроз, зокрема, атак, пов'язаних із гібридною війною, фішингом та DDoS-атаками, що підкреслює необхідність удосконалення заходів кібербезпеки та захисту цифрових платіжних систем.

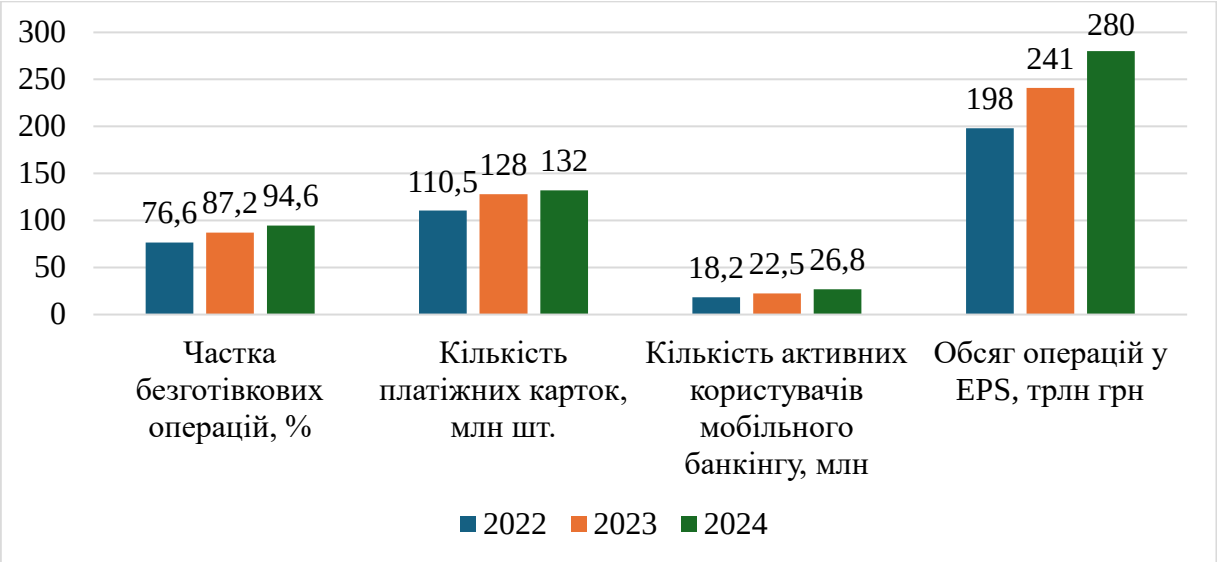

Рис. 1 Динаміка діджиталізації платіжних операцій
Джерело: складено на основі даних НБУ [5].

Відповідно до рис. 1 у період 2022–2024 рр. спостерігається стабільне зростання частки безготівкових операцій у банківському секторі України — з 76,6 % у 2022 році до 94,6 % у 2024 році, що свідчить про активну цифровізацію фінансових розрахунків та підвищення ролі електронних платіжних інструментів. Кількість платіжних карток зросла з 110,5 млн у 2022 році до 132 млн у 2024 році, що відображає збільшення

доступності банківських послуг та розширення платіжної інфраструктури. Паралельно зростає кількість активних користувачів мобільного банкінгу — з 18,2 млн у 2022 році до 26,8 млн у 2024 році, що демонструє підвищення популярності мобільних фінансових сервісів та зміщення користувачів у бік дистанційного обслуговування. Обсяг операцій у Єдиній платіжній системі (EPS) збільшився з 198 трлн грн у 2022 році до 280 трлн грн у 2024 році, що відображає зростання активності фінансових транзакцій та ефективність безготівкових розрахунків у національному масштабі. Загалом, наведені дані свідчать про тенденцію до інтенсивної цифровізації фінансового сектору, підвищення рівня доступності банківських послуг та зростання довіри населення до безготівкових та мобільних платіжних технологій.

У сучасних умовах цифровізації фінансових послуг банківський сектор стає все більш вразливим до кіберзагроз, що потребує системного аналізу та класифікації можливих атак. Розподіл типів кібератак на банківську систему (рис. 2) дозволяє визначити основні напрямки загроз, їхні методи та потенційні наслідки для безпеки фінансових операцій, захисту персональних даних клієнтів та стабільності роботи банківських установ.

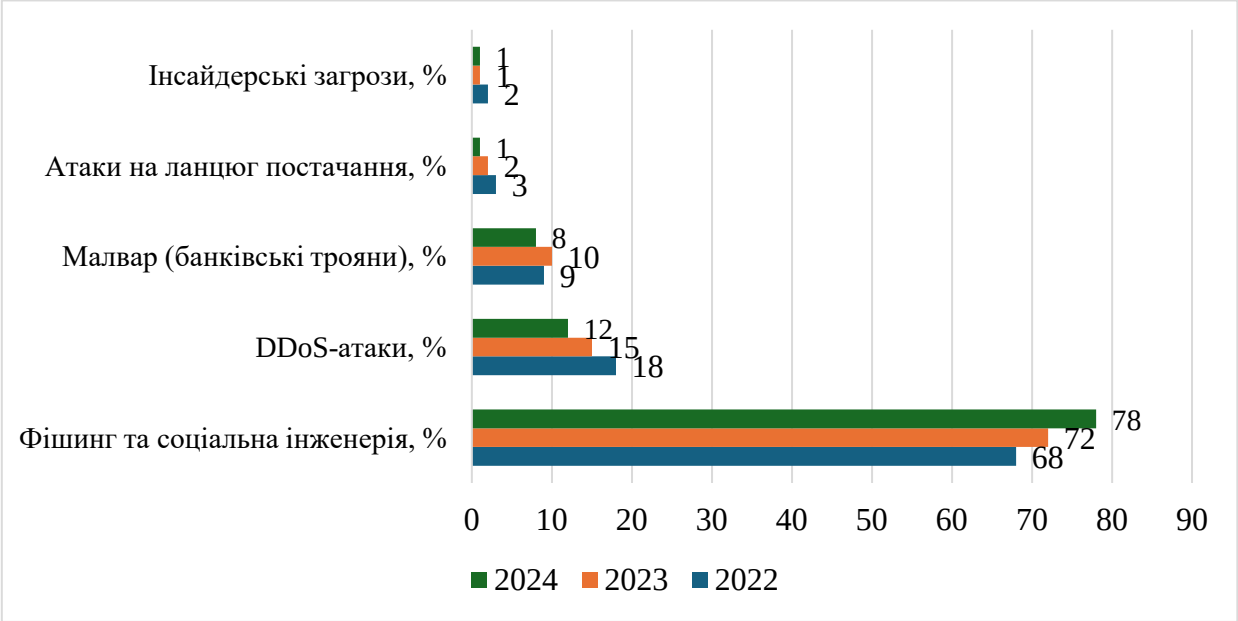

Рис. 2 Динаміка типів кібератак на банківський сектор
Джерело: складено на основі даних НБУ [5].

Аналіз динаміки типів кібератак на банківський сектор за період 2022–2024 рр. демонструє чітку тенденцію зростання загрози фішингу та соціальної інженерії, частка яких зросла з 68% у 2022 році до 78% у 2024 році, що свідчить про підвищену активність кіберзлочинців у маніпулюванні користувачами та викраденні конфіденційної інформації. Водночас відзначається зменшення частки DDoS-атак із 18% до 12%, а також зниження ризику атак на ланцюг постачання з 3% до 1%, що може свідчити про ефективність заходів технічного захисту та моніторингу інфраструктури банків. Частка малварі та інсайдерських загроз залишається відносно стабільною, однак потребує постійного контролю, оскільки навіть невеликі зміни можуть мати значні наслідки для безпеки банківських операцій. У сукупності ці дані підкреслюють необхідність комплексного підходу до кіберзахисту, поєднуючи технічні рішення та підвищення кібергігієни серед співробітників і клієнтів.

У сучасних умовах цифровізації банківської діяльності кіберзагрози стають одним із ключових факторів ризику для фінансових установ. Аналіз вибіркових інцидентів високого рівня за період 2022–2024 років дозволяє виявити основні типи атак, оцінити їхні наслідки для банківської інфраструктури та клієнтських сервісів, а також окреслити пріоритетні напрямки підвищення кіберстійкості банківського сектору. У лютому 2022 року великі банки стали об’єктами масованих DDoS-атак, що призвело до недоступності сервісів протягом 48 годин. Даний випадок демонструє високий рівень вразливості банківської інфраструктури до зовнішніх перевантажень мережевих ресурсів і підкреслює необхідність удосконалення протоколів захисту та впровадження механізмів забезпечення безперервності обслуговування клієнтів [8, с. 51].

У квітні 2022 року ПриватБанк [9] зазнав фішингових атак через Telegram-боти, що спричинило компрометацію близько 12 000 платіжних карток. Даний інцидент відображає значущість соціальної інженерії як інструменту кіберзлочинності та підкреслює потребу у підвищенні кібергігієни користувачів, впровадженні багатофакторної автентифікації та систем моніторингу фінансових транзакцій. Аналогічно, жовтнева DDoS-атака на Monobank [15], здійснена групою NoName057(16), призвела до шестигодинного простою мобільного додатку, що підтверджує стійку актуальність атак цього типу та необхідність оперативного реагування на інциденти.

На початку 2024 року Ощадбанк [6] та ПУМБ стали жертвами шкідливого програмного забезпечення Emotet, що спричинило витік персональних даних близько 8 500 клієнтів. Дані випадки показують високі ризики, пов'язані з малварними загрозами, та підтверджує необхідність регулярного оновлення антивірусних систем і застосування превентивних заходів для захисту даних. У червні 2024 року УкрСиббанк [12] зазнав API-експлойту через вразливість Log4j, що призвело до блокування транзакцій, підкреслюючи критичну важливість своєчасного патчінгу програмного забезпечення та тестування безпеки банківських додатків.

Загалом, наведені випадки підтверджують необхідність комплексного підходу до кіберзахисту банківського сектору, який передбачає інтеграцію технічних, організаційних та освітніх заходів для зниження ризиків та забезпечення стійкості фінансових сервісів.

Глобальна діджиталізація та прискорений розвиток фінансових технологій перетворили цифрові платіжні сервіси — мобільний банкінг, перекази від особи до особи, системи миттєвих платежів — на критично важливий елемент економічної та соціальної взаємодії. Швидкість, доступність та економічна ефективність цифрових платіжних сервісів зумовили їхнє домінування на фінансовому ринку. Однак, ця критична залежність від цифрової інфраструктури створює значні виклики безпеці, перетворюючи банківський сектор на пріоритетну ціль для кіберзлочинності. Сучасні загрози еволюціонують від класичного фінансового шахрайства до комплексних гібридних атак, що вимагає глибокого розуміння природи цих викликів та розробки адаптивних стратегій кіберзахисту. Виклики безпеці цифрових платіжних сервісів можна класифікувати за їхньою природою та вектором атаки:

1) Технологічні та інфраструктурні загрози спрямовані на порушення цілісності, доступності та конфіденційності даних на рівні інфраструктури та програмного забезпечення. Масштабні атаки типу «розподілена відмова в обслуговуванні» мають на меті блокування доступу до платіжних сервісів шляхом перевантаження вебсайтів, мобільних додатків або платіжних шлюзів великою кількістю запитів. У банківській сфері такі атаки критично впливають на проведення транзакцій, завдаючи фінансових та репутаційних втрат. Наприклад, банки, що активно використовують системи миттєвих платежів, можуть стати жертвами скоординованих атак на програмні інтерфейси додатків, що призводить до затримки або повного блокування переказів. Додатково, шкідливе програмне забезпечення та віруси-вимагачі здатні проникати у внутрішні мережі банків, шифрувати критичні дані та блокувати доступ до платіжних систем. Прикладом є впровадження троянського програмного забезпечення через шахрайські електронні листи для компрометації робочих станцій співробітників, які мають доступ до платіжних серверів, з подальшою вимогою викупу в криптовалюті. Також вразливості програмних інтерфейсів додатків можуть дозволяти стороннім додаткам отримувати доступ до даних клієнтів або ініціювати фальшиві транзакції, порушуючи принцип мінімальних привілеїв доступу [7, с. 129].

2) Соціально-інженерні атаки експлуатують людський фактор, який залишається найслабшою ланкою у ланцюгу безпеки. Фішинг та вішинг є основними методами викрадення облікових даних або грошових коштів. Фішинг передбачає створення підроблених банківських сайтів або розсилку електронних листів із закликом ввести конфіденційні дані, а вішинг — голосове шахрайство, коли зловмисники видають себе за співробітників банку або правоохоронних органів і маніпулюють жертвою для отримання одноразових паролів. Наприклад, шахраї можуть телефонувати клієнту, стверджуючи, що рахунок зламано, і вимагати продиктувати код із текстового повідомлення, що надає зловмиснику доступ до рахунку [11, с. 244].

3) Архітектурні та операційні виклики пов'язані з внутрішньою організацією банківських систем, їхньою стійкістю та дизайном. Ризик ланцюга постачання виникає через інтеграцію стороннього програмного забезпечення, апаратного забезпечення або хмарних сервісів; вразливість у постачальника може стати точкою входу для атаки, наприклад, через компрометацію оновлень платіжного програмного забезпечення із вбудованим прихованим механізмом доступу. Застарілі системи автентифікації та недостатня кількість факторів перевірки, наприклад, використання тільки логіна та пароля або одноразових текстових повідомлень, не забезпечують достатнього рівня захисту, особливо у випадках шахрайства із заміною сім-картки або перехоплення повідомлень шкідливим програмним забезпеченням на пристрої клієнта. Сучасні практики вимагають впровадження біометричних технологій та апаратних токенів. Недостатня операційна стійкість відображає здатність банку забезпечувати безперервну роботу цифрових платіжних сервісів навіть під час критичних інцидентів. Відсутність географічно рознесених резервних центрів обробки даних може призвести до тривалих простоїв платіжних систем у разі стихійних лих або цілеспрямованих атак, що тягне за собою значні фінансові та репутаційні втрати [8, с. 49].

Глобальна діджиталізація та прискорений розвиток фінансових технологій перетворили цифрові платіжні сервіси — мобільний банкінг, перекази від особи до особи, системи миттєвих платежів — на критично важливий елемент функціонування банківського сектору. Вони забезпечують швидкість, доступність та економічну ефективність транзакцій, проте водночас розширюють поверхню атаки для кіберзлочинців. У період останніх років виклики безпеці цифрових платіжних сервісів суттєво трансформувалися: від класичного шахрайства до комплексних гібридних кібератак, спрямованих на дестабілізацію фінансової інфраструктури, що зумовлює нагальну необхідність не лише підтримання, а й проактивного та інноваційного вдосконалення захисних механізмів. Удосконалення безпеки цифрових платіжних сервісів має бути реалізоване на трьох ключових рівнях:

1) Технологічне посилення та інтеграція штучного інтелекту є одним із найперспективніших

напрямів удосконалення систем кіберзахисту цифрових платіжних сервісів є впровадження адаптивних технологій штучного інтелекту, зокрема систем машинного навчання, які здатні виявляти нові, раніше невідомі загрози. Традиційні системи фрод-моніторингу, що базуються на фіксованих правилах, виявляються неефективними проти швидко змінюваних схем шахрайства. Застосування моделей машинного навчання дозволяє аналізувати великі обсяги даних та ідентифікувати аномальні транзакції за поведінковими ознаками клієнта. Наприклад, нейронні мережі можуть відстежувати понад п'ятдесят параметрів користувацької активності: середню суму переказу, час доби, геолокацію, швидкість введення пароля тощо. Якщо клієнт, який зазвичай здійснює невеликі перекази вдень, раптом ініціює великий міжнародний платіж уночі з нового пристрою, система автоматично позначає транзакцію як підозрілу та блокує її до додаткової перевірки.

2) Організаційно-архітектурне вдосконалення є не менш важливим напрямом є модернізація архітектури безпеки банківських систем на основі концепції «нульової довіри» (Zero Trust Architecture), цей підхід передбачає постійну перевірку всіх користувачів та процесів, незалежно від того, чи знаходяться вони всередині, чи поза межами корпоративної мережі. Наприклад, реалізація мікросегментації дозволяє обмежити доступ між внутрішніми системами: навіть якщо зловмисник отримає доступ до одного модуля (CRM-системи), він не зможе автоматично проникнути до платіжного ядра банку без повторної автентифікації. Окрім того, підвищення операційної стійкості передбачає географічне дублювання IT-інфраструктури. Так, банки розміщують резервні копії даних у кількох незалежних центрах обробки, що дає змогу оперативно перемикати операції на резервні майданчики у разі кібератак або фізичних пошкоджень, забезпечуючи безперервність обслуговування клієнтів.

3) Підвищення кібербезпеки цифрових платіжних сервісів неможливе без гармонізації нормативно-правової бази та координації дій між банками, регуляторами та технологічними партнерами. Одним із ключових аспектів є контроль за ланцюгом постачання, оскільки вразливість стороннього постачальника програмного забезпечення може стати каналом для атаки на банк. Регулятори, такі як Національний банк України [5], мають встановити обов'язкові вимоги щодо сертифікації партнерів за міжнародними стандартами безпеки (наприклад, ISO 27001 [14]) та проведення регулярних тестів на проникнення. Додатково, важливим інструментом є створення централізованих платформ обміну інформацією про кіберзагрози. Наприклад, система колективного моніторингу дозволяє банкам миттєво ділитися даними про нові типи атак або шкідливе програмне забезпечення, що підвищує швидкість реагування всього сектору та зменшує ризик масштабного компрометування фінансових систем.

Висновки. Безпека цифрових платіжних сервісів у банківському секторі є ключовою умовою стабільності фінансової системи та довіри клієнтів до електронних розрахунків. Проведений аналіз засвідчив, що основними викликами залишаються зростання кількості фішингових атак, DDoS-кампаній та шкідливого програмного забезпечення, які спрямовані на компрометацію клієнтських даних і порушення функціонування банківських систем. Удосконалення системи кіберзахисту потребує комплексного підходу, що включає впровадження сучасних технологій штучного інтелекту для моніторингу загроз, посилення захисту API-інтерфейсів, підвищення рівня цифрової грамотності користувачів та дотримання міжнародних стандартів інформаційної безпеки. Ефективна взаємодія банків, державних структур та провайдерів цифрових сервісів створює передумови для підвищення кіберстійкості платіжної інфраструктури України в умовах посилення гібридних загроз.

Список використаних джерел:

1. Гончаренко А.В. (2022). Вплив сучасних цифрових технологій на конкурентні позиції банків на фінансовому ринку. Bulletin of Sumy National Agrarian University, № 2 (88). С. 35-39. DOI: https://doi.org/10.32845/bsnau.2021.2.7
2. Данік Н., Торлопов А. (2024). Вплив цифрової трансформації на банківський сектор України. International Science Journal of Management, Economics & Finance, № 3. С. 95-103. DOI: https://doi.org/10.46299/j.isjmef.20240303.09
3. Квасницька Р., Форкун І., Гордєєва Т. (2022). Сучасні підходи забезпечення інформаційної безпеки платіжних систем та їх кіберзахист. Вісник Хмельницького національного університету. Економічні науки, № 5. Т. 1. С. 47-52. DOI: https://doi.org/10.31891/2307-5740-2022-310-5(1)-8
4. Мельник О.В. (2024). Забезпечення безпеки банківської системи на засадах метапростору FinTech-послуг. Зб. наух. праць Таврійського державного агротехнологічного університету ім. Д. Моторного (економічні науки), № 4(53). С. 109-123. DOI: https://doi.org/10.32782/2519-884X-2024-53-12
5. Національний банк України. URL: https://bank.gov.ua/
6. Ощадбанк. URL: https://www.oschadbank.ua/
7. Павленко Л.Д., Криклій О.А., Чумак О.В. (2024). Ризики банків України та організаційна система управління ними в умовах воєнного стану. Інвестиції: практика та досвід, № 5. С. 126-132. DOI: https://doi.org/10.32702/2306-6814.2024.5.126
8. Пелюх О.І., Єсіна М.В., Голубничий Д.Ю. (2024). Сучасні загрози інформаційно-комунікаційним системам та методи захисту від них. Радіотехніка, № 216. С. 46-56. DOI: https://doi.org/10.30837/rt.2024.1.216.03
9. ПриватБанк. URL: https://privatbank.ua/

10. ПУМБ. URL: https://www.pumb.ua/
11. Тарасенко А., Жаворонок А., Суховецький В. (2025). Безпека платежів у цифровій економіці: виклики для банківського карткового бізнесу. Науковий вісник Полісся, № 1(30). С. 233-247. DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-233-247
12. УкрСиббанк. URL: https://ukrsibbank.com/
13. The Basel Committee – overview. BIS. URL: https://www.bis.org/bcbs/index.htm
14. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. URL: https://www.iso.org/standard/27001
15. Monobank. URL: https://monobank.ua/

References:

1. Honcharenko, A.V. (2022). Vplyv suchasnykh tsyfrovykh tekhnolohii na konkurentni pozytsii bankiv na finansovomu rynku [The impact of modern digital technologies on the competitive positions of banks in the financial market]. Bulletin of Sumy National Agrarian University, No. 2 (88). Pp. 35-39. DOI: https://doi.org/10.32845/bsnau.2021.2.7 [in Ukrainian].
2. Danik, N., & Torlopov, A. (2024). Vplyv tsyfrovoi transformatsii na bankivskyi sektor Ukrainy [The impact of digital transformation on the banking sector of Ukraine]. International Science Journal of Management, Economics & Finance, No. 3. Pp. 95-103. DOI: https://doi.org/10.46299/j.isjmef.20240303.09 [in Ukrainian].
3. Kvasnytska, R., Forkun, I., & Hordieieva, T. (2022). Suchasni pidkhody zabezpechennia informatsiinoi bezpeky platizhnykh system ta yikh kiberzakhyst [Modern approaches to ensuring information security of payment systems and their cyber protection]. Bulletin of Khmelnytskyi National University. Economic Sciences, No. 5. Vol. 1. Pp. 47-52. DOI: https://doi.org/10.31891/2307-5740-2022-310-5(1)-8 [in Ukrainian].
4. Melnyk, O.V. (2024). Zabezpechennia bezpeky bankivskoi systemy na zasadakh metaprostoru FinTech-posluh [Ensuring the security of the banking system based on the metaspace of FinTech services]. Collection of scientific works of the Tavria State Agrotechnological University named after D. Motorny (economic sciences), No. 4(53). Pp. 109-123. DOI: https://doi.org/10.32782/2519-884X-2024-53-12 [in Ukrainian].
5. Natsionalnyi bank Ukrainy [National Bank of Ukraine]. Retrieved from: https://bank.gov.ua/ [in Ukrainian].
6. Oshchadbank [Oschadbank]. Retrieved from: https://www.oschadbank.ua/ [in Ukrainian].
7. Pavlenko, L.D., Kryklii, 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 of their management under martial law]. Investments: practice and experience, No. 5. Pp. 126-132. DOI: https://doi.org/10.32702/2306-6814.2024.5.126 [in Ukrainian].
8. Peliukh, O.I., Yesina, M.V., 7 Holubnychyi, D.Iu. (2024). Suchasni zahrozy informatsiino-komunikatsiinym systemam ta metody zakhystu vid nykh [Modern threats to information and communication systems and methods of protection against them]. Radio Engineering, No. 216. Pp. 46-56. DOI: https://doi.org/10.30837/rt.2024.1.216.03 [in Ukrainian].
9. PryvatBank [PrivatBank]. Retrieved from: https://privatbank.ua/ [in Ukrainian].
10. PUMB. Retrieved from: https://www.pumb.ua/ [in Ukrainian].
11. Tarasenko A., Zhavoronok A., Sukhovetskyi V. (2025). Bezpeka platezhiv u tsyfrovii ekonomitsi: vyklyky dlia bankivskoho kartkovoho biznesu [Payment security in the digital economy: challenges for the bank card business]. Scientific Bulletin of Polissya, No. 1(30). Pp. 233-247. DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-233-247 [in Ukrainian].
12. Ukrsibbank. Retrieved from: https://ukrsibbank.com/
13. The Basel Committee – overview. BIS. Retrieved from: https://www.bis.org/bcbs/index.htm [in English].
14. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. Retrieved from: https://www.iso.org/standard/27001 [in English].
15. Monobank. Retrieved from: https://monobank.ua/

Дата надходження статті: 16.10.2025 р.
Дата прийняття статті до друку: 06.11.2025 р.