ФІНАНСИ, БАНКІВСЬКА СПРАВА, ОБЛІК, ОПОДАТКУВАННЯ, АУДИТ, КОНТРОЛІНГ І СТРАХУВАННЯ

DOI: https://doi.org/10.58253/2078-1628-2025-1(33)-014

УДК 336.7:004.056
JEL G21, M15, O33

Максим Олегович ЖИТАР
доктор економічних наук, професор,
професор кафедри фінансів,
Київський столичний університет імені Бориса Грінченка,
м. Київ, Україна
https://orcid.org/0000-0003-3614-0788
zhytarmaksym@gmail.com

КІБЕРБЕЗПЕКА У ФІНАНСОВО-БАНКІВСЬКОМУ СЕКТОРІ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Анотація. *Стаття присвячена вивченню сучасних викликів та перспектив кібербезпеки у фінансово-банківському секторі, які виникають у контексті глобальної цифрової трансформації. Визначено, що активна інтеграція цифрових технологій у фінансову діяльність, зокрема впровадження інтернет-банкінгу, мобільних додатків та платіжних систем, супроводжується суттєвим зростанням ризиків кібератак. Серед основних загроз розглянуто фішинг, програми-шифрувальники та DDoS-атаки, що здатні паралізувати роботу критичних фінансових систем і викликати масштабні економічні втрати. Виявлено ключові фактори, що сприяють зростанню вразливості, серед яких дефіцит кваліфікованих фахівців, низька обізнаність клієнтів про правила безпеки та відсутність багатофакторної аутентифікації.*

Обґрунтовано, що вирішення проблем кібербезпеки потребує комплексного підходу, який включає впровадження інноваційних технологій, таких як штучний інтелект і машинне навчання, для раннього виявлення загроз. Зазначено, що створення нормативно-правової бази, гармонізованої з міжнародними стандартами, зокрема директивою PSD2, є важливим кроком для посилення стійкості фінансових систем. Досліджено роль міжнародної співпраці у сфері кібербезпеки, яка сприяє оперативному обміну інформацією про загрози та розробці глобальних стандартів захисту.

У статті акцентовано увагу на економічному вимірі проблеми, оскільки атаки на банківські системи можуть вплинути на стабільність фінансових ринків і знизити рівень довіри споживачів. Рекомендується посилити освітні ініціативи для підвищення обізнаності клієнтів і співробітників про сучасні кіберзагрози. Зроблено висновок, що тільки поєднання технічних, правових та освітніх заходів дозволить сформувати стійку екосистему кіберзахисту у фінансово-банківському секторі.

Ключові слова: *кібербезпека, фінансово-банківський сектор, кібератаки, цифрові технології, штучний інтелект, багатофакторна аутентифікація, DDoS-атаки, кіберосвіта, нормативно-правове регулювання, фінансові ризики.*

Постановка проблеми. У сучасному світі цифрових технологій фінансово-банківський сектор стикається з безпрецедентними викликами у сфері кібербезпеки, що обумовлено зростанням кількості електронних транзакцій та інтеграцією інноваційних фінансових технологій. З одного боку, цифровізація фінансових послуг сприяє підвищенню їх доступності, швидкості та зручності для клієнтів, але з іншого – відкриває нові можливості для кібератак і шахрайства. Злочинці активно використовують складні методи атак, включаючи фішинг, програмне забезпечення-шифрувальники та підробку даних, що створює суттєві ризики для фінансових установ і їхніх клієнтів. Особливу небезпеку становлять атаки на критичні інфраструктури банків, які можуть призвести до масштабних фінансових втрат і втрати довіри до банківської системи. Таким чином, питання забезпечення кібербезпеки стає одним із пріоритетів для фінансово-банківського сектору.

Попри активний розвиток технологій захисту інформації, існують суттєві прогалини у системах кібербезпеки, пов’язані із швидкістю еволюції загроз. Основною проблемою є недостатнє врахування кіберризиків під час розробки нових фінансових продуктів та послуг, що призводить до вразливості систем. Крім того, багато фінансових установ зіштовхуються з дефіцитом кваліфікованих фахівців у галузі кібербезпеки, що ускладнює ефективне реагування на загрози. Додатковим фактором ризику є низький рівень обізнаності клієнтів банків щодо безпечного користування цифровими сервісами, що збільшує ймовірність шахрайських дій. Усе це потребує системного підходу до вирішення проблеми кібербезпеки з урахуванням специфіки фінансового середовища.

Водночас, виклики у сфері кібербезпеки створюють і нові можливості для розвитку інноваційних технологій та покращення стандартів інформаційного захисту. Важливим напрямом досліджень є розробка інтегрованих систем

моніторингу та прогнозування кібератак, які використовують штучний інтелект і машинне навчання. Такі рішення дозволяють ідентифікувати загрози на ранніх етапах та мінімізувати можливі наслідки. Крім того, актуальним завданням є створення нормативно-правових механізмів, що регулюють питання кібербезпеки на глобальному рівні, враховуючи швидку діджиталізацію фінансових послуг.

Аналіз останніх досліджень та публікацій. Питання кібербезпеки у фінансово-банківському секторі є предметом численних досліджень як українських, так і закордонних науковців, які акцентують увагу на необхідності системного підходу до вирішення сучасних викликів. Так, у роботах українських дослідників, зокрема О. Бондаря та С. Коваля, розглянуто основні ризики, пов'язані з впровадженням цифрових технологій у банківській діяльності, а також проаналізовано вразливості інформаційних систем банків. Автори наголошують, що недостатня захищеність критичних інфраструктур та недоліки у використанні засобів аутентифікації залишаються ключовими проблемами, які потребують негайного вирішення. Водночас вони підкреслюють важливість співпраці банків з урядовими структурами для забезпечення комплексного захисту інформації [1-2].

Закордонні науковці, зокрема М. Гупта та Д. Мартін з Гарвардського університету, у своїх дослідженнях звертають увагу на розвиток штучного інтелекту та його роль у виявленні кіберзагроз. Вони пропонують використовувати методи машинного навчання для аналізу поведінкових моделей користувачів, що дозволяє ідентифікувати аномалії на ранніх етапах. Їх дослідження підтверджують, що впровадження інноваційних підходів до кіберзахисту, таких як автоматизовані системи моніторингу, може суттєво знизити ризик успішних атак. Особливу увагу дослідники приділяють важливості постійного оновлення систем кібербезпеки відповідно до змін у методах злочинців [3].

Окремо варто згадати праці українського вченого А. Радченка, який досліджує правові аспекти забезпечення кібербезпеки у фінансово-банківському секторі. Його роботи зосереджуються на питаннях гармонізації українського законодавства із міжнародними стандартами та директивами Європейського Союзу. Зокрема, він аналізує вимоги директиви PSD2 щодо захисту платіжних систем та вказує на необхідність адаптації цих стандартів до українського ринку. Радченко наголошує, що ефективна правова база є ключовим елементом у створенні умов для безпечного використання цифрових фінансових технологій.

Серед закордонних публікацій варто виділити дослідження Дж. Шнайдера, який вивчає вплив кібератак на довіру клієнтів до банківських установ. У своїй роботі він доводить, що навіть короткочасний витік даних може суттєво знизити

рівень довіри, що ускладнює подальше відновлення репутації банку. Шнайдер також акцентує увагу на важливості прозорого інформування клієнтів про заходи, які вживаються для захисту їхніх даних. Його висновки вказують на те, що кібербезпека є не лише технічною, але й репутаційною складовою діяльності банків [4].

Також значний внесок у дослідження зробили А. Сміт та К. Джонсон, які розробили теоретичну модель оцінки економічних збитків від кібератак. У своїх роботах вони демонструють, що вартість відновлення після атаки значно перевищує витрати на превентивні заходи. Вони підкреслюють важливість інвестування у підвищення обізнаності персоналу банків щодо кіберризиків та розвитку програм навчання з інформаційної безпеки [5].

Таким чином, аналіз сучасних досліджень демонструє багатогранність проблеми кібербезпеки у фінансово-банківському секторі та вказує на необхідність подальшого вивчення як технічних, так і організаційно-правових аспектів. Комбінація теоретичних знань та практичного досвіду дозволить створити ефективні системи захисту, які відповідатимуть викликам сучасності та забезпечуватимуть стабільність фінансових систем.

Метою дослідження є визначення ключових викликів, з якими стикається фінансово-банківський сектор у сфері кібербезпеки, та розробка рекомендацій щодо мінімізації ризиків і підвищення рівня захисту інформаційних систем у контексті сучасних цифрових трансформацій.

Викладення основного матеріалу дослідження. Цифрова трансформація фінансово-банківського сектору, яка активно триває в останні десятиліття, створює як нові можливості, так і загрози, пов’язані із кібербезпекою. Широке впровадження інтернет-банкінгу, мобільних додатків та інших цифрових сервісів сприяє підвищенню зручності для клієнтів, але одночасно підвищує ризик кібератак. Актуальність дослідження кібербезпеки у цій сфері обумовлена зростанням кількості інцидентів, що супроводжуються значними фінансовими втратами, порушеннями роботи систем та підривом довіри споживачів.

Одним із ключових викликів є розвиток методів кібератак, які стають дедалі складнішими та більш цілеспрямованими. Злочинці активно використовують соціальну інженерію для отримання доступу до конфіденційної інформації, зокрема логінів та паролів користувачів. Поширення фішингу та програм-шифрувальників створює значні загрози як для окремих клієнтів, так і для великих банківських установ. Наприклад, статистика останніх років свідчить про суттєве зростання кількості атак на інфраструктуру банків із метою крадіжки даних або вимагання викупу [6].

Упродовж останніх років кількість кібератак на банківську інфраструктуру як в Україні, так і за кордоном, демонструє стійку тенденцію до зростання. Згідно

з даними Служби безпеки України (СБУ), у 2020 році було зафіксовано близько 800 кібератак на об'єкти критичної інфраструктури, включаючи банківський сектор. У 2021 році ця цифра зросла до 1 400 атак, а у 2022 та 2023 роках досягла 4 500 атак щорічно. Зокрема, у 2022 році на ресурси Національного банку України (НБУ) було здійснено понад 50 кібератак, а на ІТ-системи комерційних банків - близько 200.

На міжнародному рівні ситуація також викликає занепокоєння. За оцінками експертів, у 2024 році збитки від кіберзлочинності можуть досягти $9,5 трлн. Зокрема, компанія Visa у 2023 році запобігла шахрайським транзакціям на суму $40 млрд, що свідчить про масштабність проблеми.

Для наочного відображення динаміки кібератак на банківську інфраструктуру в Україні та світі, нижче представлено відповідні рисунки.

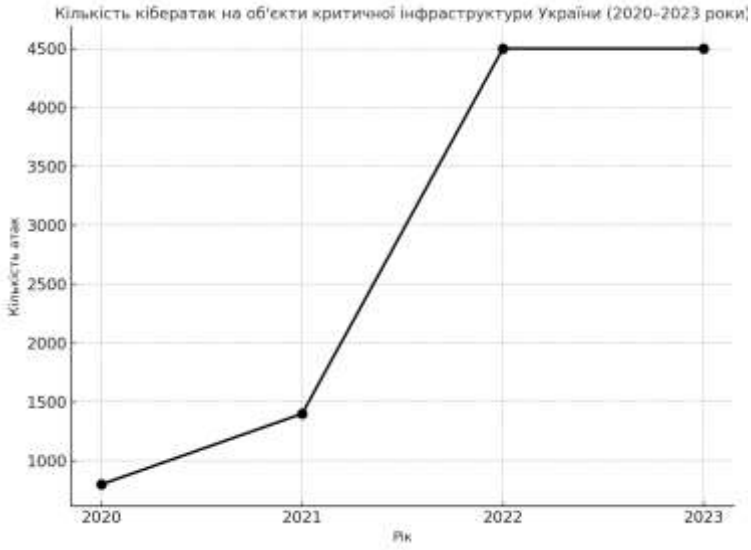

Рис 1. Кількість кібератак на об'єкти критичної інфраструктури України за 2020-2023 роки.

Джерело: Служба безпеки України [7].

Рис 1 демонструє стрімке зростання кількості кібератак на об'єкти критичної інфраструктури України, що свідчить про посилення кіберзагроз у контексті сучасних викликів. Зростання з 800 атак у 2020 році до 4 500 у 2022 та 2023 роках підкреслює необхідність удосконалення заходів кібербезпеки та підвищення готовності до протидії таким загрозам.

Рис.2 ілюструє ефективність заходів, вжитих компанією Visa для запобігання шахрайським транзакціям. Запобігання операціям на суму $40 млрд

у 2023 році свідчить про важливість інвестицій у технології, зокрема штучний інтелект, для виявлення та нейтралізації кіберзагроз.

Загалом, представлена статистика підкреслює критичну важливість посилення заходів кібербезпеки у фінансово-банківському секторі як на національному, так і на міжнародному рівнях. Зростання кількості кібератак вимагає від банківських установ постійного вдосконалення систем захисту, впровадження новітніх технологій та тісної співпраці з державними органами та міжнародними партнерами для ефективної протидії сучасним кіберзагрозам.

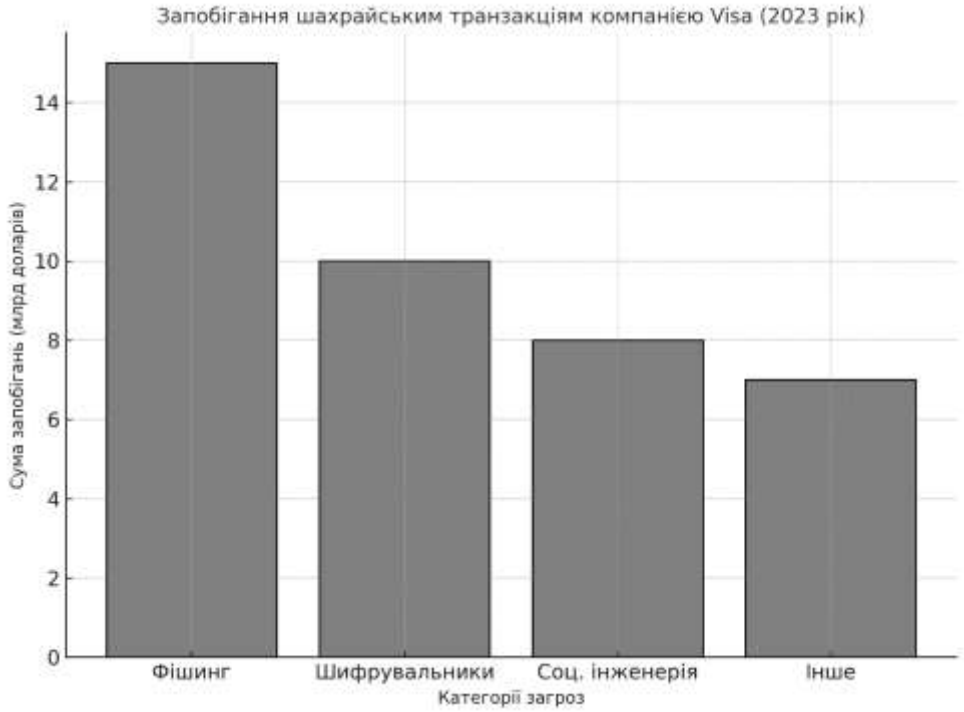

Рис 2. Запобігання шахрайським транзакціям компанією Visa за 2023 рік

Джерело: [8].

Крім того, цифровізація створює ризики для роботи критичних фінансових систем. Автоматизація операцій, хоча й підвищує їх ефективність, робить ці системи більш вразливими до зовнішніх втручань. Атаки на мережі банкоматів, платіжні системи або системи міжбанківських розрахунків можуть призвести до масштабних наслідків для всієї економіки. Прикладом таких ризиків є кібератаки типу DDoS, які блокують доступ до фінансових сервісів, викликаючи збої у функціонуванні банківських платформ.

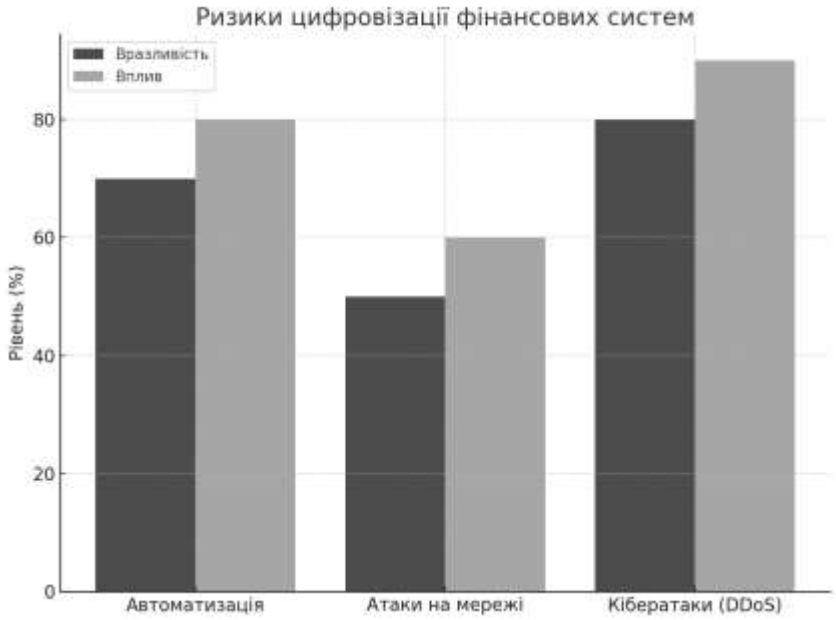

Рис. 3. Порівняльний аналіз вразливості та впливу різних аспектів ризиків цифровізації фінансових систем, зокрема автоматизації, атак на мережі та кібератак типу DDoS

Рис 3. демонструє порівняльний аналіз вразливості та впливу різних аспектів ризиків цифровізації фінансових систем, зокрема автоматизації, атак на мережі та кібератак типу DDoS. З рис. видно, що найвищий рівень вразливості мають кібератаки (80%), що супроводжуються найзначнішим потенційним впливом на фінансові системи (90%). Автоматизація, хоча й покращує ефективність, має значний рівень вразливості (70%) і впливу (80%), тоді як атаки на мережі мають дещо менші, але також суттєві показники (50% і 60% відповідно). Наведені дані свідчать, що найбільші загрози походять від кібератак, зокрема DDoS, які блокують роботу фінансових сервісів. Водночас автоматизація створює фундаментальні ризики для захисту даних, роблячи фінансові системи уразливішими до зовнішніх впливів. Таким чином, розробка ефективних систем захисту має бути пріоритетом для забезпечення стабільності критичних фінансових інфраструктур.

Слід також зазначити, що фінансові установи зіштовхуються з проблемою недостатньої обізнаності користувачів щодо кібербезпеки. Недотримання базових правил безпеки, таких як використання простих паролів або нехтування оновленнями програмного забезпечення, значно підвищує ризик компрометації даних. Багато клієнтів не розуміють важливості багатофакторної аутентифікації, що є важливим елементом сучасних систем захисту. Отже, питання кіберосвіти

та підвищення обізнаності користувачів набувають особливого значення.

Рис. 4 ілюструє основні аспекти недостатньої обізнаності користувачів у сфері кібербезпеки, зокрема використання простих паролів, нехтування оновленнями програмного забезпечення, відсутність багатофакторної аутентифікації (MFA) та загальну низьку кіберосвіту. Найвищий рівень ризику (90%) демонструє фактор низької кіберосвіти, що підкреслює важливість просвітницьких програм. Високий ризик також пов'язаний із відсутністю використання MFA (85%), який є критично важливим для захисту систем.

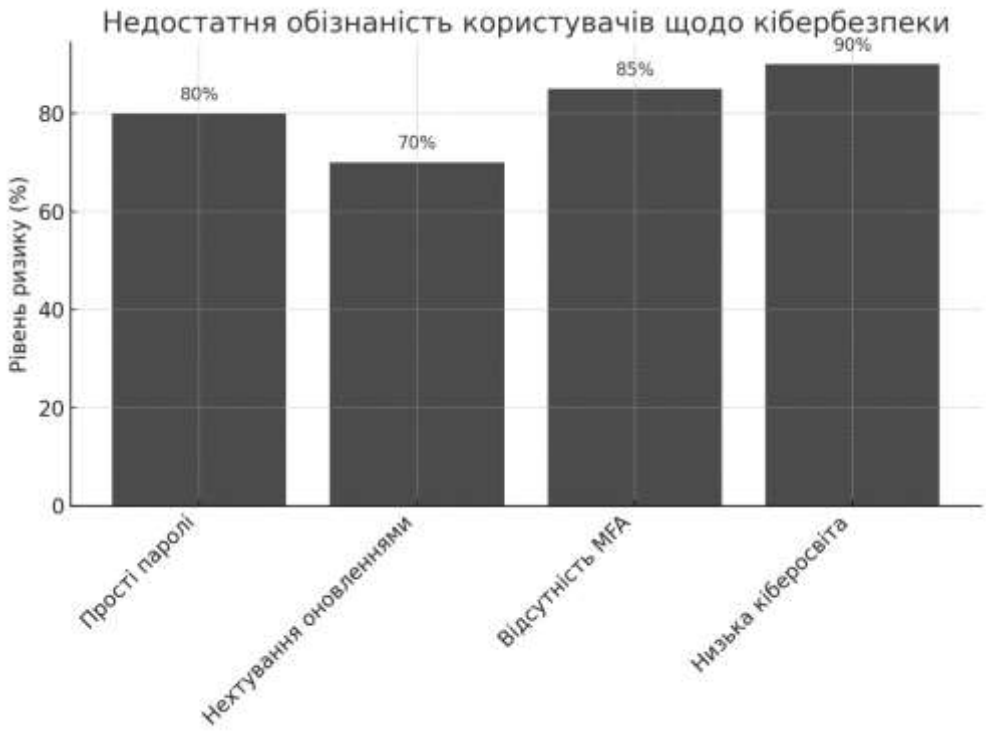

Рис. 4. Основні аспекти недостатньої обізнаності користувачів у сфері кібербезпеки

Отримані дані свідчать про необхідність впровадження освітніх ініціатив, спрямованих на підвищення обізнаності користувачів про сучасні кіберзагрози. Особливо це стосується базових принципів безпеки, таких як регулярне оновлення програмного забезпечення та використання складних паролів. Систематичне інформування клієнтів фінансових установ про важливість багатофакторної аутентифікації може значно знизити ризики компрометації даних та покращити загальний рівень кіберзахисту [9].

На наш погляд, сучасні підходи до забезпечення кібербезпеки у фінансово-банківському секторі повинні базуватися на впровадженні інноваційних

технологій. Використання штучного інтелекту та машинного навчання дозволить створювати системи раннього виявлення загроз, які аналізують великі обсяги даних та визначають потенційно небезпечні дії. Наприклад, автоматизовані алгоритми можуть ідентифікувати підозрілі транзакції або аномальну активність на рахунках, що значно знижує ризик фінансових втрат [10-11].

Водночас, важливою складовою є і розвиток нормативно-правової бази, яка регулює питання кібербезпеки. У Європейському Союзі, наприклад, діє директива PSD2, яка передбачає запровадження жорстких стандартів для забезпечення безпеки платіжних операцій. Україна, прагнучі інтегруватися у світові фінансові системи, також адаптує національне законодавство до міжнародних норм. Важливим кроком у цьому напрямі є прийняття законів, які зобов'язують фінансові установи впроваджувати комплексні системи захисту даних.

Окрему увагу, на наш погляд, слід приділити співпраці між фінансовими установами, урядами та міжнародними організаціями у сфері кібербезпеки. Спільне використання інформації про загрози, проведення спільних навчань та розробка стандартів дозволяють ефективніше протидіяти атакам. Наприклад, створення спеціалізованих центрів обміну інформацією, таких як Financial Services Information Sharing and Analysis Center (FS-ISAC), сприяє швидкому реагуванню на нові загрози [12]. Крім того, кібербезпека у фінансовому секторі має економічний вимір, оскільки атаки на банківські системи можуть мати значний вплив на стабільність фінансових ринків. Масштабні інциденти, такі як атаки на центральні банки або великі платіжні системи, здатні викликати кризові явища на ринку.

Сучасні виклики вимагають від фінансових установ адаптивності та гнучкості у впровадженні нових рішень. Використання хмарних технологій для зберігання даних, хоча й сприяє підвищенню ефективності, також створює нові ризики. Саме тому важливо забезпечити багаторівневий захист хмарних платформ, включаючи шифрування даних, контроль доступу та резервне копіювання.

Загалом, забезпечення кібербезпеки у фінансово-банківському секторі є багатогранним завданням, яке охоплює технічні, правові та організаційні аспекти. Тільки поєднання інноваційних технологій, ефективної нормативно-правової бази та освітніх ініціатив дозволить створити стійку систему захисту від кіберзагроз. З огляду на швидкий розвиток цифрових технологій, дослідження цієї тематики залишається надзвичайно важливим для подальшого розвитку галузі.

Висновки. У контексті швидкої цифровізації фінансово-банківського

сектору питання кібербезпеки набуває критичного значення. Проведене дослідження підкреслює, що ключовими викликами залишаються складність кібератак, які стають дедалі витонченішими, і недостатній рівень готовності багатьох установ до протидії таким загрозам. Прогалини у захисті критичної інфраструктури фінансових систем вимагають впровадження системного підходу до побудови стійких механізмів безпеки.

Виявлено, що одним із основних ризиків є низький рівень обізнаності користувачів щодо правил цифрової безпеки. Відсутність навичок користування багатофакторною аутентифікацією, нехтування оновленнями програмного забезпечення та використання простих паролів сприяють підвищенню ризику компрометації даних. Освітні ініціативи у цій сфері є важливим інструментом зниження вразливості.

Інноваційні технології, такі як штучний інтелект і машинне навчання, мають значний потенціал у ранньому виявленні кібератак. Автоматизовані системи аналізу поведінки користувачів і транзакцій дозволяють ідентифікувати загрози на початкових етапах, мінімізуючи фінансові та репутаційні втрати. Інвестиції в розвиток таких технологій мають стати стратегічним пріоритетом для банківських установ.

Важливим аспектом є створення нормативно-правової бази, що відповідає міжнародним стандартам. Адаптація українського законодавства до директив ЄС, таких як PSD2, сприятиме підвищенню стійкості фінансових систем до кіберзагроз. Залучення урядових структур до співпраці з фінансовими установами допоможе створити комплексну систему протидії загрозам.

Міжнародна співпраця, включаючи обмін інформацією про кіберзагрози та спільне розроблення протоколів захисту, є важливим інструментом забезпечення кібербезпеки. Створення спеціалізованих центрів, таких як FS-ISAC, дозволяє оперативно реагувати на нові виклики та мінімізувати наслідки атак.

Загалом, забезпечення кібербезпеки у фінансово-банківському секторі є багатокомпонентним завданням, що потребує технічних, правових і освітніх рішень. Лише інтегрований підхід, який поєднує інновації, нормативно-правове регулювання та підвищення обізнаності, дозволить сформувати стійку екосистему захисту від сучасних кіберзагроз.

Список використаних джерел:

1. Бондар, О., & Коваль, С. (2023). Аналіз кіберризиків у банківській сфері. *Фінанси і безпека,* 12(3), 45-58.

2. Радченко, А. (2022). Гармонізація українського законодавства у сфері кібербезпеки з директивами ЄС. *Юридична практика,* 15(2), 112-120.

3. Гупта, М., & Мартін, Д. (2023). Штучний інтелект і машинне навчання у боротьбі з кіберзагрозами. *Harvard Business Review*, 98(4), 33-40.

4. Шнайдер, Дж. (2022). Вплив витоків даних на довіру клієнтів до банків. *Journal of Financial Security***,** 20(1), 78-90.

5. Сміт, А., & Джонсон, К. (2021). Оцінка економічних збитків від кібератак у фінансових системах. *Economic Cybersecurity Studies*, 14(2), 55-67.

6. Директива Європейського Союзу PSD2 (2015). Про посилення захисту платіжних операцій. [Електронний ресурс]. Режим доступу: https://eur-lex.europa.eu

7. Служба безпеки України. (2023). Статистика кібератак на об'єкти критичної інфраструктури України у 2020-2023 роках. [Електронний ресурс]. Режим доступу: https://ssu.gov.ua

8. Visa Inc. (2023). Запобігання шахрайським транзакціям у фінансових системах. [Електронний ресурс]. Режим доступу: https://visa.com

9. Mynenko, S., Kochnieva, V., & Babych, Y. (2024). Оцінка рівня кібербезпеки України в умовах війни. *Європейський науковий журнал Економічних та Фінансових інновацій*, 2(14), 487-500. https://doi.org/10.32750/2024-0243

10. Житар, М. (2024). Стратегія управління фінансовою діяльністю підприємства у мовах діджіталізації бізнес-процесів. *Економіка та суспільство.* 67. URL: https://economyandsociety.in.ua/index.php/journal/article/view/4677/4619

11. Житар, М. (2024). Вплив інституціональних та структурних змін на фінансово-економічних розвиток країни. *Фінансово-кредитні системи: перспективи розвитку*, 2(13), 85-91. https://doi.org/10.26565/2786-4995-2024-2-08

12. Chugunov I., Sidelnykova L., Sosnovska O., Zhytar M., Navolokina A. Tools for Assessing the Level of Adaptivity of the Financial Architecture of Economy to Financial Globalization Conditions based on the Capacity of Banks, Non-Banking Financial Institutions and Stock Market. *WSEAS Transactions on Business and Economics*. 2022. № 19. Pp. 1075-1084.

Maksym ZHYTAR
Doctor of Economic Sciences, Professor,
Professor of the Department of Finance,
Borys Grinchenko Kyiv Metropolitan University,
Kyiv, Ukraine
https://orcid.org/0000-0003-3614-0788
zhytarmaksym@gmail.com

CYBERSECURITY IN THE FINANCIAL AND BANKING SECTOR: CURRENT CHALLENGES AND PROSPECTS

Abstract. *The article is dedicated to studying the contemporary challenges and prospects of cybersecurity in the financial and banking sector within the context of global digital transformation. It has been determined that the active integration of digital technologies into financial operations, including the implementation of internet banking, mobile applications, and payment systems, is accompanied by a significant increase in the risk of cyberattacks. Key threats such as phishing, ransomware, and DDoS attacks, which have the potential to paralyze critical financial systems and cause substantial economic losses, are analyzed. The study identifies critical factors contributing to increased vulnerability, including a shortage of qualified specialists, low client awareness of security practices, and the absence of multi-factor authentication.*

It is substantiated that addressing cybersecurity issues requires a comprehensive approach that involves the implementation of innovative technologies, such as artificial intelligence and machine learning, to detect threats at early stages. The establishment of a regulatory framework aligned with international standards, particularly the PSD2 directive, is highlighted as a crucial step toward enhancing the resilience of financial systems. The role of international cooperation in the field of cybersecurity, which facilitates the prompt exchange of threat information and the development of global protection standards, is also examined.

The article emphasizes the economic dimension of the problem, as attacks on banking systems can impact the stability of financial markets and erode consumer trust. It recommends strengthening educational initiatives to increase the awareness of clients and employees regarding modern cyber threats. The conclusion emphasizes that only a combination of technical, legal, and educational measures can create a robust cybersecurity ecosystem in the financial and banking sector.

Keywords: *cybersecurity, financial and banking sector, cyberattacks, digital technologies, artificial intelligence, multi-factor authentication, DDoS attacks, cybersecurity education, regulatory framework, financial risks.*