https://doi.org/10.31891/2307-5740-2025-340-20
УДК 336.7:004.056:005.334

ПРИХОДЬКО Борис
Київський національний економічний університет імені Вадима Гетьмана
https://orcid.org/0009-0005-3076-6191
e-mail: pavlovskyidmytro1590@gmail.com

КІБЕРРИЗИКИ ФІНАНСОВОГО СЕКТОРУ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

У статті проведено комплексний аналіз сучасних кіберзагроз для фінансового сектору, із акцентом на їхній вплив на стабільність фінансових установ та платіжних систем. Розглянуто основні вектори кібератак, зокрема фішинг, DDoS, шкідливе програмне забезпечення, а також цілеспрямовані APT-атаки та інсайдерські загрози. На основі досвіду українських і зарубіжних фінансових установ визначено ключові принципи побудови систем кібербезпеки, включно з багаторівневим захистом, управлінням вразливостями, належною аутентифікацією та планами реагування на інциденти. Окрему увагу приділено ролі штучного інтелекту та машинного навчання як інструментам підвищення кіберстійкості. Проаналізовано перспективи впровадження блокчейну й децентралізованих фінансів (DeFi) у глобальному фінансовому середовищі та відповідні виклики для інформаційної безпеки. Наголошено на важливості інтегрованого управління кіберризиками в межах загальної системи операційного ризик-менеджменту фінансових установ. Запропоновано низку практичних рекомендацій щодо оптимізації структури захисту, впровадження міжнародних стандартів та посилення міждержавної координації задля забезпечення довгострокової стійкості фінансового сектору в умовах цифрової трансформації.

Ключові слова: кіберризики, діджиталізація, інформаційна безпека, управління операційним ризиком, штучний інтелект, децентралізовані фінанси, стійкість фінансових установ, оцінка ризиків, ризик-менеджменту

PRYKHODKO Borys
Kyiv National EconomicUniversitynamed after Vadym Hetman

CYBER RISKS IN THE FINANCIAL SECTOR IN THE CONTEXT OF DIGITAL TRANSFORMATION

This article presents a comprehensive analysis of contemporary cyber threats to the financial sector, emphasizing their impact on the stability of financial institutions and payment systems. The study addresses the primary vectors of cyberattacks—phishing, DDoS, malware, targeted APT attacks, and insider threats. Drawing on the experiences of Ukrainian and international financial institutions, the paper identifies key principles for constructing cybersecurity systems, encompassing multi-layered protection, vulnerability management, proper authentication, and incident response planning. Special attention is devoted to artificial intelligence and machine learning as instruments for enhancing cyber resilience. The article also examines the potential for implementing blockchain and decentralized finance (DeFi) within the global financial landscape and the associated information security challenges. The significance of integrated cyber risk management within financial institutions' broader operational risk management framework is underscored. Finally, practical recommendations are offered on optimizing security frameworks, adopting international standards, and bolstering intergovernmental coordination to ensure the financial sector's long-term resilience in the face of digital transformation.

Keywords: cyber risks, digitalization, information security, operational risk management, artificial intelligence, decentralized finance, resilience of financial institutions, risk assessment, risk management.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Фінансовий сектор є однією з найбільш уразливих сфер до кібератак через високу концентрацію коштів і конфіденційних даних. Банківські установи, біржі, платіжні системи зберігають та оперують величезними обсягами фінансової інформації, що робить їх привабливими для кіберзлочинців [1, 2]. З огляду на те, що постійно вдосконалюються методи атак для заволодіння коштами, даними клієнтів, порушення роботи платіжних систем чи шантажу, то кіберінциденти спричиняють не лише прямі фінансові збитки, але й підривають довіру клієнтів, провокують паніку на ринках та мають системні наслідки. За даними досліджень, у 2021 році майже чверть (22,4%) усіх зафіксованих кібератак припадала саме на організації фінансового та страхового сектору [1, 3]. Фінансові установи в середньому більш як у 300 разів частіше піддаються атакам, ніж компанії інших секторів, що підкреслює стратегічність та масштаб проблеми. На міжнародному рівні кіберризики визнані одними з найсерйозніших операційних ризиків, зокрема у США понад 80% банків назвали кіберризики «надзвичайно важливими», що перевищує всі інші категорії операційних ризиків. В Україні питання кібербезпеки також є критичним, особливо в умовах військової агресії рф та зростання кількості атак на фінансовий сектор. У лютому 2022 року українські банки зазнали однієї з найбільших DDoS-атак в історії, яка тимчасово порушила роботу багатьох онлайн-сервісів [4]. Такі інциденти підсвічують потенціал масштабних кіберзагроз для фінансових установ, саме тому проблема забезпечення кіберстійкості фінансового сектору є надзвичайно актуальною і потребує комплексного дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблема забезпечення кібербезпеки у фінансовій сфері набула стратегічного значення і стала предметом пильної уваги як міжнародної, так і української наукової спільноти, особливо з розвитком

глобальної мережи глобальних фінансових інституцій та індустрії фінансових технологій 4,0. Іноземні вчені зазначають, що однією з ключових загроз для фінансових інституцій залишаються атаки типу «фішинг», DDoS, шкідливе програмне забезпечення, а також внутрішні загрози, пов'язані з несанкціонованим доступом до критичної інформації [5]. Водночас, глобальний аналіз загроз підтверджує, що кіберризики мають системний характер, зокрема зазначається, що високий ступінь взаємопов'язаності великих банків провокує каскадне розповсюдження кіберризиків по усьому фінансовому ринку [6]. За оцінками іноземних дослідників, в окремих сценаріях кібератаки можуть спричинити втрати у розмірі 10–30% чистого прибутку фінансових установ [7]. Незважаючи на зростання уваги до проблеми, інституціоналізовані підходи до оцінки кіберризиків залишаються недостатньо розвиненими. На думку Курті Ф., відсутність уніфікованої класифікації та методів кількісного вимірювання кіберризиків унеможливлює ефективну розробку стратегій управління ними [8]. Зазначається, що провідним напрямом підвищення кіберстійкості фінансового сектору є впровадження комплексних систем захисту, побудованих на багаторівневому підході. До таких систем включаються заходи з шифрування, контролю доступу, моніторингу трафіку, управління інцидентами, регулярного аудиту та навчання персоналу [9]. У дослідженні Дорош І., наголошується на важливості створення культури кібербезпеки на рівні організацій та державного регулювання [10]. Водночас, сучасні дослідження виділяють штучний інтелект як перспективний інструмент кіберзахисту, що дає змогу виявляти аномалії в режимі реального часу, автоматизувати реагування на атаки та зменшити людський фактор ризику [11, 12]. Зокрема, машинне навчання ефективно використовується для розпізнавання шкідливих патернів у даних і попередження кібератак ще до їх реалізації. У контексті зростаючої взаємозалежності фінансових систем і впровадження FinTech-рішень, особливу увагу приділяють архітектурі цифрової фінансової інфраструктури, оскільки її уразливість до системних атак ставить нові виклики перед регуляторами та фахівцями з кібербезпеки [13, 14].

Українські дослідники також активно долучаються до вивчення даної проблематики. Зокрема Хомишина І. і Гавц О. підкреслюють необхідність адаптації міжнародних правових механізмів до українського контексту та впровадження цифрових технологій захисту з урахуванням воєнних ризиків [15]. Дослідники Трусова Н. та Чкан І. аналізують сучасні кіберзагрози банківського сектору України, наголошуючи на необхідності формування національної стратегії кіберзахисту на базі ризик-орієнтованого підходу [16]. Інші праці вітчизняних авторів, зокрема Лавренюка В.В., зосереджуються на аналізі практик кіберзахисту у вітчизняних банках, пропонуючи модель управління кіберризиками, адаптовану до українських реалій [17, 18]. Загалом, як глобальний, так і український науковий дискурс сходиться в тому, що ефективна кібербезпека у фінансовому секторі потребує комплексної міждисциплінарної взаємодії, а саме інтеграції технологій, правового забезпечення, організаційного менеджменту та безперервного навчання персоналу.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Дослідження наукових праць іноземних та вітчизняних дослідників дозволило сформулювати ряд невирішених питань, які потребують відповідей. Зокрема, відсутній цілісний механізм інтеграції кіберзахисту в загальну систему корпоративного управління ризиками, що ускладнює планування стійких до атак фінансових бізнес-моделей, особливо у складних цифрових екосистемах. Також, проблема кіберризиків посилюється й тим, що мережевий фінансовий бізнес (використання інтегрованих фінтех-платформ, API, хмарних сервісів) недостатньо вивчений у контексті геополітичних, міждержавних і міжкорпоративних кіберризиків, що відкриває перспективу дослідження нової архітектури кіберстійкості в умовах глобалізації фінансових сервісів.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є проведення комплексного аналізу стану кібербезпеки фінансового сектору та напрацювання практичних рекомендації щодо підвищення кіберстійкості фінансових корпорацій. Для досягнення мети визначено такі завдання: 1) виявити ключові кіберзагрози та ризики у фінансовому секторі; 2) дослідити принципи й кращі практики побудови ефективних систем кіберзахисту фінансових установ, у тому числі міжнародні стандарти безпеки; 3) проаналізувати роль штучного інтелекту та машинного навчання у запобіганні та реагуванні на кіберінциденти в фінансовій сфері; 4) оцінити сучасні тенденції розвитку глобального фінансового середовища (цифровізація, DeFi, блокчейн) та їхній вплив на кібербезпеку.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У сучасних умовах цифрової трансформації фінансовий сектор стає дедалі вразливішим до кіберзагроз, які створюють серйозні виклики не лише для стабільності окремих фінансових установ, а й для цілісності національної та глобальної фінансової системи. Високий рівень автоматизації процесів у банках та інших фінансових установах означає, що навіть поодинокі кіберінциденти можуть спричинити масштабні фінансові, репутаційні та правові наслідки. У зв'язку з цим аналіз ключових кіберзагроз і ризиків є необхідною передумовою для розроблення ефективних механізмів захисту фінансової інфраструктури.

Встановлено, що фінансові установи стикаються з широким спектром кіберзагроз, які постійно еволюціонують. Еволюція цих загроз зумовлена не лише технологічним прогресом, а й зростанням складності фінансових екосистем, зокрема через інтеграцію з фінтех-компаніями та впровадження відкритих API в рамках концепції open banking, що створює нові точки вразливості. Кожна з цих загроз має свої специфічні ризики, але їх об'єднує потенціал значних фінансових втрат і репутаційних збитків (рис. 1).

Рис. 1. Ключові кіберзагрози для фінансового сектору

Джерело: складено автором на основі [2-4, 20-24]

Для ефективної протидії необхідний комплексний підхід до кібербезпеки, який включає впровадження сучасних технологій, таких як штучний інтелект для прогнозування атак, системи SIEM (Security Information and Event Management) для моніторингу в реальному часі, а також посилення регуляторних вимог на національному та міжнародному рівнях.

Шахрайські розсилки та повідомлення, що імітують офіційні комунікації банківських установ, залишаються основним каналом компрометації. Такі атаки спрямовані як на клієнтів, з метою виманювання облікових даних, одноразових паролів чи іншої конфіденційної інформації, так і на співробітників банків через розсилання заражених документів або шкідливих посилань, що можуть призвести до несанкціонованого доступу до внутрішніх систем. Унаслідок цього фішинг є найпоширенішим початковим вектором проникнення, що підтверджується результатами опитувань більшості банків [3]. Для протидії фішингу банки можуть застосовувати системи поведінкового аналізу, які використовують машинне навчання для виявлення аномалій у поведінці користувачів, наприклад, нетипових спроб входу в систему.

Водночас спеціалізовані банківські трояни, такі як TrickBot і Dridex, націлені на крадіжку облікових даних для доступу до систем інтернет-банкінгу і найчастіше поширюються через фішингові листи. Ці шкідливі програми дозволяють зловмисникам не лише викрадати дані, а й отримувати віддалений доступ до банківських систем, що може призводити до значних фінансових втрат. Крім того, програми-вимагачі (ransomware) становлять серйозну загрозу, шифруючи внутрішні дані банків, вимагаючи викуп за їх розблокування та провокуючи збої в роботі критичних систем. Останнім часом атаки програм-вимагачів на фінансові установи стали особливо руйнівними, завдаючи не лише фінансової, а й репутаційної шкоди. Згідно з даними [3], у 2021 році програми-вимагачі становили 21% усіх кібератак на банки, а середні виплати викупу у світі у 2022 році перевищили 800 тис. доларів США і продовжують зростати [19]. Зростання кіберзагроз частково зумовлене низьким рівнем кіберграмотності серед клієнтів і співробітників банків, що робить їх легкою мішенню для зловмисників. Для протидії цьому банки можуть впроваджувати регулярні тренінги з кібербезпеки для персоналу та клієнтів, а також використовувати системи поведінкового аналізу для раннього виявлення фішингових атак.

Зі стрімким розвитком онлайн- і мобільного банкінгу зловмисники активно експлуатують уразливості веб-додатків використовуючи такі типові вектори атак як SQL-ін'єкції, міжсайтовий скриптинг (XSS) та атаки на API сервіси відкритого банкінгу. Такі атаки можуть призводити до викрадення конфіденційних даних клієнтів або несанкціонованих переказів коштів. Не менш серйозною загрозою є кібератаки на системи онлайн-платежів і платіжні шлюзи, які спрямовані на маніпуляцію транзакціями, що може призводити до шахрайських операцій або перехоплення платежів [20]. Для захисту від таких атак банки можуть застосовувати технології шифрування даних і впроваджувати стандарти безпеки, такі як OAuth 2.0 і OpenID Connect, для захисту API. Водночас, розподілені атаки на відмову в обслуговуванні (DDoS) використовуються для виведення з ладу веб-сайтів банків, платіжних систем, та навіть в цілому процесингових центрів. Такі атаки досить часто мотивовані вимаганням викупу за припинення атаки або політичним тиском на фінансові установи. Яскравим прикладом таких атак є DDoS-атаки на найбільші банки України напередодні повномасштабного вторгнення рф у 2022 році, коли системи інтернет-банкінгу ПриватБанку та Ощадбанку стали тимчасово недоступним. Незважаючи на те, що прямі фінансові втрати від DDoS зазвичай не є значними, проте вони суттєво підривають довіру клієнтів до банківської установи та можуть слугувати прикриттям для інших, більш складних проникнень і кібератак [4].

Великі хакерські групи і добре організовані кіберзлочинні картелі (наприклад, Carbanak/FIN7) постійно здійснюють складні, багатоступеневі операції проти фінансових установ по всьому світі [21]. Вони можуть використовувати фішинг для початкового доступу, далі внутрішньомережеве шпигунство, крадіжку облікових даних адміністраторів і, зрештою, викрадення коштів через SWIFT-перекази або компрометацію банкоматів. Відомим випадком є атака на Бангладеський центробанк у 2016 р., коли було викрадено 81 млн дол. шляхом фальшивих SWIFT-транзакцій (класичний приклад, який спричинив посилення безпеки SWIFT на глобальному рівні) [22]. Не менш актуальними є інсайдерські загрози: співробітники з високими привілеями можуть навмисно чи через недбалість сприяти атакам, наприклад, передаючи паролі або встановлюючи бекдори. Для попередження таких ризиків банки можуть впроваджувати системи DLP (Data Loss Prevention) для моніторингу витоку даних і посилювати внутрішній контроль доступу, зокрема через двофакторну аутентифікацію для співробітників.

Кількість кіберінцидентів у фінансовому секторі глобально зростає починаючи з 2010-х рр. і залишається на високому рівні і станом на 2025 рік. У багатьох країнах фінансові установи зобов'язані звітувати про серйозні кібератаки. Наприклад, у США з 2023 р. запроваджено вимогу Комісії з цінних паперів і бірж (SEC) розкривати інформацію про суттєві кібератаки протягом 4 днів [23]. В Україні Національний банк України (НБУ) також посилює вимоги до кібербезпеки, зокрема через впровадження стандартів ISO/IEC 27001 і співпрацю з CERT-UA для оперативного реагування на кіберінциденти. Аналіз кіберризиків демонструє, що прямі фінансові втрати це лише частина збитків, тоді як с супутні витрати (розслідування, відновлення систем, штрафи регуляторів за витік даних, судові позови клієнтів) інколи перевищують прямі втрати від реалізації кіберризиків. Для порівняння, у Великій Британії середній зареєстрований збиток від кіберінцидентів (без урахування великих витоків) для середніх компаній у 2023 році становив близько 10,8 тисяч фунтів стерлінгів, але ця цифра не враховує потенційно катастрофічні сценарії [24]. У США, за даними IBM Security (2023), середня вартість витоку даних у фінансовому секторі сягала 5,9 млн доларів, що значно перевищує середній показник по інших галузях (4,45 млн доларів), що підкреслює особливу вразливість фінансових установ.

В Україні, від початку повномасштабного вторгнення кількість кіберінцидентів постійно зростає, що посилюється активністю кібератак на критичну інфраструктуру, в тому числі фінансову. За даними команди реагування на комп'ютерні надзвичайні події України (CERT-UA) загальна кількість кіберінцидентів потроїлася у 2024 році, порівняно з 2021 роком (рис. 2). Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи. Фахівці CERT-UA зазначають, що об'єктами кібератак є об'єкти фінансового сектору, які відіграють критичну роль для підтримки, обслуговування оборонно-промислового комплексу та військових.

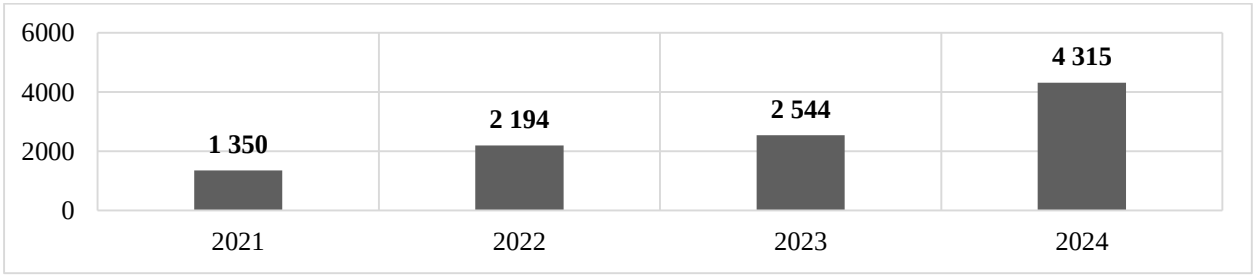

Рис. 2. Кіберінциденти зафіксовані CERT-UA за 2021-2024 рр.

Джерело: складено автором на основі [25-28]

Водночас, за даними Ситуаційного центру забезпечення кібербезпеки Служби безпеки України частка реалізації кіберризиків фінансового сектору у загальному переліку інцидентів складає близько 20% за останні 2 роки (рис. 3). Отже, кіберризики у фінансовому секторі є системною загрозою, що вимагає проактивного управління.

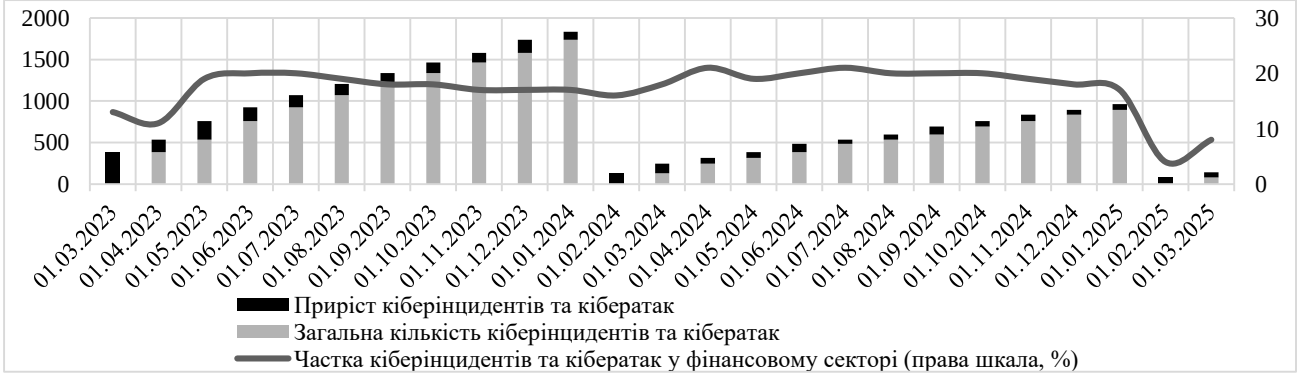

Рис. 3. Кіберінциденти зафіксовані СЦЗК СБУ з 01.03.2023 по 01.03.2025 рр.

Джерело: складено автором на основі [29]

Для протидії згаданим загрозам фінансові установи мають вибудовувати багаторівневу систему захисту, що охоплює всі технології, процеси та персонал. На основі аналізу міжнародних стандартів і практик сформулюємо ключові принципи кіберзахисту фінансового сектора [30, 31]:

— багаторівневий захист (defense-in-depth);
— постійний моніторинг і виявлення інцидентів;
— надійна аутентифікація та управління доступом;
— управління вразливостями та оновлення;
— управління інцидентами та забезпечення безперервності бізнесу;
— відповідність міжнародним та вітчизняним стандартам і регуляціям;
— навчання персоналу та підвищення культури безпеки.

Відзначимо, що жоден окремий інструмент кібербезпеки не гарантує повний захист, тому має використовуватися концепція «глибоко ешелонованої кібербезпеки» через впровадження декількох незалежних шарів контролю безпеки: 1) мережеві брандмауери та системи запобігання вторгненням (IPS); 2) захист кінцевих точок (антивірус, EDR); 3) засоби аутентифікації та авторизації, шифрування даних, контроль доступу на основі ролей тощо. Кожен шар слугує буфером для попереднього, тому якщо кібератака обійшла мережевий екран, її може зупинити відсутність необхідних прав доступу або моніторинг аномалій в поведінці

Ефективна система кібербезпеки повинна не лише запобігати вторгненням, а й вчасно їх виявляти і для цього фінансові установи мають розгортати центри моніторингу безпеки (SOC), оснащені SIEM-системами, які збирають логи з усіх критичних систем та в режимі реального часу аналізують їх на предмет підозрілих інцидентів. Водночас, важливо вести журнали реєстрації подій (лог-файли) на всіх вузлах і зберігати їх достатньо довго, утім, за даними опитувань, лише близько 15% українських підприємств загалом займаються повноцінним веденням логів безпеки [32], що вказує на прогалини у можливостях виявлення кіберінцидентів (рис. 4).

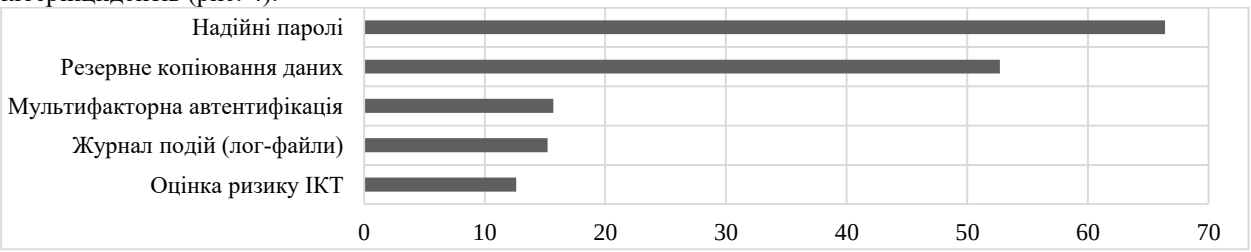

Рис. 4. Частка українських підприємств, що впроваджують окремі заходи кібербезпеки (2023 р.), %
Джерело: складено автором на основі [32]

Зауважимо, що саме компрометація облікових записів є одним із найнебезпечніших сценаріїв, тому критичною є реалізація багатофакторної автентифікації (MFA) для доступу до важливих систем. У міжнародній практиці MFA є усталеною практикою для адміністраторів і користувачів, проте багато організацій ще ігнорують такі інструменти. Наприклад, в Україні MFA запровадили лише близько 16% підприємств, тоді як більшість (понад 66%) обмежуються тільки складними паролями [32].

Фінансові установи мають застосовувати принцип мінімальних привілеїв де кожен співробітник повинен мати тільки той рівень доступу, який необхідний для виконання його функцій та регулярно проводити перегляд прав доступу, особливо при зміні посад чи звільненні персоналу. Оскільки фінансові установи експлуатують складні IT-екосистеми тому важливо налагодити процес управління вразливостями, а саме регулярне сканування систем на наявність вразливостей, оперативне встановлення оновлень безпеки (патчів). Багато атак (наприклад, експлойти EternalBlue у вірусі NotPetya) стали можливими через несвоєчасне оновлення критичних систем тому фінансові установи все частіше впроваджують практику bug bounty та пентестів залучаючи незалежних експертів для перевірки захищеності власних систем. Наприклад, у Великій Британії програмою CBEST визначено регулярне проведення контрольованих пентестів критично важливих фінансових організацій за сценаріями, наближеними до реальних кібератак.

Важливо розуміти, що жодна система не гарантує 100% кіберзахисту, тому фінансова установа повинна бути готовою до швидкого реагування та відновлення діяльності, тому принципово необхідно мати план дій на випадок кіберінцидентів (Incident Response Plan), де розписані ролі й процедури (виявлення і локалізації атаки, ліквідація наслідків та повідомлення регуляторів і клієнтів). Водночас, важливо регулярно проводити тренування (table-top exercises) які допомагають відпрацювати такі кризові плани. Крім того, одночасно повинні впроваджуватися плани забезпечення безперервності бізнесу (BCP) та план відновлення після катастроф (DRP), що також охоплюють сценарії кібератак. Наприклад, міжнародні стандарти BIS рекомендують фінансовим ринковим інфраструктурам забезпечувати відновлення критичних функцій не більше ніж за 2 години після серйозної кібератаки [33].

У такому контексті управління кіберризиками зокрема в Україні набуває стратегічного значення як один із ключових компонентів загальної системи управління операційними ризиками фінансових установ.

Вважаємо, що управління ризиками інформаційної безпеки (ІБ) та інформаційно-комунікаційних технологій (ІКТ) має бути повністю інтегроване у внутрішню політику та базуватись на моделі трьох ліній захисту, яка охоплює всі рівні управлінських та контрольних функцій. Враховуючи міжнародні практики та вітчизняний досвід виділено ключові організаційні підходи до управління кіберризиками фінансового бізнесу (табл. 1).

Таблиця 1

Ключові положення щодо управління кіберризиками

№ з/п	Напрям регулювання	Вимоги
1	Інтеграція в ERM	Кіберризики (ІСТ-ризики та ризики ІБ) визнаються частиною операційного ризику, інтегрованого в загальну систему управління ризиками
2	Три лінії захисту	Чітко визначена відповідальність першої (бізнес-підрозділи), другої (підрозділи з ризиків) та третьої лінії (аудит)
3	Політика управління ризиками ІБ та ІСТ	Повинна містити мету, цілі, вплив на стратегію, структуру управління, критерії інцидентів, інструменти, моніторинг
4	Оцінка ризиків	Щорічна оцінка ризиків, включно з кількісними та якісними індикаторами
5	Стрес-тестування кіберризиків	Вимагається щороку. Можливе використання сценарного аналізу або математичного моделювання
6	Безперервність діяльності	План має враховувати ризики кіберінцидентів. Визначається RTO та RPO
7	Аутсорсинг функцій ІБ/ІСТ	Дозволено лише з дотриманням вимог щодо конфіденційності, відповідальності та звітності
8	Звітування	KRI, база подій, самооцінка, сценарний аналіз, інформування правління про критичні ризики

Джерело: складено автором на основі [34, 35].

Важливо, що фінансовий сектор високорегульований в частині кібербезпеки, зокрема, фінансові установи дотримуються вимог стандартів PCI DSS (для захисту даних власників платіжних карток), SWIFT CSP (програма безпеки для членів системи SWIFT), національних нормативів (наприклад, вимоги НБУ в Україні або FFIEC в США). У ЄС з 2025 року набула чинності регуляція DORA, яка зобов'язує банки та інші фінансові установи впровадити цілісний підхід до управління IT-ризиками та регулярно проводити розширені тестування (TLPT) своїх інформаційних та комунікаційних систем [36, 37]. Однак, відповідність стандартам не гарантує відсутності інцидентів, але створює необхідний базис безпеки та підзвітності. Водночас, ефективне управління кіберризиками неможливе без системної оцінки рівня загроз, вразливостей і залишкових ризиків. У цьому контексті регуляторні вимоги та міжнародні підходи передбачають застосування комплексу аналітичних інструментів, що дозволяють забезпечити як стратегічне, так і тактичне бачення ризикового профілю установи крізь призму кіберзагроз (табл. 2).

Таблиця 2

Інструменти оцінки кіберризиків у фінансовому бізнесі

Інструмент оцінки	Призначення	Частота застосування
База внутрішніх подій	Агрегація кіберінцидентів і збитків	Постійно
Самооцінка ризиків (RSA)	Визначення вразливостей і залишкових ризиків	Щорічно
Сценарний аналіз	Оцінка екстремальних подій з низькою ймовірністю	Щорічно
Стрес-тестування	Аналіз впливу різних сценаріїв кіберкатастроф	Щорічно (мінімум)
KRI (ключові індикатори ризику)	Моніторинг динаміки ризику в реальному часі	Квартально або частіше

Джерело: складено автором на основі [35].

Для посилення оцінки кіберризиків пропонується вдосконалити наявний інструментарій шляхом систематизації загроз за рівнем імовірності їх настання та масштабами потенційних втрат. З цією метою автором розроблено матрицю оцінки кіберінцидентів (табл. 3), яка дозволяє структурувати та класифікувати ризики з урахуванням їхньої специфіки у фінансовому секторі.

Для побудови цієї матриці автором ґрунтовно проаналізовано і враховано передові практики та дослідження провідних організацій у галузі кібербезпеки фінансових установ, зокрема: IBM, ENISA, SWIFT CSP Guidance, Deloitte, FireEye, Mandiant, Cisco, Recorded Future. Також важливо інтегрувати напрацювання вітчизняних організацій, дотичних до протидії кіберзагрозам у фінансовій сфері, а саме Національного банку України та спеціалізованого структурного підрозділу CERT-UA Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Такий синтез міжнародного досвіду та локальних підходів дозволить адаптувати матрицю до реалій українського банківського сектору, враховуючи його унікальні виклики, такі як підвищена вразливість до геополітичних кібератак. Запропонований комплексний підхід дозволить класифікувати типові кіберінциденти за низкою ключових параметрів: категорія кіберінциденту, ймовірність його настання, розмір потенційних втрат для фінансової установи, характеристика ймовірних втрат (фінансові, репутаційні, операційні). Завдяки цьому банки отримують практичний інструмент для ідентифікації, оцінки та пріоритизації кіберризиків, що сприяє ефективнішому управлінню безпекою.

Крім того, вважаємо, що авторська матриця може бути інтегрована в ширшу систему ризик-менеджменту банків, зокрема в рамках вимог НБУ до внутрішнього контролю та комплаєнсу. Це дозволить не

лише реагувати на інциденти, а й прогнозувати потенційні загрози, що є особливо актуальним в умовах швидкої цифровізації банківських послуг і зростання складності кібератак. Таким чином, запропонований підхід не лише відповідає сучасним викликам, а й закладає основу для проактивного управління кіберризиками в банківському секторі України.

Таблиця 3

Матриця оцінки кіберінцидентів у фінансовому секторі

Категорія кіберінциденту	Ймовірність	Потенційні втрати	Обгрунтування ймовірності	Обгрунтування втрат	Джерела
Несанкціонований доступ	Висока	Високі	Висока частота інцидентів у фінансовому секторі	Компрометація адміністраторів = доступ до критичних систем	IBM; ENISA
Порушення цілісності інформації	Середня	Високі	Менш поширене, однак складне виявлення змін у даних	Може призвести до маніпуляцій з транзакціями	Deloitte; SWIFT CSP Guidance
DoS / DDoS-атаки	Висока	Середні	Регулярно фіксуються атаки на банківські сайти	Порушення доступності → втрати довіри, штрафи, рідко прямі фінансові втрати	CERT-UA; НБУ; Cloudflare
Несанкціоноване використання ресурсів	Середня	Середні	Використовується ботнетами, менш поширене, але зростає	Ресурси можуть бути використані для зловмисної діяльності	Verizon; CrowdStrike
Шкідливе ПЗ (Ransomware)	Висока	Високі	Ransomware — 21% усіх інцидентів у фінансовому секторі	Шифрування даних, простої, виплата викупу. $5–10 млн/інцидент	IBM; Mandiant
Фішинг і соціальна інженерія	Дуже висока	Середні	Фішинг — причина до 90% атак	Компрометація облікових записів клієнтів, фінансові збитки	Verizon; ENISA; CERT-UA
Компрометація каналів зв'язку	Середня	Середні	Технічно складні атаки на VPN, DNS; менш часті, але небезпечні	Компрометація внутрішнього трафіку, прослуховування, підміна	ENISA; Cisco
Порушення ІКС критичної інфраструктури	Низька	Дуже високі	Дуже рідкісне, але критичне за потенціалом	Може зупинити процесинг, банкомати, розрахунки; потенціал системного ефекту	CERT-UA; НБУ; IMF
Zero-day уразливості	Середня	Дуже високі	Середня ймовірність, але часто використовується в APT-атаках	Повний контроль над системами після експлуатації критичних вразливостей	FireEye M-Trends; ENISA; Recorded Future
Витік даних через третіх сторін	Середня	Середні - Високі	Зростання інцидентів через постачальників; проблема ланцюгів постачання	Витоки персональних даних, штрафи за GDPR або локальне регулювання	ENISA; IBM X-Force Cloud Security

Джерело: складено автором на основі [25-28, 34, 38-43].

Відзначимо, людський фактор все ще залишається вразливим місцем фінансових компаній, оскільки навіть ідеальні технічні рішення можуть бути даремними, якщо співробітники порушують правила. Саме тому ефективні системи кіберзахисту мають передбачати програми регулярного навчання персоналу: 1) тренінги з розпізнавання фішингу; 2) симуляції атак (фішинг-кампанії з навчальною метою); 3) інструктажі щодо реагування при підозрілих подіях. Кібергігієна та високий рівень культури кібербезпеки має стати частиною корпоративної культури, що вимагає від керівництва компанії формування чіткої політики кібербезпеки, проведення тренінгів з підвищення обізнаності та пропаганди ризик-орієнтованого мислення.

Зауважимо, що ключові аспекти кіберзахисту фінансового сектора варто підсилювати і сучасними, трендовими технологіями. Саме штучний інтелект (ШІ) та машинне навчання (ML) вже стають невід'ємною складовою сучасних систем кібербезпеки, особливо у фінансовому секторі, де обсяги даних і швидкість атак вимагають автоматизації захисних заходів. Проведене дослідження підтверджує, що ШІ /ML технології вже зараз виконують важливі функції у забезпеченні безпеки фінансових установ: 1) інтелектуальне виявлення загроз; 2) автоматизація реагування на інциденти; 3) виявлення шахрайства та аномалій у транзакціях; 4) оцінка кіберризиків та уразливостей; 5) аналіз поведінки користувачів (UBA) та виявлення інсайдерів.

Алгоритми машинного навчання можуть аналізувати величезні масиви даних (мережевий трафік, логи, транзакції) для пошуку патернів, що вказують на кіберзагрозу. Наприклад, фінансова мережа генерує тисячі подій на секунду – ШІ-системи навчені розрізняти нормальну активність від аномальної (нетиповий порядок запитів, незвичний час звернень до систем тощо). На основі цього вони здатні виявляти вторгнення у реальному часі, зокрема атаки «нульового дня», які не розпізнаються сигнатурними антивірусами і за рахунок безперервного самонавчання на нових даних такі моделі підвищують точність детектування з плином часу [44]. До прикладу, сучасні рішення класу SOAR (Security Orchestration, Automation and Response) дедалі частіше доповнюються ШІ -модулями, що дозволяє автоматично виконувати початкові кроки реагування на

загрози. Далі, якщо ШІ виявив аномальну активність на робочій станції, система може автоматично ізолювати цей хост від мережі, сповістити адміністраторів і розпочати збір даних про інцидент [44]. Для фінансових установ, де кібератаки швидко поширюються, така швидкість реагування штучного інтелекту критично важлива і мінімізує ймовірні збитки. В останні роки, завдяки ML-алгоритмам багато фінансових установ значно покращили власні системи fraud detection. Такі моделі аналізують поведінку клієнтів (типові суми, торгові точки, час операцій) і миттєво ставлять під сумнів транзакції, що відхиляються від нормального профілю. Наприклад, якщо раптом з картки здійснюється незвично велика покупка в іншій країні, система може автоматично заблокувати операцію або попросити додаткове підтвердження. За оцінками, впровадження AI для моніторингу транзакцій дозволило деяким фінансовим установам скоротити прямі збитки від платіжного шахрайства на 30-50% [45]. Важливо, що такі системи можуть самонавчатися оскільки вони підлаштовуються під зміни в поведінці клієнтів або появу нових схем шахрайства. Також, ШІ використовується для проактивного сканування вразливостей та оцінки ризику, зокрема спеціалізовані моделі аналізують конфігурацію мережі компанії і прогнозують, які вузли є найбільш вразливими, або яку шкоду завдасть компрометація того чи іншого сервера, що допомагає пріоритизувати зусилля з посилення захисту. Деякі великі банки використовують ШІ для кіберстрес-тестування через моделювання тисячі можливих сценаріїв атак і на основі результатів оцінюють ймовірні збитки, щоб визначити адекватність резервів і страхового покриття [44, 46, 47].

Встановлено, що впровадження ШІ у кібербезпеку фінансових установ вже приносить результат, зокрема інструменти User Behavior Analytics на базі ML відслідковують типові шаблони дій кожного користувача в системі (робочий час, частота доступу до тих чи інших даних, типові запити) [48]. При ідентифікації відхилень, наприклад, співробітник починає масово копіювати бази клієнтів або звертатися до систем, якими раніше не користувався то система сигналізує про потенційно небезпечну поведінку. Таким чином ШІ допомагає виявляти як зламані акаунти, так і інсайдерські загрози, особливо у великих банках з десятками тисяч працівників де робити це вручну неможливо. Згідно з галузевими опитуваннями, 74% фінансових установ вже застосовують ШІ для виявлення фінансових злочинів та шахрайства [46]. Великі банки інвестують у власні центри розробки ШІ-рішень або співпрацюють зі стартапами у сфері кібербезпеки. У 2023 році світові витрати фінансового сектору на ШІ (не лише в безпеці) становили близько 35 млрд дол., значна частка з яких витрачені саме на ризик-менеджменту і кіберзахист [47]. Водночас, дослідження вказують на ряд викликів, пов'язаних із ШІ в кібербезпеці, зокрема: 1) хибні спрацьовування і брак прозорості; 2) проблеми з даними та конфіденційністю; 3) інтеграція зі спадковими системами; 4) нові загрози, пов'язані з ШІ [44-47].

ШІ-моделі часто працюють як «чорні скриньки», що може приводити до неправильного ігнорування загроз (якщо модель недонавчена), так і до надмірної чутливості (коли генерується багато помилкових тривог). Останнє особливо проблемно для SOC, де аналітики можуть почати ігнорувати сигнали системи тому потрібен баланс та налаштування алгоритмів, а також залучення кваліфікованих експертів для перевірки хибних спрацьовувань. Також, для навчання моделей потрібні великі вибірки даних про кібератаки та природню поведінку користувачів. Найчастішою проблемою є те, що фінансові установи не мають достатньої бази якісних даних або дані диверсифіковані по різних джерелах. Окрім цього, використання конфіденційних даних клієнтів для навчання ШІ може суперечити регуляторним вимогам (GDPR тощо), тому дедалі частіше застосовується аномалізовані або синтетичні дані, а також техніки федеративного навчання, коли модель навчається без прямого доступу до конфіденційних даних. Також, багато фінансових установ мають застарілі соге-системи, які складно інтегрувати із сучасними ШІ -рішеннями, що вимагає оновлення інфраструктури, побудови data lake, об'єднання розрізнених сховищ даних. Є досвід вирішення цієї проблеми шляхом побудови окремого шару безпеки над існуючими системами, куди потім агрегуються потрібні дані. Варто відзначити, що ШІ являється інструментом, доступним не лише для безпеки, а і для проведення кібератак, оскільки вже фіксуються випадки, коли для створення переконливих фішингових повідомлень або для автоматизації пошуку вразливостей застосовують генеративні моделі. Також, з'являється ризик атак на самі ШІ-системи, зокрема внесення модифікованих даних для «обману» моделі.

Відповідно, роль штучного інтелекту у кібербезпеці фінансового сектора має двоякий характер. З одного боку, ШІ вже зараз суттєво покращує можливості виявлення та реагування на загрози, дозволяючи випереджати більшість автоматизованих атак. З іншого боку, швидка еволюція ШІ вимагає від фінансових корпорацій підходити з обережністю, враховуючи можливі побічні ефекти використання і забезпечуючи належний нагляд за алгоритмами (наприклад, введенням ролі офіцера з питань ШІ-етики або кіберризиків). В цілому, більшість експертів сходяться на думці, що переваги ШІ у кіберзахисті переважають ризики, і його грамотне використання стане одним з ключових факторів кіберстійкості банків майбутнього.

Досліджені технології важливі у контексті сучасних кіберзагроз, оскільки глобальний фінансовий бізнес протягом останніх років зазнав стрімкої цифрової трансформації, що змінило його «мережеву організацію» – тобто спосіб, у який фінансові послуги надаються та взаємопов'язані через цифрові мережі. Такі процеси створюють нові можливості для розвитку, але й генерують нові виклики у сфері безпеки, тому важливо розуміти ключові тенденції (рис. 5).

Рис. 5. Цифрові тенденції розвитку мережевої організації глобального фінансового бізнесу
Джерело: складено автором на основі [49-52].

Станом на 2020 рік кількість користувачів онлайн-банкінгу у світі досягла 2,6 млрд, а за оцінками, до 2024 р. цифровими каналами буде користуватися 3,6 млрд осіб. Уже до 2025 року до 90% всіх взаємодій клієнтів з банками відбуватиметься через цифрові канали (мобільні додатки, інтернет-банкінг) [49]. Така масова міграція в онлайн дозволила фінансовим установам суттєво розширити охоплення та підвищити ефективність, але водночас різко збільшила навантаження на IT-інфраструктуру і зробила її критично важливою. Будь-який збій або кібератака, що порушує роботу цифрових сервісів, безпосередньо впливає на мільйони користувачів. Водночас, цифровізація розмиває межі між внутрішньою і зовнішньою мережею банку – клієнтські застосунки, інтернет-банкінг, хмарні сервіси тісно інтегровані з основними системами установи. У такому контексті, необхідно переосмислити архітектуру безпеки, наприклад перехід до Zero Trust, сегментація мережі або захист API. Також зростає значення віддаленого банкінгу, особливо після пандемії COVID-19 коли більшість банків оптимізували відділення і зробили ставку на дистанційні послуги, що збільшило залежність від мережевих технологій.

Останні роки характеризуються стрімким розвитком фінтех-компаній та платформ, що супроводжується інтеграцією нових учасників у фінансову екосистему, такмх як необанки, платіжні стартапи та платформи P2P-кредитування, які , які дедалі частіше співпрацюють із традиційними фінансовими установами. Згідно з дослідження PwC, 82% традиційних фінансових установ планують в найближчі роки посилити партнерство з фінтех-компаніями, що свідчить про формування єдиної фінансової мережі. У такий мережібанки, наприклад, надають інфраструктуру та ліцензію, а фінтех-компанії забезпечують інноваційні рішення та зручні сервіси дя клієнтів. Водночас, ініціатива відкритого банкінгу (open banking), регламентована в ЄС директивою PSD2, зобов'язує банки надавати доступ до своїх даних і сервісів через API стороннім розробникам за умови дотриманням згоди клієнтів. Станом на 2022 рік понад 56% банків у світі вже реалізували відкриті API в рамках open banking [49]. Такий порядок речей створює нову мережеву архітектуру фінансів (чи фінансової системи), де дані передаються між різними організаціями через стандартизовані інтерфейси забезпечуючи більшу прозорість і доступність фінансових послуг. З погляду кібербезпеки така трансформація породжує нові виклики. Забезпечення захисту API стає критично важливим завданням, що включає аутентифікація запитів, шифрування, захист від ботів та ретельний контроль доступу третіх сторін до банківських систем. Відзначимо, що кількість атак на API фінансових сервісів постійно зростає, адже вони є привабливим каналом для доступу до цінних даних. У зв'язку з цим впровадження сучасних стандартів безпеки, таких як OAuth 2.0 та OpenID Connect (OIDC) , та ефективна клієнтська аутентифікація стають обов'язковими вимогами для забезпечення безпеки відкритих фінансових екосистем. Це також вимагатиме від банків розробки чітких процедур оцінки ризиків співпраці з новими партнерами, а також регулярно проводити аудит безпеки API-інтерфейсів.

Цікавим трендом, який може сприяти мінімізації кіберризиків у фінансовій сфері є розвиток DeFi, що являє собою сукупність фінансових сервісів, які працюють на базі блокчейн-платформ без традиційних фінансових посередників. Пік розвитку DeFi припав на 2020–2021 роки, коли обсяг заблокованих коштів у таких протоколах виріс у десятки разів і перевищив 100 млрд дол. [50]. За такої ситуації проявився потенціал DeFi як альтернативи традиційному фінансовому посередництву, що у перспективі може зробити DeFi частиною глобальної фінансової системи (використання смарт-контрактів для клірингу і розрахунків пришвидшує та здешевлює операції). Зокрема, Central Bank Digital Currencies (CBDC), які зараз розглядаються багатьма країнами, також технологічно споріднені з блокчейном. Однак, у 2021–2023 рр. виявлено значну кількість уразливостей DeFi-протоколів, коли хакери активно експлуатували помилки в смарт-контрактах та компрометували приватні ключі, і сумарні збитки від зломів за 2016–2023 рр. оцінено в понад 7,4 млрд дол. [51, 52]. Проте, вже сьогодні з'являються компанії аудиту смарт-контрактів, страхові протоколи для покриття

кіберризиків та вдосконалюються стандарти програмування безпечних смарт-контрактів (наприклад, Solidity Secure Development Guidelines). Окрім суто децентралізованих додатків, технологія розподіленого реєстру (DLT) активно досліджується і впроваджується консорціумами фінансових установ у світі. Хоча блокчейн технологія вважається стійкою до несанкціонованої модифікації даних (завдяки криптографічним методам), але захист кінцевих вузлів (нод) і ключів залишається критичним, оскільки компрометація даних одного з учасників консорціуму може порушити цілісність всіх даних. Також, якщо алгоритми консенсусу чи смарт-контракти містять логічні помилки, це може бути так використано для кібератак. В цілому, інтеграція блокчейн-рішень у фінансову інфраструктуру вимагає дотримання всіх традиційних заходів кібербезпеки додатково із специфічними (захист приватних ключів, аудит смарт-контрактів).

Міжнародні платіжні системи (SWIFT, VISA, Mastercard), фінансові ринки, обмін фінансовим даними все це формує єдину мережу, де учасники залежать один від одного, що означає, якщо кіберінцидент станеться в одній країні це може мати наслідки і на глобальному рівні. Наприклад, атака вірусу NotPetya у 2017 р., націлена здебільшого на Україну, паралізувала й міжнародні компанії, включно з дочірніми структурами великих банків. Регулятори і міжнародні організації усвідомлюють цей системний кіберризик, зокрема МВФ у Звіті про глобальну фінансову стабільність моделював сценарії, за яких одночасна кібератака на системно важливі фінансові установи може призвести до глобальної кризи. Відповідно, посилюється транскордонна співпраця у сфері кібербезпеки шляхом створення міжнародних платформ обміну інформацією про кіберзагрози. Наприклад FS-ISAC (Financial Services Information Sharing and Analysis Center) об'єднує понад 7 000 фінансових організацій по всьому світу для оперативного обміну сповіщеннями про нові атаки та індикаторами компрометації.

Тенденції цифровізації і нових технологій зумовили реакцію регуляторів у різних країнах. Зокрема ЄС запровадив DORA, яка набула чинності на початку 2025 р. і вимагає від фінансових установ створити цілісну систему кібербезпеки з регулярною звітністю про інциденти та аудитом постачальників ІКТ. У Великій Британії Банк Англії опублікував вимоги до операційної стійкості фінансового сектору, зокрема щодо контролю ризиків в ланцюгах постачання технологій [53]. У США регулятори (FED, OCC) оновили керівництва FFIEC, а також впроваджують положення щодо обов'язкового розкриття кібератак публічними компаніями [54]. Отже, на глобальному рівні формується тренд до обов'язкового дотримання кіберстандартів і тестування, що повинно підвищити стійкість мережевої фінансової екосистеми. Для України, яка є частиною світової фінансової спільноти, ці тенденції також є визначальними і вітчизняні фінансові установи вже впроваджують сучасні цифрові практики кіберзахисту. Україна поступово гармонізує нормативну базу з ЄС, зокрема ухвалено Закон «Про критичну інфраструктуру» [55], впроваджуються вимоги НБУ щодо кіберзахисту банків [34]. Проте викликом залишається протидія кіберзагрозам у контексті війни – російські хакерські групи й надалі намагаються атакувати фінансову систему України. Незважаючи на це, позитивно, що український фінансовий сектор постійно посилює співпрацю з міжнародними партнерами у сфері кібербезпеки, отримуючи допомогу у підвищенні кіберстійкості.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Проведене дослідження підтвердило, що кібербезпека фінансового сектору в сучасних умовах є критичним чинником стабільності та успішності фінансових інституцій. Зокрема, встановлено, що спектр кіберзагроз для фінансового сектору є вкрай широким та динамічним і фінансові установи залишаються пріоритетними для кіберзлочинців, про що свідчить непропорційно висока частка атак на цей сектор. Основні загрози включають фішинг, шкідливе ПЗ (особливо програми-вимагачі), експлуатацію уразливостей веб-систем, DDoS та APT-атаки. Особливо небезпечними є комплексні атаки на платіжну інфраструктуру та міжбанківські мережі, які можуть мати системний ефект, тому кіберризики слід розглядати як одні з найзначніших операційних ризиків фінансового бізнесу. Доведено, що ефективний кіберзахист фінансових компаній має бути багаторівневим і всеосяжним оскільки вимагає глибокої інтеграції у цифрову інфраструктуру та структуруватися із незалежних шарів безпеки. Важливими компонентами є сучасні засоби захисту мережі та кінцевих точок; системи моніторингу та аналізу подій з використанням ШІ-аналітики; жорсткі політики керування доступом (MFA, Zero Trust); регулярне оновлення та пентестування систем; готовність до інцидентів (плани реагування, резервні копії, тренування персоналу). Керівництво повинно приділяти належну увагу кіберризикам – зокрема, включати метрики кібербезпеки до KPI бізнесу, інвестувати у підготовку кадрів, а дотримання принципів кібергігієни має стати частиною корпоративної культури фінансових установ. Водночас, для глобальної фінансової стабільності важливо, щоб усі вузли мережі мали мінімально необхідний рівень кібербезпеки, що вимагає розширення інтернаціональних програм обміну досвідом, грантову підтримку кіберініціатив, спільних досліджень кіберризиків. Окремо слід координувати зусилля з протидії кіберзлочинності, зокрема удосконалювати транскордонні правові механізми притягнення до відповідальності. Фінансові компанії, які активно інвестують у кіберстійкість не лише запобігають ймовірним збиткам, а й підвищують довіру клієнтів та регуляторів, зміцнюючи свою конкурентну позицію на ринку. Український фінансовий сектор, інтегрований у світовий і має всі передумови для впровадження найкращих практик кібербезпеки та повинен розглядати її як невід'ємну складову своєї стратегії розвитку в

цифрову епоху. Розширення державної політики та міжнародної підтримки в цій сфері здатні прискорити прогрес і забезпечити надійний фундамент для безпечного розвитку фінансової системи.

Література

1. Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022. *Automated Security Validation Platform. Picus*. URL: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022#:~:text=Dr,2022 (дата звернення: 29.02.2025)
2. Cyber Security in Finance: Key Threats and Strategies. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/#:~:text=According%20to%20Statista,%20in%20the,continuous%20evolution%20in%20security%20practices (дата звернення: 29.02.2025)
3. Top Cybersecurity Statistics, Facts, and Figures for 2022. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics#:~:text=1,worry%20about%20ransomware (дата звернення: 29.02.2025)
4. DDOS-атаки, що здійснювалися на українські банки. *НАБУ*. URL: https://nabu.ua/ua/ddos-ataki-shcho-zdiysnyuvalisya-na-ukrayinski-banki-vidbito.html (дата звернення: 29.02.2025)
5. Darem A. A., Alhashmi A. A., Alkhaldi T. M., Alashjaee A. M., Alanazi S. M., Ebad S. A. Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. *IEEE Access*. 2023. Vol. 11. P. 125138–125158. URL: https://doi.org/10.1109/ACCESS.2023.3327016 (дата звернення: 29.02.2025)
6. Johnson K. N. Cyber Risks: Emerging Risk Management Concerns for Financial Institutions. *Regulation of Financial Institutions eJournal*. 2015. URL: https://digitalcommons.law.uga.edu/glr/vol50/iss1/7/ (дата звернення: 29.02.2025)
7. Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *SSRN Electronic Journal*. 2018. URL: https://doi.org/10.2139/ssrn.3203026 (дата звернення: 29.02.2025)
8. Curti F., Gerlach J. R., Kazinnik S., Lee M., Mihov A. Cyber risk definition and classification for financial risk management. *Journal of Operational Risk*. 2023. URL: https://doi.org/10.21314/jop.2022.036 (дата звернення: 29.02.2025)
9. Reddem P.R. Cybersecurity in Banking and Finance : Navigating the Digital Threat Landscape. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2024. Т. 10, № 5. С. 852–861. URL: https://doi.org/10.32628/cseit241051073 (дата звернення: 29.02.2025)
10. Dorosh I. Cyber security and its role in the financial sector: threats and protection measures. *Economics. Finances. Law*. 2023. Т. 10. С. 48–51. URL: https://doi.org/10.37634/efp.2023.10.10 (дата звернення: 29.02.2025)
11. Nwafor K. C., Ikudabo A. O., Onyeje C. C., Ihenacho D. O. T. Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. *International Journal of Science and Research Archive*. 2024. Т. 13, № 1. С. 2895–2910. URL: https://doi.org/10.30574/ijsra.2024.13.1.2014 (дата звернення: 29.02.2025)
12. Eriamiatoe F. E. The Role of Machine Learning in Solving Cybersecurity Challenges in the Financial Sector. *International Journal of Scientific and Research Publications*. 2024. Т. 14, № 9. С. 68–72. URL: https://doi.org/10.29322/ijsrp.14.09.2024.p15313 (дата звернення: 29.02.2025)
13. Umoga U. J., Sodiya E. O., Amoo O. O., Atadoga A. A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*. 2024. Т. 11, № 1. С. 1810–1817. URL: https://doi.org/10.30574/ijsra.2024.11.1.0284 (дата звернення: 29.02.2025)
14. Dhingra D., Ashok S., Kumar U. Demystifying Global Cybersecurity Threats in Financial Services. *Handbook of Research on Advancing Cybersecurity for Digital Transformation*. 2021. С. 181–202. URL: https://doi.org/10.4018/978-1-7998-6975-7.ch010 (дата звернення: 29.02.2025)
15. Хомишин І., Гавц О. Забезпечення кібербезпеки у фінансовому секторі: правовий та технологічний аспекти. *Електронне наукове видання «Науковий вісник Ужгородського національного університету». Серія: Право*. 2023. Т. 10, № 40. С. 170–178. URL: https://doi.org/10.23939/law2023.40.170 (дата звернення: 29.02.2025)
16. Трусова Н. В., Чкан І. О. Кіберзахист банківської системи України в умовах цифрових трансформацій. *Науковий вісник Таврійського державного агротехнологічного університету*. 2023. Т. 1, № 47. С. 151–163. URL: https://doi.org/10.31388/2519-884x-2023-47-151-163 (дата звернення: 29.02.2025)
17. Лавренюк В. В. Ключові драйвери кібер-ризиків фінансових установ. *Сучасні гроші, банківські послуги та фінансові інновації в цифровій економіці : матеріали IV Всеукр. наук.-практ. інтернет-конф. студентів, аспірантів і молодих вчених, Київ, 12 квіт. 2021 р.* М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. В. Гетьмана», Фін.-екон. ф-т, Каф. банк. справи, Банк. клуб КНЕУ. Дніпро: Середняк Т. К., 2021. С. 297–300. URL: https://ir.kneu.edu.ua/bitstream/handle/2010/36143/sgbp_21_4_8.pdf?sequence=1 (дата звернення: 29.02.2025)

18. Ситник Н. С., Половчак І. Р. Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни. *Галицький економічний вісник.* Тернопіль: ТНТУ. 2024. Том 89. № 4. С. 70–81. URL: https://elartu.tntu.edu.ua/handle/lib/46455 (дата звернення: 29.02.2025)

19. Sobers R. 157 Cybersecurity Statistics and Trends [updated 2024]. *Varonis: Automated Data Security, DSPM, AI*. URL: https://www.varonis.com/blog/cybersecurity-statistics#:~:text=Ransomware%20and%20malware%20attack%20statistics,·%20The%20number%20of (дата звернення: 29.02.2025)

20. Стражник Б. О., Смирнов С. А. Найпопулярніші атаки на веб-додатки та методи протидії їм. *Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених. Системи та технології кібернетичної безпеки.* 2023. с. 307-309. URL: https://ela.kpi.ua/server/api/core/bitstreams/68a81487-152c-4eac-9988-2a9dd32553ea/content (дата звернення: 29.02.2025)

21. Загрози для фінансових організацій: огляд та прогноз на 2019 - ITPRO.UA. *ITPRO*. URL: https://itpro.ua/post/ugrozy_dlya_finansovykh_organizatsii_obzor_i_prognoz_na_2019/?srsltid=AfmBOoqKYmDbcvqww7voDGKNLuvMJ_F4fXJ7B1rStzxzKm1hp5FeoepT (дата звернення: 29.02.2025)

22. Хакери пограбували центробанк Бангладеш на $81 млн. *Укрінформ - актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-world/2007069-hakeri-pograbuvali-centrobank-banglades-na-81-mln.html (дата звернення: 29.02.2025)

23. 2024 Cybersecurity Spending & Cyber Insurance Premium Trends. *Beinsure - Insurance, Reinsurance, InsurTech Insights*. URL: https://beinsure.com/cybersecurity-spending-trends/#:~:text=Cyber%20risk%20continues%20to%20grow,and%20evolve (дата звернення: 29.02.2025)

24. UK business leaders struggle to recognise cyber risk as a financial threat: Resilience - Reinsurance News. *ReinsuranceNe.ws*. URL: https://www.reinsurancene.ws/uk-business-leaders-struggle-to-recognise-cyber-risk-as-a-financial-threat-resilience/#:~:text=The%20survey%20also%20emphasises%20the,average%20of%20£10,830%20in%202023 (дата звернення: 29.02.2025)

25. Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Опер. центр реагування на кіберінциденти Держ. центру кіберзах. Держ. служби спец. зв'язку та зах. інформації.* 2021. 8 с. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf (дата звернення: 29.02.2025)

26. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Опер. центр реагування на кіберінциденти Держ. центру кіберзах. Держ. служби спец. зв'язку та зах. інформації.* 2022. 10 с. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=50943 (дата звернення: 29.02.2025)

27. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Опер. центр реагування на кіберінциденти Держ. центру кіберзах. Держ. служби спец. зв'язку та зах. інформації.* 2023. 12 с. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (дата звернення: 29.02.2025)

28. Річний звіт системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Опер. центр реагування на кіберінциденти Держ. центру кіберзах. Держ. служби спец. зв'язку та зах. інформації.* 2024. 24 с. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 29.02.2025)

29. Статистика Ситуаційного центру забезпечення кібербезпеки Служби безпеки України. *Служби безпеки України.*URL: https://surl.li/cceurv (дата звернення: 29.02.2025)

30. Bayle De Jessé M. The Eurosystem's cyber resilience strategy for financial market infrastructures. *Cyber Security: A Peer-Reviewed Journal*. 2019. URL: https://doi.org/10.69554/dfbj2963 (дата звернення: 29.02.2025)

31. Cyber resilience and financial market infrastructures. *European Central Bank*. URL: https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html (дата звернення: 29.02.2025)

32. Банк даних Державної служби статистики України. *Державна служба статистики України*. URL: https://stat.gov.ua/uk/explorer?urn=SSSU:DF_INFORM_COMMUN_TECH_ENTRP(8.0.0) (дата звернення: 29.02.2025)

33. Guidance on cyber resilience for financial market infrastructures. *Bank for International Settlements*. URL: https://www.bis.org/cpmi/publ/d146.htm (дата звернення: 29.02.2025)

34. Національний банк України. Контроль за кіберзахистом та інформаційною безпекою банків посилюється. *Національний банк України*. URL: https://bank.gov.ua/ua/news/all/kontrol-za-kiberzahistom-ta-informatsiynoyu-bezpekoyu-bankiv-posilyuyetsya (дата звернення: 29.02.2025)

35. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : Постанова Нац. банку України від 11.06.2018 № 64 : станом на 1 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text (дата звернення: 29.02.2025)

36. Digital Operational Resilience Act (DORA). *European Insurance and Occupational Pensions Authority*. URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-

dora_en#:~:text=The%20Digital%20Operational%20Resilience%20Act,as%20of%2017%20January%202025 (дата звернення: 29.02.2025)

37. Understanding DORA Regulation: A Paradigm shift for Cybersecurity in the Financial Sector - LOQR. *LOQR*. URL: https://loqr.com/resources/understanding-dora-regulation-a-paradigm-shift-for-cybersecurity-in-the-financial-sector/ (дата звернення: 29.02.2025)

38. Cost of a data breach 2024. *IBM - United States*. URL: https://www.ibm.com/reports/data-breach (дата звернення: 29.02.2025)

39. ENISA Threat Landscape 2024. *ENISA*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 29.02.2025)

40. Swift Customer Security Controls Framework. *Swift*. URL: https://www.swift.com/ru/node/300801 (дата звернення: 29.02.2025)

41. Cloudflare 2023 Year in Review. *Cloudflare*. URL: https://cf-assets.www.cloudflare.com/slt3lc6tev37/3Z7xOV53lGEIAwCqw5SncT/69eaca7bd5d2395ee0274b15e7854dd6/2023_Impact_Report.pdf (дата звернення: 29.02.2025)

42. 2024 Data Breach Investigations Report. *Verizon Business*. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 29.02.2025)

43. M-Trends 2024 Special Report. *Mandiant*. URL: https://services.google.com/fh/files/misc/m-trends-2024.pdf (дата звернення: 29.02.2025)

44. The Role of AI and Cybersecurity in the Financial Sector - FinTech Scotland. *FinTech Scotland*. URL: https://www.fintechscotland.com/the-role-of-ai-and-cybersecurity-in-the-financial-sector/#:~:text=AI%20offers%20several%20advantages%20for,cybersecurity%20in%20the%20financial%20sector (дата звернення: 29.02.2025)

45. Balkan B. Impacts of Digitalization on Banks and Banking. *Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application*. Singapore, 2021. С. 33–50. URL: https://doi.org/10.1007/978-981-33-6811-8_3 (дата звернення: 29.02.2025)

46. 2024 AI Fraud Financial Crime Survey. *BioCatch - Behavioral Biometrics to Prevent Fraud & Build Trust*. URL: https://www.biocatch.com/ai-fraud-financial-crime-survey#:~:text=2024%20AI%20Fraud%20Financial%20Crime,respondents%20expect%20both%20financial (дата звернення: 29.02.2025)

47. Artificial Intelligence in Financial Services: white paper. *AI Governance Alliance*. 2025. URL: https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf (дата звернення: 29.02.2025)

48. IBM. What is User Behavior Analytics? (UBA). *IBM - United States*. URL: https://www.ibm.com/think/topics/user-behavior-analytics (дата звернення: 29.02.2025)

49. Online Banking Statistics and Facts (2025). *Market.us Scoop*. URL: https://scoop.market.us/online-banking-statistics/#:~:text=,(Source:%20Deloitte (дата звернення: 29.02.2025)

50. 2021: DeFi Pulse's Year in Indices. Defi Pulse Blog. URL: https://www.defipulse.com/blog/2021-defi-pulse-year-in-indices (дата звернення: 29.02.2025)

51. Knight O. Defi Hacks Remain a Major Threat Despite 50% Decline in 2023: Halborn. *CoinDesk*. URL: https://www.coindesk.com/business/2024/08/12/defi-hacks-remain-a-major-threat-despite-50-decline-in-2023-halborn (дата звернення: 29.02.2025)

52. George K. The Largest Cryptocurrency Hacks So Far. *Investopedia*. URL: https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/#:~:text=Ronin%20Network:%20$625%20Million (дата звернення: 29.02.2025)

53. New rules to strengthen resilience of UK's financial sector. *FCA*. URL: https://www.fca.org.uk/news/statements/new-rules-strengthen-resilience-uks-financial-sector#:~:text=New%20rules%20to%20strengthen%20resilience,resilience%20of%20critical%20third%20parties (дата звернення: 29.02.2025)

54. Annual Report 2023. *Federal Financial Institutions Examination Council*. 2024. URL: https://www.ffiec.gov/PDF/annrpt23.pdf (дата звернення: 29.02.2025)

55. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 29.02.2025)

References

1. Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022. Automated Security Validation Platform. Picus. URL: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022#:~:text=Dr,2022 (data zvernennia: 29.02.2025)

2. Cyber Security in Finance: Key Threats and Strategies. SentinelOne. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/#:~:text=According%20to%20Statista,%20in%20the,continuous%20evolution%20in%20security%20practices (data zvernennia: 29.02.2025)

3. Top Cybersecurity Statistics, Facts, and Figures for 2022. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics#:~:text=1,worry%20about%20ransomware (data zvernennia: 29.02.2025)
4. DDOS-ataky, shcho zdiisniuvalysia na ukrainski banky. NABU. URL: https://nabu.ua/ua/ddos-ataki-shcho-zdiysnyuvalisya-na-ukrayinski-banki-vidbito.html (data zvernennia: 29.02.2025)
5. Darem A. A., Alhashmi A. A., Alkhaldi T. M., Alashjaee A. M., Alanazi S. M., Ebad S. A. Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. IEEE Access. 2023. Vol. 11. P. 125138–125158. URL: https://doi.org/10.1109/ACCESS.2023.3327016 (data zvernennia: 29.02.2025)
6. Johnson K. N. Cyber Risks: Emerging Risk Management Concerns for Financial Institutions. Regulation of Financial Institutions eJournal. 2015. URL: https://digitalcommons.law.uga.edu/glr/vol50/iss1/7/ (data zvernennia: 29.02.2025)
7. Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. SSRN Electronic Journal. 2018. URL: https://doi.org/10.2139/ssrn.3203026 (data zvernennia: 29.02.2025)
8. Curti F., Gerlach J. R., Kazinnik S., Lee M., Mihov A. Cyber risk definition and classification for financial risk management. Journal of Operational Risk. 2023. URL: https://doi.org/10.21314/jop.2022.036 (data zvernennia: 29.02.2025)
9. Reddem P.R. Cybersecurity in Banking and Finance : Navigating the Digital Threat Landscape. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024. Т. 10, № 5. S. 852–861. URL: https://doi.org/10.32628/cseit241051073 (data zvernennia: 29.02.2025)
10. Dorosh I. Cyber security and its role in the financial sector: threats and protection measures. Economics. Finances. Law. 2023. Т. 10. S. 48–51. URL: https://doi.org/10.37634/efp.2023.10.10 (data zvernennia: 29.02.2025)
11. Nwafor K. C., Ikudabo A. O., Onyeje C. C., Ihenacho D. O. T. Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. International Journal of Science and Research Archive. 2024. Т. 13, № 1. S. 2895–2910. URL: https://doi.org/10.30574/ijsra.2024.13.1.2014 (data zvernennia: 29.02.2025)
12. Eriamiatoe F. E. The Role of Machine Learning in Solving Cybersecurity Challenges in the Financial Sector. International Journal of Scientific and Research Publications. 2024. Т. 14, № 9. S. 68–72. URL: https://doi.org/10.29322/ijsrp.14.09.2024.p15313 (data zvernennia: 29.02.2025)
13. Umoga U. J., Sodiya E. O., Amoo O. O., Atadoga A. A critical review of emerging cybersecurity threats in financial technologies. International Journal of Science and Research Archive. 2024. Т. 11, № 1. S. 1810–1817. URL: https://doi.org/10.30574/ijsra.2024.11.1.0284 (data zvernennia: 29.02.2025)
14. Dhingra D., Ashok S., Kumar U. Demystifying Global Cybersecurity Threats in Financial Services. Handbook of Research on Advancing Cybersecurity for Digital Transformation. 2021. S. 181–202. URL: https://doi.org/10.4018/978-1-7998-6975-7.ch010 (data zvernennia: 29.02.2025)
15. Khomyshyn I., Havts O. Zabezpechennia kiberbezpeky u finansovomu sektori: pravovyi ta tekhnolohichnyi aspekty. Elektronne naukove vydannia «Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu». Seriia: Pravo. 2023. Т. 10, № 40. S. 170–178. URL: https://doi.org/10.23939/law2023.40.170 (data zvernennia: 29.02.2025)
16. Trusova N. V., Chkan I. O. Kiberzakhyst bankivskoi systemy Ukrainy v umovakh tsyfrovykh transformatsii. Naukovyi visnyk Tavriiskoho derzhavnoho ahrotekhnolohichnoho universytetu. 2023. Т. 1, № 47. S. 151–163. URL: https://doi.org/10.31388/2519-884x-2023-47-151-163 (data zvernennia: 29.02.2025)
17. Lavreniuk V. V. Kliuchovi draivery kiber-ryzykiv finansovykh ustanov. Suchasni hroshi, bankivski posluhy ta finansovi innovatsii v tsyfrovii ekonomitsi : materialy IV Vseukr. nauk.-prakt. internet-konf. studentiv, aspirantiv i molodykh vchenykh, Kyiv, 12 kvit. 2021 r. M-vo osvity i nauky Ukrainy, DVNZ «Kyiv. nats. ekon. un-t im. V. Hetmana», Fin.-ekon. f-t, Kaf. bank. spravy, Bank. klub KNEU. Dnipro: Seredniak T. K., 2021. S. 297–300. URL: https://ir.kneu.edu.ua/bitstream/handle/2010/36143/sgbp_21_4_8.pdf?sequence=1 (data zvernennia: 29.02.2025)
18. Sytnyk N. S., Polovchak I. R. Tsyfrovizatsiia ta kiberbezpeka u zabezpechenni finansovoi bezpeky bankiv v umovakh viiny. Halytskyi ekonomichnyi visnyk. Ternopil: TNTU. 2024. Tom 89. № 4. S. 70–81. URL: https://elartu.tntu.edu.ua/handle/lib/46455 (data zvernennia: 29.02.2025)
19. Sobers R. 157 Cybersecurity Statistics and Trends [updated 2024]. Varonis: Automated Data Security, DSPM, AI. URL: https://www.varonis.com/blog/cybersecurity-statistics#:~:text=Ransomware%20and%20malware%20attack%20statistics,·%20The%20number%20of (data zvernennia: 29.02.2025)
20. Strazhnyk B. O., Smyrnov S. A. Naipopuliarnishi ataky na veb-dodatky ta metody protydii yim. Vseukrainska naukovo-praktychna konferentsiia studentiv, aspirantiv ta molodykh vchenykh. Systemy ta tekhnolohii kibernetychnoi bezpeky. 2023. c. 307-309. URL: https://ela.kpi.ua/server/api/core/bitstreams/68a81487-152c-4eac-9988-2a9dd32553ea/content (data zvernennia: 29.02.2025)
21. Zahrozy dlia finansovykh orhanizatsii: ohliad ta prohnoz na 2019 - ITPRO.UA. ITPRO. URL: https://itpro.ua/post/ugrozy_dlya_finansovykh_organizatsii_obzor_i_prognoz_na_2019/?srsltid=AfmBOoqKYmDbcvqww7voDGKNLuvMJ_F4fXJ7B1rStzxzKm1hp5FeoepT (data zvernennia: 29.02.2025)
22. Khakery pohrabuvaly tsentrobank Banhladesh na $81 mln. Ukrinform - aktualni novyny Ukrainy ta svitu. URL: https://www.ukrinform.ua/rubric-world/2007069-hakeri-pograbuvali-centrobank-banglades-na-81-mln.html (data zvernennia: 29.02.2025)
23. 2024 Cybersecurity Spending & Cyber Insurance Premium Trends. Beinsure - Insurance, Reinsurance, InsurTech Insights. URL: https://beinsure.com/cybersecurity-spending-trends/#:~:text=Cyber%20risk%20continues%20to%20grow,and%20evolve (data zvernennia: 29.02.2025)
24. UK business leaders struggle to recognise cyber risk as a financial threat: Resilience - Reinsurance News. ReinsuranceNe.ws. URL: https://www.reinsurancene.ws/uk-business-leaders-struggle-to-recognise-cyber-risk-as-a-financial-threat-resilience/#:~:text=The%20survey%20also%20emphasises%20the,average%20of%20£10,830%20in%202023 (data zvernennia: 29.02.2025)
25. Zvit roboty systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky. Oper. tsentr reahuvannia na kiberintsydenty Derzh. tsentru kiberzakh. Derzh. sluzhby spets. zviazku ta zakh. informatsii. 2021. 8 s. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf (data zvernennia: 29.02.2025)
26. Zvit pro robotu systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky. Oper. tsentr reahuvannia na kiberintsydenty Derzh. tsentru kiberzakh. Derzh. sluzhby spets. zviazku ta zakh. informatsii. 2022. 10 s. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=50943 (data zvernennia: 29.02.2025)
27. Zvit pro robotu systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky. Oper. tsentr reahuvannia na kiberintsydenty Derzh. tsentru kiberzakh. Derzh. sluzhby spets. zviazku ta zakh. informatsii. 2023. 12 s. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (data zvernennia: 29.02.2025)
28. Richnyi zvit systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky. Oper. tsentr reahuvannia na kiberintsydenty Derzh. tsentru kiberzakh. Derzh. sluzhby spets. zviazku ta zakh. informatsii. 2024. 24 s. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (data zvernennia: 29.02.2025)
29. Statystyka Sytuatsiinoho tsentru zabezpechennia kiberbezpeky Sluzhby bezpeky Ukrainy. Sluzhby bezpeky Ukrainy.URL: https://surl.li/cceurv (data zvernennia: 29.02.2025)

30. Bayle De Jessé M. The Eurosystems cyber resilience strategy for financial market infrastructures. Cyber Security: A Peer-Reviewed Journal. 2019. URL: https://doi.org/10.69554/dfbj2963 (data zvernennia: 29.02.2025)
31. Cyber resilience and financial market infrastructures. European Central Bank. URL: https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html (data zvernennia: 29.02.2025)
32. Bank danykh Derzhavnoi sluzhby statystyky Ukrainy. Derzhavna sluzhba statystyky Ukrainy. URL: https://stat.gov.ua/uk/explorer?urn=SSSU:DF_INFORM_COMMUN_TECH_ENTRP(8.0.0) (data zvernennia: 29.02.2025)
33. Guidance on cyber resilience for financial market infrastructures. Bank for International Settlements. URL: https://www.bis.org/cpmi/publ/d146.htm (data zvernennia: 29.02.2025)
34. Natsionalnyi bank Ukrainy. Kontrol za kiberzakhystom ta informatsiinoiu bezpekoiu bankiv posyliuietsia. Natsionalnyi bank Ukrainy. URL: https://bank.gov.ua/ua/news/all/kontrol-za-kiberzahistom-ta-informatsiynoyu-bezpekoyu-bankiv-posilyuyetsya (data zvernennia: 29.02.2025)
35. Pro zatverdzhennia Polozhennia pro orhanizatsiiu systemy upravlinnia ryzykamy v bankakh Ukrainy ta bankivskykh hrupakh : Postanova Nats. banku Ukrainy vid 11.06.2018 № 64 : stanom na 1 sich. 2025 r. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text (data zvernennia: 29.02.2025)
36. Digital Operational Resilience Act (DORA). European Insurance and Occupational Pensions Authority. URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en#:~:text=The%20Digital%20Operational%20Resilience%20Act,as%20of%2017%20January%202025 (data zvernennia: 29.02.2025)
37. Understanding DORA Regulation: A Paradigm shift for Cybersecurity in the Financial Sector - LOQR. LOQR. URL: https://loqr.com/resources/understanding-dora-regulation-a-paradigm-shift-for-cybersecurity-in-the-financial-sector/ (data zvernennia: 29.02.2025)
38. Cost of a data breach 2024. IBM - United States. URL: https://www.ibm.com/reports/data-breach (data zvernennia: 29.02.2025)
39. ENISA Threat Landscape 2024. ENISA. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (data zvernennia: 29.02.2025)
40. Swift Customer Security Controls Framework. Swift. URL: https://www.swift.com/ru/node/300801 (data zvernennia: 29.02.2025)
41. Cloudflare 2023 Year in Review. Cloudflare. URL: https://cf-assets.www.cloudflare.com/slt3lc6tev37/3Z7xOV53lGEIAwCqw5SncT/69eaca7bd5d2395ee0274b15e7854dd6/2023_Impact_Report.pdf (data zvernennia: 29.02.2025)
42. 2024 Data Breach Investigations Report. Verizon Business. URL: https://www.verizon.com/business/resources/reports/dbir/ (data zvernennia: 29.02.2025)
43. M-Trends 2024 Special Report. Mandiant. URL: https://services.google.com/fh/files/misc/m-trends-2024.pdf (data zvernennia: 29.02.2025)
44. The Role of AI and Cybersecurity in the Financial Sector - FinTech Scotland. FinTech Scotland. URL: https://www.fintechscotland.com/the-role-of-ai-and-cybersecurity-in-the-financial-sector/#:~:text=AI%20offers%20several%20advantages%20for,cybersecurity%20in%20the%20financial%20sector (data zvernennia: 29.02.2025)
45. Balkan B. Impacts of Digitalization on Banks and Banking. Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application. Singapore, 2021. S. 33–50. URL: https://doi.org/10.1007/978-981-33-6811-8_3 (data zvernennia: 29.02.2025)
46. 2024 AI Fraud Financial Crime Survey. BioCatch - Behavioral Biometrics to Prevent Fraud & Build Trust. URL: https://www.biocatch.com/ai-fraud-financial-crime-survey#:~:text=2024%20AI%20Fraud%20Financial%20Crime,respondents%20expect%20both%20financial (data zvernennia: 29.02.2025)
47. Artificial Intelligence in Financial Services: white paper. AI Governance Alliance. 2025. URL: https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf (data zvernennia: 29.02.2025)
48. IBM. What is User Behavior Analytics? (UBA). IBM - United States. URL: https://www.ibm.com/think/topics/user-behavior-analytics (data zvernennia: 29.02.2025)
49. Online Banking Statistics and Facts (2025). Market.us Scoop. URL: https://scoop.market.us/online-banking-statistics/#:~:text=,(Source:%20Deloitte (data zvernennia: 29.02.2025)
50. 2021: DeFi Pulses Year in Indices. Defi Pulse Blog. URL: https://www.defipulse.com/blog/2021-defi-pulse-year-in-indices (data zvernennia: 29.02.2025)
51. Knight O. Defi Hacks Remain a Major Threat Despite 50% Decline in 2023: Halborn. CoinDesk. URL: https://www.coindesk.com/business/2024/08/12/defi-hacks-remain-a-major-threat-despite-50-decline-in-2023-halborn (data zvernennia: 29.02.2025)
52. George K. The Largest Cryptocurrency Hacks So Far. Investopedia. URL: https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/#:~:text=Ronin%20Network:%20$625%20Million (data zvernennia: 29.02.2025)
53. New rules to strengthen resilience of UKs financial sector. FCA. URL: https://www.fca.org.uk/news/statements/new-rules-strengthen-resilience-uks-financial-sector#:~:text=New%20rules%20to%20strengthen%20resilience,resilience%20of%20critical%20third%20parties (data zvernennia: 29.02.2025)
54. Annual Report 2023. Federal Financial Institutions Examination Council. 2024. URL: https://www.ffiec.gov/PDF/annrpt23.pdf (data zvernennia: 29.02.2025)
55. Pro krytychnu infrastrukturu : Zakon Ukrainy vid 16.11.2021 № 1882-IX : stanom na 21 veres. 2024 r. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (data zvernennia: 29.02.2025)