СВІТОВИЙ ДОСВІД ДЕРЖАВНОГО УПРАВЛІННЯ

DOI: https://doi.org/10.26565/1684-8489-2024-2-18
УДК 351.72:004.056.53

Живило Євген Олександрович,
кандидат наук з державного управління, доцент,
докторант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна

e-mail: zhivilka@i.ua *https://orcid.org/0000-0003-4077-7853*

МАКРОФІНАНСОВА СТАБІЛЬНІСТЬ ДЕРЖАВИ В УМОВАХ КІБЕРЗАГРОЗ

Анотація. Стаття присвячена актуальній проблемі забезпечення макрофінансової стабільності держави в умовах зростаючих кіберзагроз. Стабільність фінансових ринків є основою економічного розвитку та добробуту будь-якої країни, адже вона забезпечує ефективний рух капіталу, знижує невизначеність та сприяє зростанню інвестицій. Однак ця стабільність є вразливою до різноманітних зовнішніх і внутрішніх загроз, зокрема до кіберризиків, які можуть значно порушити функціонування фінансових установ і навіть спричинити серйозні економічні потрясіння. Автор підкреслює критичну важливість цього питання в епоху цифрової трансформації економіки, коли фінансові системи стають все більш вразливими до потенційно катастрофічних наслідків кібератак. У статті проаналізовано основні канали впливу кіберінцидентів на фінансову стабільність, зокрема порушення роботи платіжних систем, втрата довіри з боку інвесторів та споживачів, збої в наданні критичних послуг через взаємопов'язаність фінансових установ. Особлива увага приділяється проблемам кіберготовності країн, що розвиваються, які часто не мають достатніх ресурсів та досвіду для ефективної протидії цифровим загрозам. Автор наголошує на необхідності розробки та впровадження всеосяжних національних стратегій кібербезпеки, які б визначали чіткі цілі, пріоритети та механізми захисту фінансової інфраструктури. Ці стратегії мають ґрунтуватися на найкращих світових практиках та передбачати широкий спектр заходів: від створення ефективної нормативно-правової бази до інвестицій у розвиток людського капіталу. Стаття також підкреслює важливість активізації міжнародної співпраці для зміцнення кіберстійкості, враховуючи транскордонний характер цифрових загроз. У цьому контексті відзначається ключова роль глобальних інституцій, таких як Міжнародний валютний фонд, у наданні країнам технічної допомоги, проведенні навчань та розробці універсальних інструментів оцінки кіберризиків. Загалом, стаття робить внесок у дослідження проблематики кібербезпеки фінансо-

Як цитувати: Живило Є. О. Макрофінансова стабільність держави в умовах кіберзагроз. *Актуальні проблеми державного управління*. 2024. № 2 (65). С. 347–369. DOI: https://doi.org/10.26565/1684-8489-2024-2-18

In cites: Zhyvylo, Ye. O. (2024). National Macrofinancial Stability in the Context of Cyber Threats. *Pressing Problems of Public Administration, 2 (65), 347–369.* DOI: https://doi.org/10.26565/1684-8489-2024-2-18 [in Ukrainian].

© Живило Є. О., 2024
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0

вого сектора та пропонує авторське бачення шляхів її вирішення на національному та міжнародному рівнях.

Ключові слова: публічне управління, система захисту інформації, кібербезпека, інформаційні технології, інформаційна безпека, кібербезпека, фінансові установи.

Постановка проблеми. У епоху стрімкої цифрової трансформації та глобальної інтеграції фінансових систем, проблема забезпечення макрофінансової стабільності держави в умовах зростаючих кіберзагроз набуває критичного значення. Фінансова система, як кровоносна система економіки, стає все більш вразливою до потенційно катастрофічних наслідків кібератак. Уявіть собі ситуацію, коли хакери зламують системи центрального банку країни і викрадають мільярди доларів резервів або блокують роботу платіжних систем. Такий сценарій може призвести до масштабної фінансової кризи, панічного відтоку капіталу, знецінення національної валюти та колапсу економіки. І це не просто теоретичні міркування – подібні інциденти вже траплялися в реальному житті. Згадаймо атаку вірусу «NotPetya» на Україну в 2017 р., яка завдала збитків на суму понад 10 мільярдів доларів, або злам криптовалютної біржі Coincheck у 2018 р. з втратою цифрових активів на півмільярда доларів.

Але справа не лише в прямих фінансових втратах. Кіберінциденти підривають довіру населення та бізнесу до фінансової системи, що має довгострокові негативні наслідки. Люди починають побоюватися тримати гроші в банках, інвестори виводять капітали в більш надійні юрисдикції, компанії відмовляються від цифровізації через страх перед хакерами. Все це гальмує економічний розвиток та інновації. Особливо гостро ця проблема стоїть для країн, що розвиваються, які не мають достатніх ресурсів та досвіду для ефективної протидії кіберзагрозам. За оцінками Світового банку, щорічні втрати від кіберзлочинності в країнах з низьким та середнім рівнем доходу складають близько 445 мільярдів доларів, або 0,5% їх сукупного ВВП. Це величезна сума, яка могла б бути спрямована на розвиток економіки та підвищення добробуту населення.

Ще один важливий аспект проблеми – це зв'язок між кібербезпекою та монетарною політикою держави. Центральні банки в усьому світі активно вивчають можливості впровадження цифрових валют (CBDC), які можуть докорінно змінити архітектуру фінансової системи. Але разом з перевагами, такими як зниження транзакційних витрат та розширення фінансової інклюзії, CBDC несуть і нові ризики. Зокрема, вони можуть стати привабливою мішенню для хакерів та створити додаткові вектори атак на фінансову інфраструктуру. Тому розробка надійних механізмів кібербезпеки є критично важливою умовою для успішного впровадження CBDC та забезпечення монетарної стабільності в цифрову епоху. Як приклад можна навести пілотний проєкт е-крони в Швеції, де особлива увага приділяється саме питанням кібербезпеки та захисту персональних даних користувачів.

Підсумовуючи, можна сказати, що забезпечення макрофінансової стабільності в умовах кіберзагроз – це комплексний виклик [19], який вимагає консолідації зусиль на національному та міжнародному рівнях. Необхідно розвивати культуру кібергігієни, інвестувати в інноваційні рішення для захисту фінансової інфраструктури, вдосконалювати регуляторні механізми та зміцнювати міжнародну співпрацю в сфері кібербезпеки. Україна, яка вже має

гіркий досвід кібератак, може стати регіональним лідером у розробці ефективних стратегій кіберстійкості фінансового сектору. Але для цього потрібна політична воля, достатнє фінансування та активна участь усіх стейкхолдерів – від регуляторів та банків до ІТ-компаній та громадянського суспільства. Тільки так ми зможемо побудувати надійний цифровий фундамент для стабільного та інклюзивного економічного розвитку в XXI столітті.

Аналіз останніх досліджень і публікацій. Проблема забезпечення макрофінансової стабільності в умовах зростаючих кіберзагроз привертає все більшу увагу науковців та експертів у галузі економіки, фінансів та кібербезпеки. В останні роки з'явилася низка ґрунтовних досліджень [13; 11; 19], які розглядають різні аспекти цієї багатогранної теми. Одним з ключових напрямків досліджень є аналіз впливу кіберінцидентів на фінансову систему та економіку в цілому. У роботі [18], підготовленій експертами Міжнародного валютного фонду, проаналізовано потенційні канали впливу кібератак на фінансову стабільність, такі як порушення роботи платіжних систем, втрата конфіденційних даних, втрата довіри з боку інвесторів та споживачів. Її автори наголошують на необхідності розробки комплексних стратегій кібербезпеки на рівні фінансових установ та регуляторів. Схожі висновки містяться і в дослідженні Європейського центрального банку [10], де запропоновано набір принципів та рекомендацій щодо підвищення кіберстійкості фінансової інфраструктури.

Значна увага в літературі приділяється також аналізу економічних наслідків кібератак. У статті [14] автори розглядають прямі та непрямі витрати, пов'язані з кіберзлочинністю, такі як втрата інтелектуальної власності, репутаційні збитки, витрати на відновлення систем та виплати страхових відшкодувань. За їх оцінками, глобальні економічні втрати від кібератак можуть сягати 1-2% світового ВВП. В іншому дослідженні [8], проведеному компанією Accenture, наводяться дані про середню вартість кіберінцидентів для компаній в різних секторах економіки – від $1,4 млн для сфери послуг до $17,8 млн для енергетичного сектору.

Окремим напрямком досліджень є вивчення зв'язку між кібербезпекою та монетарною політикою центральних банків в умовах цифровізації. У роботі [17], підготовленій фахівцями Банку міжнародних розрахунків, розглядаються потенційні ризики та виклики, пов'язані з впровадженням цифрових валют центробанків (CBDC) [15]. Автори наголошують на необхідності розробки надійних механізмів кібербезпеки для CBDC, таких як багатофакторна автентифікація, шифрування даних, розподілена архітектура систем.

Згідно з останніми дослідженнями та публікаціями, кіберінциденти, включаючи кібератаки, зломи даних, шкідливі програми та блокування фінансових транзакцій, становлять суттєву загрозу для фінансових ринків і можуть викликати серйозні економічні наслідки. Публікації останніх років, зокрема звіти Міжнародного валютного фонду (*далі – МВФ*) і Світового економічного форуму, наголошують на зростаючій взаємозалежності між цифровими та фінансовими секторами економіки. Інститути, біржі, платіжні системи та банківські установи все більше використовують цифрові платформи для здійснення фінансових операцій, що робить їх уразливими до кіберзагроз [9].

Останні дослідження, зокрема публікації МВФ, наголошують, що кіберзагрози є одними з головних факторів ризику для макрофінансової стабільності. Відсутність універсальних регуляційних стандартів кібербезпеки для

ФУ є однією з основних проблем, що створює прогалини у захисті цих установ від масштабних кіберінцидентів. Багато фінансових інститутів не готові до масштабних атак, що може призвести до серйозних фінансових втрат і зниження рівня довіри до ринку [21]. Серед основних загроз, пов'язаних зі зростаючими кіберінцидентами, дослідники виділяють кілька ключових аспектів: ризик для фінансової інфраструктури (*далі – ФІ*) – зростання кількості КІ може спричинити серйозні порушення в роботі критичних фінансових інститутів і послуг; фінансова нестабільність через втрату довіри – атаки на ФС можуть призвести до паніки на ринку, втрати довіри до ФУ і падіння інвестиційної привабливості; міжнародні економічні наслідки – кіберзагрози можуть мати транснаціональний характер, впливаючи на глобальні фінансові ринки та економічну стабільність; ризики для цифрових активів і криптовалют – зростання популярності криптовалют підвищує ризики для ринків цифрових активів, оскільки кіберінциденти можуть призвести до великих фінансових втрат на криптовалютних біржах.

Дослідження підтверджують, що кібератак на криптовалютні біржі можуть призвести до втрат великих сум капіталу і спричинити серйозні коливання на ринку цифрових активів, що має значний вплив на фінансові ринки загалом. Так, останні публікації та звіти свідчать, що кіберзагрози можуть стати каталізатором фінансових криз, оскільки відсутність належного захисту цифрових активів ставить під сумнів стабільність ФС у глобальному контексті. Згідно з останніми публікаціями, зокрема матеріалами Всесвітнього економічного форуму 2023 р. і звітами EY/IIF 2024, проблема КБ в фінансовому секторі набула особливої актуальності. Банки та ФУ активно впроваджують цифрову трансформацію, модернізуючи інфраструктуру і адаптуючись до нових вимог ринку. Однак, паралельно з цими змінами, постійно зростають обсяги і різноманіття кіберзагроз, що ставить під загрозу не тільки ефективність операцій, а й загальний рівень макрофінансової стабільності. Водночас, адаптація ФУ до кіберзагроз потребує комплексного підходу і активних зусиль для підвищення рівня кіберстійкості в умовах постійно зростаючих ризиків. У цьому контексті дослідження міжнародних організацій, таких як МВФ, Європейський центральний банк та Банк міжнародних розрахунків, підкреслюють необхідність розробки загальних стандартів безпеки для ФУ, а також створення координаційних органів для боротьби з кіберзагроз на міжнародному рівні. Публікації МВФ звертають увагу на важливість оцінки впливу кіберінцидентів на ФС та розробки стратегій для мінімізації цих ризиків.

Необхідно відзначити, що останні значні кіберінциденти, зокрема атака шкідливого програмного забезпечення (*далі – ПЗ*) на американське відділення найбільшого китайського банку Industrial and Commercial Bank of China 8 листопада 2023 р. та призупинення торгів в казначействі США, ще раз підтвердили загрозу, яку кіберінциденти становлять для фінансової стійкості великих фінустановах, а в умовах таких кіберзагроз приватний сектор все більше адаптується до наявних кіберризиків, що дозволяє швидше реагувати на атаки та зменшувати потенційні збитки.

Занепокоєння щодо кібербезпеки також проявляється в збільшенні частки компаній, що укладають страхові договори для захисту від фінансових збитків, пов'язаних з кіберінцидентами. Це відображає усвідомлення ФУ важливості кіберстійкості в умовах зростаючих ризиків. Так, центральні банки та фінансові регулятори, такі як Європейський комітет із системних ризиків та

Рада з нагляду за фінансовою стабільністю США, класифікували кіберризики як важливе джерело системного ризику. У відповідь на ці виклики глобальні зусилля з «пом'якшення кіберризиків» прискорилися. Організації, що розробляють і встановлюють стандарти безпеки, опублікували ряд документів і рекомендацій для посилення кіберстійкості у фінансовому секторі. У підсумку, сучасні публікації акцентують увагу на необхідності розвитку концептуальних підходів, які дозволяють оцінити фінансові збитки, спричинені кіберінциденти, визначити фактори, що сприяють їх виникненню, та аналізувати вразливість фінансового сектору до кіберзагроз. З огляду на зростаючі обсяги кіберзагроз, важливо, щоб фінансові установи та міжнародні організації вжили ефективних заходів для зміцнення кіберстійкості, що сприятиме збереженню макрофінансової стабільності на глобальному рівні.

Метою статті є детальна оцінка наслідків кіберризиків для фінансової стабільності та розробка опорних пропозицій для ефективної політики безпеки, спрямованої на мінімізацію цих ризиків. У рамках цієї мети можна виокремити такі ключові дослідницькі завдання:

– проаналізувати основні кіберзагрози для фінансового сектора та їх потенційний вплив на макрофінансову стабільність;

– дослідити особливості вразливості фінансових установ до кіберінцидентів та фактори, що сприяють цьому;

– запропонувати напрямки розвитку стратегій кібербезпеки для підвищення стійкості фінансової системи до кіберзагроз.

Використана методологія. Щодо методології, автор спирається на комплексний підхід, поєднуючи теоретичний аналіз проблеми з емпіричними даними та прикладами реальних кіберінцидентів. Зокрема, використовуються статистичні дані щодо кібератак, результати опитувань центральних банків та наглядових органів, а також приклади відомих кіберінцидентів у фінансовому секторі. Це дозволяє не лише концептуально осмислити проблему, а й продемонструвати її практичну значущість.

Щодо концептуальної основи, стаття спирається на теоретичні засади забезпечення фінансової стабільності та управління системними ризиками в умовах цифровізації. Автор розглядає кіберстійкість як невід'ємний компонент операційної надійності та фінансової стабільності в сучасних умовах. При цьому наголошується на важливості комплексного та проактивного підходу до управління кіберризиками з боку фінансових установ, регуляторів та наглядових органів. Концептуально обґрунтовується необхідність інтеграції кібербезпеки в загальні системи ризик-менеджменту та забезпечення безперервності діяльності установ. Автор наголошує, що в умовах зростаючої цифрової взаємозалежності питання кібербезпеки виходить за рамки окремих установ і потребує скоординованих зусиль на національному та міжнародному рівнях. У цілому концептуальна основа статті відповідає сучасним науковим поглядам на проблематику кіберризиків у фінансовому секторі та шляхи її вирішення.

Поряд з концептуальним аналізом, автор активно використовує емпіричні дані з авторитетних джерел. Статистичні дані щодо частоти кібератак, розмірів збитків від них, індекси кіберготовності країн роблять дослідження більш обґрунтованим та наочним. Також наводяться результати експертних опитувань, які відображають оцінки та погляди професійної спільноти на проблему. Конкретні кейси відомих кіберінцидентів у фінансових установах

ілюструють практичний бік проблеми та підкреслюють її актуальність. Таким чином, емпіричний матеріал не лише доповнює, але й «оживляє» теоретичні положення, демонструючи їх дієвість на практиці.

Виклад основного матеріалу. ФУ оперують величезною кількістю грошей і чималим масивом конфіденційних даних, що робить їх привабливою мішенню для кіберзлочинців. Ось, чому кібербезпреки стає критичною проблемою у фінансовій галузі. Так, на сьогодні, основними елементами фінансових послуг (*далі – ФП*), та спрямованість векторів по виконанню заходів, які безпосередньо підлягають захисту інформації та кібербезпеці (*далі – ЗІ* та кібербезпеки) є:

1) Захист конфіденційних даних. Фінансові установи обробляють величезну кількість особистої та фінансової інформації, включаючи імена клієнтів, адреси, номери соціального страхування, дані кредитних карток та історію транзакцій. Ці дані є цінними не лише для клієнтів, але й для кіберзлочинців, які використовують їх для шахрайства. Фінансові організації використовують різні інструменти кібербезпеки для захисту конфіденційних фінансових даних. Від шифрування та захищених мереж до надійних механізмів автентифікації, КБ гарантує, що дані доступні лише авторизованим особам і системам. Ними також використовуються механізми щодо виявлення та реагування на будь-який несанкціонований доступ (*далі – НсД*) або порушення даних [22], мінімізуючи потенційну шкоду.

2) Запобігання фінансовим втратам. Кібератки можуть призвести до значних фінансових втрат. Дії кіберзлочинців можуть бути спрямовані не тільки на безпосереднє викрадення коштів з банківських рахунків, але й на використання даних викраденої кредитної картки для шахрайських операцій. За цих умов порушення даних може призвести до штрафів, судових витрат і шкоди репутації людини. Вартість кіберзлочинності в галузі ФП продовжує стало зростати. Кібербезпека ФП є важливою у запобіганні втратам. За допомогою мережевої безпеки, систем виявлення вторгнень, захисту від зловмисного програмного забезпечення та інших заходів кібербезпеки фінансових установ можуть запобігти кібераптаки і пом'якшити їхній вплив.

3) Підтримання довіри споживачів. Довіра є наріжним каменем індустрії ФП. Клієнти довіряють свої гроші та особисті дані фінансової установи, очікуючи, що вони збережуть їх у безпеці. Будь-яке порушення цієї довіри, як-от витік даних або успішна кібератака, може завдати серйозної шкоди репутації фінансової установи та відносинам з клієнтами. Захищаючи фінансові операції та дані клієнтів, кібербезпеки ФП допомагає підтримувати довіру споживачів. Це запевняє клієнтів, що їхні дані та гроші в безпеці, а також зміцнює довіру до послуг фінансових установ.

4) Відповідність нормативним вимогам. Фінансові установи працюють у суворому нормативному середовищі, яке встановлює вимоги щодо забезпечення безпеки та цілісності фінансової стабільності і захисту споживачів. Серед них такі нормативні акти, як Закон про банківську таємницю (BSA), Закон Додда-Франка, Закон Сарбейнса-Окслі (SOX) і Стандарт безпеки даних індустрії платіжних карток (PCI DSS) тощо.

Ці норми передбачають виконання різноманітних заходів з захисту інформації і кібербезпеки. Наприклад, стандарт безпеки даних індустрії платіжних карток (PCI-DSS) вимагає від компаній захищати дані власників карток, впроваджувати надійні заходи контролю доступу, підтримувати політику

інформаційної безпеки, а також регулярно тестувати та контролювати мережі. Було детально розглянуто провідні протоколи відповідності з захисту інформації та кібербезпеки, які фінансові організації повинні впроваджувати в своїх установах [21].

Кіберзагрози для фінансового сектора охоплюють широкий спектр ризиків, які можуть призвести до значних матеріальних збитків і порушити довіру клієнтів до ФУ (таблиця 1).

Таблиця 1. – Основні кіберзагрози для фінансового сектора
Table 1. – Key cyber threats to the financial sector

Назва	Сутність	Заходи захисту
Фішинг і атаки соціальної інженерії	Примушення клієнтів ФУ обманним шляхом розкрити їх особисту чи фінансову інформацію, часто видаючи себе за довірену особу.	– навчання клієнтів ризикам фішингових і атак соціальної інженерії [2]; – впровадження систем фільтрації електронної пошти для блокування фішингових листів; – використання багатофакторної автентифікації для запобігання несанкціонованого доступу, навіть якщо облікові дані для входу скомпрометовані.
Зловмисне ПЗ та програми-вимагачі	– порушення роботи персонального комп'ютера; – збір конфіденційної інформації; – отримання несанкціонованого доступу до електронних комунікаційних мереж/систем; – шифрування файлів; – викуп за розшифрування.	– регулярне оновлення програмного забезпечення; – виправлення системних помилок; – встановлення та оновлення антивірусного програмного забезпечення; – моніторинг мережевого трафіку на наявність ознак зловмисного програмного забезпечення; – регулярне резервне копіювання даних.
Розподілені атаки на відмову в обслуговуванні (DDoS)	– переповнення мережі, служб чи інфраструктури, трафіку; – порушення роботи ФП; – нанесення фінансових збитків або відволікання з метою руйнування системи в цілому.	– впровадження систем захисту від DDoS; – "пом'якшення" трафіку DDoS; – підтримка резервних систем; – моделювання інцидентів DDoS у власних системах.
Внутрішні загрози (Інсайдерські загрози)	– загрози з середини організації будь-яких осіб які мають авторизований доступ до систем і даних установи; – несанкціоновані дії співробітників, підрядників які мають законний доступ до системи та процесів установи.	– контроль доступу, моніторинг та навчання; – персонал повинен мати доступ лише до тих даних і систем, які їм необхідні для роботи; – відстеження незвичайної або підозрілої поведінки; – навчання персоналу розпізнавати ризики кібербезпреки та реагувати на них [2].
Уразливості інтерфейсів прикладного програмування (API)	– забезпечення інтеграції між різними системами та службами; – використання API для отримання НсД до систем і даних.	– впровадження методів безпечного кодування; – проведення регулярного тестування безпеки; – використання шлюзів безпеки API; – моніторинг діяльності API.

Основною низкою рішень з захисту послуг та даних клієнтів від кібератак, КЗах корпоративних фінансових мереж наведені в таблиці 2.

Таблиця 2. – Характеристика основних інструментів забезпечення кібербезпеки фінансових систем

Table 2. – Characteristics of the main tools for ensuring cybersecurity of financial systems

Назва	Сутність	Заявлена реалізація
Брандмауери веб-додатків (WAF)	– захист між веб-програмою та Інтернетом; – фільтр та блокатор пакетів даних під час їх переміщення до веб-сайту чи веб-програми та з них; – запобігає поширеним веб-атакам, таким як міжсайтовий сценарій (XSS), впровадження SQL і атаки грубою силою.	– впровадження політик безпеки; – визначення який трафік слід блокувати, а який пропускати; – оновлення політики WAF; – регулярні перевірки безпеки, виявлення області вразливостей.
Захист від DDoS	– переповнення мережі, служб або серверу потоком Інтернет-трафіку; – уповільнення або збій служб, збої у їх роботі.	– відстеження мережевого трафіку; – виявлення незвичних сплесків активності; – перенаправлення підозрілого трафіку з мережі.
Боротьба з шахрайством і онлайн-шахрайством	– фішинг; – викрадення особистих даних; – шахрайство з картками; – конфіденційні фінансові дані.	– використання/пошук: – вдосконаленої аналітики; – алгоритмів машинного навчання; – підозрілих моделей і поведінки.
Керування ідентифікацією та доступом (IAM)	– підтримка керування ідентифікацією: – багатофакторна автентифікація (MFA); – єдиний вхід (SSO); – надання доступу користувачам; – мінімізація ризику витоку даних.	– визначена категорія персоналу має доступ до потрібних ресурсів 24/7 за необхідністю; – запобігання несанкціонованого доступу до конфіденційних даних і систем; – впровадження суворого контролю доступу.
Розширені рішення захисту від КЗ	– застосування комбінації технологій: – захист кінцевих точок; – безпека мережі; – безпека електронної пошти; – аналітика зловмисної поведінки.	– розвідка про кіберзагрози в реальному часі; – можливості автоматичного реагування; – захист від передових кіберзахисту.
Оцінка вразливості та тестування на проникнення (VAPT)	– комплексна оцінка, щодо виявлення слабких місць і оцінки стану безпеки системи; – виявлення, кількісна оцінка та визначення пріоритетів уразливостей у системі.	– захист важливих даних; – запобігання витоку даних; – ідентифікація та нейтралізація потенційних кіберзагроз; – відповідність нормативним вимогам.
Програми підвищення рівня безпеки та навчання	– ознайомлення користувачів із різними кіберзагрозами, способами їх дії та найкращими методами протидії їм [2].	– захист конфіденційних фінансових даних.
Моніторинг активності даних	– відстеження та запис всіх дій в базі даних у режимі реального часу.	– додатковий рівень безпеки; – захист від зовнішніх та внутрішніх кіберзагроз; – забезпечення цілісності і конфіденційності фінансових даних.
Аналітика ризиків даних	– проактивний підхід до кібербезпеки; – аналіз даних/виявлення шаблонів та аномалій, які можуть вказувати на кіберзагрози.	– прогнозування потенційних загроз; – надання об'єктивної оцінки ризикам даних.

**Джерело: розробка автора.*

**Source: developed by the author.*

З огляду на вищевикладене, слід зазначити, що кіберінциденти у фінансових установах можуть загрожувати МС через три основні канали (рис. 1).

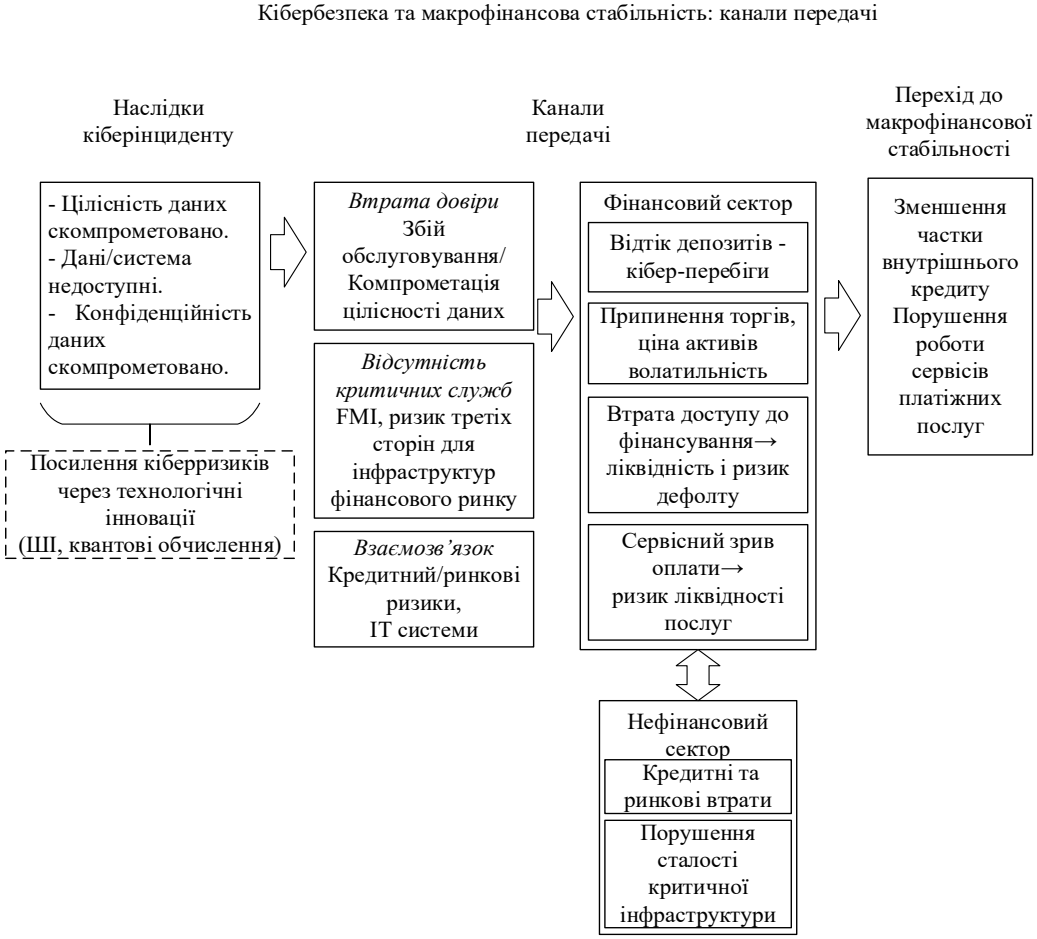

Рисунок 1. – Канали передачі для кібербезпеки і макрофінансової стабільності

Figure 1. – Transmission channels for cybersecurity and macrofinancial stability

**Джерело: розробка автора.*
**Source: developed by the author.*

По-перше, порушення даних може призвести до втрати довіри до життєздатності установи, що, у свою чергу, збільшує ризики ліквідності, наприклад, через зняття депозитів або втечу капіталу з банків – "кіберпобіги" [12]. Такі ризики ліквідності можуть призвести до проблем із платоспроможністю, які можуть поширитися на пов'язані сторони у ФС. По-друге, кіберзахист фінансовій стабільності може швидко реалізуватися, якщо кіберінциденти вплине на ключову установу або важливу ФІ, яку складно замінити. Наприклад, атака програм-вимагачів на великий банк, який бере участь у системі виплат, збій у постачальників хмарних послуг, злом центрального банку або

порушення роботи ключових хабів у фінустановах (наприклад, систем електронної торгівлі або розрахункових центрів) можуть швидко розповсюдитися і підірвати фінансову стабільність.

По-друге, взаємопов'язаність установ через технологічні зв'язки (наприклад, використання одного й того ж програмного забезпечення кількома компаніями) або фінансові зв'язки (наприклад, міжбанківський ринок, системи розрахунків або спільні активи) може посилити наслідки КІ для всієї фінансової стабільності.

Складні та всеохоплюючі кіберінциденти можуть негативно вплинути на макроекономічні результати, наприклад, через скорочення кредитування або збій платіжних систем. Фінансова стабільність також може бути підірвана кіберінцидентами у нефінансових установах. Наприклад, кібератаки на кіберінфраструктуру, таку як електромережі, може ускладнити сталу роботу ФУ, що спричинить негативні ефекти для макроекономіки. Серйозні кіберінциденти в системних нефінансових установах можуть також збільшити кредитний ризик або ризик ліквідності для ФУ. Ці ефекти можуть посилитися через потенційне зростання кіберризиків під час несприятливих фінансових умов. Кіберінциденти в державних установах можуть порушити функціонування уряду, наприклад, негативно вплинути на управління державним боргом і опосередковано вплинути на фінансовий сектор через підвищення суверенних премій за ризик.

Нові технології та інновації у ФП можуть посилити кіберризики. Хоча розвиток штучного інтелекту може допомогти в покращенні виявлення ризиків і шахрайства, наприклад, шляхом моніторингу аномальної поведінки [6; 20]. При цьому штучний інтелект (залежності від моделі і його типу) може бути використаний і для зловмисної діяльності, зокрема і через генеративний штучний інтелект. Складні фішингові повідомлення або глибокі фейки можуть бути використані для крадіжки особистих даних або шахрайства. Наприклад, у січні 2024 року шахраї змогли обдурити співробітників транснаціональної компанії, в результаті чого було переказано 200 мільйонів гонконгських доларів (або $26 млн). Також слід звернути увагу і на використання технології deepfake для створення фальшивих групових відеодзвінків. Крім того, штучний інтелект наражає компанії на ризик щодо витоку даних, таких як інформація, що використовується для навчання алгоритмів штучного інтелекту, або даних, які аналізуються сторонніми постачальниками штучного інтелекту [16]. У майбутньому поява квантових обчислень та їх потенційна здатність швидко ламати алгоритми шифрування, які застосовуються у фінансових установах, також може збільшити масштаби збитків від кібератак.

У цілому, збитки від кіберінцидентів для компаній, про які повідомляють в засобах масової інформації, наразі вважаються загалом скромними, але при визначених умовах вони можуть суттєво зрости. На основі доступних даних, прямі збитки від кіберінцидентів на американські компанії складають приблизно $0,4 млн, при цьому три чверті повідомлених втрат не перевищують $2,8 млн доларів. Хоча збитки від шкідливого програмного забезпечення значно перевищують втрати від несанкціонованого доступу, що складає приблизно $0,5 мільйона, вони все ще є відносно скромними в абсолютних числах. Наприклад, більшість атак шкідливого програмного забезпечення або випадків зловмисного витоку даних призводять до збитків, приблизно $12 млн. Проте розподіл збитків сильно спотворений, за деякими даними, реальний стан збитків

складає сотні мільйонів доларів. Такі втрати можуть призвести до проблем з ліквідністю і навіть загрожувати платоспроможності компаній. Оскільки великі втрати від офіційно проведених кібератак є поодинокими, точне кількісне оцінювання їх ймовірності є складним завданням. Для вирішення цієї проблеми можна використовувать підхід узагальненого розподілу екстремальних значень, який часто застосовується в техніці для моделювання екстремальних результатів випадкових експериментів, що мають сильно спотворений розподіл.

Результати показують, що середній максимальний збиток для провідних країн світу за рік, або інакше кажучи, максимальний очікуваний збиток за більшість років, зріс більш ніж удвічі з 2017 р., досягнувши 141 мільйону доларів у 2021 р. Це еквівалентно приблизно 50% операційному доходу середньої компанії. При цьому очікується, що раз на десять років, кіберінциденти будуть завдавати збитків у розмірі $2,5 мільярда, що складає приблизно 800% середнього операційного доходу компанії і може серйозно загрожувати її ліквідності та платоспроможності. Зокрема, для фінансових установ орієнтовний максимальний річний збиток може досягати близько 152 мільйонів доларів, а в разі критичного порушення системи захисту інформації та кібербезпеки може становити до 2,2 мільярда доларів раз на десять років. Варто зазначити, що висвітлені прямі збитки можуть не повністю відображати загальну економічну вартість кіберінцидентів. Компанії часто не повідомляють про непрямі збитки, такі як втрати бізнесу, шкода репутації або витрати на кібербезпеку, оскільки ці витрати важко точно зафіксувати або вони можуть проявлятися з часом [3]. Однак загальні втрати від кібератак, як прямі, так і непрямі, можна оцінити через реакцію курсу акцій на відомості про обставини КІ, оскільки фондові ринки є передбачуваними і відображають оцінки учасників ринку щодо вартості компаній.

Проведений аналіз вказує на те, що при врахуванні ринкових коливань та інших відповідних факторів, ціни акцій в середньому не демонструють значної реакції на кіберінциденти. Однак, фінансові установи все ж таки відчувають певний вплив від кібератак. В середньому доходність акцій зменшується на 0,1-0,2%-х пункти, хоча цей ефект не є статистично значним. Найбільші втрати і найзначніші ефекти спостерігаються у малих компаній, де зниження доходності акцій коливається від 0,3 до майже 0,6%-х пунктів. Це свідчить про те, що невеликі фірми мають менше ресурсів для управління та пом'якшення наслідків кіберінцидентів. Загалом ці реакції фондового ринку можуть відповідати збиткам компаній до 90 мільйонів доларів США у ринковій вартості, що значно перевищує прямі збитки, про які повідомляється в відкритих джерелах.

Розуміння факторів, що сприяють виникненню або попередженню кіберінцидентів, є ключовим для розробки ефективних політик і стратегій кібербезпеки. Кіберінциденти визначаються загальною вразливістю компанії до кіберзагроз та її здатністю до запобігання. Наприклад, великі і прибуткові фірми з розвиненою цифровою присутністю і значною залежністю від інформаційних та комунікаційних технологій можуть бути більш привабливими мішенями для кібератак, ніж менші компанії з обмеженим цифровим слідом. Проте ці великі фірми часто мають більше можливостей інвестувати в кібербезпеки, що може зменшити їх вразливість до кіберінцидентів. Компанії, що знаходяться в країнах з високим рівнем геополітичної напруги, також можуть бути більш схильні до кібератак, що є результатом загроз з боку конкурентних держав.

Компанії ефективною системою кіберуправління та ті, що функціонують у країнах із «суворим» кіберзаконодавством, мають більші шанси запобігти кіберінцидентам. Економетричний аналіз показує, що цифровізація та геополітична напруженість значно підвищують ризик кіберінцидентів. Країни з високим рівнем геополітичної напруги також демонструють підвищений ризик виникнення кіберінцидентів. Великі компанії і фірми з високою часткою нематеріальних активів, особливо в IT-секторі, мають значно вищу ймовірність стати жертвою кіберінцидентів. Навпаки, компанії, що діють у країнах з розвиненим кіберзаконодавством, менше схильні до кіберзагроз.

Компанії, які перейшли на дистанційну роботу під час пандемії COVID-19, стали більш вразливими до кіберінцидентів. Аналіз показує, що компанії, які раніше помірно використовували дистанційну роботу, але під час пандемії повністю перейшли на цей формат, зазнали значного зростання кіберінцидентів. До пандемії фірми з високим рівнем дистанційної роботи мали більшу ймовірність стати жертвами кіберзагроз, ймовірно, через більшу залежність від IT-інфраструктури.

Однак після пандемії ймовірність того, що ці компанії зазнають кіберінциденти, знизилася. Компанії, які до пандемії не мали сильної дистанційної робочої практики, рідше переходили на дистанційну роботу і менше постраждали від кіберзагроз під час пандемії. Це можна пояснити тим, що недостатні механізми управління кібербезпекою під час пандемії підвищили вразливість фірм. Фірми, які вже мали добре розвинуті системи кібербезпеки та управління, а також адаптовану робочу силу до дистанційного формату до пандемії, були краще підготовлені до кіберзагроз. Отже, фірми в секторах з високою схильністю до дистанційної роботи до пандемії мали кращі механізми управління для зменшення кіберризиків. Ці компанії частіше мали членів правління з досвідом у сфері кібербезпеки, розроблені політики кібербезпеки та захисту конфіденційності даних, а також отримували вищі бали за індексом здатності управляти ризиками конфіденційності даних. Під час пандемії ці фірми продовжували вдосконалювати свої практики управління кібербезпеки. Аналізуючи вплив пандемії COVID-19 на корпоративну кібербезпеку з точки зору публічного управління, важливо відзначити кілька ключових тенденцій та уроків. По-перше, компанії, які ще до пандемії мали розвинуті практики дистанційної роботи та надійні системи кіберзахисту, виявилися значно стійкішими до зростання кіберзагроз в умовах масового переходу на віддалений формат. Це підкреслює критичну важливість проактивного підходу до управління кіберризиками, який передбачає не лише впровадження відповідних технологічних рішень, але й формування належної корпоративної культури та компетенцій персоналу.

З іншого боку, організації, які до кризи не приділяли достатньої уваги розвитку дистанційних форматів роботи та кібербезпеці, опинилися в більш вразливому становищі. Раптовий та неконтрольований перехід співробітників на віддалений доступ часто відбувався на тлі недостатніх механізмів захисту корпоративних даних та систем. Така ситуація створила додаткові можливості для зловмисників, які активно експлуатували «людський фактор» та технічні прогалини у кіберзахисті компаній [1]. Водночас, навіть в умовах кризи, українські та міжнародні компанії демонструють здатність швидко адаптуватися та посилювати свою кіберстійкість. Організації, які зазнали кібератак, активно вдосконалюють свої підходи до управління кіберризиками, впроваджуючи

передові практики та залучаючи топ-менеджерів з відповідними компетенціями до наглядових органів. Це свідчить про зростаюче усвідомлення на найвищому управлінському рівні, що кібербезпека є не просто технічним питанням, а стратегічним пріоритетом, від якого залежить безперервність бізнесу та довіра стейкхолдерів.

З точки зору державної політики, ці тенденції актуалізують потребу в розробці та впровадженні комплексних стратегій кіберстійкості, які б стимулювали та підтримували зусилля приватного сектора. Важливими напрямками є формування сприятливого регуляторного середовища, яке б заохочувало компанії інвестувати в кібербезпеку, а також забезпечення ефективного державно-приватного партнерства та обміну інформацією про кіберзагрози. Держава також має відігравати ключову роль у розвитку експертного потенціалу та підвищенні обізнаності про кіберризики серед організацій та громадян. В українських реаліях ці завдання набувають своєрідного значення в контексті тривалої гібридної агресії та зростаючої геополітичної нестабільності. Забезпечення кіберстійкості критичної інфраструктури та бізнес-середовища є питанням не лише економічної, але й національної безпеки. Відтак, розбудова ефективної екосистеми кібербезпеки, яка охоплює органи влади, приватний сектор, наукові установи та громадянське суспільство, має стати стратегічним пріоритетом державної політики [23].

Фінансова стабільність є особливо вразливою до кібератак, оскільки фінустанови обробляють величезні масиви клієнтських даних і транзакцій, що робить їх привабливою мішенню для кіберзлочинців, які прагнуть до фінансової вигоди або спробують порушити економічну діяльність. Кіберінциденти в фінансовому секторі складають значну частину від світових, причому банки стикаються приблизно з половиною інцидентів у цьому секторі. Великі банки особливо вразливі, що підтверджуються рейтингами організацій за загальними показниками кібербезпеки, і це може бути пов'язано з тим, що великі банки частіше стають цілями, навіть якщо вони можуть мати більш розвинені кіберзахищені практики. Зазначені вразливості підкреслюють критичну важливість управління і подолання кіберризиків для забезпечення глобальної фінансової стабільності.

Фінансові установи особливо вразливі до кіберінцидентів через три ключові характеристики:

1) по-перше, висока ринкова концентрація. На національному та глобальному рівнях банки демонструють високу ринкову концентрацію в критичних послугах, таких як платіжні системи та зберігання банківських активів [5]. Платіжні мережі, що управляються банками, є важливою частиною ФІ. Кіберінциденти, які порушують ці мережі, можуть серйозно вплинути на економічну діяльність. Іншим напрямком є вразливість фінансової інфраструктури. Інфраструктура фінансових ринків, включаючи платіжні системи, системи розрахунків за цінними паперами, центральні депозитарії, центральні контрагенти та торговельні сховища, характеризується високою ринковою концентрацією та низькою взаємозамінністю. Це робить фінансову інфраструктуру особливо вразливою до кібератак. Важливість і специфічність цих ФП ускладнює заміну або відновлення після атаки. Успішна кібератака на ці критичні компоненти фінансової інфраструктури може мати серйозні наслідки для **фінансових установ**.

2) по-друге, операції фінансових фірм дедалі більше залежать від сторонніх ІТ-провайдерів, що забезпечують економію на масштабах і мережевих ефектах. Це включає впровадження стандартних програмних рішень, використання подібного обладнання та перехід на послуги глобальних постачальників хмарних технологій або критичних послуг. Сьогодні більше 50% ІТ-провайдерів, що мають глобальне системне значення, постачають свої продукти та послуги двом або більше великим системно важливим банкам, що свідчить про значний рівень перекриття. Аналогічно, близько 20% страховиків і 25% менеджерів активно отримують послуги від ІТ-провайдерів, які обслуговують дві або більше установ у відповідних секторах. Ці залежності, часто міжнародні, зросли разом із цифровізацією фінансового сектору. Хоча сторонні ІТ-провайдери можуть забезпечити фінансові вигоди, такі як підвищена оперативна стійкість, вони також несуть певні ризики. Якщо управління цими зовнішніми послугами не є належним, високий рівень перекриття у постачанні може призвести фінансові установи до загальних потрясінь і порушень критичних служб у разі кіберінцидентів яким запобігли за допомогою засобів кіберзахисту, що становить значний ризик для фінансових установ і загальної фінансової стабільності. Наприклад, кіберінциденти в ІТ-секторі часто поширюються на інші сектори.

3) по-третє, високий рівень взаємозв'язку між фінансовими установами може посилити ризик зараження та призвести до вищої ймовірності системних наслідків від КА. Наприклад, кіберінцидент, що порушує обробку платежів в одній фінансовій фірмі, може мати хвильовий ефект, впливаючи на ліквідність та діяльність інших фірм. Складніші ситуації, такі як серйозний кіберінцидент у вагомій фінансові установі, може ще більше підірвати довіру до фінансових установ в цілому. Це може призвести до масштабних ринкових розпродажів або навіть до банківських криз, коли вкладники масово знімають свої кошти з банків, що викликано побоюваннями про платоспроможність фінансових установ.

Кіберінциденти також можуть суттєво вплинути на ліквідність банків. Вкладники, особливо великі інституційні інвестори, можуть піддатися сумнівам щодо спроможності банків виконувати свої зобов'язання, якщо кіберінциденти порушить їх фінансові операції. Це може призвести до масового виведення коштів як запобіжного заходу, що в свою чергу може викликати фінансові проблеми для банку, відомі як кіберпобіги. Крім того, витік інформації про вкладників може завдати тривалої репутаційної шкоди банкам, що може зменшити притік нових депозитів і погіршити фінансове становище установи. Хоча суттєві кібервпливи ще не стали частими, і кіберінциденти загалом мали обмежений вплив на фінансові операції, наявні емпіричні дані свідчать про помірний, але стійкий відтік депозитів у банках США після кібератак. Наприклад, менші банки демонструють більшу вразливість до відтоку депозитів після кіберінцидентів, що свідчить про те, що такі банки не здатні швидко відновити довіру вкладників. У середньому роздрібні та оптові депозити в менших банках зменшуються приблизно на 5% у сукупному вираженні протягом шести кварталів після виявленого кіберінциденту.

Банки, які є більш вразливими до ризиків ліквідності, також мають підвищену вразливість до кіберризиків. Щоб оцінити можливий вплив КІ на ліквідність банків, необхідно проаналізувати відтік депозитів, при якому коефіцієнт покриття ліквідності банку впаде нижче нормативної вимоги в 100%.

Результати демонструють значну варіацію в ставках відтоку депозитів серед 80 великих світових банків. При відтоку депозитів на рівні 25% оптових (роздрібних) вкладів, коефіцієнти покриття ліквідності у банках знижуються до близько 20 (60)%, що може призвести до порушення нормативних вимог. Зокрема, банки з нижчими рейтингами кібербезпеки демонструють вищу вразливість до ризиків ліквідності, що підкреслює потребу у зміцненні кіберзахисту як частини стратегії управління ліквідністю для зменшення загрози від кіберінцидентів.

Швидка еволюція фінансових технологій (фінтех) вводить нові кіберризики, які загрожують ФС через їхні цифрові операції та взаємозв'язок. Нижче наведено основні аспекти цих проблематик. Фінтех-компанії, завдяки своїм інноваційним цифровим рішенням, стають більш вразливими до кіберзагроз: їх інтеграція в ФС збільшує загальний рівень кіберризиків. Наприклад, впровадження технологій на основі розумних контрактів у децентралізованих фінансах (DeFi) стало популярним, але також і небезпечним. Від 2020 року кібератаки на DeFi-платформи стали доволі частішими, що призвело до великих фінансових втрат.

Децентралізовані фінанси, що базуються на блокчейн-технології, використовують розумні контракти для автоматизації фінансових угод. Однак, ці контракти можуть бути вразливими до атак. Через їхню відкриту і часто неадекватно захищену природу, зловмисники можуть експлуатувати уразливості в коді, що призводить до значних фінансових збитків. Хоча на даний момент центральні банки не повідомляють про кіберінциденти що ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів з участю CBDC, необхідно зазначити, що потенційний ризик все ж таки існує. CBDC використовують новітні технології, такі як розподілені реєстраційні технології, які ще не мають повністю відпрацьованих стандартів КБ. Це може призвести до непередбачуваних кіберзагроз.

Криптоактиви та усі біржові платформи криптовалют також є популярними цілями кібератак. Кібератаки на криптобіржі збільшуються, оскільки криптоактиви стають все більш інтегрованими у ФС. Ці атаки можуть мати серйозні наслідки для ФС, особливо у випадках з стабільними монетами, забезпеченими фіатною валютою [1]. Як висновок, можна відмітити, що криптоактиви та інші нові фінансові технології стають все більш важливими для ФС, їх уразливість до КА може спричинити значні ризики для глобальної фінансової стабільності. Тому важливо постійно вдосконалювати та нарощувати систему захисту інформації та кібербезпеки та знижувати потенційні загрози для забезпечення стійкості фінансової стабільності. Згідно з опитуванням центральних банків МВФ у 2021 році та наглядових фінансових органах, політика кібербезпеки на ринках, що розвиваються, часто залишається недостатньою. Опитування, що було проведено в 2021 році і продовжено в 2023 році охоплювало 74 ринки, що розвиваються, і складалось з 43 питань за різними аспектами кібербезпеки. Воно показало, що лише 47% опитаних країн розробили національну та фінансову стратегії кібербезпеки. Близько половини країн впровадили спеціальні правила КБ, а 54% прийняли закони про захист даних. Аналіз різних аспектів опитування показує, що підходи до нагляду за кібербезпекою та тестування на ринках, що розвиваються, дещо покращилися з 2021 року, а саме:

1) майже половина опитаних ринків, що розвиваються, і країн з ринками, що розвиваються, повідомили про наявність спеціалізованих підрозділів для нагляду за кіберризиками. 72% з них вимагають регулярних кібервипробувань та навчань, з яких 22% активно управляють такими тестами;

2) майже половина опитаних юрисдикцій має повноваження перевіряти сторонніх постачальників послуг, що є важливим з урахуванням зростання кількості ФУ, які переходять на хмарні технології;

3) офіційні тести щодо стану кібербезпеки залишаються мало поширеними, лише 27% опитаних економік включають кіберризики у свої стрес-тестові програми. Лише 8% юрисдикцій мають розроблену кіберкарту, що визначає ключові технологічні та сервісні зв'язки між фінансовими установами;

4) механізми обміну інформацією у фінансовому секторі є важливими для запобігання кіберзагрозам, але тільки 28% юрисдикцій повідомляють про систематичний обмін інформацією між фінансовими організаціями. Хоча центральні банки та наглядові органи активніше залучаються до обміну інформацією всередині галузі, кількість країн, що обмінюються даними з іншими юрисдикціями, не зросла і залишається на рівні близько 50%. Лише 49% країн мають режими звітності про інциденти кібербезпеки.

Індекс готовності до кібербезпеки є важливим інструментом оцінки спроможності країн протидіяти зростаючим кіберзагрозам у фінансовому секторі. Цей індекс, розроблений провідними міжнародними експертами, використовує комплексну методологію для вимірювання рівня зрілості регуляторних і наглядових механізмів у сфері кібербезпеки. За шкалою від 0 до 5, де 5 відповідає найвищому рівню готовності, характерному для розвинених економік як США, індекс дозволяє проводити компаративний аналіз кіберстійкості фінансових систем різних країн світу.

Результати індексу за 2023 рік свідчать, що для ринків, які розвиваються, середній бал становить 3, що лише на 0,2 пункти вище показника 2021 року. Хоча цей результат вказує на певний прогрес, він все ще відображає лише помірний рівень готовності цих країн до кіберзагроз. Більше того, половина досліджуваних країн має оцінку нижче 3 балів, а понад 20% – нижче 2 балів. Такі показники є тривожним сигналом, який свідчить про значні прогалини в системах кіберзахисту фінансового сектора цих держав.

З точки зору державного управління, ці дані вказують на необхідність невідкладних та рішучих кроків для зміцнення кіберстійкості на національному та глобальному рівнях. Зокрема, країнам, що розвиваються, потрібно терміново розробляти і впроваджувати комплексні стратегії кібербезпеки, які б визначали чіткі цілі, пріоритети та механізми захисту критичної фінансової інфраструктури від цифрових загроз.

Ці стратегії повинні ґрунтуватися на найкращих світових практиках та стандартах, що розробляються провідними міжнародними організаціями, такими як Міжнародний валютний фонд, Світовий банк, Рада з фінансової стабільності тощо. Важливими елементами таких стратегій мають бути:

1) створення ефективної нормативно-правової бази, яка б чітко визначала вимоги до кібербезпеки фінансових установ, встановлювала відповідальність за порушення, а також заохочувала обмін інформацією про інциденти та співпрацю між зацікавленими сторонами;

2) розбудова потужних інституційних механізмів кібербезпеки, зокрема створення спеціалізованих підрозділів в регуляторних та наглядових органах,

які б мали належну компетенцію та ресурси для оцінки і моніторингу кіберризиків;

3) налагодження тісної координації та обміну інформацією між державним та приватним секторами, а також між різними державними агенціями, відповідальними за кібербезпеку, фінансову стабільність, правоохоронну діяльність тощо;

4) впровадження регулярних програм оцінки та тестування кіберстійкості фінансових установ, включаючи стрес-тести, тренування з реагування на інциденти, «червоні команди» тощо. Такі заходи дозволяють виявляти вразливості та покращувати готовність до реальних кіберзагроз;

5) інвестиції в розвиток людського капіталу та експертизи в сфері кібербезпеки. Це передбачає створення спеціалізованих освітніх та тренінгових програм, залучення висококваліфікованих фахівців, а також підвищення обізнаності персоналу фінансових установ та громадськості щодо кіберзагроз.

Окрім зусиль на національному рівні, забезпечення кіберстійкості фінансового сектора вимагає активізації міжнародної співпраці. Враховуючи транскордонний характер кіберзагроз, країни повинні розвивати спільні протоколи та механізми обміну інформацією, координації дій та взаємодопомоги в разі масштабних кіберінцидентів. Важливу роль у цьому відіграють глобальні інститути, такі як МВФ, які надають країнам-членам технічну допомогу, проводять навчання та розробляють уніфіковані інструменти оцінки кіберризиків. Крім того, МВФ активно співпрацює з органами, що встановлюють міжнародні стандарти кібербезпеки для фінансового сектора. Така координація на глобальному рівні дозволяє уніфікувати регуляторні підходи, обмінюватися найкращими практиками та швидко реагувати на нові виклики.

Результати Індексу готовності до кібербезпеки красномовно свідчать про нагальну потребу в рішучих діях з боку урядів як на національному, так і на глобальному рівнях для зміцнення кіберстійкості фінансового сектора. Особливо це стосується країн, що розвиваються, де прогалини в системах кіберзахисту є найбільш відчутними. Розробка та імплементація національних стратегій кібербезпеки має стати безумовним пріоритетом для цих держав. Такі стратегії повинні базуватися на найкращому світовому досвіді та рекомендаціях впливових міжнародних інституцій, таких як МВФ, Світовий банк чи Рада фінансової стабільності. Вони мають передбачати широкий спектр заходів - від створення надійної нормативно-правової бази та потужних регуляторних механізмів до інвестицій у розвиток кадрового потенціалу та просвітницьку роботу з підвищення обізнаності про кіберзагрози.

Яскравим прикладом такого підходу є Індія, яка в 2022 р. прийняла прогресивну Національну стратегію кібербезпеки. Ця амбітна п'ятирічна програма передбачає створення централізованого регуляторного органу – Індійського управління з кібербезпеки, а також запуск масштабної ініціативи з підготовки 500 тисяч фахівців у цій галузі. Не менш вражаючий кейс демонструє Сінгапур, який ще в 2018 р. запровадив обов'язкове звітування про кіберінциденти для всіх ключових секторів економіки, включаючи фінанси. Цей крок дозволив значно покращити розуміння ландшафту кіберзагроз та оперативність реагування на них. Водночас, навіть найсильніші національні стратегії не можуть бути повністю ефективними без тісної міжнародної співпраці. Кібератаки не знають кордонів, тож і протидія їм має носити глобальний характер. В цьому контексті надзвичайно важливою є роль таких організацій,

як МВФ, який активно допомагає країнам-членам зміцнювати їхню кіберстійкість шляхом технічної підтримки, навчальних програм та розробки універсальних інструментів оцінки ризиків.

Ще одним перспективним напрямком зміцнення кіберстійкості є розвиток ринку кіберстрахування. Страхові поліси можуть покривати збитки фінансових установ від кібератак, знижуючи їх вразливість до операційних та репутаційних ризиків. Однак поточне покриття кіберстрахування залишається обмеженим: більшість полісів у США мають ліміт до 1 млн доларів. Наприклад, Великобританія в рамках своєї Стратегії кібербезпеки до 2025 року планує запровадити спеціальні податкові пільги для компаній, які інвестують у кіберстрахування. А влада ОАЕ взагалі розглядає можливість зробити таке страхування обов'язковим для критичної інфраструктури, включно з фінансовим сектором. Тому на державному рівні важливо стимулювати розвиток цього ринку, створюючи сприятливе регуляторне середовище та заохочуючи страховиків розробляти нові продукти.

Підсумовуючи, можна констатувати, що зміцнення кібербезпеки фінансового сектора є комплексним завданням, яке вимагає узгоджених зусиль на національному та міжнародному рівнях. Розробка ефективних стратегій, інвестиції в потенціал, активна міжнародна співпраця та розвиток кіберстрахування – все це критично важливі складові для підвищення стійкості фінансових систем в умовах ескалації цифрових загроз. Лише за рахунок системного та проактивного підходу, який поєднує регуляторні, наглядові, освітні та ринкові інструменти, держави зможуть належним чином захистити свій фінансовий сектор та забезпечити довіру і стабільність в епоху тотальної цифровізації. Це вимагатиме політичної волі, значних ресурсів та постійної адаптації до нових викликів. Але враховуючи масштаб потенційних збитків від кібератак, такі інвестиції є критично необхідними для стійкого розвитку як окремих країн, так і глобальної фінансової екосистеми.

Висновки і перспективи подальших розвідок у даному напрямку. На основі проведених досліджень можна зробити такі узагальнені висновки.

1) Для забезпечення макрофінансової стабільності і підвищення стійкості фінансових інститутів важливо розробити комплексну стратегію кібербезпеки, яка буде супроводжуватися ефективним регулюванням та наглядом. Така стратегія має включати створення кваліфікованих підрозділів для контролю кіберризиків, здатних регулярно проводити оцінки та здійснювати моніторинг кібербезпеки в фінансових установах. Це дозволить виявляти потенційні загрози та швидко реагувати на них. Важливим елементом стратегії є картографування фінансових та технологічних зв'язків для виявлення системних ризиків, зокрема тих, що пов'язані з концентрацією та взаємозв'язками з сторонніми постачальниками послуг. Така ідентифікація потенційних уразливих місць дозволяє своєчасно вжити заходів для мінімізації ризиків, що можуть загрожувати стабільності фінансових установ.

2) Швидка еволюція фінансових технологій створює нові виклики для кібербезпеки, які вимагають постійної адаптації регуляторних підходів. Інтеграція інноваційних фінтех-рішень робить фінансову систему більш вразливою до кіберзагроз. Децентралізовані фінанси на основі блокчейну та смарт-контрактів, хоча й пропонують переваги, також несуть суттєві ризики через свою відкритість та часто недостатній захист. Атаки на криптобіржі та платформи стають дедалі частішими та масштабнішими. Навіть розвиток таких

перспективних технологій, як цифрові валюти центробанків, потребує ретельного опрацювання стандартів кібербезпеки. Застосування штучного інтелекту хоч і допомагає виявляти anomalies, але водночас створює нові загрози, як складні фішингові атаки на основі діпфейків. Ці виклики вимагають від регуляторів постійно переглядати та адаптувати свої підходи, розвиваючись разом з технологіями. Потрібні гнучкі, ризик-орієнтовані моделі регулювання, які б стимулювали відповідальні інновації та водночас надійно захищали систему. Регулярний діалог наглядових органів з фінтех-індустрією та експертами, стрес-тестування нових продуктів, розробка специфічних наглядових технологій (SupTech) – все це стає обов'язковою умовою ефективного управління кіберризиками на фінансових ринках майбутнього.

3) Наглядові органи повинні заохочувати фінансові компанії до розвитку кіберзрілості. Це передбачає не лише наявність кіберекспертизи на рівні управлінських органів, а й запровадження підходу з трьома лініями захисту, який включає управління ризиками в бізнес-процесах, управління ризиками на рівні підприємства та належний рівень аудиту. Важливими аспектами є також покращення кібергігієни, захист від шкідливого програмного забезпечення, багатофакторна автентифікація та регулярне навчання персоналу з метою підвищення обізнаності щодо кіберзагроз.

4) Недостатність даних щодо кіберінцидентів є серйозною перешкодою для ефективного нагляду та управління ризиками. Хоча звітування про КІ та пов'язані з ними втрати покращилось останнім часом, ці дані все ще залишаються неповними і часто надходять із затримкою. Тому критично важливо зробити збір даних про КІ пріоритетом на глобальному рівні, а також стимулювати фінансовий сектор до активного обміну інформацією, що дозволить підвищити колективну готовність та забезпечити більш ефективне управління ризиками.

5) Наглядові органи повинні вимагати від фінансових установ розробки і регулярного тестування процедур реагування на кіберінциденти та відновлення після них. Це важливо для забезпечення безперервності надання критичних послуг, навіть під час збоїв у системах. Банки повинні ідентифікувати критичні бізнес-послуги та забезпечити наявність перевірених планів аварійного відновлення і кризового управління, що допоможе мінімізувати перебої в роботі фінансового сектору.

Перспективи подальших досліджень прямо пов'язуються зі значущістю кіберризиків і, відповідно, з зусиллями фінансових установ, які повинні бути підготовлені до можливих операційних втрат, зокрема через КІ. Окрім вимог до капіталу для покриття операційного ризику, банки повинні забезпечити наявність ресурсів для безперебійної роботи навіть у разі серйозних кіберзагроз. Це потребує інтеграції кібербезпеки в загальний процес управління ризиками та фінансовою стабільністю установ. Отже, ефективна стратегія кібербезпеки в фінансовому секторі є необхідною умовою для забезпечення його стійкості в умовах постійно зростаючих кіберзагроз. Розвиток відповідних інструментів для оцінки ризиків, моніторингу та реагування на кіберінциденти, а також впровадження міжнародної співпраці, сприятиме зміцненню кіберстабільності фінансових установ і зменшенню їх уразливості до кіберзагроз.

Розвиток ринку кіберстрахування є перспективним, але поки недостатньо використаним інструментом зміцнення кіберстійкості фінансового сектора.

Страхові поліси здатні суттєво знизити вразливість фінансових установ до кібератак, покриваючи як прямі, так і непрямі збитки. Це особливо важливо з огляду на масштаби потенційних втрат. За оцінками, раз на десятиліття кіберінциденти можуть завдавати фінустановам збитків до $2,2 млрд. Втім, поточне покриття кіберризиків лишається обмеженим – ліміти більшості полісів у США не перевищують $1 млн. Причини – брак якісних даних для оцінки ризиків, відсутність стандартизованих умов, побоювання страховиків щодо кумуляції збитків. Тому на державному рівні критично важливо створювати стимули для розвитку кіберстрахування, як через удосконалення регулювання, так і непрямі механізми на кшталт податкових пільг. Приклади Великобританії з її Стратегією кібербезпеки-2025, чи ОАЕ з планами обов'язкового страхування для критичної інфраструктури, вказують на перспективність такого підходу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Басюк О. Рекомендації до впровадження технологій розподіленого реєстру (блокчейн) у публічний сектор України на основі світового досвіду. *Актуальні проблеми державного управління*. 2023. № 1 (62), С. 131–154. DOI: https://doi.org/10.26565/1684-8489-2023-1-08 URL: https://periodicals.karazin.ua/apdu/article/view/22631
2. Живило Є., Живило І. Об'єднана підготовка персоналу складових сил оборони сфери кібербезпеки в умовах тотальної оборони держави. *Теорія та практика державного управління.* 2021. № 2 (73). С. 144–153. DOI: https://doi.org/10.34213/tp.21.02.16 URL: https://periodicals.karazin.ua/tpdu/article/view/20552
3. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) : *Аналітична записка Національного інституту стратегічних досліджень*. Березень 2017 р. URL: http://old.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf
4. Потій О. В., Козлов Ю. Н., Дьяченко І. І. Базові принципи електронної ідентифікації. Концепція інфраструктури електронної ідентифікації України. *Прикладна радіоелектроніка*. 2015. Т. 14. № 4. С. 366–369. URL: http://nbuv.gov.ua/UJRN/Prre_2015_14_4_18
5. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Кабінету міністрів України від 11 листопада 2020 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text
6. Akomea-Frimpong I., Adeabah D., Ofosu D., Tenakwah E. J. A review of studies on green finance of banks, research gaps and future directions. *Journal of Sustainable Finance & Investment.* 2021. Vol. 12. No. 4. P. 1241–1264. DOI: https://doi.org/10.1080/20430795.2020.1870202
7. AlBenJasim S., Dargahi T., Takruri H., Al-Zaidi R. FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. *Journal of Computer Information Systems*. 2023. Vol. 64. No. 6. P. 835–851. DOI: https://doi.org/10.1080/08874417.2023.2251455
8. Bissell K., Lasalle R. M., Cin P. D. The cost of cybercrime: Ninth annual cost of cybercrime study. Accenture. 2019. URL: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (дата звернення: 22.12.2024).
9. Carver J. European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy.* 2024. Vol. 31. No. 8. P. 2250–2286. DOI: https://doi.org/10.1080/13501763.2023.2295523
10. Cyber resilience oversight expectations for financial market infrastructures. *European Central Bank.* 2018. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.cyberresilienceoversightexpectations201812.en.pdf (дата звернення: 22.12.2024).
11. Donnelly S., Ríos Camacho E., Heidebrecht S. Digital sovereignty as control: the regulation of digital finance in the European Union. *Journal of European Public Policy*. 2023. Vol. 31. No. 8. P. 2226–2249. DOI: https://doi.org/10.1080/13501763.2023.2295520
12. Duffie D., Younger J. Cyber runs: How a cyber attack could affect U.S. financial institutions. *Brookings.* 2019. URL: https://www.brookings.edu/articles/cyber-runs/ (дата звернення: 22.12.2024).

13. Gutiérrez Ponce H., Chamizo González J., Al-Mohareb M. Sustainable finance in cybersecurity investment for future profitability under uncertainty. *Journal of Sustainable Finance & Investment*. 2021. Vol. 13. No. 1. P. 614–633. DOI: https://doi.org/10.1080/20430795.2021.1985951

14. Hernandez-Castro J., Boiten E. The Economic Impact of Cybercrime. Cybersecurity. 2020. Vol. 3. No. 1. DOI: https://doi.org/10.1186/s42400-020-00062-6

15. Kahler J., Lai R., Weber W. Cybersecurity and Financial Stability: The Role of Central Banks. *Journal of Financial Stability*. 2019. Vol. 42. P. 1–12. DOI: https://doi.org/10.1016/j.jfs.2019.05.014

16. Kashkevich S., Shyshatskyi A., Dmytriieva O., Zhyvylo Y., Plekhova G., Neronov S. The development of management methods based on bio-inspired algorithms. Information and control systems: modelling and optimizations: collective monograph. Kharkiv : Technology Center Pc, 2024. P. 35–69. DOI: https://doi.org/10.15587/978-617-8360-04-7

17. Knoop T., Perry J., González A. Central Bank Digital Currencies and Cyber Resilience. *BIS Working Papers.* 2021. No. 949. URL: https://www.bis.org/publ/work949.htm (дата звернення: 22.12.2024).

18. Kopp E., Lincoln B., Hesse H. Cybersecurity and Financial Stability. *IMF Working Papers*. 2020. No. 2020/208. DOI: https://doi.org/10.5089/9781513562834.001

19. Madnick B., Huang K., Madnick S. The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal: A Global Perspective*. 2023. Vol. 33. No. 3. P. 204–225. DOI: https://doi.org/10.1080/19393555.2023.2201482

20. Musleh Al-Sartawi A. M. A., Hussainey K., Razzaque A. The role of artificial intelligence in sustainable finance. Journal of Sustainable Finance & Investment. 2022. P. 1–6. DOI: https://doi.org/10.1080/20430795.2022.2057405

21. Onyshchenko S., Zhyvylo Y., Cherviak A., Bilko S. Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies*. 2023. Vol. 5. No. 13 (125). P. 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175

22. Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS). Computer Security Resource Center. URL: https://csrc.nist.gov/pubs/sp/800/94/final (дата звернення: 22.12.2024).

23. Zhyvylo Y., Kuz V. Risk Management of Critical Information Infrastructure: Threas-Vulnerabilities-Consequences. *Theoretical and Applied Cyber Security.* 2023. Vol. 5. No. 2. P. 68–80. URL: http://surl.li/vzrhfs

Стаття надійшла до редакції 20.09.2024 р.
Стаття рекомендована до друку 25.10.2024 р.

Zhyvylo Ye. O.,
PhD, Post-doc Fellow of the Department of Public Policy,
Education and Research Institute of Public Administration, V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: zhivilka@i.ua https://orcid.org/0000-0003-4077-7853

NATIONAL MACROFINANCIAL STABILITY IN THE CONTEXT OF CYBER THREATS

Abstract. This article addresses the critical issue of ensuring state macrofinancial stability in the face of growing cyber threats. Financial market stability forms the foundation of any country's economic development and prosperity, as it ensures efficient capital movement, reduces uncertainty, and promotes investment growth. However, this stability is vulnerable to various external and internal threats, particularly cyber risks, which can significantly disrupt financial institutions' operations and even cause serious economic turmoil. The author emphasizes the critical importance of this issue in the era of digital economic transformation, where financial systems become increasingly vulnerable to potentially catastrophic consequences of cyberattacks. The article analyzes the main channels through which cyber incidents impact financial stability, including payment system disruptions, loss of investor and consumer confidence, and critical service failures due to the interconnectedness of

financial institutions. Special attention is paid to cyber readiness challenges in developing countries, which often lack sufficient resources and experience to effectively counter digital threats. The author emphasizes the necessity of developing and implementing comprehensive national cybersecurity strategies that would define clear objectives, priorities, and mechanisms for protecting financial infrastructure. These strategies should be based on global best practices and encompass a wide range of measures: from establishing an effective regulatory framework to investing in human capital development. The article also emphasizes the importance of enhancing international cooperation to strengthen cyber resilience, considering the cross-border nature of digital threats. In this context, the key role of global institutions, such as the International Monetary Fund, in providing technical assistance to countries, conducting training, and developing universal cyber risk assessment tools is noted. Overall, the article contributes to the study of financial sector cybersecurity issues and offers the author's vision for addressing them at both national and international levels.

Keywords: public administration, information protection system, cybersecurity, information technology, information security, cybersecurity, financial institutions.

REFERENCES

1. Basiuk, O. (2023). Recommendations for the implementation of distributed ledger technologies (blockchain) in the public sector of Ukraine based on world experience*. Pressing Problems of Public Administration, 1(62), 131–154.* DOI: https://doi.org/10.26565/1684-8489-2023-1-08 [in Ukrainian].

2. Zhyvylo, Ye., & Zhyvylo, I. (2021). [United training of personnel of the components of the defense forces in the field of cybersecurity in the conditions of total defense of the state]. *Theory and Practice of Public Administration, 2(73), 144–153*. DOI: https://doi.org/10.34213/tp.21.02.16 [in Ukrainian].

3. Threats to critical infrastructure and their impact on the state of national security (monitoring the implementation of the National Security Strategy). (2017). Analytical note of the National Institute of Strategic Studies. March. URL: http://old.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf (accessed: 15.12.2024) [in Ukrainian].

4. Potii, O.V., Kozlov, Yu.N., & Diachenko, I.I. (2015). Basic principles of electronic identification. The concept of electronic identification infrastructure of Ukraine. *Applied radio electronics, 14(4), 366–369.* URL: http://nbuv.gov.ua/UJRN/Prre_2015_14_4_18 (accessed: 15.12.2024) [in Ukrainian].

5. On approval of the Procedure for conducting a review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law: Resolution of the Cabinet of Ministers of Ukraine № 1176. (2020, November 11). URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (accessed: 15.12.2024) [in Ukrainian].

6. Akomea-Frimpong, I., Adeabah, D., Ofosu, D., & Tenakwah, E.J. (2021). A review of studies on green finance of banks, research gaps and future directions. *Journal of Sustainable Finance & Investment, 12(4), 1241–1264.* DOI: https://doi.org/10.1080/20430795.2020.1870202

7. AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. *Journal of Computer Information Systems, 64(6), 835–851.* DOI: https://doi.org/10.1080/08874417.2023.2251455

8. Bissell, K., Lasalle, R.M., & Cin, P.D. (2019). The cost of cybercrime: Ninth annual cost of cybercrime study. Accenture. URL: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

9. Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy, 31(8), 2250–2286.* DOI: https://doi.org/10.1080/13501763.2023.2295523

10. European Central Bank. (2018). Cyber resilience oversight expectations for financial market infrastructures. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.cyberresilienceoversightexpectations201812.en.pdf

11. Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2023). Digital sovereignty as control: the regulation of digital finance in the European Union. *Journal of European Public Policy, 31(8), 2226–2249.* DOI: https://doi.org/10.1080/13501763.2023.2295520

12. Duffie, D., & Younger, J. (2019). Cyber runs: How a cyber attack could affect U.S. financial institutions. Brookings. URL: https://www.brookings.edu/articles/cyber-runs/

13. Gutiérrez Ponce, H., Chamizo González, J., & Al-Mohareb, M. (2021). Sustainable finance in cybersecurity investment for future profitability under uncertainty. *Journal of Sustainable Finance & Investment, 13(1), 614–633.* DOI: https://doi.org/10.1080/20430795.2021.1985951

14. Hernandez-Castro, J., & Boiten, E. (2020). The Economic Impact of Cybercrime. *Cybersecurity, 3(1).* DOI: https://doi.org/10.1186/s42400-020-00062-6

15. Kahler, J., Lai, R., & Weber, W. (2019). Cybersecurity and Financial Stability: The Role of Central Banks. *Journal of Financial Stability, 42, 1–12.* https://doi.org/10.1016/j.jfs.2019.05.014

16. Kashkevich, S., Shyshatskyi, A., Dmytriieva, O., Zhyvylo, Y., Plekhova, G., & Neronov, S. (2024). The development of management methods based on bio-inspired algorithms. In Information and control systems: modelling and optimizations: collective monograph (pp. 35-69). Technology Center Pc. DOI: https://doi.org/10.15587/978-617-8360-04-7

17. Knoop, T., Perry, J., & González, A. (2021). Central Bank Digital Currencies and Cyber Resilience. *BIS Working Papers, No 949.* DOI: https://www.bis.org/publ/work949.htm

18. Kopp, E., Lincoln, B., & Hesse, H. (2020). Cybersecurity and Financial Stability. *IMF Working Papers, 2020(208).* DOI: https://doi.org/10.5089/9781513562834.001

19. Madnick, B., Huang, K., & Madnick, S. (2023). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal: A Global Perspective, 33(3), 204–225*. DOI: https://doi.org/10.1080/19393555.2023.2201482

20. Musleh Al-Sartawi, A.M.A., Hussainey, K., & Razzaque, A. (2022). The role of artificial intelligence in sustainable finance. *Journal of Sustainable Finance & Investment, 1–6*. DOI: https://doi.org/10.1080/20430795.2022.2057405

21. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., & Bilko, S. (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies, 5(13(125)), 65–76.* DOI: https://doi.org/10.15587/1729-4061.2023.288175

22. Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS). (n.d.). Computer Security Resource Center. URL: https://csrc.nist.gov/pubs/sp/800/94/final

23. Zhyvylo, Y., & Kuz, V. (2023). Risk Management of Critical Information Infrastructure: Threas-Vulnerabilities-Consequences. *Theoretical and Applied Cyber Security, 5(2), 68–80.* URL: http://surl.li/vzrhfs

The article was received by the editors 20.09.2024.

The article is recommended for printing 25.10.2024.