УДК 336.71 doi: 10.20998/2519-4461.2025.3.20

В.В. ЧАПАЙЛО

ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ БАНКІВ У КОНТЕКСТІ ЦИФРОВІЗАЦІЇ ПРОЦЕСІВ

У статті обґрунтовуються теоретико-практичні засади підвищення кібербезпеки банківського сектору в умовах активної цифрової трансформації економіки. Метою дослідження є виявлення взаємозв'язку між рівнем цифровізації банківської діяльності та ефективністю заходів кіберзахисту, а також визначення напрямів удосконалення захисних технологій і організаційних механізмів, що забезпечують інформаційну безпеку банків. Для досягнення мети використано комплексний підхід, який включає аналіз сучасних кіберзагроз, огляд нормативно-правової бази, оцінку технологічних рішень, а також вивчення міжнародного досвіду у сфері інформаційної безпеки фінансових установ. У результаті дослідження встановлено, що процес цифровізації банківської системи супроводжується зростанням складності ІТ-інфраструктури, збільшенням кількості вразливих точок доступу і обсягів оброблюваних даних, що значно підвищує ризики кібератак. Враховуючи це, ефективний кіберзахист можливий лише за умови впровадження інноваційних технологій, серед яких системи раннього виявлення та реагування на інциденти інформаційної безпеки, зокрема Security Information and Event Management (SIEM) і User and Entity Behavior Analytics (UEBA), а також застосування архітектури нульової довіри, багатофакторної автентифікації і криптографічних методів захисту даних. Досліджено роль міжнародних стандартів, зокрема ISO/IEC 27001, у формуванні системи управління інформаційною безпекою, що дозволяє підвищити рівень кіберстійкості банківських установ. Проаналізовано досвід провідних країн, зокрема Європейського Союзу, Сполучених Штатів Америки, Японії та Південної Кореї, які демонструють ефективні моделі організації кібербезпеки фінансового сектору на основі міжгалузевої координації, впровадження передових стандартів і розвитку центрів реагування на інциденти. Значну увагу приділено діяльності Національного банку України у сфері кіберзахисту, а також необхідності посилення міжвідомчої співпраці, удосконалення нормативної бази і підвищення цифрових компетенцій працівників банків. Висновки дослідження підкреслюють, що лише комплексний підхід, який поєднує технічні інновації, нормативно-правове регулювання та управлінські рішення, сприяє формуванню надійної та стійкої банківської системи в умовах сучасної цифрової економіки.

Ключові слова: кібербезпека банків, цифрова трансформація, інформаційна безпека, системи виявлення інцидентів, архітектура нульової довіри, міжнародні стандарти, кіберзагрози, кіберстійкість, цифрові компетенції.

V.CHAPAILO

IMPROVING CYBERSECURITY OF BANKS IN THE CONTEXT OF DIGITALIZATION OF PROCESSES

The article substantiates the theoretical and practical foundations for enhancing cybersecurity in the banking sector amid the active digital transformation of the economy. The study aims to identify the relationship between the level of digitalization in banking activities and the effectiveness of cybersecurity measures, as well as to determine directions for improving protective technologies and organizational mechanisms that ensure information security in banks. To achieve this goal, a comprehensive approach was applied, including the analysis of current cyber threats, review of regulatory frameworks, evaluation of technological solutions, and examination of international experience in financial institutions' information security. The research findings reveal that the process of digitalizing the banking system is accompanied by increasing complexity of IT infrastructure, a growing number of vulnerable access points, and expanded volumes of processed data, which significantly heighten cyberattack risks. Considering this, effective cybersecurity is possible only through the implementation of innovative technologies, including early detection and response systems such as Security Information and Event Management (SIEM) and User and Entity Behavior Analytics (UEBA), as well as the adoption of Zero Trust architecture, multi-factor authentication, and cryptographic data protection methods. The study also investigates the role of international standards, particularly ISO/IEC 27001, in forming an information security management system that enhances the cyber resilience of banking institutions. The experience of leading countries, including the European Union, the United States, Japan, and South Korea, is analyzed, demonstrating effective models of organizing financial sector cybersecurity based on intersectoral coordination, implementation of advanced standards, and development of incident response centers. Special attention is given to the activities of the National Bank of Ukraine in cybersecurity, as well as the need to strengthen interagency cooperation, improve the regulatory framework, and enhance the digital competencies of bank personnel. The study concludes that only an integrated approach combining technological innovation, regulatory governance, and management decisions contributes to building a reliable and resilient banking system in the context of the modern digital economy.

Keywords: banking cybersecurity, digital transformation, information security, incident detection systems, Zero Trust architecture, international standards, cyber threats, cyber resilience, digital competencies.

Вступ. У сучасних умовах цифрової трансформації економіки банківський сектор являється одним із ключових об'єктів впливу інноваційних технологій. Впровадження цифрових інструментів, таких як мобільний банкінг, відкриті API, хмарні платформи, аналітика великих даних, штучний інтелект, переосмислює й оновлює операційні процеси, моделі ведення бізнесу, а також підходи до взаємодії з клієнтами. Разом з тим цифровізація створює нові вектори вразливості, оскільки обсяги електронних даних збільшуються, ІТ-інфраструктура стає більш відкритою, а інтенсивність та складність кібератак зростає.

Особливо актуальним питанням у цьому контексті є забезпечення кібербезпеки банківського сектору. Кібератаки на фінансову систему не лише загрожують фінансовими втратами для окремих банків, а й несуть потенційні системні ризики для економіки в цілому. За даними Національного банку України, протягом останніх років спостерігається зростання кількості кіберінцидентів у банківському секторі, попри покращення загальної технологічної спроможності установ [1]. Така ситуація актуалізує потребу у системному дослідженні взаємозв'язку між рівнем цифровізації та стійкістю банків до кіберзагроз.

Разом із тим, зростає роль міжнародних стандартів, практик та ініціатив у сфері управління інформаційною безпекою, які можуть бути адаптовані в межах національного банківського ринку. Комплексний підхід до цифрової трансформації повинен включати не лише впровадження нових технологій, але й модернізацію організаційної структури, підвищення цифрових компетенцій співробітників, створення культури безпеки та запровадження ефективних регламентів реагування на інциденти.

Аналіз останніх досліджень і публікацій. Проблематиці забезпечення фінансової безпеки банківських установ та впровадженню інноваційних технологій у банківській сфері присвячено чимало наукових праць, зокрема дослідження І. Кулиняка, Н. Давиденко, В. Міщенко, В. Коваленко, В. Сидської та інші. Проте, попри наявність широкого кола робіт, що стосуються кібербезбеки та інновацій у банківській діяльності, комплексному дослідженню взаємозв'язку між цифровізацією банків і підвищенням рівня кібербезпеки приділено недостатньо уваги. Це зумовлює наукову актуальність обраної теми, особливо в умовах воєнного стану, цифрових трансформацій та зростання загроз інформаційній безпеці.

Мета роботи. Метою даної роботи є обґрунтування теоретико-практичних засад підвищення кібербезпеки банків у контексті цифрової трансформації економіки, з урахуванням вітчизняного та міжнародного досвіду, а також виявлення напрямів удосконалення захисних інструментів.

Викладення основного матеріалу дослідження. Цифрова трансформація банківської системи – це складний багатовимірний процес, що охоплює впровадження інноваційних інформаційно-комунікаційних технологій з метою оптимізації внутрішніх процесів, покращення взаємодії з клієнтами, розширення спектра фінансових послуг і забезпечення конкурентоспроможності. У контексті сучасної економіки цифровізація стає не лише технологічним інструментом, а й стратегічною відповіддю на виклики глобального фінансового середовища.

Цифровізація банку передбачає глибоку зміну моделі ведення бізнесу. Традиційна банківська діяльність, що базується на фізичному обслуговуванні та централізованих процесах, поступається місцем цифровим каналам взаємодії, автоматизованим платформам, сервісам на базі штучного інтелекту, мобільним застосункам та хмарним рішенням. Відповідно, змінюються й підходи до управління ризиками, безпекою, персоналом та клієнтським досвідом. Внаслідок цифрової трансформації, як один із ключових напрямів, є зростання ролі інформаційної безпеки. Поняття кібербезпеки в цьому контексті розглядається як сукупність організаційних, технічних і правових заходів, спрямованих на захист інформаційних активів банку від несанкціонованого доступу, втрати, пошкодження або маніпуляцій. Сучасне розуміння кібербезпеки охоплює не лише захист ІТ-систем, але й забезпечення безперервного функціонування бізнесу, збереження конфіденційності даних, цифрову ідентифікацію клієнтів, а також дотримання регуляторних вимог. З теоретичної точки зору цифрова трансформація та кібербезпека мають взаємопов'язаний характер. З одного боку, цифровізація виступає каталізатором оновлення інструментів захисту (використання біометрії, блокчейну, штучного інтелекту для захисту даних), з іншого – вона створює нові загрози через підвищену складність цифрових систем, зростання обсягів даних і кількості точок доступу. Таким чином, кіберзахист повинен інтегруватися у всі етапи цифрової трансформації, від стратегічного планування до розробки нових цифрових продуктів. Окремої уваги заслуговує концепція кіберстійкості, яка поєднує здатність банків протистояти кіберзагрозам, адаптуватися до інцидентів, оперативно їх виявляти, мінімізувати наслідки та швидко відновлювати свою діяльність [2]. Цей підхід є основою новітніх стратегій цифрової безпеки, які застосовують провідні фінансові установи світу. Він акцентує увагу не лише на технічному захисті, а й на організаційній культурі безпеки, безперервному вдосконаленні систем захисту та постійному моніторингу ризиків.

Усі зазначені аспекти формують теоретичне підґрунтя для подальшого дослідження взаємозв'язку між цифровізацією банківської діяльності та забезпеченням кібербезпеки, що стає ключовим чинником надійності, довіри та стабільності в умовах цифрової економіки.

Аналіз сучасних кіберзагроз та тенденцій. У процесі цифрової трансформації банківські установи дедалі більше інтегруються у глобальну цифрову інфраструктуру, що, з одного боку, відкриває широкі можливості для розвитку, а з іншого значно підвищує їхню вразливість до кіберзагроз. У 2024 році урядова команда CERT-UA опрацювала 4315 кіберінцидентів, що на 69,8% більше, ніж роком раніше, що свідчить про стрімке зростання інтенсивності атак на критичну інформаційну інфраструктуру. Основними цілями кіберзлочинців залишаються органи влади, енергетичний сектор, телекомунікації та об'єкти оборонно-промислового комплексу, а найбільш поширеними типами атак є фішинг, розповсюдження шкідливого ПЗ та компрометація облікових записів [3]. З розвитком цифрових каналів обслуговування та зростанням обсягів обробки персональних і фінансових даних банки стають одними з найпривабливіших об'єктів для кібершахраїв. При цьому характер атак постійно ускладнюється, а методи зловмисників стають дедалі витонченішими.

Серед найбільш поширених загроз для банків у цифровому середовищі можна виокремити :

Згідно з аналітичними даними Національного банку України, у 2023 році банки України зафіксували зростання кількості кіберінцидентів, пов'язаних із шахрайством із платіжними картками, спробами несанкціонованого доступу до систем та зломом акаунтів онлайн-банкінгу. Попри незначне зниження кількості карткових шахрайств у 2025 році, загальні втрати від таких операцій залишаються значними, що свідчить про зростання масштабності окремих атак і про необхідність посилення превентивного захисту [6].

На глобальному рівні аналогічні тенденції фіксують і міжнародні аналітичні платформи. Зокрема, IBM зазначає, що фінансові установи залишаються одними з найчастіше атакованих секторів у світі, а головним мотивом атак є фінансова вигода. Більшість атак є складно виявлюваними, комбінованими за своїм типом і мають довготривалий вплив на операційну діяльність установ [7].

Таблиця 1 - Таблиця складена на основі джерела 4, 5 та 7

Тип загрози	Опис	Рекомендовані рішення
Фішинг та соціальна інженерія	Спроби обманом змусити користувачів розкрити облікові дані або доступи до систем.	Навчання персоналу, впровадження багатофакторної автентифікації, email-фільтри.
Програми-вимагачі (Ransomware)	Блокування даних і вимагання викупу. Поширюється через фішинг або незахищене ПЗ.	Регулярне резервне копіювання, ізоляція критичних систем, антивірусне ПЗ нового покоління.
DDoS-атаки	Масове перевантаження інфраструктури через фальшивий трафік.	Використання хмарних CDN, мережевих фаєрволів, контрактів з DDoS-провайдерами.
Уразливості в API та інтеграціях	Атаки через відкриті API або слабко захищене стороннє ПЗ.	API-гейти, аудит безпеки API, контроль доступів, обмеження за IP.
Інсайдерські загрози	Витоки даних через помилки або навмисні дії персоналу.	Обмеження прав доступу, журналювання дій користувачів, політики нульової довіри (Zero Trust).
Помилки конфігурації хмарних систем	Уразливості через неправильні налаштування хмарної інфраструктури.	Автоматизований моніторинг конфігурацій, шифрування даних, контроль доступів.

Крім технічного аспекту, не менш важливою є динаміка людського фактору у структурі кіберзагроз. Значна частина атак реалізується через недотримання базових правил цифрової гігієни, використання слабких паролів, невчасне оновлення ПЗ або несанкціоноване використання службових пристроїв. Саме тому комплексна політика кібербезпеки має включати не лише технологічний арсенал, а й системну просвітницьку роботу серед персоналу, чіткі регламенти користування IT-інфраструктурою та регулярні навчання.

Сучасні тенденції також свідчать про зміщення акценту з простих атак на інфраструктурні й координовані кампанії, що можуть мати ознаки кібершпигунства або бути частиною гібридних загроз. У зв'язку з цим важливо розглядати кібербезпеку не лише як елемент IT-політики, а як частину загальної стратегії безперервності банківського бізнесу та управління репутаційними ризиками.

Таким чином, у цифрову епоху банки функціонують у середовищі підвищеного рівня кіберризику. Їхня здатність розпізнавати нові типи загроз, адаптувати захисні системи та формувати цифрову культуру безпеки стає ключовим фактором забезпечення стабільності та довіри з боку споживачів фінансових послуг.

Технології та підходи до кіберзахисту. Підвищення кіберстійкості банківської системи в умовах цифровізації потребує застосування не лише базових засобів інформаційного захисту, а й впровадження сучасних технологій, що відповідають динаміці загроз і масштабу цифрової трансформації. Ефективна система кіберзахисту повинна бути комплексною, тобто охоплювати як технічні, так і організаційні, регламентні та освітні компоненти.

Одним із ключових технологічних інструментів сучасного кіберзахисту є системи виявлення та реагування на інциденти, такі як SIEM (Security Information and Event Management) і UEBA (User and Entity Behavior Analytics). SIEM-платформи забезпечують збір, кореляцію та аналіз подій безпеки з різних джерел у реальному часі, а UEBA використовує алгоритми машинного навчання для виявлення нетипової поведінки користувачів, яка може свідчити про внутрішні чи зовнішні атаки. Ці інструменти дають змогу не лише фіксувати інциденти, а й попереджати потенційні вторгнення на ранніх стадіях [8].

Широкого поширення набуває також концепція архітектури нульової довіри (Zero Trust Architecture), що базується на принципі постійної перевірки кожного доступу незалежно від його походження. Такий підхід унеможливлює використання єдиного привілейованого доступу, мінімізуючи ризики компрометації облікових записів. У практиці банків він реалізується через мікросегментацію мереж, застосування багатофакторної автентифікації, обмеження прав доступу, постійний моніторинг і аналіз запитів [9].

Важливе значення має захист персональних і транзакційних даних, що забезпечується завдяки токенізації, шифруванню, цифровим підписам та ізольованим середовищам виконання. Окремі банки впроваджують блокчейн-рішення у внутрішніх процесах для забезпечення незмінності даних, прозорості аудиту та підвищення довіри до транзакцій.

Суттєвою складовою сучасної безпеки є використання штучного інтелекту для автоматичного виявлення загроз, фільтрації підозрілих дій, аналізу трафіку та поведінки користувачів. Такі системи здатні самостійно приймати рішення щодо блокування дій, що мають ознаки атаки, не вимагаючи втручання оператора в режимі реального часу.

Не менш важливою є організаційна складова кібербезпеки, яка охоплює впровадження політик інформаційної безпеки, проведення регулярних аудитів, тестування на проникнення, реагування на інциденти та навчання персоналу. Визнаним міжнародним стандартом у цій сфері є ISO/IEC 27001:2022, який встановлює вимоги до створення, впровадження, функціонування та вдосконалення систем управління інформаційною безпекою [10].

Інтеграція цього стандарту в діяльність банків дозволяє систематизувати процеси управління ризиками, контролювати доступ до активів, регламентувати дії у випадку інцидентів та забезпечити відповідність правовим вимогам. Національний банк України, у свою чергу, підтримує впровадження принципів ISO/IEC 27001 через відповідні положення та рекомендації для банків щодо організації кіберзахисту.

Крім технологічних і регуляторних рішень, ефективність кіберзахисту значною мірою залежить від цифрових компетенцій працівників банку, рівня кіберосвіти та внутрішньої культури безпеки. Банки активно впроваджують навчальні програми,

створюють внутрішні служби реагування на інциденти, проводять симуляції атак для оцінки готовності до реагування.

Отже, побудова надійної системи кібербезпеки в умовах цифровізації потребує мультидисциплінарного підходу, що поєднує інноваційні технології, нормативне регулювання, управлінську відповідальність та постійний розвиток співробітників. Такий підхід дає змогу не лише мінімізувати ризики, а й підвищити рівень довіри до банків та їх послуг.

Практика провідних країн та українські ініціативи. Підвищення кібербезпеки в умовах цифрової трансформації банківського сектору потребує не лише технічної модернізації, а й стратегічного бачення, яке реалізується через національні та міжнародні ініціативи. Досвід країн із розвиненою фінансовою інфраструктурою демонструє, що ефективна протидія кіберзагрозам можлива лише за умови гармонізації нормативно-правового регулювання, міжгалузевої взаємодії та широкого впровадження стандартів інформаційної безпеки.

У країнах Європейського Союзу питання кібербезпеки фінансових установ регулюються низкою директив та актів. Зокрема, Директива NIS2 (2022) встановлює вимоги до цифрової стійкості критично важливої інфраструктури, включно з банками, та зобов'язує фінансові організації впроваджувати процедури управління ризиками, реагування на інциденти й звітування перед національними центрами кіберзахисту [11]. Європейський центральний банк також ініціював TIBER-EU – програму тестування на проникнення (Threat Intelligence-based Ethical Red Teaming), яка дозволяє банкам перевіряти стійкість до цільових атак у режимі наближеному до реального [12].

У США стратегія кіберзахисту банківської системи передбачає тісну співпрацю між державними регуляторами (Federal Reserve, OCC, FDIC), службами національної безпеки (CISA, FBI) та приватними установами. У 2021 році було ухвалено Executive Order 14028, що передбачає обов'язкове впровадження принципів Zero Trust Architecture у критичній інфраструктурі, у тому числі у фінансовому секторі. Також широко застосовуються моделі управління безпекою на основі фреймворків NIST (зокрема, Cybersecurity Framework v1.1 і нова версія 2.0), які охоплюють як технічні, так і організаційні аспекти [13].

Досвід Японії є прикладом збалансованого підходу до кібербезпеки у фінансовому секторі, який поєднує технологічну прогресивність із регуляторною виваженістю. Японське Агентство фінансових послуг (JFSA) розробило багаторівневу політику управління кіберризиками, що охоплює як інституційні вимоги до банків, так і рекомендації для небанківських установ. Серед ключових елементів цієї політики – оцінювання вразливостей через внутрішні та зовнішні тести, аудит кіберзахисту, посилення моніторингу ризиків, пов'язаних із залученням сторонніх IT-постачальників. Особлива увага приділяється побудові довіри до цифрової інфраструктури, підвищенню обізнаності працівників щодо кіберзагроз і формуванню культури безпеки на всіх рівнях організації. Важливу роль у реалізації цієї стратегії відіграють також Центр інформаційних систем фінансової індустрії (FISC) та міжвідомча координація з IT-компаніями і банківськими асоціаціями [14]. Такий комплексний підхід дозволяє Японії підтримувати високий рівень кіберстійкості фінансового сектору навіть в умовах зростання глобальних загроз.

Досвід Південної Кореї є показовим у контексті швидкої цифрової трансформації банків при одночасному посиленні кіберзахисту. У країні функціонує Korea Financial Security Institute – центральний орган, що координує стандарти інформаційної безпеки, здійснює аудит банківських систем, проводить навчання персоналу й інформує громадськість про загрози. Південна Корея також є однією з перших країн, яка впровадила обов'язкову біометричну автентифікацію в електронних фінансових операціях на рівні законодавства [15].

У національному контексті Україна активно адаптує міжнародний досвід до власних умов. Важливу роль у цьому процесі відіграє Національний банк України, який протягом останніх років системно реалізує заходи, спрямовані на зміцнення кіберстійкості банківського сектору, з особливим акцентом на забезпеченні його надійного функціонування під час воєнного стану. Центр кіберзахисту НБУ та команда CSIRT-NBU функціонували в режимі постійного моніторингу та реагування, обробивши понад 3 тисячі кіберінцидентів та ініціювавши блокування десятків тисяч фішингових ресурсів. Важливою складовою стала міжвідомча координація з державними органами (СБУ, ДССЗЗІ, кіберполіція) та міжнародними партнерами, зокрема підписання меморандуму з Міністерством фінансів США щодо співпраці у сфері кіберзахисту [1]. Такий комплексний підхід дозволив не лише мінімізувати наслідки кібератак, а й сформувати основу для стійкого функціонування фінансової системи України в умовах високої динаміки загроз.

Незважаючи на прогрес, вітчизняна банківська система все ще стикається з низкою викликів: обмеженість фінансування на кібербезпеку в невеликих банках, брак спеціалістів, фрагментарність реалізації нормативних вимог. Тому одним з пріоритетів має стати створення єдиної цифрової екосистеми кіберзахисту, що охоплює регуляторів, банки, технологічних провайдерів та освітні установи.

Отже, успішний міжнародний досвід свідчить, що кібербезпека банків не є лише технологічною функцією, а має розглядатися як складова стратегії управління ризиками та довірою клієнтів. Україна, адаптуючи ці підходи, має всі підстави для створення сучасної кіберстійкої банківської системи, здатної ефективно функціонувати в умовах глобальних цифрових викликів.

Висновки та перспективи дослідження. У результаті проведеного дослідження встановлено, що цифровізація банківської системи є не лише ключовим чинником її модернізації, а й критичним викликом у сфері кібербезпеки. Активне впровадження цифрових технологій таких як мобільний банкінг, хмарні обчислення, відкриті API, штучний інтелект,

призводить до зростання складності ІТ-інфраструктури банків та підвищує їхню вразливість до кіберзагроз.

Проаналізовано основні тенденції розвитку кіберзагроз у фінансовому секторі, від традиційних атак типу фішинг і DDoS до високотехнологічних цільових атак на інформаційні системи банків. Встановлено, що ефективне протистояння цим загрозам можливе лише за умови комплексного підходу, який охоплює як технологічні рішення, так і організаційні компоненти.

У дослідженні узагальнено міжнародний досвід країн ЄС, США, Японії та Південної Кореї, які продемонстрували ефективні моделі побудови кіберстійкої банківської системи на основі міжгалузевої координації, впровадження новітніх стандартів і розвитку центрів реагування на інциденти. У національному контексті позитивною є динаміка активності Національного банку України щодо формування нормативної бази кіберзахисту.

Список літератури

1. Національний банк України. Річний звіт за 2024 рік. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2024.pdf?v=13 (дата звернення: 10.07.2025)
2. Користін, О. Є., & Демедюк, С. В. (2023). Актуалізація кіберстійкості та історичні витоки концепції" стійкість". Аналітично-порівняльне правознавство, (6), 708-713.
3. Державна служба спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 10.07.2025)
4. Гончаренко, І. (2023). Кіберзагрози фінансового сектора в умовах війни. *Економіка та суспільство*, (50). DOI:https://doi.org/10.32782/2524-0072/2023-50-82
5. Edward Kost (2023) The 6 Biggest Cyber Threats for Financial Services in 2023. URL: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services (дата звернення: 10.07.2025)
6. Національний банк України. Платіжне шахрайство у 2024 році. URL: https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli (дата звернення: 10.07.2025)
7. IBM Security (2024). X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index (дата звернення 10.07.2025)
8. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.
9. Stafford, V. (2020). Zero trust architecture. *NIST special publication*, *800*(207), 800-207.
10. International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL : https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en (дата звернення : 10.07.2025).
11. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890.
12. Європейський центральний банк. *TIBER-EU Framework – Cyber resilience testing for the financial sector*. URL: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (дата звернення: 10.07.2025)
13. Executive Order 14028 of May 12, 2021–Improving the Nation's Cybersecurity. Federal Register. URL: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity (дата звернення: 10.07.2025)
14. Japan Financial Services Agency (JFSA)**.** *Cybersecurity Policies and Approaches – Japan Financial Services Agency (JFSA).* Sustainable Insurance Forum. URL: https://sustainableinsuranceforum.org/wp-content/uploads/2021/03/Japan-Japan-Financial-Services-Agency-JFSA.pdf (дата звернення: 10.07.2025)
15. Financial Security Institute. URL: https://www.fsec.or.kr/en (дата звернення: 10.07.2025)

References (transliterated)

1. Natsionalnyi bank Ukrainy. Richnyi zvit za 2024 rik. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2024.pdf?v=13 (data zvernennia: 10.07.2025)
2. Korystin, O. Ye., & Demediuk, S. V. (2023). Aktualizatsiia kiberstiikosti ta istorychni vytoky kontseptsii" stiikist". Analitychno-porivnialne pravoznavstvo, (6), 708-713.
3. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (data zvernennia: 10.07.2025)
4. Honcharenko, I. (2023). Kiberzahrozy finansovoho sektora v umovakh viiny. Ekonomika ta suspilstvo, (50). DOI:https://doi.org/10.32782/2524-0072/2023-50-82
5. Edward Kost (2023) The 6 Biggest Cyber Threats for Financial Services in 2023. URL: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services (data zvernennia: 10.07.2025)
6. Natsionalnyi bank Ukrainy. Platizhne shakhraistvo u 2024 rotsi. URL: https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli (data zvernennia: 10.07.2025)
7. IBM Security (2024). X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index (data zvernennia 10.07.2025)
8. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.
9. Stafford, V. (2020). Zero trust architecture. NIST special publication, 800(207), 800-207.
10. International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL : https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en (data zvernennia : 10.07.2025).
11. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 52, 105890.
12. Yevropeiskyi tsentralnyi bank. TIBER-EU Framework – Cyber resilience testing for the financial sector. URL: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (data zvernennia: 10.07.2025)
13. Executive Order 14028 of May 12, 2021–Improving the Nations Cybersecurity. Federal Register. URL: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity (data zvernennia: 10.07.2025)
14. Japan Financial Services Agency (JFSA). Cybersecurity Policies and Approaches – Japan Financial Services Agency (JFSA). Sustainable Insurance Forum. URL: https://sustainableinsuranceforum.org/wp-content/uploads/2021/03/Japan-Japan-Financial-Services-Agency-JFSA.pdf (data zvernennia: 10.07.2025)
15. Financial Security Institute. URL: https://www.fsec.or.kr/en (data zvernennia: 10.07.2025)

Received 25.04.2025

Відомості про авторів / About the Authors

Чапайло Вадим Валерійович (Chapailo Vadym) – здобувач третього (освітньо-наукового) рівня вищої освіти, Національний технічний університет «Харківський політехнічний інститут» м. Харків; ORCID: https://orcid.org/0009-0001-9995-7384;e-mail: vadym.chapailo@emmb.khpi.edu.ua