DOI: https://doi.org/10.32782/2524-0072/2025-77-69

УДК 336.1:004.056

КІБЕРБЕЗПЕКА У СФЕРІ ПУБЛІЧНИХ ФІНАНСІВ

CYBERSECURITY IN PUBLIC FINANCE

Качула Світлана Валентинівна
доктор економічних наук, професор,
Дніпровський державний аграрно-економічний університет
ORCID: https://orcid.org/0000-0003-2540-862X

Kachula Svitlana
Dnipro State Agrarian and Economic University

У статті розглянуто актуальні питання кібербезпеки у сфері публічних фінансів в умовах цифрової трансформації державного управління. Показано, що зростання кібератак на фінансові органи та інформаційні системи вимагає переходу від реактивної до проактивної моделі захисту. Проаналізовано технологічні, організаційні та інституційні інструменти забезпечення кіберзахисту, серед яких системи виявлення та запобігання вторгненням, використання криптографії, блокчейн-технологій, аудити безпеки, розвиток державно-приватного партнерства і транскордонної співпраці. Наголошено на необхідності вдосконалення нормативно-правової бази у згоді з міжнародними стандартами, імплементації директив ЄС, активного співробітництва з міжнародними мережами CERT. Зроблено висновок, що комплексний підхід, який поєднує технічні рішення, організаційні заходи і міжнародну узгодженість, є ключем до створення стійкої системи кіберзахисту публічних фінансів України.

Ключові слова: кібербезпека, інформаційна безпека, захист даних, публічні фінанси, фінансова інформація, цифрові технології, кіберзагрози, управління ризиками, державний сектор, інформаційна інфраструктура.

The article examines the issue of cybersecurity in the field of public finance in the context of the rapid digital transformation of public administration and the global growth of cyber threats. It is emphasized that financial stability of the state, transparency of budget processes and citizens' trust in governmental institutions increasingly depend on the reliability of digital infrastructure and the ability to counteract complex cyberattacks. The study identifies key risks for public finance systems, including targeted attacks on treasury platforms, attempts of unauthorized access to databases, phishing campaigns against employees of financial authorities, as well as large-scale ransomware incidents affecting continuity of financial operations. The research highlights the urgent necessity to move from a reactive approach, limited to responding to incidents, to a proactive cybersecurity model, based on prediction, prevention, early detection, and continuous monitoring of threats. Special attention is devoted to technological and organizational tools of protection such as intrusion detection and prevention systems, cryptographic methods of data protection, blockchain solutions ensuring transparency and immutability of financial transactions, as well as artificial intelligence applications in anomaly detection and fraud prevention. In addition, the importance of organizational mechanisms such as regular security audits, staff training programs, and development of national cyber response centers is underlined. The article stresses that successful protection of public finance requires not only technical measures, but also institutional cooperation between state bodies, private sector, and international partners. Harmonization of Ukrainian legislation with EU directives, in particular NIS2, and active participation in international information exchange networks such as CERT are defined as strategic priorities. The conclusion is drawn that only a comprehensive approach, integrating technological innovations, organizational frameworks, and international coordination, will allow Ukraine to create a sustainable cybersecurity system for public finance, capable of resisting current and future digital challenges.

Keywords: cybersecurity, information security, data protection, public finance, financial information, digital technologies, cyber threats, risk management, public sector, information infrastructure.

Постановка проблеми. Сучасний етап розвитку фінансової системи характеризується масштабною цифровізацією процесів управління публічними фінансами, що включає електронне адміністрування податків, функціонування державних інформаційних ресурсів, використання автоматизованих систем контролю та моніторингу бюджетних потоків. Разом із підвищенням ефективності управління та прозорості зростає й рівень

уразливості цих систем до кіберзагроз. Атаки на державні фінансові інформаційні ресурси, витоки конфіденційних даних, порушення цілісності та доступності інформації створюють суттєві ризики для фінансової стабільності, підзвітності та довіри громадян до органів влади. Особливої актуальності набуває проблема захисту інформаційних ресурсів у сфері публічних фінансів в умовах посилення гібридних загроз та воєнних дій, коли державні інформаційні системи стають об'єктом цілеспрямованих кібератак. Недостатній рівень інтегрованої політики кібербезпеки, обмеженість фінансових і кадрових ресурсів, фрагментарність нормативно-правового забезпечення ускладнюють формування ефективного механізму протидії кіберризикам у державному секторі. Таким чином, виникає необхідність комплексного наукового дослідження проблеми кібербезпеки та інформаційного захисту у сфері публічних фінансів, з урахуванням міжнародних практик, сучасних технологічних рішень і національної особливості фінансової системи.

Аналіз останніх досліджень і публікацій. Вивченням тенденцій розвитку кіберзагроз у фінансовому секторі, виявлення детермінант їх поширення та дослідження практик протидії займались вчені І. Гончаренко [1], І. Дорош [3], Н. Петруха, С. Петруха, А. Жмаєв та М. Синкевич [6] т ін. Зростанням втрат від кіберзлочинності та визначення дієвих механізмів забезпечення кібербезпеки для суб'єктів глобальної економіки досліджували О. Дзяд та Д. Стародуб [2] та ін. Взагалі, науковий дискурс з кібербезпеки у публічних фінансах сформувався на перетині трьох напрямів: управління інформаційною безпекою в державному секторі; регулювання та комплаєнс у сфері захисту даних; технологічні підходи до протидії кіберінцидентам у фінансових системах. У сфері управління інформаційною безпекою в державному секторі останні роки дослідження зосереджуються на ризик-орієнтованих моделях управління, побудові систем управління інформаційною безпекою (ISMS) та узгодженні процесів безпеки з цілями публічного фінансового менеджменту. Теоретичною і практичною «точкою збору» є фреймворки загального призначення, адаптовані для держсектору. В сфері регулювання та комплаєнсу у сфері захисту даних дослідження концентруються на двох «опорних» режимах: захист персональних даних, законність обробки, права суб'єктів, DPIA/оцінки впливу, повідомлення про порушення та горизонтальних вимогах до кіберстійкості організацій, інцидент-репортинг, управління ризиками ланцюга постачання, вимоги до керівництва. Для публічних фінансів це означає обов'язковість прозорих підстав обробки та мінімізації даних у податкових, казначейських і соціальних виплатах, поєднаних з підвищеними вимогами до готовності/звітності про інциденти й управлінням постачальниками IT-послуг. В сфері технологічних підходів до протидії кіберінцидентам у фінансових системах практична лінія досліджень фокусується на конвергенції SIEM (керування захистом інформації) та Threat Intelligence (розвідка про загрози) для побудови циклу detect–respond–recover (виявити–відреагувати–відновити) у середовищах з високою транзакційною інтенсивністю.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значні напрацювання наукової спільноти у вивченні кібербезпеки, недостатньо дослідженими залишаються проблеми забезпечення кіберзахисту саме у сфері публічних фінансів, інтеграції механізмів кібербезпеки в систему управління бюджетними процесами, а також оцінка економічних наслідків кібератак для державних фінансових ресурсів, що визначає потребу у подальших наукових дослідженнях, спрямованих на пошук ефективних інструментів і механізмів підвищення рівня інформаційної безпеки у державному секторі.

Формулювання цілей статті (постановка завдання). Метою статті є аналіз сучасних аспектів кібербезпеки у сфері публічних фінансів, виявлення основних проблем та ризиків, а також визначення перспектив розвитку системи кіберзахисту в умовах цифрової трансформації та інтеграції України у світовий кіберпростір.

Виклад основного матеріалу дослідження. Сучасний розвиток інформаційних технологій та цифровізація державних фінансових систем створили нові передумови для забезпечення ефективного управління публічними фінансами, водночас породжуючи численні ризики, пов'язані з кіберзагрозами та інформаційною безпекою. Кібербезпека у контексті публічних фінансів виступає комплексною науково-практичною категорією, що включає організаційні, технологічні та нормативно-правові заходи, спрямовані на забезпечення цілісності, конфіденційності та доступності фінансових даних. Важливість даної проблематики обумовлена тим, що інформаційні системи державного сектору

обробляють великий обсяг чутливої інформації, включаючи персональні дані платників податків, бюджетні асигнування, облікові записи державних установ та фінансові транзакції. Порушення цілісності або конфіденційності таких даних може призвести не лише до економічних втрат, а й до значного зниження довіри суспільства до державних інституцій, що, у свою чергу, підриває стабільність фінансової системи.

Науковці визначають кібербезпеку як сукупність заходів, процедур та технологій, що спрямовані на протидію кіберзагрозам, забезпечення безперебійного функціонування інформаційних систем та захист інформаційних ресурсів від несанкціонованого доступу, модифікації або знищення [2; 3; 13]. У контексті публічних фінансів такі заходи набувають особливої значущості, оскільки вони стосуються не лише технічного захисту систем, а й регулятивних, економічних та управлінських аспектів. Ключовим завданням кібербезпеки у державних фінансових структурах є формування ефективної системи управління ризиками, яка забезпечує ідентифікацію потенційних загроз, їх оцінку, впровадження превентивних заходів та контроль результативності протидії. Загрози інформаційним системам публічних фінансів різноманітні і охоплюють як зовнішні, так і внутрішні фактори. До зовнішніх належать цілеспрямовані кібератаки, зловмисне втручання третіх сторін, атаки через мережеві та інтернет-канали, використання шкідливого програмного забезпечення та соціальна інженерія. Внутрішні загрози пов'язані з недотриманням стандартів доступу, випадковими помилками персоналу, зловживаннями службовим становищем, а також обмеженою кваліфікацією співробітників щодо процедур інформаційної безпеки. Комплексний підхід до управління кіберризиками вимагає інтеграції всіх цих аспектів у єдину стратегію, що охоплює організаційні процеси, технологічні рішення і нормативно-правове забезпечення.

Важливим аспектом є класифікація основних ризиків та загроз у публічних фінансах, яка дозволяє систематизувати методи їхнього запобігання та контролю. Згідно з науковими підходами [3], такі ризики можна поділити на технічні, операційні, адміністративні та стратегічні. Технічні ризики охоплюють загрози функціонуванню апаратного та програмного забезпечення, збої мережевого обладнання, втрату даних через кібератаки або збої систем. Операційні ризики пов'язані з процесами обробки та управління фінансовою інформацією, включаючи помилки у введенні даних, недосконалі процедури контролю та моніторингу, недостатню автоматизацію процесів. Адміністративні ризики виникають через недоліки у організації управління, слабку регламентацію доступу, відсутність навчання персоналу та неузгодженість функцій між структурними підрозділами. Стратегічні ризики відображають можливий негативний вплив кіберінцидентів на репутацію державних органів, довіру громадян та стабільність фінансової системи в цілому.

Сучасні теоретичні підходи до кібербезпеки у публічних фінансах спираються на концепції управління інформаційною безпекою, інтегрованого управління ризиками та стандартів міжнародного рівня. Зокрема, стандарт ISO/IEC 27002:2024 визначає принципи побудови систем управління інформаційною безпекою, серед яких виділяють систематичну ідентифікацію активів, класифікацію інформації, управління доступом, шифрування, аудит та моніторинг [4]. NIST Cybersecurity Framework [11] пропонує модель, що включає п'ять основних функцій: ідентифікацію, захист, виявлення, реагування та відновлення, що дозволяє організаціям визначати критичні активи та планувати дії у разі виникнення кібератак.

У сфері публічних фінансів застосування стандартів забезпечує єдину методологічну основу для формування політик кібербезпеки, дозволяє інтегрувати технічні й організаційні заходи та оцінювати ефективність реалізованих заходів. З методологічної точки зору кіберзахист у сфері публічних фінансів можна розглядати в наступних напрямках:

– ризик-орієнтований підхід, коли основна увага приділяється виявленню та мінімізації можливих ризиків;

– системний підхід, що передбачає розгляд кібербезпеки як частини загальної фінансової безпеки держави;

– інноваційний підхід, де акцент робиться на використанні новітніх технологій (штучний інтелект, блокчейн, Big Data) для запобігання кібератакам.

Особливістю сфери публічних фінансів є те, що вона функціонує на стику державного управління, банківського сектора та міжнародних фінансових інституцій, що створює складне середовище, де будь-які збої або витік інформації можуть мати масштабні економічні та політичні наслідки. Основні відмінності кіберзахисту у приватному та публічному секторах наведено в табл. 1.

Таблиця 1

Основні відмінності кіберзахисту у приватному та публічному секторах

Ознака	Приватний сектор	Публічний сектор (державні фінанси)
Основна мета	Захист комерційної таємниці та активів компанії	Забезпечення стійкості фінансової системи держави, захист бюджету
Масштаб	Локальний або корпоративний	Національний, міжвідомчий
Ризики	Фінансові втрати, втрата клієнтів	Підрив економічної стабільності, загроза національній безпеці
Інструменти	Корпоративні IT-рішення, страхування кіберризиків	Державні стандарти, нормативні акти, міждержавна співпраця

Джерело: сформовано автором

Кібербезпека у сфері публічних фінансів має більш широкий масштаб і потребує координації між численними інституціями, включаючи органи влади, банки, міжнародних партнерів та приватні компанії. Кіберзагрози у сфері публічних фінансів мають багатовимірний характер і можуть проявлятися як у вигляді цілеспрямованих атак на державні інформаційні системи, так і у формі масових кібератак на платіжну інфраструктуру. Найбільш поширеними загрозами є:

1) Фішинг та соціальна інженерія – спрямовані на отримання конфіденційних даних користувачів, працівників державних фінансових установ.

2) DDoS-атаки – призводять до блокування роботи електронних систем, включаючи портали державних закупівель чи системи управління бюджетом.

3) Шкідливе програмне забезпечення (віруси, трояни, криптолокери), яке може знищити або заблокувати доступ до даних фінансових систем.

4) Маніпуляції у фінансових транзакціях – підробка або зміна даних під час їх передачі.

5) Атаки на критичну фінансову інфраструктуру, включаючи банківські системи, державні реєстри, податкові бази.

Дослідження Світового Банку свідчать, що саме фінансовий сектор є одним із найбільш вразливих до кібератак. У 2023 р понад 27% усіх великих кібератак у ЄС були спрямовані на фінансові інститути [14]. В Україні упродовж останніх років зафіксовано низку кібератак на державні установи. У 2022–2023 рр під час повномасштабної війни росії проти України кібератаки посилилися та часто мали на меті блокування державних онлайн-сервісів, у тому числі порталу «Дія» та ресурсів Міністерства фінансів та Державної казначейської служби (табл. 2).

Кібератаки стають дедалі більш складними та комбінованими. Зловмисники використовують одночасно кілька методів (наприклад, DDoS у поєднанні з фішингом), що підвищує їхню ефективність. Для держави це означає необхідність постійного вдосконалення механізмів моніторингу, виявлення та реагування на загрози. Ефективний захист публічних фінансів від кіберзагроз потребує комплексного поєднання технологічних, організаційних та інституційних інструментів.

На технологічному рівні йдеться насамперед про використання систем виявлення та запобігання вторгненням, які забезпечують моніторинг мережевого трафіку й блокування підозрілої активності, а також про застосування криптографічних методів захисту, зокрема електронного цифрового підпису, двофакторної автентифікації та шифрування

Таблиця 2

Кіберзлочини у сфері публічних фінансів України

Рік	Країна/організація	Тип атаки	Наслідки
2017	Україна (держустанови, банки)	Вірус Petya	Паралізація фінансових операцій, блокування доступу до даних
2022	Україна (вебсайти Міноборони, МЗС, ДСНС, Дії)	DDoS-атака	Тимчасове блокування доступу до державних послуг
2024	Україна (державні реєстри України та сайт Міністерства юстиції України)	DDoS-атака	Призупинено роботу Єдиних і Державних реєстрів Міністерства юстиції України

Джерело: сформовано автором за [13]

даних. Не менш важливим є впровадження систем резервного копіювання та відновлення інформації, що гарантують безперервність функціонування державних фінансових органів навіть у разі масштабних атак.

Серед інноваційних рішень варто виділити технології блокчейн, які забезпечують прозорість і неможливість підробки транзакцій, а також використання алгоритмів штучного інтелекту та машинного навчання для виявлення аномальної поведінки у фінансових операціях.

Разом із технологічними рішеннями необхідно застосовувати організаційні інструменти, які передбачають розробку та впровадження стандартів інформаційної безпеки у державному секторі, регулярні аудити безпеки інформаційних систем, підвищення кваліфікації персоналу, а також створення механізмів швидкого реагування на інциденти. Прикладом такої практики є діяльність урядових команд реагування на комп'ютерні надзвичайні події (CERT-UA), які координують дії у разі виявлення загроз.

На інституційному рівні особливого значення набуває координація між державними та приватними структурами, що дозволяє поєднати зусилля та ресурси для створення більш стійкої системи кіберзахисту.

Необхідно й надалі розвивати міжнародне співробітництво, яке б передбачало обмін інформацією про інциденти, впровадження глобальних стандартів та участь у програмах ЄС і НАТО. Крім того, дедалі актуальнішим стає формування ефективних механізмів державно-приватного партнерства у сфері кіберзахисту фінансів.

Узагальнення основних підходів наведено у таблиці 3, яка демонструє взаємозв'язок між різними типами інструментів та їх впливом на безпеку публічних фінансів. Технологічні інструменти, зокрема блокчейн чи системи IDS/IPS, забезпечують захист від технічних атак і збереження цілісності даних. Організаційні механізми (стандарти ISO/IEC 27001, аудити та тренінги для персоналу) сприяють підвищенню готовності до інцидентів і зменшують ризик, пов'язаний із людським фактором. Інституційні інструменти – співпраця з міжнародними партнерами та діяльність CERT-UA, що спрямовані на координацію дій як на національному, так і на міжнародному рівнях.

Лише інтеграція технологічних, організаційних та інституційних заходів дозволяє сформувати цілісну та ефективну систему кіберзахисту публічних фінансів, яка здатна протистояти сучасним викликам та загрозам. Перспективи розвитку кібербезпеки у сфері публічних фінансів безпосередньо пов'язані з динамікою глобальних цифрових трансформацій і зростанням кількості кібератак на державні установи. В умовах активного впровадження електронного урядування та цифрових послуг, фінансова система України потребує переходу до проактивної моделі захисту, мета якої реагувати не лише на інциденти, а й передбачати можливі ризики та усувати їх, що зумовлює необхідність поступового переходу до інтеграції інтелектуальних систем моніторингу, здатних автоматично аналізувати великі масиви даних і виявляти аномальні транзакції чи дії користувачів.

Досить важливим є впровадження технології блокчейн, яка дозволяє забезпечити прозорість державних фінансових операцій та мінімізувати ризики маніпуляцій із даними. Дана технологія здатна істотно підвищити рівень довіри суспільства до публічних фінансів, адже забезпечує незмінність записів і унеможливлює несанкціоноване втручання. Паралельно з цим, доцільним є розширення використання штучного інтелекту, який може забезпечити оперативне реагування на потенційні атаки.

Таблиця 3

Інструменти кіберзахисту у сфері публічних фінансів

Тип інструменту	Приклади	Очікуваний ефект
Технологічні	IDS/IPS, блокчейн, резервні копії, AI-системи	Захист від технічних атак, збереження цілісності даних
Організаційні	Аудити, стандарти ISO/IEC 27001, тренінги персоналу	Підвищення готовності до інцидентів, зменшення людського фактору
Інституційні	CERT-UA, співпраця з ЄС та НАТО, державно-приватні партнерства	Координація національного та міжнародного рівня

Джерело: сформовано автором

На нашу думку, є особлива потреба в формуванні єдиної інтегрованої системи кіберзахисту публічних фінансів, яка б об'єднала державні органи та фінансові інституції у спільний простір моніторингу та реагування. Така система має функціонувати у форматі постійного обміну інформацією між усіма зацікавленими структурами, що дозволить скоротити час від виявлення інциденту до його нейтралізації. У цьому контексті надзвичайно важливо розвивати механізми державно-приватного партнерства, які передбачають залучення комерційних банків, страхових компаній та ІТ-компаній до створення спільних рішень.

Не менш актуальним є вдосконалення нормативно-правового поля з урахуванням міжнародних стандартів. Перспективним є гармонізація українського законодавства із положеннями Директиви ЄС NIS2, що забезпечить уніфікацію підходів до кіберзахисту в усій Європі та полегшить інтеграцію України до єдиного цифрового простору що, у свою чергу, дозволить розширити співпрацю з міжнародними партнерами, такими як Європейське агентство з кібербезпеки (ENISA), НАТО чи Світовий банк.

Важливою умовою розвитку кібербезпеки є підготовка висококваліфікованих фахівців. Система освіти та професійного навчання має передбачати створення спеціалізованих програм у сфері захисту інформації, а також розвиток центрів сертифікації кадрів, що працюватимуть із державними фінансовими системами. Формування кадрового резерву забезпечить стійкість фінансової безпеки держави навіть в умовах зростання кількості кіберзагроз.

Таким чином, перспективи розвитку кібербезпеки у сфері публічних фінансів України полягають у поєднанні інноваційних технологій, інтеграції міжнародного досвіду, вдосконаленні правового регулювання та підготовці професійних кадрів. Лише комплексний підхід, що включає проактивні стратегії, сучасні технічні рішення та інституційне забезпечення, здатний гарантувати стійкість та прозорість функціонування державних фінансових систем у цифрову епоху.

Висновки. Отже, кібербезпека у сфері публічних фінансів постає як стратегічний пріоритет держави, адже від її рівня залежить стабільність фінансової системи та довіра суспільства до органів влади. Дослідження засвідчило, що ефективний захист можливий лише за умови поєднання технологічних рішень, організаційних заходів та інституційної взаємодії. Використання сучасних інструментів моніторингу, блокчейн-технологій і штучного інтелекту має супроводжуватися удосконаленням нормативно-правової бази, розвитком міжнародної співпраці та підготовкою фахівців. Лише комплексний підхід дозволить створити стійку систему кіберзахисту публічних фінансів, здатну протистояти сучасним викликам і забезпечувати прозорість та безперервність фінансових процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гончаренко І. Г. Кіберзагрози фінансового сектора в умовах війни. *Економіка і суспільство*. 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-82 (дата звернення: 15.08.2025)

2. Дзяд О. В., Стародуб Д. С. Економічні втрати та механізми протидії кіберзлочинності у світовому господарстві. *Ефективна економіка*. 2022. № 1. DOI: https://doi.org/10.32702/2307-2105-2022.1.91 (дата звернення: 15.08.2025)

3. Дорош І. М. Кібербезпека та її роль у фінансовому секторі: загрози та заходи захисту. *Економіка фінанси право*. 2023. № 10. С. 48–51. DOI: https://doi.org/10.37634/efp.2023.10.10

4. ДСТУ EN ISO/IEC 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=106958 (дата звернення: 15.08.2025)

5. МЕЖА-МЕДІА: Топ кіберзагроз для фінансового сектору у 2025 році. Як захистити бізнес? URL: https://mezha.media/articles/top-kiberzahroz-2025-yak-zakhystyty-biznes/ (дата звернення: 16.08.2025)

6. Петруха Н. М., Петруха С. В., Жмаєв А. Ю., Синкевич М. Е. Кібербезпека економіки та державних фінансів: історіографія та повоєнна траєкторія розвитку. *Бізнес Інформ.* 2024. № 6. С. 64–79. DOI: https://doi.org/10.32983/2222-4459-2024-6-64-79

7. Про затвердження Змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту: Постанова НБУ від 25 лютого 2025 року № 24. URL: https://zakon.rada.gov.ua/laws/show/v0024500-25#Text (дата звернення: 16.08.2025)

8. Fintech insider: Кібербезпека як ключовий фінтех-тренд року: що варто знати про загрози та захист. URL: https://fintechinsider.com.ua/kiberbezpeka-yak-klyuchovyj-finteh-trend-roku-shho-varto-znaty-pro-zagrozy-ta-zahyst/ (дата звернення: 16.08.2025)

9. KYIVSTAR BUSINESS HUB Кібератаки на банківський сектор: як захистити фінансові установи? URL: https://hub.kyivstar.ua/articles/kiberataky-na-bankivskyj-sektor-yak-zahystyty-finansovi-ustanovy (дата звернення: 16.08.2025)

10. Lysiak L, Kachula S., Hrabchuk O., Filipova M., Kushnir A. Assessment of financial sustainability of the local budgets: case of Ukraine. *Public and Municipal Finance*. 2020. 9/1. PP. 48-59. DOI: http://dx.doi.org/10.21511/pmf.09(1).2020.05

11. NIST Cybersecurity Framework. URL: https://www.nist.gov/cyberframework (дата звернення: 16.08.2025)

12. Romenska K., Kachula S., Huba M., Dudchyk O., Lapa M. State financial flows for ensuring security in the international economic environment. *Financial and credit activity: problems of theory and practice*. 2024. Vol. 4 (57). C. 317–331. DOI: https://doi.org/10.55643/fcaptp.4.57.2024.4430

13. USAID: Огляд ринку кібербезпеки в Україні. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 16.08.2025)

14. World Bank. Financial Sector's Cybersecurity: A Regulatory Digest. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099062624064012530 (дата звернення: 16.08.2025)

REFERENCES:

1. Honcharenko I. H. (2023) Kiberzahrozy finansovoho sektora v umovakh viiny [Cyber threats of the financial sector in the conditions of war]. *Ekonomika i suspilstvo – Economy and Society*, vol. 50. Available at: https://economyandsociety.in.ua/index.php/journal/article/view/2442 (accessed August 15, 2025)

2. Dzyad O. V., Starodub D. C. (2022) Ekonomichni vtraty ta mekhanizmy protydii kiberzlochynnosti u svitovomu hospodarstvi [Economic losses and international methods against cybercrimes and ways to oppose cybercrimes worldwide]. *Efektyvna ekonomika – Efficient Economy*, vol. 1. Available at: http://www.economy.nayka.com.ua/?op=1&z=9903 (accessed August 15, 2025)

3. Dorosh I. M. (2023) Kiberbezpeka ta yii rol u finansovomu sektori: zahrozy ta zakhody zakhystu [Cyber security and its role in the financial sector: threats and protection measures]. *Ekonomika. Finansy. Pravo – Economics. Finances. Law*, vol. 10, pp. 48–51.

4. DSTU EN ISO/IEC 27002:2024 Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinosti. Zakhody zabezpechennia informatsiinoi bezpeky [Information security, cybersecurity and privacy protection. Information security measures]. Available at: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=106958 (accessed August 16, 2025)

5. MEZhA-MEDIA: Top kiberzahroz dlia finansovoho sektoru u 2025 rotsi. Yak zakhystyty biznes? [Top cyber threats for the financial sector in 2025. How to protect your business?]. Available at: https://mezha.media/articles/top-kiberzahroz-2025-yak-zakhystyty-biznes/ (accessed August 16, 2025)

6. Petrukha N. M., Petrukha S. V., Zhmaiev A. Yu., Synkevych M. E. (2024) Kiberbezpeka ekonomiky ta derzhavnykh finansiv: istoriohrafiia ta povoienna traiektoriia rozvytku [Cyber Security of the Economy and Public Finances: Historiography and Post-War Trajectory of Development]. *Biznes Inform – Business Inform*, vol. 6, pp. 64–79.

7. Pro zatverdzhennia Zmin do deiakykh normatyvno-pravovykh aktiv Natsionalnoho banku Ukrainy z pytan informatsiinoi bezpeky ta kiberzakhystu: Postanova NBU [On approval of Amendments to certain regulatory legal acts of the National Bank of Ukraine on information security and cyber protection: NBU Resolution]. Available at: https://zakon.rada.gov.ua/laws/show/v0024500-25#Text (accessed August 16, 2025)

8. Fintech insider: Kiberbezpeka yak kliuchovyi fintekh-trend roku: shcho varto znaty pro zahrozy ta zakhyst [Cybersecurity as the key fintech trend of the year: what you should know about threats and protection]. Available at: https://fintechinsider.com.ua/kiberbezpeka-yak-klyuchovyj-finteh-trend-roku-shho-varto-znaty-pro-zagrozy-ta-zahyst/ (accessed August 16, 2025)

9. KYIVSTAR BUSINESS HUB Kiberataky na bankivskyi sektor: yak zakhystyty finansovi ustanovy? [Cyberattacks on the banking sector: how to protect financial institutions?]. Available at: https://hub.kyivstar.ua/articles/kiberataky-na-bankivskyj-sektor-yak-zahystyty-finansovi-ustanovy (accessed August 16, 2025)

10. Lysiak L, Kachula S., Hrabchuk O., Filipova M., Kushnir, A. (2020) Assessment of financial sustainability of the local budgets: case of Ukraine. *Public and Municipal Finance*, vol. 9(1), pp. 48–59.

11. NIST Cybersecurity Framework [Cybersecurity Framework]. Available at: https://www.nist.gov/cyberframework (accessed August 16, 2025)

12. Romenska K., Kachula S., Huba M., Dudchyk, O., Lapa M. (2024) State financial flows for ensuring security in the international economic environment. *Financial and credit activity: problems of theory and practice*, vol. 4 (57), pp. 317–331.

13. USAID Ohliad rynku kiberbezpeky v Ukraini [Overview of the cybersecurity market in Ukraine]. Available at: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (accessed August 16, 2025)

14. World Bank. Financial Sectors Cybersecurity: A Regulatory Digest [Financial Sector's Cybersecurity: A Regulatory Digest]. Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099062624064012530 (accessed August 16, 2025)