DOI: https://doi.org/10.32782/2524-0072/2026-85-168

УДК 336.012.23:004.9

РОЛЬ ЦИФРОВІЗАЦІЇ У ФОРМУВАННІ СИСТЕМИ ФІНАНСОВОЇ БЕЗПЕКИ IT-ПІДПРИЄМСТВ

THE ROLE OF DIGITALISATION IN THE DEVELOPMENT OF A FINANCIAL SECURITY SYSTEM FOR IT-COMPANIES

Дранус Валентин Вікторович
кандидат економічних наук, доцент кафедри фінансів і кредиту,
Чорноморський національний університет імені Петра Могили
ORCID: https://orcid.org/0000-0001-5617-6740

Дранус Любов Сергіївна
кандидат економічних наук, доцент кафедри менеджменту,
Чорноморський національний університет імені Петра Могили
ORCID: https://orcid.org/0000-0002-6427-1315

Прокопишин Оксана Степанівна
кандидат економічних наук, доцент кафедри обліку і оподаткування,
Львівський національний університет ветеринарної медицини та біотехнологій
ім. С. Ґжицького
ORCID: https://orcid.org/0000-0002-7027-3499

Dranus Valentyn, Dranus Liyubov
Petro Mohyla Black Sea National University

Prokopyshyn Oksana
Stepan Gzhytskyi L'viv National University of Veterinary Medicine and Biotechnology

Стаття присвячена дослідженню ролі цифровізації у формуванні та зміцненні системи фінансової безпеки IT-підприємств в умовах нестабільного зовнішнього середовища. Визначено сутність фінансової безпеки IT-підприємств, її ключові функції та специфічні особливості в контексті розвитку цифрової економіки. Досліджено основні загрози, ризики та виклики, що виникають у фінансовій сфері IT-компаній у процесі цифрової трансформації, зокрема кіберризики, інформаційні загрози та фінансові втрати. Систематизовано сучасні цифрові інструменти управління фінансовою безпекою, включаючи технології штучного інтелекту, блокчейн, великі дані та автоматизовані системи моніторингу. Встановлено взаємозв'язок між рівнем цифровізації, адаптивністю підприємства та ефективністю системи фінансового захисту. Обґрунтовано практичні рекомендації щодо впровадження цифрових рішень для підвищення стійкості, конкурентоспроможності та фінансової стабільності IT-компаній.

Ключові слова: цифровізація, фінансова безпека, IT-підприємство, цифрова трансформація, фінансові ризики, штучний інтелект, блокчейн, кібербезпека, управління ризиками, фінансовий моніторинг.

The purpose of this study is to examine the role of digitalization in shaping and strengthening the financial security system of IT enterprises operating in a volatile and competitive external environment. The relevance of the topic is driven by the rapid digital transformation of the global economy, which simultaneously creates new opportunities and generates unprecedented financial risks for IT companies. In the context of digitalization, financial security is no longer a static concept – it requires continuous adaptation to emerging technological threats, cybercriminal activity, and volatile market conditions. The research employs a combination of scientific methods, including systematic analysis and synthesis for examining the theoretical foundations of financial security; comparative analysis for evaluating the effectiveness of various digital instruments; economic-statistical methods for assessing the relationship between digitalization indicators and the level of financial security; and the expert assessment method for validating practical recommendations. The study identifies the essential characteristics of financial security specific to IT enterprises and distinguishes them from those of traditional industries. Key threats in the financial domain include revenue concentration risk, cybersecurity breaches leading to financial loss, intellectual property theft, currency and liquidity risks, and regulatory compliance challenges across multiple jurisdictions. The research systematizes modern digital tools applicable to financial security management, including artificial intelligence and machine learning for

anomaly detection and fraud prevention, blockchain technology for transaction transparency and smart contract execution, big data analytics for real-time financial monitoring, and cloud-based financial management platforms. The results demonstrate a statistically significant positive correlation between the level of enterprise digitalization and the resilience of its financial security system. Enterprises that have implemented advanced digital monitoring tools exhibit a substantially lower incidence of financial losses from cyber threats and operational disruptions. The practical value of this research lies in the development of a conceptual framework for integrating digital solutions into the financial security management system of IT enterprises, which can be applied by financial directors, risk managers, and policymakers in designing corporate financial protection strategies.

Keywords: digitalization, financial security, IT enterprise, digital transformation, financial risks, artificial intelligence, blockchain, cybersecurity, risk management, financial monitoring.

Постановка проблеми. В умовах стрімкого розвитку цифрової економіки та глобальної трансформації бізнес-середовища IT-підприємства стають одночасно рушіями та об'єктами цифровізації. Особливості діяльності IT-підприємств – висока залежність від нематеріальних активів, розподілені моделі роботи, значна частка транскордонних операцій, концентрація доходів в декількох замовників – формують специфічний профіль фінансових ризиків, що суттєво відрізняється від традиційних секторів економіки.

Водночас цифрові технології пропонують принципово нові механізми захисту фінансових інтересів підприємства: від систем автоматизованого моніторингу фінансових потоків до алгоритмів машинного навчання, здатних виявляти аномалії в реальному часі. Проте питання системного використання цифрових інструментів саме для цілей фінансової безпеки IT-підприємств залишається недостатньо дослідженим у вітчизняній науковій літературі.

Вирішення цієї проблеми набуває особливої актуальності в контексті посилення кіберзагроз, волатильності валютних ринків та необхідності відповідати зростаючим регуляторним вимогам міжнародного характеру, що разом утворюють складний комплекс викликів для фінансової стійкості IT-компаній [1, с. 45].

Аналіз останніх досліджень і публікацій. Теоретичні та прикладні засади фінансової безпеки підприємств в умовах цифровізації досліджено в низці наукових праць. Зокрема, А. Гаврікова, Т. Свинаренко та Я. Самодрига обґрунтували сценарії розвитку цифрової трансформації та їх вплив на фінансово-економічну безпеку підприємств [2; 6]. М. Солонько та А. Войтів систематизували загрози, що виникають в контексті цифровізації, та запропонували адаптивні стратегії управління фінансово-економічною безпекою із застосуванням Big Data та штучного інтелекту [3]. І. Надточій, І. Крамаренко та Н. Гришина розкрили наукові засади та особливості управління фінансово-економічною безпекою в умовах цифрової економіки і суспільства, зосередившись на ризиках електронних платіжних систем [4].

Проблематику формування системи фінансової безпеки IT-підприємств, як специфічного суб'єкта господарювання, досліджено О. Мініною, І. Поцелуйком та С. Олійник, які ідентифікували ключові компоненти фінансової безпеки в умовах цифрової економіки та виокремили галузеві ризики IT-бізнесу [11]. Концептуальні підходи до забезпечення фінансової безпеки IT-компаній в контексті смарт-економіки обґрунтовано в дослідженні І. Румик та П. Пузирьової [12]. Аспекти цифрової трансформації фінансових систем та вплив блокчейну висвітлено Д. Тапскоттом [5], а питання цифровізації аналітики – в дослідженнях McKinsey Global Institute [7].

Виділення невирішених раніше частин загальної проблеми. Разом із тим, в сучасній науковій літературі недостатньо уваги приділяється синтезу концепцій фінансової безпеки та цифровізації стосовно IT-підприємств, як специфічного суб'єкта господарювання. Відсутня комплексна модель інтеграції цифрових інструментів у систему фінансового захисту IT-компаній, що й обумовлює актуальність цього дослідження.

Формулювання цілей статті. Метою статті є дослідження ролі цифровізації у формуванні системи фінансової безпеки IT-підприємств, систематизація сучасних цифрових інструментів управління фінансовими ризиками та розробка концептуальних підходів до їх практичного застосування.

Для досягнення зазначеної мети поставлено такі завдання: розкрити сутність фінансової безпеки IT-підприємств та її специфіку; ідентифікувати основні загрози фінансовій безпеці в умовах цифровізації; систематизувати цифрові інструменти управління фінансовою безпекою; обґрунтувати взаємозалежність між рівнем цифровізації та ефективністю фінансового захисту.

Виклад основного матеріалу дослідження. Фінансова безпека підприємства – це такий стан фінансово-економічних відносин, при якому суб'єкт господарювання здатний ефективно протистояти зовнішнім та внутрішнім загрозам, забезпечувати фінансову стійкість та реалізовувати стратегічні цілі розвитку [4]. Для ІТ-підприємств ця дефініція набуває додаткових вимірів, пов'язаних із специфікою їхньої діяльності.

Нематеріальний характер основних активів (програмне забезпечення, патенти, бази даних, компетенції персоналу) ускладнює їх оцінку та захист від несанкціонованого використання, що безпосередньо впливає на вартість компанії та її фінансові показники. Модель доходів ІТ-підприємств часто базується на підписних платежах або довгострокових контрактах із обмеженим колом замовників, що формує підвищений ризик концентрації. Транскордонний характер надання послуг генерує валютні та регуляторні ризики одночасно в кількох юрисдикціях [8, с. 56].

Таким чином, фінансова безпека ІТ-підприємства може бути визначена як динамічний стан захищеності фінансових інтересів компанії, що досягається через систему заходів із управління специфічними фінансовими ризиками цифрового бізнесу та забезпечення стабільного фінансового розвитку. Цифровізація бізнес-середовища породжує подвійний ефект для фінансової безпеки ІТ-підприємств: з одного боку, вона розширює можливості моніторингу та управління ризиками, з іншого – формує нові вектори загроз. Систематизація основних загроз ІТ-підприємств наведена в таблиці 1.

Аналіз показників таблиці 1 дозволяє виокремити основні груп загроз фінансовій безпеці ІТ-підприємств, що суттєво відрізняються від ризиків традиційних галузей, як за природою виникнення, так і за механізмами ней-

Таблиця 1

Класифікація загроз фінансовій безпеці ІТ-підприємств в умовах цифровізації

Група загроз	Конкретні прояви	Ймовірність*	Фінансові наслідки	Цифрові методи нейтралізації
1	2	3	4	5
Кібербезпекові загрози	Ransomware-атаки, злам систем Витік конфіденційних даних DDoS, supply chain attacks AI-фішинг, соціальна інженерія	Висока (72%)	Прямі збитки: 5,08 млн USD/ інцидент Штрафи GDPR/NIS2 до 4% обороту Репутаційні втрати: відтік клієнтів Витрати на відновлення: 24,6 доби	EDR/XDR з AI-моніторингом SIEM/SOAR-платформи Блокчейн-аудит транзакцій
Ризики концентрації доходів	Залежність від 1–3 клієнтів (>50% доходу) Географічна концентрація ринків Технологічна залежність від платформ	Висока	Раптове падіння доходів на 30–70% Касові розриви при розриві контракту Загроза операційній стійкості	Big Data-аналіз структури доходів FP&A стрес-тестування сценаріїв Цифрова диверсифікація клієнт. бази
Валютні та ринкові ризики	Доходи в USD/EUR, витрати в UAH Волатильність обмінних курсів Зміни ринкової кон'юнктури Цінова конкуренція на глобальних ринках	Середня	Волатильність маржинальності ±15–25% Знецінення контрактної вартості Зниження конкурентоспроможності	Хмарні FP&A для хеджування позицій Big Data-моніторинг валютних ринків Автоматизовані форвардні контракти

Продовження Таблиці 1

1	2	3	4	5
Регуляторні та правові ризики	GDPR, CCPA, NIS2 – вимоги захисту даних Зміни податкового законодавства Санкційні обмеження та ліцензування Суперечки щодо права ІВ у різних юрисдикціях	Середня	Штрафи до 4% глобального обороту Судові витрати та блокування діяльності Витрати на комплаєнс до 5% бюджету	RegTech-автоматизація комплаєнсу AI-моніторинг регуляторних змін Блокчейн для захисту прав ІВ
Кадрові та операційні ризики	Відтік ключових спеціалістів (brain drain) Залежність від окремих розробників Збої у процесах доставки продукту Помилки при оцінці проектів (scope creep)	Висока	Зрив термінів -штрафи за SLA Підвищення витрат на рекрутинг 20–40% Переоцінка проектів: збитки до 30%	HR-аналітика на основі Big Data ERP-системи контролю проектів AI-прогнозування ризиків затримок
Ризики ліквідності та фінансові ризики	Затримки платежів від замовників Сезонність та нерівномірність замовлень Недостатнє фінансування зростання Залежність від зовнішнього фінансування	Середня	Касові розриви, порушення зобов'язань Вимушені позики за невигідними ставками Обмеження інвестиційних можливостей	AI-прогнозування грошових потоків FP&A-платформи планування ліквідності Цифровий резервний фонд безпеки
Ризики інтелектуальної власності	Несанкціоноване копіювання коду (IP theft) Reverse engineering продуктів Порушення open-source ліцензій Витік алгоритмів через колишніх співробітників	Середня	Знецінення нематеріальних активів Судові витрати на захист патентів Втрата конкурентних переваг	Блокчейн-реєстр прав ІВ DRM-системи захисту коду AI-моніторинг ринку аналогів
Ризики ланцюга постачання (Supply Chain)	Вразливості в сторонніх бібліотеках Компрометація хмарних провайдерів Збої впостачальників API/SaaS Залежність від вузького кола техн. рішень	Зростає (+30% 2025 р.)	Каскадні збої у клієнтських сервісах SLA-штрафи та відтік клієнтів Юридична відповідальність перед downstream	Автома-тизований аудит залежностей Zero-trust архітектура AI-моніторинг вразливостей (CVE)
Репутаційні та довірчі ризики	Публічні інциденти безпеки Негативні відгуки у ЗМІ та соцмережах Порушення конфіденційності даних клієнтів Провали великих проектів	Середня	Відтік клієнтів (churn rate +15–30%) Зниження вартості контрактів Складнощі із залученням нових клієнтів	Real-time моніторинг медіапростору AI-аналіз сентименту клієнтів Цифрові кризові комунікаційні протоколи

* Рівень ймовірності визначено на основі галузевих даних для ІТ-сектору [9; 15: 16; 17]

Джерело: сформовано авторами на основі [2; 4; 8; 9; 11; 15: 16; 17]

тралізації. Найбільш критичними за рівнем ймовірності є кібербезпекові загрози, кадрові ризики та ризики концентрації доходів – всі вони мають високий рівень прояву Зокрема, кібербезпекові загрози безпосередньо трансформуються у фінансові втрати: за даними IBM Security, середній сукупний збиток від однієї ransomware-атаки в 2025 році досяг 5,08 млн дол. США, що на 17% більше порівняно з 2024 роком [9]. При цьому 72% підприємств щорічно зазнають спроб ransomware-атак, а середній час простою після успішного інциденту становить 24,6 доби. Окремої уваги заслуговують ризики ланцюга постачання (supply chain), рівень яких зріс на 30% в 2025 році: подвоєння частки third-party атак в структурі інцидентів з 15% до 30% [17] свідчить про формування нового системного вектора загроз для IT-підприємств [9; 15]. Кожній групі ризиків у таблиці відповідають конкретні цифрові методи нейтралізації, що формують основу для побудови трирівневої моделі захисту.

Сучасна цифрова екосистема пропонує широкий арсенал інструментів, що можуть бути інтегровані у систему фінансової безпеки IT-підприємств. Розглянемо ключові з них.

Штучний інтелект та машинне навчання (AI/ML). Алгоритми машинного навчання дозволяють аналізувати великі масиви фінансових транзакцій в режимі реального часу, виявляючи аномалії та патерни, характерні для шахрайства або несанкціонованих операцій. Впровадження EDR-систем з AI-моделюванням поведінки дозволяє виявляти до 89% відомих ransomware-штамів на стадії підготовки атаки [9]. Предиктивна аналітика на основі AI забезпечує прогнозування касових розривів та ризиків ліквідності, а платформи SIEM/SOAR скорочують середній час реагування на інцидент на 42% [9].

Технологія блокчейн. Децентралізований розподілений реєстр забезпечує незмінність фінансових записів та прозорість транзакцій, що критично важливо для запобігання внутрішньому шахрайству. Смарт-контракти автоматизують виконання фінансових зобов'язань при дотриманні заздалегідь визначених умов, знижуючи операційні ризики та транзакційні витрати [5]. Практичне застосування блокчейну для захисту прав на інтелектуальну власність дозволяє однозначно встановити пріоритет розробки програмних продуктів, що захищає нематеріальні активи IT-компаній.

Великі дані (Big Data). Технології обробки великих даних у поєднанні з інструментами бізнес-аналітики дозволяють формувати комплексні дашборди фінансової безпеки, що агрегують дані із різних внутрішніх та зовнішніх джерел: ERP-систем, банківських платформ, ринкових індикаторів, новинних потоків. Це надає можливість приймати обґрунтовані рішення щодо управління ризиками на основі актуальних даних [7].

Хмарні фінансові платформи. Хмарні рішення класу FP&A (Financial Planning & Analysis) – Anaplan, Adaptive Insights, Oracle EPM – надають IT-підприємствам можливість централізованого планування, моніторингу та стрес-тестування фінансових сценаріїв. Критично важливою перевагою таких платформ є забезпечення безперервності фінансового управління в умовах дистанційної роботи, що набуло особливого значення в умовах воєнного часу. Хмарні компанії відновлюються після інцидентів на 35% швидше порівняно з гібридною інфраструктурою [9].

На основі проведеного аналізу пропонується концептуальна модель (рисунок 1), що включає три рівні захисту фінансових інтересів IT-підприємства. Перший (операційний) охоплює AI/ML-моніторинг транзакцій, RegTech-рішення та блокчейн-захист. Другий (тактичний) – хмарні FP&A-платформи, Big Data-аналітику ризиків та управління концентрацією клієнтської бази. Третій (стратегічний) – предиктивну аналітику загроз, цифрову диверсифікацію доходів та формування резервного фонду фінансової безпеки [2; 13]. Взаємозв'язок між рівнями забезпечується єдиною Data Management Platform.

Для оцінювання ефективності моделі підприємства класифіковано на три групи: рівень 0 – традиційний контроль без цифрових інструментів, реагування на інциденти постфактум; рівень 1–2 (частковий) – впроваджено один-два рівні моделі, наявний щонайменше один цифровий інструмент (EDR, SIEM або FP&A-платформа), часткова автоматизація без міжрівневої інтеграції; рівень 3 (повний) – реалізовано всі три рівні в комплексі з інтегрованою Data Management Platform та регулярним тестуванням систем відновлення.

Порівняльний аналіз ключових показників фінансової безпеки для трьох груп підприємств та методологію, що пропонується для їх розрахунку, наведено у таблиці 2.

Вагові коефіцієнти визначено методом попарного порівняння (AHP-метод) на основі оцінок експертів галузі: $w_1 = 0{,}20$ (ліквідність); $w_2 = 0{,}20$ (платоспроможність); $w_3 = 0{,}30$ (захист від кіберризиків); $w_4 = 0{,}20$ (опе-

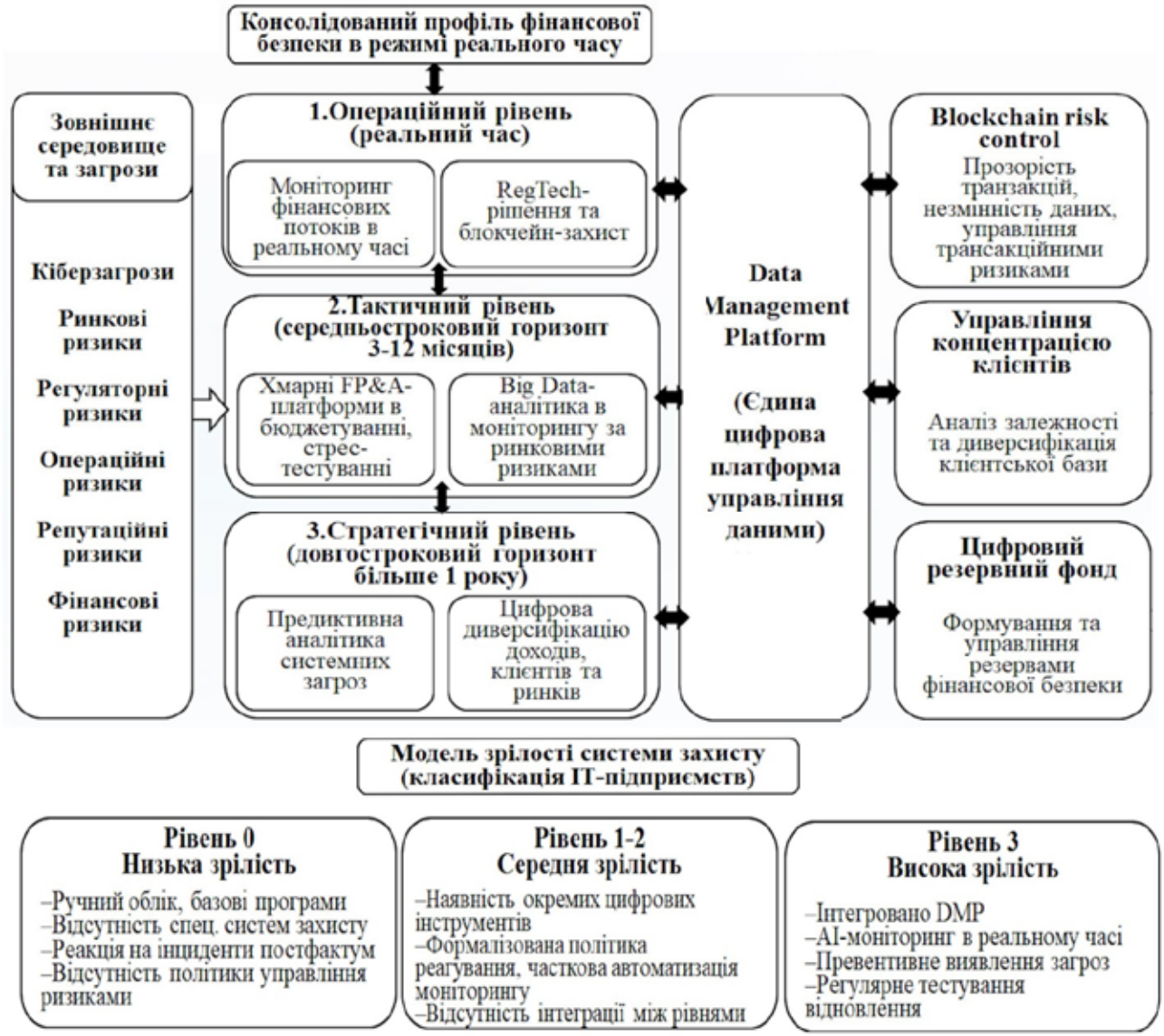

Рис. 1. Концептуальна модель інтеграції цифрових інструментів в систему фінансової безпеки IT-підприємств та модель зрілості системи захисту

Джерело: сформовано авторами

раційна стійкість); $w_5 = 0{,}10$ (регуляторна відповідність). Підвищена вага субіндексу кіберризиків (0,30) обґрунтована специфікою IT-підприємств, для яких кіберзагрози є домінуючим вектором фінансових втрат [9; 15].

Аналіз таблиці 2 засвідчує, що середній збиток від кіберінциденту знижується від 5080 до 890 тис. USD (в 5,7 рази) із зростанням рівня цифровізації. Ключовим драйвером є зростання $P_{ПВ}$ з 12% до 89%: превентивне виявлення атаки виключає компоненти $L_П$, $L_р$ і $L_Ш$ із формули збитку. MTTR скорочується в 3,6 рази (з 24,6 до 6,8 доби), а $P_{ВИК}$ – з 61% до 11%, оскільки перевірені резервні копії нівелюють головний важіль тиску зловмисників. Приріст ІФС від рівня 0 до рівня 1–2 становить +2,7 бали (+87%), від рівня 1–2 до рівня 3 – +2,6 бали (+45%), що підтверджує найвищу граничну ефективність першого етапу впровадження і доцільність поетапної імплементації моделі навіть за обмежених ресурсів.

Висновки. Цифровізація суттєво трансформує як профіль загроз фінансовій безпеці IT-підприємств, так і можливості їх нейтралізації. Специфіка IT-бізнесу зумовлює формування унікального комплексу фінансових ризиків, що включає кібербезпекові загрози, ризики концентрації, валютні та регуляторні ризики, управління якими потребує спеціалізованих цифрових інструментів. Сучасний

Таблиця 2

Порівняльний аналіз показників фінансової безпеки IT-підприємств залежно від рівня цифровізації системи захисту з методологією розрахунку

Показник	Формула	Пояснення складових	Рівень 0	Рівень 1–2	Рівень 3
Середній збиток від кібер-інциденту, тис. USD	$L = L_в + L_п + L_т + L_р + L_ш$	$L_в$ – виплата викупу, крадіжка коштів; $L_п$ – добовий простій × кількість діб; $L_т$ – технічне відновлення систем; $L_р$ – відтік клієнтів × середній контракт; $L_ш$ – штрафи GDPR, NIS2	5080	2970	890
Середній час відновлення, діб	$\mathrm{MTTR} = \frac{t_в + t_л + t_тв}{n}$	$t_в$ – час виявлення інциденту; $t_л$ – час локалізації загрози; $t_тв$ – час технічного відновлення; n – кількість інцидентів у вибірці	24,6	14,2	6,8
Частка превентивно виявлених інцидентів, %	$P_{пв} = \frac{N_{пв}}{N_{заг}} * 100\%$	$N_{пв}$ – інциденти, виявлені до завдання шкоди (стадія підготовки, раннє проникнення); $N_{заг}$ – загальна кількість зафіксованих атак	12	48	89
Витрати на відновлення, % від річного доходу	$R_в = \frac{L_{від}}{D_р} * 100\%$	$L_{від}$ – сукупні витрати на відновлення за рік (USD); $D_р$ – річний дохід підприємства (USD). Розраховано для медіанного IT-підприємства: $D_р$ = 5 млн USD	4,1	2,3	0,7
Частка підприємств, що сплатили викуп, %	$P_{вик} = \frac{N_{вик}}{N_{заг}} * 100\%$	$N_{вик}$ – кількість підприємств, що сплатили викуп; $N_{заг}$ – підприємства, що зазнали успішної ransomware-атаки.	61	38	11
Індекс фінансової стійкості, балів (0–10)	$\mathrm{ІФС} = w_1 * I_л + w_2 * I_п + w_3 * I_к + w_4 * I_о + w_5 * I_р$	$I_л$ = ПА / ПЗ ПА – поточні активи, ПЗ – поточні зобов'язання; $I_п$ = ВК / З ВК – власний капітал, З – зобов'язання; $I_к = 10 * (1 - L/L_{max})$ $I_о = 10 * (1 - \mathrm{MTTR}/30)$ $I_р$ = частка виконаних стандартів безпеки.	3,1	5,8	8,4

Джерело: сформовано та розраховано авторами на основі [9; 14; 15; 16]

арсенал цифрових інструментів – технології AI/ML, блокчейн, Big Data та хмарні FP&A-платформи – забезпечує якісно новий рівень захисту фінансових інтересів ІТ-підприємств. Проведені розрахунки підтверджують, що комплексне впровадження трирівневої моделі дозволяє скоротити середній збиток від кіберінциденту в 5,7 рази, зменшити час відновлення після атаки з 24,6 до 6,8 доби та підвищити індекс фінансової стійкості підприємства з 3,1 до 8,4 бала за десятибальною шкалою.

Запропонована трирівнева концептуальна модель інтеграції цифрових інструментів у систему фінансової безпеки (операційний, тактичний, стратегічний рівні) забезпечує комплексний захист фінансових інтересів ІТ-підприємства в короткостроковому, середньостроковому та довгостроковому горизонтах.

Перспективами подальших досліджень є розробка кількісних методів оцінки ефективності цифрових інструментів фінансової безпеки, а також дослідження особливостей їх застосування в умовах воєнного стану та постконфліктного відновлення економіки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Момот Т. В., Філатова І. О. Фінансова безпека підприємства: сучасні виклики та механізми забезпечення. *Проблеми економіки.* 2021. № 2. С. 42–51.

2. Гаврікова А. В., Свинаренко Т. І., Самодрига Я. The Role of Digitalization in Formation the Financial and Economic Security of an Enterprise. *SWorldJournal.* 2025. № 31-03. С. 79–85. DOI: https://doi.org/10.30888/2663-5712.2025-31-03-051. (дата звернення: 21.04.2026 р.).

3. Войтів А. В., Солонько М. Ю. Інноваційні підходи до забезпечення фінансово-економічної безпеки підприємств в умовах глобальних викликів. *Дослідження та інновації.* 2025. № 1(4). С. 40–45. URL: https://rni.com.ua/index.php/ri/article/view/46. (дата звернення: 21.04.2026 р.).

4. Надточій І. І., Крамаренко І. С., Гришина Н. В. Фінансово-економічна безпека в умовах цифрової економіки та суспільства: наукові засади, особливості управління та регулювання. *Український економічний часопис.* 2024. № 4. С. 83–88. DOI: https://doi.org/10.32782/2786-8273/2024-4-16

5. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. New York: Portfolio/Penguin, 2018. 368 p.

6. Гаврікова А. В., Свинаренко Т. І. Розвиток фінансово-економічної безпеки підприємства в умовах цифрової економіки. *Collection of Scientific Papers «SCIENTIA»*. 2025. С. 46–53. URL: https://previous.scientia.report/index.php/archive/article/view/2483. (дата звернення: 21.04.2026 р.).

7. McKinsey Global Institute. The Age of Analytics: Competing in a Data-Driven World. McKinsey & Company, 2022. 80 p.

8. Захаркіна Л. С., Євдокимова А. В. Цифрова трансформація фінансового менеджменту ІТ-підприємств. *Вісник СумДУ. Серія «Економіка».* 2022. № 3. С. 53–63.

9. IBM Security. Cost of a Data Breach Report 2025. Armonk: IBM Corporation, 2025. 82 p. URL: https://www.ibm.com/reports/data-breach. (дата звернення: 21.04.2026 р.).

10. Христенко О. В. Управління фінансовою безпекою підприємства в умовах цифровізації економіки. *Економіка та держава.* 2023. № 1. С. 130–138.

11. Мініна О., Поцелуйко І., Олійник С. Формування системи фінансової безпеки ІТ-підприємств: ідентифікація ключових компонентів в умовах цифрової економіки. *Економіка та суспільство.* 2026. № 83. DOI: https://doi.org/10.32782/2524-0072/2026-83-50

12. Rumyk I., Puzyrova P. Conceptual Approaches to Ensuring Financial Security of IT Companies in the Context of Smart Economy and Digitalization. Economics, *Finance and Management Review.* 2025. № 1(21). P. 85–97. DOI: https://doi.org/10.36690/2674-5208-2025-1-85-97

13. Варналій З. С., Мехед А. Фінансова безпека суб'єктів підприємництва в умовах цифрової економіки. *Financial and Credit Activity Problems of Theory and Practice.* 2022. № 4(45). С. 267–275. DOI: https://doi.org/10.55643/fcaptp.4.45.2022.3813

14. Mollenkamp D. T. Economic security. Investopedia. 2022. August 31. URL: https://www.investopedia.com/economic-security-5213404. (дата звернення: 21.04.2026 р.).

15. Sophos. The State of Ransomware 2025. Oxford: Sophos Ltd., 2025. 48 p. URL: https://www.sophos.com/en-us/whitepaper/state-of-ransomware. (дата звернення: 21.04.2026 р.).

16. Resilience. Midyear 2025 Cyber Risk Report. San Francisco: Resilience Insurance, 2025. 36 p. URL: https://cyberresilience.com/pr_2025_cyber_risk_report/. (дата звернення: 21.04.2026 р.).

17. 2025 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/. (дата звернення: 21.04.2026 р.).

REFERENCES:

1. Momot, T. V., & Filatova, I. O. (2021). Finansova bezpeka pidpryiemstva: suchasni vyklyky ta mekhanizmy zabezpechennia [Financial security of enterprise: modern challenges and mechanisms of ensuring]. *Problemy ekonomiky*, 2, 42–51.

2. Havrikova, A. V., Svynarenko, T. I., & Samodryha, Ya. (2025). The Role of Digitalization in Formation the Financial and Economic Security of an Enterprise. *SWorldJournal*, 3(31-03), 79–85. DOI: https://doi.org/10.30888/2663-5712.2025-31-03-051

3. Voitiv, A. V., & Solonko, M. Yu. (2025). Innovatsiini pidkhody do zabezpechennia finansovo-ekonomichnoi bezpeky pidpryiemstv v umovakh hlobalnykh vyklykiv [Innovative approaches to ensuring financial and economic security of enterprises in the context of global challenges]. *Doslidzhennia ta innovatsii*, 1(4), 40–45. URL: https://rni.com.ua/index.php/ri/article/view/46. (accessed April 21, 2026). [in Ukrainian].

4. Nadtochii, I. I., Kramarenko, I. S., & Hryshyna, N. V. (2024). Finansovo-ekonomichna bezpeka v umovakh tsyfrovoi ekonomiky ta suspilstva: naukovi zasady, osoblyvosti upravlinnia ta rehuliuvannia [Financial and economic security in the conditions of digital economy and society: scientific foundations, management and regulation features]. *Ukrainskyi ekonomichnyi chasopys*, 4, 83–88. DOI: https://doi.org/10.32782/2786-8273/2024-4-16

5. Tapscott, D., & Tapscott, A. (2018). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. Portfolio/Penguin.

6. Havrikova, A. V., & Svynarenko, T. I. (2025). Rozvytok finansovo-ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovoi ekonomiky [Development of financial and economic security of an enterprise in the digital economy]. *Collection of Scientific Papers «SCIENTIA»*. 46–53. URL:https://previous.scientia.report/index.php/archive/article/view/2483/ (accessed April 21, 2026). [in Ukrainian].

7. McKinsey Global Institute. (2022). The Age of Analytics: Competing in a Data-Driven World. McKinsey & Company.

8. Zakharkina, L. S., & Yevdokymova, A. V. (2022). Tsyfrova transformatsiia finansovoho menedzhmentu IT-pidpryiemstv [Digital transformation of financial management of IT enterprises]. *Visnyk SumDU. Seriia «Ekonomika»*, 3, 53–63.

9. IBM Security. (2025). Cost of a Data Breach Report 2025. IBM Corporation. URL:https://www.ibm.com/reports/data-breach. (accessed April 21, 2026).

10. Khrystenko, O. V. (2023). Upravlinnia finansovoiu bezpekoiu pidpryiemstva v umovakh tsyfrovizatsii ekonomiky [Management of financial security of enterprise in the conditions of digitalization of economy]. *Ekonomika ta derzhava*, 1, 130–138.

11. Minina, O., Potseluiko, I., & Oliinyk, S. (2026). Formuvannia systemy finansovoi bezpeky IT-pidpryiemstv: identyfikatsiia kliuchovykh komponentiv v umovakh tsyfrovoi ekonomiky [Formation of the financial security system of IT enterprises: identification of key components in the digital economy]. *Ekonomika ta suspilstvo,* 83. DOI: https://doi.org/10.32782/2524-0072/2026-83-50

12. Rumyk, I., & Puzyrova, P. (2025). Conceptual Approaches to Ensuring Financial Security of IT Companies in the Context of Smart Economy and Digitalization. *Economics, Finance and Management Review*, 1(21), 85–97. DOI: https://doi.org/10.36690/2674-5208-2025-1-85-97

13. Varnalii, Z. S., & Mekhed, A. (2022). Finansova bezpeka subiektiv pidpryiemnytstva v umovakh tsyfrovoi ekonomiky [Financial security of business entities in the digital economy]. *Financial and Credit Activity Problems of Theory and Practice*, 4(45), 267–275. DOI: https://doi.org/10.55643/fcaptp.4.45.2022.3813

14. Mollenkamp, D. T. (2022, August 31). Economic security. Investopedia. URL:https://www.investopedia.com/economic-security-5213404. (accessed April 21, 2026).

15. Sophos. (2025). The State of Ransomware 2025. Sophos Ltd. URL:https://www.sophos.com/en-us/white-paper/state-of-ransomware. (accessed April 21, 2026).

16. Resilience Insurance. (2025). Midyear 2025 Cyber Risk Report. Resilience. URL: https://cyberresilience.com/pr_2025_cyber_risk_report/. (accessed April 21, 2026).

17. Data Breach Investigations Report (2025). URL: https://www.verizon.com/business/resources/reports/dbir/. (accessed April 21, 2026).

Дата надходження статті: 15.04.2026
Дата прийняття статті: 05.05.2026
Дата публікації статті: 13.05.2026