DOI: https://doi.org/10.25140/2411-5215-2026-1(45)-312-332
УДК 336.7:004.056
JEL Classification: G32; D81; L86

Олена Вікторівна Шишкіна
доктор економічних наук, професор, професор кафедри фінансів,
банківської справи та страхування,
Національний університет «Чернігівська політехніка» (м. Чернігів, Україна).
E-mail: shyshkina.olena.v@gmail.com. **ORCID:** http://orcid.org/0000-0002-8946-1027
ResearcherID: F-3208-2014. **Scopus Author ID:** 58995081900

ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ІТ-ПІДПРИЄМСТВ У ЦИФРОВОМУ СЕРЕДОВИЩІ

У статті досліджено теоретико-методичні засади формування інструментарію забезпечення фінансової безпеки ІТ-підприємств в умовах цифровізації. Уточнено поняття фінансової безпеки ІТ-підприємства з урахуванням домінування нематеріальних активів, гіперзалежності від людського капіталу, глобальної операційної моделі та нестандартних профілів грошових потоків. Ідентифіковано та систематизовано шість груп специфічних загроз фінансовій безпеці (кіберфінансові, інтелектуального капіталу, контрактно-регуляторні, інфраструктурно-операційні, цифрових бізнес-моделей, репутаційно-цифрові) з визначенням каналів їх впливу та пріоритетності. Проведено критичний аналіз адаптованості традиційних та цифрових інструментів до умов ІТ-підприємств. Розроблено функціональну класифікацію інструментів (превентивні, моніторингові, захисні, відновлювальні) та сформовано диференційовані рекомендації щодо їх застосування залежно від масштабу підприємства (малі, середні, великі) та бізнес-моделі (аутсорсинг, продуктове ІТ, SaaS). Отримані результати мають практичну цінність для побудови комплексних систем фінансової безпеки ІТ-підприємств в умовах воєнного стану та повоєнного відновлення.

Ключові слова: фінансова безпека; ІТ-підприємства; цифровізація, загрози, ризики, традиційні та цифрові інструменти забезпечення фінансової безпеки, кіберфінансові загрози, цифрове середовище, продуктове ІТ, SaaS, аутсорсинг.

Табл.: 6. Бібл.: 27.

Постановка проблеми. Цифровізація економіки створює нові можливості для прискореного розвитку підприємств ІТ сектору, але водночас породжує значний спектр ризиків і загроз, які здатні негативно впливати на забезпечення фінансової безпеки. Це пов’язано з тим, що впровадження цифрових технологій (великі дані, інтернет речей, блокчейн, хмарні обчислення, штучний інтелект та машинне навчання тощо), з одного боку, змінює структуру фінансових потоків та операцій і підвищує ефективність діяльності, а з іншого – збільшує ризики кібератак та фінансових шахрайств, що у свою чергу, негативно позначається на рівні доходів і прибутків суб’єктів підприємництва.

Фінансова безпека в цифровому середовищі виступає ключовим фактором захисту економічних суб’єктів від внутрішніх та зовнішніх загроз і ризиків. Для ІТ-підприємств, які працюють у висококонкурентних і швидкозмінних галузях цифрової економіки, де обсяги цифрових фінансових операцій постійно зростають, а витрати на розробку і провадження інновацій та захист активів стають визначальними для виживання бізнесу, упровадження системи фінансової безпеки, яка б враховувала всі їх галузеві особливості, набуває особливої актуальності.

ІТ-підприємства, які через високу залежність їхніх бізнес-процесів від цифрового середовища, яке характеризується безперервним збільшенням кількості кібератак, є одними з найбільш вразливих суб'єктів господарювання. Так, Державний центр кіберзахисту державної служби спеціального зв’язку та захисту інформації України у своєму звіті за 2025 зафіксував «17,3 тис. подій безпеки і 730 кіберінцидентів різного рівня складності», переважна більшість з яких стосувалась використання шкідливого програмного забезпечення [1]. Щодо глобального масштабу кібератак, то за даними Федерального бюро розслідувань США – центру, який через свій сайт приймає скарги на кіберзлочини від громадян будь-

якої країни світу, загальна сума збитків від інтернет-злочинності у 2022 році становила 10,3 млрд дол., у 2023 році – 12,5 млрд дол., а у 2024 – вже 16,6 млрд дол., причому найпоширенішими типами атак є фішинг та програми-вимагачі (ransomware) [2-4].

Для ІТ-підприємств, котрим властиві унікальні характеристики, які ускладнюють забезпечення його фінансової безпеки і чиїм основним активом є інтелектуальна власність та клієнтські дані, реалізація таких загроз спричиняє не лише прямі фінансові втрати, але й втрати частки ринку та репутації. Традиційні методи захисту (наприклад, антивіруси, міжмережеві екрани) вже не є достатніми, що вимагає дослідження та впровадження сучасних інструментів забезпечення фінансової безпеки ІТ-підприємств, здатних функціонувати в умовах високої невизначеності та динамічності цифрового середовища, що підкреслює необхідність і своєчасність науково-прикладних досліджень у даній сфері.

Аналіз останніх досліджень і публікацій. Проблема забезпечення фінансової безпеки підприємств у цифровому середовищі привертає все більшу увагу не тільки вітчизняних і зарубіжних науковців, а й аналітичних центрів.

Зокрема, PwC – міжнародна мережа аудиторських компаній, у своєму дослідженні «Міжнародне аналітичне дослідження довіри до цифрових технологій 2025», дійшло висновків, що найвищим пріоритетом для 59 % представників фінансового сектору (у тому числі в банківському секторі – 67 %, а у страховому – до 62 %) є кіберризики. При цьому лише «2 % організацій впровадили заходи для забезпечення кіберстійкості на всіх рівнях», хоча бюджети на кібербезпеку зростають і все більше спрямовуються на захист даних, технологічну модернізацію та впровадження штучного інтелекту для виявлення ризиків і загроз [5].

У вітчизняній науковій літературі останніх років питання фінансової безпеки підприємств різних видів діяльності у цифровому середовищі досліджувались як науковцями одноосібно, так і авторськими колективами. Зупинимось на окремих наукових роботах, вивчення яких дало підстави сформувати концептуальну ідею нашого наукового дослідження та виділити спектр проблем, які потребують вирішення вже у короткостроковій перспективі.

Так, науковий інтерес становить обґрунтування колективом авторів на чолі О. Правдивець стратегічних напрямів інноваційного розвитку системи фінансово-економічної безпеки підприємств ІТ-сфери на основі цифрових технологій. Науковці застосували метод Дельфі та провели порівняльний аналіз, чим підтвердили незмінну актуальність цих напрямів упродовж останніх п’яти років, що створило підґрунтя для подальших досліджень в умовах воєнного стану [6].

І Румик і П. Пузирова в статті «Концептуальні підходи до забезпечення фінансової безпеки іт-компаній в контексті розумної економіки та цифровизації» розробили концептуальні підходи до забезпечення фінансової безпеки ІТ-компаній в умовах розумної економіки та цифровізації, довели, що цифрова трансформація підвищує стійкість підприємств, та запропонували алгоритм забезпечення фінансової безпеки, а також обґрунтували ключову роль інтегрованого управління фінансовими потоками та ризиками. Заслуговує на особливу увагу запропонований авторами «алгоритм забезпечення фінансової безпеки ІТ-компаній … в контексті розумної економіки та цифровізації» [7].

А. Мехед і З. Варналій досліджують вплив цифровізації на підприємства та організацію системи фінансової безпеки, формують авторське визначення фінансової безпеки в контексті цифрової економіки. Ними обґрунтовані ключові положення механізму фінансової безпеки, адаптованого до цифрового середовища з урахуванням сучасних ІТ-систем та бізнес-моделей [8].

О.Захаркін, А. Захаркин, А. Бойко і Л. Сокол досліджуючи особливості забезпечення фінансової безпеки бізнесу в умовах цифрової трансформації доводять важливість цифрових інновацій для управління ризиками, у тому числі штучного інтелекту та аналітики великих даних, обґрунтовують роль цифрових технологій у забезпеченні кібербезпеки, автоматизації процесів управління ризиками та підвищення прозорості фінансових операцій. На нашу думку, заслуговує на детальне вивчення проведений авторами аналіз переваг хмарних обчислень та технології блокчейн для управління фінансовими ризиками та сформульовані науковцями висновки з дослідження щодо того, що «цифрові технології надають інструменти для моніторингу ризиків у реальному часі та швидкого реагування на них», що у свою чергу дозволяє «покращити стратегії зменшення ризиків та уникнути фінансових проблем» [9].

А. Мохненко і Р. Антоновим у роботі «Характеристика основних факторів конкурентоспроможності підприємств ІТ сфери в умовах воєнного стану» визначено основні фактори конкурентоспроможності ІТ-підприємств, включаючи технологічні інновації, людські ресурси, фінансову стабільність та гнучкість. Автори акцентують увагу на важливості фінансової стабільності як ключового конкурентного фактора для ІТ-підприємств, що працюють у кризових умовах [10].

Значну увагу у своїх дослідженнях науковці приділяють проблематиці управління ризиками в ІТ-сфері. Зокрема, заслуговує на особливу увагу наукова робота І. Данилюка, який з метою виявлення інструментів впливу на величину ризику досліджує діяльність успішних компаній в ІТ-сфері й розглядає види ІТ-ризиків. Вчений обґрунтував фактори впливу на ризики в бізнесі та здійснив оцінку потенційних загроз безпеці, які можуть виникнути в процесі роботи з ІТ-системами [11].

Заслуговують на увагу результати проведеного дослідження В. Лук'янової і Р. Маліцького представленого у статті «Якісний аналіз та кількісне оцінювання ризику підприємств в Україні за умов війни: фокус на ІТ-сектор» де здійснена систематизація основних видів ризиків ІТ-підприємств, характерних для воєнного періоду в Україні та визначені їхні ключові джерела та наслідки для економічної діяльності. Учені підкреслюють, що фінансова стабільність та довгострокове виживання ІТ-підприємств залежать від їхньої здатності виявляти, оцінювати та мінімізувати ризики, що потребує комбінованих якісних та кількісних підходів до оцінки ризиків. Як теоретичний, так і практичний інтерес становить запропонована авторами інтегрована матриця ризиків для українських ІТ-підприємств, яка враховує нефінансову природу ключових загроз (кадрових, кібернетичних, репутаційних) та дозволяє кількісну інтерпретацію їхнього економічного впливу [12].

Виділення недосліджених частин загальної проблеми. Проведений аналіз наукових публікацій дозволяє виокремити цілу низку невирішених проблем.

По-перше, більшість наявних теоретичних моделей фінансової безпеки розроблені для підприємств традиційних галузей і не є коректними для ІТ-підприємств, які на відміну від традиційних, характеризуються домінуванням нематеріальних активів, підписними та сервісними моделями монетизації, розподіленими командами та глобальною клієнтською базою, що, на нашу думку, потребує уточнення поняття «фінансова безпека ІТ-підприємства» в контексті цифрового середовища.

По-друге, в наукових джерелах представлені окремі цифрові інструменти забезпечення фінансової безпеки, однак у жодній із досліджених публікацій не сформовано систему інструментів фінансової безпеки ІТ-підприємств, яка б охоплювала превентивні, моніторингові, захисні, відновлювальні та інші компоненти у їх взаємодії та взаємозалежності.

По-третє, відсутній диференційований підхід за розміром (наприклад, стартап, суб'єкт малого / середнього підприємництва, велика ІТ-компанія) та бізнес-моделлю ІТ-підприємства (наприклад, аутсорсинг, продуктовий бізнес, SaaS, маркетплейс), хоча очевидно, що потреби та можливості цих суб'єктів суттєво різняться.

Це далеко не повний перелік виявлених проблем, які потребують вирішення, однак, вважаємо, що вищенаведені положення доводять необхідність комплексного дослідження, спрямованого на розробку галузево-специфічної, практично орієнтованої та адаптованої до умов цифрового середовища системи інструментів фінансової безпеки ІТ-підприємств України в умовах війни і повоєнного відновлення економіки.

Метою статті є розвиток теоретико-методичних засад формування інструментарію забезпечення фінансової безпеки ІТ-підприємств в умовах цифрового середовища та розробка практичних рекомендацій щодо його ефективного застосування з урахуванням специфіки діяльності суб'єктів ІТ-галузі.

Для досягнення поставленої мети визначено такі завдання:

– уточнити сутність поняття «фінансова безпека ІТ-підприємства» в контексті цифрового середовища та визначити її відмінності від фінансової безпеки підприємств традиційних галузей.

– ідентифікувати та систематизувати специфічні загрози фінансовій безпеці ІТ-підприємств, що генеруються цифровим середовищем;

– провести критичний аналіз існуючих інструментів забезпечення фінансової безпеки та оцінити ступінь їх адаптованості до умов діяльності ІТ-підприємств;

– розробити класифікацію інструментів фінансової безпеки ІТ-підприємств за функціональними групами: превентивні, моніторингові, захисні та відновлювальні;

– розкрити можливості сучасних цифрових технологій (RegTech, FinTech-рішень, систем автоматизованого фінансового моніторингу, блокчейну) як інструментів підвищення рівня фінансової безпеки;

– сформулювати науково обґрунтовані рекомендації щодо формування комплексної системи інструментів фінансової безпеки для ІТ-підприємств різних масштабів та бізнес-моделей.

Виклад основного матеріалу. Категорія фінансової безпеки у класичних трактуваннях розглядалась переважним чином через призму захисту фінансових ресурсів від зовнішніх і внутрішніх загроз та забезпечення платоспроможності суб’єктів підприємництва. Хоча науковці у своїх роботах демонструють певні відмінності до розуміння цієї категорії, спільним для різних підходів при визначенні рівня фінансової безпеки є орієнтація на традиційні фінансові показники – фінансову стійкість, ліквідність, платоспроможність, рентабельність – які розраховуються на основі даних бухгалтерської звітності та відображають стан матеріальних і фінансових активів. Це безумовно є ефективним для підприємств реального сектора економіки, де матеріальні активи формують основу вартості та є головним об'єктом захисту. Однак масштабна цифрова трансформація економіки, яка прискорилася після 2015 року й набула якісно нових рис у 2020-х роках, радикально змінила природу підприємницької діяльності в ІТ-секторі, що зумовило об'єктивну потребу в переосмисленні категорії фінансової безпеки ІТ підприємств, які характеризується низькою системних особливостей, котрі суттєво змінили природу фінансових ризиків і загроз.

До основних особливостей вважаємо доцільними віднести нематеріальний характер активів і продуктів, гіперзалежність від людського капіталу, глобальну цифрову операційну модель та нестандартний профіль грошових потоків, а також кіберпростір як основне операційне середовище.

Нематеріальний характер активів і продуктів зумовлений тим, що ІТ-компанії створюють і реалізують продукти та послуги, котрі не мають фізичного втілення (програмне забезпечення, алгоритми, бази даних, цифрові, інтелектуальні послуги тощо). У зв’язку з цим головним об'єктом захисту фінансової безпеки виступають не матеріальні засоби, а інтелектуальний капітал, програмний код, клієнтські дані та репутація.

Основним виробничим ресурсом ІТ-підприємства є висококваліфіковані фахівці, компетенції яких важко замінити. Втрата навіть одного ключового розробника може призвести до зриву контрактів і суттєвих фінансових збитків, що визначає таку особливість ІТ-підприємств, як *гіперзалежність від людського капіталу.*

ІТ-підприємства, серед іншого, обслуговують клієнтів із різних країн, отримують виторг в іноземній валюті, залучають розподілені команди та використовують хмарну інфраструктуру, що розміщена в різних юрисдикціях. Така г*лобальна цифрова операційна модель* породжує специфічні валютні, контрактні та регуляторні ризики, які відсутні у підприємств реального сектора економіки з локальною операційною моделлю.

ІТ компанії використовують цифрові бізнес-моделі з *нестандартним профілем грошових потоків.* До таких моделей можна віднести:

– підписні моделі (SaaS), наприклад, Microsoft 365;

– фриміум моделі (Zoom, Telegram Premium, Canva);

– маркетплейси (Prom.ua, Rozetka, Upwork);

– модель розподілу доходів (App Store, партнерські програми, спільні ІТ-проєкти тощо).

Зазначені моделі відрізняються одним ключовим принципом «коли і як підприємство отримує гроші». На відміну від традиційної моделі по принципу «продав товар і отримав оплату», ці моделі формують особливі грошові потоки (відстрочені, рекурентні або умовні), до яких недоцільно використовувати класичні схеми фінансового аналізу я які потребують спеціальних інструментів управління фінансовою безпекою.

Кіберпростір є основним операційним середовищем ІТ-підприємств, що робить їх вразливими до кіберзагроз. При цьому кіберінциденти, які виникають у діяльності цих економічних суб'єктів мають прямі фінансові наслідки (наприклад, витік даних клієнтів тягне штрафні санкції і втрату контрактів; атака на інфраструктуру спричинює зупинку сервісів і порушення угоди про рівень обслуговування **(**SLA); компрометація репутації – відтік замовників і, як наслідок втрату доходів).

Проведені дослідження суб'єктів підприємництва реального сектору економіки (промислових підприємств) та ІТ-підприємств дозволили порівняти ключові детермінанти фінансової безпеки, які дозволити більш глибоко зрозуміти специфічні особливості функціонування і розвитку ІТ-компаній (табл. 1).

Таблиця 1

Порівняльна характеристика фінансової безпеки ІТ-підприємств та промислових підприємств традиційних галузей

Параметр порівняння	**Промислові підприємства традиційних галузей**	**ІТ-підприємства**
1	2	3
Основний об'єкт захисту	Матеріальні активи, виробничі фонди, запаси	Інтелектуальний капітал, програмний код, клієнтські дані, репутація
Природа ключових загроз	Фізичні, ринкові, кредитні	Кіберзагрози, кадрові, контрактні, репутаційні в цифровому середовищі
Ключові ризики	Знос активів, логістика, ринкові ціни	Кібератаки, втрата даних, технологічне старіння
Джерела формування вартості	Матеріальне виробництво, земля, обладнання	Людський капітал, алгоритми, мережеві ефекти, клієнтська база
Структура грошових потоків	Стабільні, передбачувані цикли	Рекурентні підписки, нерівномірні проєктні виплати, відстрочені платежі
Модель доходів	Прямий продаж товарів/послуг	Передплати (SaaS), ліцензії, роялті
Операційна географія	Переважно локальна або регіональна	Глобальна, мультивалютна, мультиюрисдикційна

Закінчення таблиці 1

1	2	3
Роль персоналу	Один із ресурсів, замінний	Критичний актив, основне джерело вартості
Регуляторне середовище	Стабільне галузеве регулювання	Швидкозмінне цифрове регулювання (GDPR, NIS2, AI Act тощо)
Інструменти захисту	Страхування, диверсифікація, хеджування	Кіберстрахування, RegTech, SIEM-системи, контрактний захист, резервування хмарної інфраструктури
Часовий горизонт загроз	Середньо- / довгостроковий	Миттєвий (кібератака) до довгострокового (репутаційний)
Масштабованість	Обмежена фізичними потужностями	Висока завдяки хмарним технологіям
Індикатори безпеки	Традиційні фінансові коефіцієнти	Традиційні коефіцієнти + цифрові метрики (MRR, churn rate, NPS, cyber risk score)
Вплив воєнного чинника	Переважно через фізичні руйнування та логістику	Через міграцію персоналу, кіберактивність, контрактні форс-мажори

Джерело: розроблено автором на основі [6; 14-17].

Як видно з таблиці 1, для промислових підприємств фінансова безпека традиційно асоціюється із захистом матеріальних активів (обладнання, виробничих фондів, запасів тощо), а для ІТ-підприємств головним об’єктом захисту є нематеріальні активи (програмний код, клієнтські дані, інтелектуальна власність та репутація). З огляду на ці аспекти принципова відмінність ІТ підприємств в тому, що їх активи не мають фізичної форми, важко піддаються традиційній вартісній оцінці, але при цьому виступають основним джерелом ринкової вартості та конкурентоспроможності компанії.

Загрози для промислових підприємств здебільшого збільшуються поступово (фізичний знос активів, коливання ринкових цін, логістичні збої), що дає відповідальним особам час для реагування. Натомість загрози для ІТ-підприємств є миттєвими (кібератака може паралізувати роботу за лічені хвилини), глобальними (необмеженими географічно) і багатовимірними (одночасно вражають фінансові показники, репутацію та операційну продуктивність), що кардинально змінює вимоги до системи моніторингу та реагування.

Традиційні інструменти забезпечення фінансової безпеки (страхування матеріальних активів, хеджування валютних ризиків, класичні фінансові коефіцієнти ліквідності та платоспроможності тощо) розраховані на іншу природу активів і загроз. Натомість ІТ-підприємства потребують поєднання традиційних інструментів із принципово новими (кіберстрахуванням, RegTech-рішеннями, SIEM-системами, а також спеціальними цифровими метриками (MRR, churn rate, NPS, cyber risk score)), які відображають реальний стан фінансової безпеки таких компаній в цифровому середовищі.

Таким чином, ІТ-підприємство є якісно відмінним типом економічного суб'єкта, фінансова безпека якого формується переважно в нематеріальному, цифровому просторі, що зумовлює потребу у систематизації та економічній оцінці специфічних загроз, а також розробки та впровадження спеціального інструментарію її забезпечення, адаптованого до особливостей цифрового середовища.

Для систематизації загроз пропонуємо використовувати класифікаційну модель**,** яка передбачає розгляд кожної загрози за трьома вимірами: джерело виникнення (зовнішнє / внутрішнє середовище), природа загрози (технологічна / кадрова / ринкова / регуляторна / воєнна) та вплив на фінансовий стан (прямий / опосередкований). Застосування цієї моделі до сукупності загроз, характерних для ІТ-підприємств, дозволило виділити шість якісно відмінних груп, кожна з яких має власний профіль, джерела виникнення та вплив на фінансовий стан. Це наступні групи загроз:

– *кіберфінансові загрози* генеруються зловмисними діями у цифровому просторі й уражають фінансові потоки, операційну спроможність і збереження даних ІТ-підприємства;

– *загрози цифрових бізнес-моделей* зумовлені специфікацією монетизації цифрових продуктів і послуг, нестабільністю клієнтської бази та стрімким технологічним оновленням ринку;

– *загрози інтелектуального капіталу* пов'язані з утратою, знеціненням або несанкціонованим використанням головного активу ІТ-підприємства – його людського, наукового та творчого потенціалу;

– *контрактно-регуляторні загрози* виникають внаслідок невиконання договірних зобов'язань, які зазнали змін у наслідок трансформації регуляторного середовища або валютно-правової нестабільності операційного середовища.

– *інфраструктурно-операційні загрози* зумовлені збоями в технічній та енергетичній інфраструктурі, які забезпечують безперервність цифрових процесів ІТ-підприємства;

– *репутаційно-цифрові загрози* пов'язані з формуванням негативного іміджу ІТ-підприємства в цифровому середовищі, що підриває довіру клієнтів і партнерів та опосередковано скорочує його доходи.

Узагальнення результатів ідентифікації дозволяє представити систематизовану класифікацію специфічних загроз фінансової безпеки ІТ-підприємств у вигляді табл. 2.

Таблиця 2

Систематизація спеціальних загроз фінансовій безпеці ІТ-підприємств у цифровому середовищі

Група загроз	**Конкретні загрози / ризики**	**Джерело**	**Природа загрози**	**Вплив на фінансовий стан**	**Пріоритетність**
1	2	3	4	5	6
І. Кіберфінансові	– *програми-вимагачі та інфраструктури шифрування* (блокування доступу до критичних систем і вимоги викупу зумовлюють простій сервісів, призводять до порушення SLA-зобов'язання, штрафних санкцій і втрати клієнтів; – *витік конфіденційних даних* клієнтів для ІТ-підприємств, які обробляють персональні дані спричинюють штрафні санкції та репутаційні втрати; – *атаки на ланцюг постачання програмного забезпечення* відкриває доступ до системи численних кінцевих клієнтів й може призвести до масштабних фінансових і репутаційних втрат; – *DDOs-атаки на цифрових сервісах* спричиняють недоступність продуктів і сервісів для кінцевих користувачів, що порушує договірні зобов'язання та є підставою для виставлення штрафних санкцій; – *компрометація фінансових транзакцій* через підміну реквізитів або злам платіжних систем іноді уражає фінансові потоки підприємства.	Зовнішнє	Технологічна	Прямий	Критична

Продовження таблиці 2

1	2	3	4	5	6
II. Цифрових бізнес-моделей	– *ризик відтоку підписників* ключовою загрозою для SaaS-компаній, яка суттєво впливає на довгострокову вартість компанії та прогнозованість грошових потоків; – *монетизаційний ризик фріміум (freemium) -моделей* виникає внаслідок генерування операційних витрат «безкоштовною» базою користувачів без гарантованої конверсії у платних клієнтів, що може призвести до накопичення збитків; – технологічне застарювання продукту в умовах стрімкого розвитку AI та суміжних технологій може призвести до знецінення продукту та скорочення виторгу; – *робота на чужій платформі* створює ризик зміни умов або блокування облікового запису, що може миттєво знищити операційну модель; – *залежність від пошукових алгоритмів чи алгоритмів соцмереж* для залучення клієнтів може призвести до необхідності значних витрат на платний трафік	Зовнішнє / внутрішнє	Ринкова / технологічна	Опосередкований	Висока
III. Інтелектуального капіталу	– *міграція фахівців – розробників продукту* може спричинити зрив контрактів і безповоротну втрату клієнтів; – *крадіжка інтелектуальної власності* (коду, алгоритму) яка може бути використана конкурентами без можливості фізичного відстеження; – *ризик несанкціонованого розголошення комерційної таємниці* актуальний в умовах роботи розподілених команд через числові цифрові канали зв'язку; – *ризик втрати інституційної пам'яті* - при масовому відтоку персоналу компанія втрачає накопичені знання, архітектурні рішення та клієнтські зв'язки, що має безпосередні фінансові наслідки	Зовнішнє / внутрішнє	Кадрова	Прямий / опосередкований	Критична
IV. Контрактно-регуляторні	– *порушення договірних (SLA) - зобов'язань* запускає механізм штрафних санкцій, що впливає прямо на фінансовий результат; – *регуляторний ризик цифрового середовища* пов'язаний із стрімкою еволюцією законодавства у сфері захисту персональних даних та оподаткування цифрового бізнесу, що загрожує штрафами і припиненням діяльності. – *валютно-контрактний ризик* створює вразливість до валютної волатильності та обмежень НБУ в умовах воєнного стану; – *ризик форс-мажорного розірвання контрактів* призводить до скорочення виторгу; – *ризик офшорної юрисдикції* пов'язаний із змінами в податковому законодавстві країн реєстрації або посиленням вимог до реальної присутності, що може вплинути на фінансову ефективність операційної моделі.	Зовнішнє	Регуляторна / воєнна	Прямий	Висока

Закінчення таблиці 2

1	2	3	4	5	6
V. Інфраструктурно-операційні	– *хмарна залежність* – зумовлена концентрацією критичної інфраструктури на одному хмарному провайдер; – *перебої енергопостачання* – що впливає на операційну спроможність ІТ-підприємств; – *технічний борг* зумовлений архітектурними недоліками коду і потребами його рефакторингу, що генерує незаплановані витрати й уповільнює розвиток; – *цифрова інтероперабельність* – інтеграція систем різних вендорів може порушити роботу всього технологічного стека через несумісність або оновлення API однієї з систем	Зовнішнє / внутрішнє	Технологічна / воєнна	Прямий / опосередкований	Висока
VI. Репутаційно-цифрові	– цифрова репутація - Негативні відгуки на глобальних платформах або в соцмережах поширюються миттєво і можуть завдати шкоди, яка важко піддається контролю; – *дипфейки і дезінформаційні атаки,* у тому числі за рахунок розвитку генеративного штучного інтелекту (AI) можуть спричинити серйозні репутаційні та фінансові наслідки.; – *репутаційні збитки від публічного розкриття інформації про кіберінциденти* часто значно перевищують прямі фінансові втрати	Зовнішнє	Ринкова / технологічна	Опосередкований	Середня

Джерело: розроблено автором на основі [1; 7; 12; 13; 18].

Попередньо ідентифіковані загрози (табл. 2) мають різну природу впливу на фінансовий стан підприємства. Відповідно до запропонованої класифікації каналів реалізації ризику, їх можна розподілити таким чином:

– *прямий канал* (групи I і IV) – означає, що загроза відразу і без проміжних ланок трансформується в конкретні грошові втрати (наприклад, штрафи за SLA, виплата викупу програмі-вимагачів, валютні збитки);

– *опосередкований канал* (групи II і VI) означає, що втрати настають через ланцюжок проміжних подій: спочатку скорочується репутація або відбувається відтік клієнтів, а лише потім це відображається у фінансових результатах (наприклад, Негативні відгуки → зниження довіри → зменшення кількості нових клієнтів → падіння виручки в довгостроковому періоді);

– *прямий / опосередкований* (групи III і V) – подвійний канал, коли загроза одночасно генерує і прямі збитки (зрив контракту через відхід ключового розробника), і довгострокові опосередковані (втрата *знань,* зниження якості продукту тощо).

Пріоритетність кожної групи загроз визначимо за сукупністю трьох критеріїв: швидкість матеріалізації втрат (тобто наскільки швидко загроза перетворюється на реальні збитки), масштабних показників фінансових наслідків (наприклад, розмір можливих втрат відносно річного обороту підприємства) та відновлення складності (наскільки витратно відновити той стан ІТ-підприємства, який передував реалізації загрози).

Пріоритетність групи I – кіберфінансові загрози є критичною, оскільки миттєвість кібератак зазвичай не залишає часу на превентивне реагування. За оцінками колективу дослідників на чолі з С.С. Панчалом (2025), сукупні збитки від одного кіберінциденту для ІТ-компанії середнього розміру можуть сягати від 15 до 40% річного обороту за рахунок прямих втрат, штрафних санкцій та витрат на відновлення [13]. При цьому репутаційні наслідки витоку даних клієнтів є практично незворотними в короткостроковій перспективі.

Також є критичною пріоритетність групи III – загрози інтелектуального капіталу, які відображають специфіку ІТ-підприємств пов'язану із людським капіталом. Зокрема, втрата одного чи кількох розробників, які працюють над ключовим продуктом, може порушити поточні контракти, а відновлення компетенцій може потребувати значного періоду часу.

Групи II, IV, V мають високу пріоритетність щодо причин загроз. Вони мають менш миттєвий та/або масштабний фінансовий вплив порівняно з критичними групами. Зокрема, реалізація контрактно-регуляторних загроз (група IV) є відносно передбачуваною та залишає ІТ-підприємствам час для реагування (мінімізацію, нейтразізацію). Загрози цифрових бізнес-моделей (група II) мають переважно опосередкований характер і є «розтягнутими» в часі, що дозволяє вжити своєчасних заходів щодо їх мінімізації / нейтралізації за наявності системи моніторингу. Інфраструктурно-операційні загрози (група V) є особливо актуальними для українських реалій сьогодення через ризики перебоїв енергопостачання, але їхні наслідки, як правило, є тимчасовими і піддаються плануванню.

VI група – репутаційно-цифрові загрози на нашу думку має середню пріоритетність, що зумовлюється не незначністю наслідків, а механізмом реалізації. Так, репутаційні загрози діють виключно через опосередкований канал із тривалим часовим лагом між подією та фінансовими втратами, що зменшує їхню безпосередню критичність, але водночас ускладнює їх кількісне вимірювання та можливість управління. Водночас репутаційні загрози часто є похідними від реалізації загроз вищих груп (наприклад, кіберінцидентів), а, отже їхня відносна пріоритетність не означає можливості ігнорування.

Проведена ідентифікація та систематизація загроз, виявлення впливу на фінансовий стан та обґрунтування пріоритетності обумовлюють необхідність проведення критичного аналізу існуючих інструментів забезпечення фінансової безпеки, оцінки ступінь їх адаптованості до умов діяльності ІТ-підприємств. Критичний аналіз інструментів забезпечення фінансової безпеки потребує чіткого визначення критеріїв оцінки їх адаптованості до специфіки ІТ-підприємств. Під інструментами забезпечення фінансової безпеки будемо розуміти сукупність методів, механізмів і процедур, застосування яких дозволяє запобігти реалізації загроз, мінімізувати їх дослідження або забезпечити відновлення фінансової стійкості підприємства після їх реалізації. Для оцінки ступеня адаптованості кожного інструменту до умов ІТ-підприємств пропонуємо використати наступні критерії:

– *відповідність природі активів* – наскільки інструмент орієнтований на захист нематеріальних, а не матеріальних активів.

– *технологічна сумісність* – здатність інструменту функціонувати в цифровому операційному середовищі без суттєвої модифікації.

– *швидкість реагування* – спроможність реагувати на загрози в режимі реального часу, характерному для цифрового середовища.

– *масштабованість* – придатність інструменту для підприємств різного розміру з урахуванням ФОП-структури українського ІТ-ринку.

– *доступність в українському контексті* – наявність правових, інституційних та ринкових умов для застосування інструменту в Україні в умовах воєнного стану.

На основі визначених критеріїв проведено оцінювання адаптованості основних інструментів фінансової безпеки до умов функціонування ІТ-підприємств, результати якого узагальнено в табл. 3.

Таблиця 3

Критична оцінка адаптованості інструментів фінансової безпеки до умов функціонування і розвитку ІТ-підприємств

Інструмент	Відповідність природи активів	Технологічна сумісність	Швидкість реагування	Доступність в Україні	Загальний ступінь адаптованості
Фінансовий аналіз (традиційний)	Низька	Середня	Низька	Висока	**Низький**
Бюджетування	Середня	Середня	Низька	Висока	**Середній**
Диверсифікація	Середня	Середня	Середня	Висока	**Середній — високий**
Страхування (традиційне)	Низька	Низька	Середня	Низька	**Низький**
Кіберстрахування	Висока	Висока	Середня	Низька	**Середній** (потенційно високий)
Внутрішній аудит і контроль	Середня	Середня	Низька	Висока	**Середній**
Хеджування валютних ризиків	Середня	Середня	Висока	Низька	**Низький – середній**
RegTech-рішення	Висока	Висока	Висока	Середня	**Середній**
Системи збору, аналізу та кореляції подій безпеки в режимі реального часу (SIEM-системи)	Висока	Висока	Висока	Середня	**Високий**
Хмарні і фінансові платформи	Висока	Висока	Висока	Висока	**Високий**
Автоматизовані системи управління контрактами (CLM-системи)	Висока	Висока	Висока	Середня	**Високий**

Джерело: розроблено автором на основі [19-22].

Проведений аналіз дозволив зробити такі проміжні висновки і узагальнення. По-перше**,** більшість традиційних інструментів фінансової безпеки мають низький або середній рівень адаптованості до умов ІТ-підприємств. Це пов’язано з тим, що вони орієнтуються на матеріальні активи, стабільні грошові потоки та розвинені фінансові ринки, жодна з цих рис не є характерною для ІТ-підприємств. По-друге**,** найбільш критичний дефіцит інструментів саме в тих групах загроз, які мають найвищу пріоритетність (кіберфінансових загрозах і загрозах інтелектуального капіталу). Наявні традиційні інструменти практично не охоплюють ці групи, тоді як сучасні цифрові інструменти є або нерозвиненими на українському ринку, або недоступними для малого та середнього ІТ-бізнесу. По-третє**,** існує системний розрив між концептуальною релевантністю інструменту та його практичною доступністю в українському контексті. Так, кіберстрахування, хеджування та частина RegTech-рішень є теоретично придатними інструментами, але через нерозвиненість відповідних ринків і регуляторні обмеження воєнного часу є практично недоступними для вітчизняних ІТ-підприємств. По-четверте, найбільш адаптованими до умов ІТ-підприємств є цифрові інструменти – SIEM-системи, хмарні фінансові платформи та CLM-системи, – однак вони охоплюють лише частину численних загроз і не формують цільної системи фінансової безпеки.

Вищезазначене зумовлює потребу в розробці комплексної класифікації інструментів фінансової безпеки, адаптованої до умов ІТ-підприємств, яку вважаємо доцільним побудувати на логіці управління реагування на загрози: «передбачити – визначити – захистити – відновити», у контексті чого пропонуємо виділити наступні функціональні групи інструментів: превентивні, моніторингові, захисні, відновлювальні (табл. 4).

Таблиця 4

Класифікація інструментів фінансової безпеки ІТ-підприємств за функціональними групами

Функціональна група	**Цільова функція**	**Часовий горизонт**	**Критерій ефективності**	Ключові інструменти	**Специфіка для ІТ**
1	2	3	4	5	6
1. Превентивні (профілактичні) інструменти	попередження виникнення загрози або суттєве зниження ймовірності їх реалізації до настання фінансових втрат.	постійна дія, довготривалий характер.	зниження частоти реалізації загроз і зменшення розміру завданих збитків.	1.1. Інструменти управління клієнтськими ризиками: – диверсифікація клієнтського портфеля**;** – контрактне структурування з елементами фінансового захисту; – географічна та юрисдикційна диверсифікація. 1.2. Інструменти управління кадровими ризиками: – програми утримання ключових спеціалістів; – документування знань і процесів; – розподілені команди в різних юрисдикціях. 1.3. Інструменти управління технологічними ризиками: – політика мультихмарної інфраструктури; – технологічний аудит і управління технічним боргом; – впровадження стандартів інформаційної безпеки. 1.4. Інструменти управління регуляторними ризиками: – комплаєнс-програми; – юридичний супровід контрактної діяльності	Акцент на кадрових і технологічних інструментах
2. Моніторингові інструменти	безпечне забезпечення індикаторів реалізації загроз і відхилення від нормального стану фінансової до настання повноцінних фінансових втрат.	безперервний режим реального часу або регулярні цикли оцінювання.	мінімізація часового лагу між виникненням загрози та початком управлінського реагування.	2.1. Системи фінансового моніторингу: – дашборди фінансових метрик у реальному часі; – система раннього передування на основі порогових значень; – прогнозування грошових потоків з ковзним горизонтом. 2.2. Системи кібербезпекового моніторингу з фінансовим виміром: – SIEM-системи; – моніторинг SLA-виконання; – моніторинг цифрової репутації. 2.3. Інструменти моніторингу кадрових ризиків: – показник аналітики управління персоналом для визначення ризику відтоку; – моніторинг концентрації критичних компетенцій**.** 2.4. Інструменти моніторингу ринкових і регуляторних змін: – регуляторний моніторинг; – конкурентна розвідка і технологічний моніторинг.	Цифрові метрики (щомісячний регулярний дохід - MRR, рівень відтоку клієнтів - churn, швидкість витрачання грошових коштів - burn rate)

Закінчення таблиці 4

1	2	3	4	5	6
III. Захисні інструменти	мінімізація фінансових втрат у момент реалізації загрози, локалізація її наслідків і запобігання каскадному розширенню збитків.	ситуативна активація при виявленні загрози або її реалізації.	мінімізація розміру фактичних фінансових втрат з боку потенційно можливими.	3.1. Фінансові захисні інструменти: – резервний фонд фінансової безпеки; – кредитні лінії та механізми екстреного фінансування; – механізми валютного захисту. 3.2. Кіберзахисні інструменти з фінансовим виміром: – план реагування на кіберінциденти; – системи резервного копіювання та відновлення; – кіберстрахування. 3.3. Контрактні захисні інструменти: – механізми форс-мажорного реагування; – ескроу-механізми та акредитиви; – CLM-системи в режимі захисту. 3.4. Кадрові захисні інструменти: – програми екстреного перерозподілу завдань; – контрактний захист інтелектуальної власності.	Кіберзахисні та контрактні інструменти
IV. Відновлювальні інструменти	відновлення фінансової стійкості, операційної продуктивності та ринкових позицій підприємства після реалізації загрози.	активація після реалізації загрози, короткостроковий і середньостроковий горизонт відновлення.	швидкість і повне відновлення до стану, що передував реалізації загрози, або досягнення нового стійкого стану.	4.1. Фінансові відновлювальні інструменти: – антикризові фінансові програми; – реструктуризація боргових зобов'язань; – залучення антикризового фінансування. 4.2. Операційні відновлювальні інструменти: – план забезпечення безперервності бізнесу; – програми швидкого відновлення клієнтських відносин. 4.3. Репутаційні відновлювальні інструменти: – антикризові PR-програми; – програми відновлення довіри клієнтів і партнерів; 4.4. Кадрові відновлювальні інструменти: – прискорені програми найму та адаптації нових робітників; – програми передачі знань і реконструкції компетенцій.	Швидкість відновлення операційної спроможності

Джерело: розроблено автором на основі [7; 16; 17; 23; 24].

324

Превентивні інструменти діють на постійній основі та орієнтовані на зниження самої ймовірності реалізації загроз; *моніторингові* – забезпечують безперервне спостереження й мінімізують часовий лаг між виникненням загрози та управлінською реакцією; *захисні* активуються ситуативно і спрямовані на локалізацію збитків у момент реалізації загрози; *відновлювальні* - забезпечують повернення підприємства до стійкого стану після зазнаних збитків.

Вважаємо, що принципова відмінність запропонованої класифікації від наявних у дослідженнях полягає в тому, що кожна група інструментів розроблена з урахуванням специфічних загроз цифрового середовища, активів нематеріальної природи та кадрової критичності ІТ-підприємств. На нашу думку, збалансований розвиток усіх чотирьох груп інструментів є необхідною умовою формування комплексної системи фінансової безпеки підприємств ІТ-галузі.

Отже, ІТ-підприємства принципово відрізняються від суб'єктів господарювання традиційних галузей, а система інструментарію фінансової безпеки охоплює не лише стан фінансових ресурсів і грошових потоків, а й захист нематеріальних активів, операційну спроможність у цифровому середовищі та стратегічний кадровий потенціал. Тобто усе те, що в сукупності визначає здатність підприємства генерувати додаткову вартість і виконувати зобов’язання перед контрагентами. З урахуванням виявленої специфіки загроз, інструментів та операційного середовища виникає необхідність уточнення самого поняття фінансової безпеки щодо ІТ-підприємств.

На нашу думку, фінансова безпека ІТ-підприємства – це динамічний стан захисту його фінансових інтересів, активів і грошових потоків від конкретних загроз цифрового середовища, що забезпечується через комплекс превентивних, моніторингових і захисних інструментів та дозволяє підприємству гарантувати фінансову стійкість, виконувати зобов'язання перед контрагентами й реалізовувати стратегічний потенціал розвитку в умовах невизначеності, кіберзагроз, волатильності цифрових ринків та воєнної нестабільності.

Проведений критичний аналіз існуючих інструментів та розроблена функціональна класифікація (табл. 4) дозволяє стверджувати, що жоден із відзначених інструментів не забезпечує комплексного захисту фінансових інтересів ІТ-підприємства самостійно. Лише зважене поєднання інструментів з урахуванням конкретного масштабу підприємства та його бізнес-моделі, здатна створити забезпечити належний рівень безпеки у мовах ризику і невизначеності зовнішнього і внутрішнього середовища, що обумовлює необхідність диференційованого підходу до формування системи фінансової безпеки залежно від розміру підприємства (малі ІТ-підприємства та стартапи, середні і великі підприємства) та його бізнес-моделі.

Реалізуючи цей підхід, у таблиці 5 систематизовано рекомендований мінімальний набір інструментів для кожної групи ІТ-підприємств, структурований за чотирма функціональними групами інструментів, що на нашу думку дозволить ІТ-компаніям самостійно оцінити достатність власної системи захисту та визначити напрями її розвитку відповідно до етапу зростання компанії.

Зауважимо, що малий бізнес та стартапи переважним чином зосереджуються на базовому захисті за принципом «мінімальна вартість – максимальна ефективність». Для нього ключовим є диверсифікація клієнтської бази, стандартизація контрактів, простий моніторинг грошових потоків і формування резервного фонду на 2–3 місяці. Для середніх підприємств характерне розширення інструментарію у всіх функціональних групах (додаються формальні комплаєнс-програми (ISO 27001, GDPR), системи моніторингу безпеки (SIEM), контрактні механізми (CLM, ескроу), повноцінний план безперервності

бізнесу (BCP) та план відновлення після катастроф (DR)). Великі підприємства впроваджують інтегровані платформи управління ризиками, цілодобовий центр управління безпекою (SOC), корпоративні програми захисту інтелектуальної власності та міжнародне кіберстрахування, а також формують спеціалізовані антикризові команди та бюджети. Таким чином, перехід від малого до великого масштабу бізнесу супроводжується зростанням глибини, автоматизації та інтеграції інструментів захисту фінансової безпеки.

Таблиця 5

Рекомендовані інструменти забезпечення фінансової безпеки за масштабом ІТ-підприємства

Функціональна група	Мале підприємство / стартап (до 50 осіб)	Середнє підприємство (50–300 осіб)	Велике підприємство (понад 300 осіб)
Превентивні	– диверсифікація клієнтів (≤30% виручки на одного); – стандартизація контрактів із авансами та форс-мажорними застереженнями; – базова документація процесів і знань; – двофакторна автентифікація, базова політика інформаційної безпеки (ІБ)	– Формальна диверсифікація (≤20–25% виручки на одного); – ESOP / довгострокове утримання ключових фахівців; – впровадження ISO 27001 або SOC 2; – комплаєнс-програма з GDPR, призначення відповідальної особи; – мультихмарна / гібридна інфраструктура	– виділена функція CISO / CRO (директор з інформаційної безпеки / директорі з управління ризхиками); – корпоративна програма управління ризиками (ISO 31000, COSO ERM) з адаптацією до воєнних умов; – програма захисту ІВ (патентування, торгові марки); – повноцінний міжнародний комплаєнс (оподаткування, загальний регламент про захист даних (GDPR), галузеві стандарти)
Моніторингові	– щотижневий моніторинг грошових потоків (13 тижнів); – просте табло (дашборд) з 3–5 метриками (MRR, burn rate, runway, active clients); – базові алерти безпеки від хмарного провайдера	– розширений фінансовий дашборд із цифровими метриками – базова система управління інформаційною безпекою та подіями (SIEM) або хмарний SOC; – моніторинг індексу лояльності клієнтів (NPS) та цифрової репутації; – Квартальний аналіз концентрації клієнтів і кадрових ризиків	– інтегрована платформа управління ризиками (єдина панель); – повноцінний SOC 24/7; – автоматизована система раннього попередження на основі ML для фінансових аномалій
Захисні	– резервний фонд на 2–3 місяці операційних витрат; – регулярне резервне копіювання з перевіркою відновлення; – базовий план дій при втраті ключового клієнта або фахівця	– резервний фонд на 3–4 місяці; – формалізований план реагування на інциденти (IRP) із тестуванням; – CLM-система для управління контрактними ризиками; – Ескроу-механізми для великих проєктів	– повноцінне кіберстрахування на міжнародних ринках; – Детальні плани BCP/DR із регулярним тестуванням; – виділений антикризовий бюджет
Відновлювальні	– шаблон антикризової комунікації із замовниками; – список резервних підрядників; – розуміння умов доступних грантових програм	– повноцінний BCP (план безперервності бізнесу); – програма швидкого відновлення відносин із клієнтами після інциденту; – партнерство з рекрутинговими агентствами	– виділена антикризова команда; – програми міжнародної релокації персоналу; – деталізовані сценарії BCP для різних типів загроз

Джерело: розроблено автором на основі [1-5; 9; 17; 25-27].

Крім масштабу підприємства, критичним фактором, що визначає склад пріоритетних інструментів фінансової безпеки, є бізнес-модель ІТ-компанії. Аутсорсинг, продуктовий бізнес та SaaS-модель мають принципово різні профілі загроз: від високої клієнтської концентрації та проєктного характеру грошових потоків в аутсорсингу до чутливості до репутаційних інцидентів і технологічного застарівання у продуктових компаніях, а також надвисокої залежності від довіри клієнтів до безпеки даних у SaaS. Відповідно, система інструментів для кожної моделі має власні акценти, які систематизовано нами в табл. 6.

Таблиця 6

Специфічні інструменти за бізнес-моделлю

Бізнес-модель	Ключові загрози	Пріоритетні інструменти	Спеціальні рекомендації
Аутсорсинг	– висока клієнтська концентрація; – проєктний характер грошових потоків; – критична залежність від кадрів	– контрактні інструменти: детальне регулювання оплати, форс-мажору, SLA; – управління кадровими ризиками; – диверсифікація клієнтів за географією та галузями	формування контрактного буфера ліквідності (авансові платежі ≥20–30% вартості контракту)
Продуктове ІТ	– рекурентні доходи; – ризик технологічного застарівання; – відтік підписників	– моніторинг рівня відтоку клієнтів та NPS; – захист інтелектуальної власності; – резервний фонд для циклу розробки нової версії	формування технологічного резервного фонду – бюджет на оновлення продукту
SaaS	– найбільш прогнозовані грошові потоки; – надвисока чутливість до репутаційних інцидентів та кіберзагроз	– кіберзахист найвищого рівня; – сертифікація безпеки (SOC 2 Type II) як сигнал довіри; – детальні SLA з прозорими механізмами компенсацій	формування SLA-резервного фонду для виплати компенсацій без загрози загальній ліквідності

Джерело: розроблено автором на основі [1; 5; 8; 10; 11].

Як видно з таблиці 6 бізнес-модель визначає не лише структуру доходів, а й специфічний набір інструментів захисту. Так, для аутсорсингових компаній, чия вразливість зумовлена високою концентрацією виторгу на окремих клієнтах і проєктною природою контрактів, пріоритетними є контрактні механізми (авансування, деталізація форс-мажору) та формування контрактного буфера ліквідності (20–30% авансу), що знижує ризик раптового скорочення доходу. Натомість продуктові ІТ-підприємства зосереджуються на захисті від технологічного застарівання та відтоку підписників. Для них ключовими є моніторинг поведінкових метрик, захист інтелектуальної власності та створення технологічного резервного фонду (цільового бюджету для оновлення продукту в разі падіння виторгу). SaaS-компанії, які працюють за найбільш передбачуваною моделлю доходу, водночас є найбільш чутливими до кіберінцидентів і репутаційних втрат. Їхній захист базується на найвищих стандартах безпеки (SOC 2 Type II), прозорих SLA та формуванні SLA-резервного фонду для гарантованого покриття компенсацій клієнтам без загрози основній ліквідності.

Таким чином, диференціація інструментарію за бізнес-моделлю на нашу думку дозволить ІТ-підприємствам спрямовувати обмежені ресурси на нейтралізацію найбільш характерних для їхньої моделі загроз й підвищити тим самим загальну ефективність системи фінансової безпеки.

Висновки і перспективи подальших досліджень. У процесі проведеного дослідження було уточнено поняття фінансової безпеки ІТ-підприємства з урахуванням нематеріального характеру активів, цифрових бізнес-моделей та воєнних ризиків. Ідентифіковано та систематизовано шість груп специфічних загроз (кіберфінансові, інтелектуальному капіталу, контрактно-регуляторні, інфраструктурно-операційні, цифрових бізнес-моделей, репутаційно-цифрові) з визначенням їх пріоритетності та каналів впливу на фінансовий стан. Розроблено функціональну класифікацію інструментів забезпечення фінансової безпеки (превентивні, моніторингові, захисні, відновлювальні) та сформовано диференційовані рекомендації щодо їх застосування залежно від масштабу підприємства та бізнес-моделі.

Перспективи подальших досліджень полягають у розробці методики кількісної оцінки ефективності впровадження запропонованих інструментів, а також адаптації системи фінансової безпеки до умов повоєнного відновлення економіки України та вимог новітніх регуляторних актів ЄС.

Список використаних джерел

1. 2025 річний звіт. Система виявлення вразливостей і реагування на кіберінциденти та кібератаки. Державний центр кіберзахисту державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=73033.

2. Federal Bureau of Investigation. 2022 internet crime report. Internet Crime Complaint Center. 2023. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

3. Federal Bureau of Investigation. 2023 internet crime report. Internet Crime Complaint Center. 2024. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

4. Federal Bureau of Investigation. 2024 internet crime report. Internet Crime Complaint Center. 2025. URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

5. PwC. «Міжнародне аналітичне дослідження довіри до цифрових технологій, 2025»: ключові висновки для сектору фінансових послуг [Звіт]. PwC Україна. 2025. URL: https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey/banking-financial.html.

6. Стратегічні напрями інноваційного розвитку системи фінансово-економічної безпеки підприємства на основі цифрових технологій / О. Правдивець та ін. *Financial and Credit Activity Problems of Theory and Practice*. 2024. Vol. 6, no. 59. P. 273–282. DOI: https://doi.org/10.55643/fcaptp.6.59.2024.4575.

7. Rumyk I., Puzyrova P. Financial security of IT enterprises in the context of digitalization of the smart economy. *Economics, Finance and Management Review*. 2025. No. 1(21). P. 85–97. DOI: https://doi.org/10.36690/2674-5208-2025-1-85-97.

8. Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Socio-economic relations in the digital society*. 2021. № 3(42). С. 55–61. URL: https://ser.net.ua/index.php/SER/article/download/440/437.

9. Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу / О. О. Захаркін та ін. 2023. № 10. URL: https://essuir.sumdu.edu.ua/server/api/core/bitstreams/a0693020-347a-4771-b39b-42e0ea6e04f5/content.

10.Мохненко А. С., Антонов Р. А. Характеристика основних факторів конкурентоспроможності підприємств ІТ сфери в умовах воєнного стану. *Проблеми сучасних трансформацій. Серія: економіка та управління*. 2025. № 17. URL: https://elibrary.ru/item.asp?id=81524649.

11.Данилюк І. Управління ризиками в ІТ-бізнесі. *Світ фінансів*. 2023. № 3(76). С. 105–114. URL: http://sf.wunu.edu.ua/index.php/sf/article/view/1635 (дата звернення: 26.03.2026).

12.Лук'янова В. В., Маліцький Р. І. Якісний аналіз та кількісне оцінювання ризику підприємств в Україні за умов війни: фокус на ІТ-сектор. *Здобутки економіки: перспективи та інновації*. 2025. № 25. URL: https://econp.com.ua/index.php/journal/article/download/737/694.

13.Cyber Risk And Business Resilience: A Financial Perspective On IT Security Investment Decisions / S. S. Panchal et al. *The American Journal of Engineering and Technology*. 2025. Vol. 7, no. 09. P. 23–48. DOI: https://doi.org/10.37547/tajet/Volume07Issue09-04.

14.Шишкіна О. В. Механізм управління фінансовими ризиками промислових підприємств: теорія, методологія, практика : монографія. Чернігів : ЧНТУ, 2020. 318 с.

15.Шишкіна О. В., Суховерський М. Ю., Даньков А. Ю. Оцінка впливу фінансових інструментів на економічну безпеку підприємств. *Науковий вісник Полісся*. 2025. № 1(30). С. 160–179. DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-160-179.

16.Шишкіна О. В., Бойчук Т. Т., Євчук Д. В. Вплив цифрових технологій на фінансовий ризик-менеджмент та безпеку транспортних і аграрних підприємств. *Проблеми і перспективи економіки та управління*. 2025. № 2(42). С. 337–360. DOI: https://doi.org/10.25140/2411-5215-2025-2(42)-337-360.

17.Deloitte. From reactive compliance to proactive command: How ITAM enables regulatory compliance. Deloitte UK. 2026. URL: https://www.deloitte.com/uk/en/Industries/technology/blogs/how-itam-enables-regulatory-compliance.html.

18.Janas T. Digital risks, real board accountability. *Warsaw Business Journal*. 2025, August 25. URL: https://wbj.pl/digital-risks-real-board-accountability/post/147006 (дата звернення: 26.03.2026).

19.6Wresearch. Ukraine cybersecurity insurance market (2025-2031): Outlook, trends, forecast, growth, size, analysis, industry, value, share, companies & revenue (Report No. ETC4386018). 2025. URL: https://www.6wresearch.com/industry-report/ukraine-cybersecurity-insurance-market.

20.6Wresearch. Ukraine cyber (liability) insurance market (2025-2031): Segmentation, forecast, size & revenue, trends, outlook, value, companies, competitive landscape, industry, growth, analysis, share (Report No. ETC9898907). 2025. URL: https://www.6wresearch.com/industry-report/ukraine-cyberliability-insurance-market.

21.GRC PROS Blog. SOC 2 Type 2 vs. ISO 27001: A deep dive comparison for third-party assurance in GRC [LinkedIn post]. 2025, September 27. URL: https://www.linkedin.com/posts/grc-pros-blog_soc-2-type-2-vs-iso-27001-a-deep-dive-comparison-activity-7378141455053316096-9gim.

22.SmartSuite. 10 best risk management software & tools in 2026. *SmartSuite Blog*. 2025, December 11. URL: https://www.smartsuite.com/blog/risk-management-software.

23.msg-insurance-suite. New reporting requirements for insurers and IT service providers – Part 2: Emerging obligations for software vendors, managed service providers, and cloud service providers. *msg-insurance-suite Blog*. 2025, September 12. URL: https://msg-insurance-suite.com/blog/rethinking-insurance/new-reporting-requirements-for-insurers-and-it-service-providers-part-2/.

24.Modern Requirements. Modern requirements for AI-driven financial compliance: From obligation to evidence across DORA, NIST, ISO 27001, SOC 2, and PCI DSS. *Modern Requirements Blog*. 2026, January 27. URL: https://www.modernrequirements.com/blogs/ai-driven-financial-compliance/.

25.CyRAACS. How FinTechs can build a future-ready compliance strategy: SOC 2, DPDP Act, RBI & ISO requirements. *CyRAACS Blog*. 2026, January 8. URL: https://cyraacs.com/how-fintechs-can-build-a-future-ready-compliance-strategy/.

26.ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/ru/standard/27001.

27.What is SOC 2®? *Secureframe*. URL: https://secureframe.com/hub/soc-2/what-is-soc-2.

References

1. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy [State Service of Special Communications and Information Protection of Ukraine]. (2025). *2025 richnyi zvit. Systema vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky* [*2025 annual report. Vulnerability detection and cyber incident/attack response system].* https://cip.gov.ua/services/cm/api/attachment/download?id=73033.

2. Federal Bureau of Investigation. (2023). *2022 internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

3. Federal Bureau of Investigation. (2024). *2023 internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

4. Federal Bureau of Investigation. (2025). *2024 internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

5. PwC Ukraine. (2025). *«Mizhnarodne analitychne doslidzhennia doviry do tsyfrovykh tekhnolohii, 2025»: kliuchovi vysnovky dlia sektoru finansovykh posluh [Global digital trust insights*

survey 2025: Key findings for the financial services sector] [Report]. https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey/banking-financial.html.

6. Pravdyvets, O., Litvin, N., Denysov, O., Polishchuk, O., & Oliinyk, V. (2024). Stratehichni napriamy innovatsiinoho rozvytku systemy finansovo-ekonomichnoi bezpeky pidpryiemstva na osnovi tsyfrovykh tekhnolohii [Strategic directions of innovative development of the financial and economic security system of the enterprise based on digital technologies]. *Finansovo-kredytna diialnist: problemy teorii ta praktyky – Financial and Credit Activity: Problems of Theory and Practice*, *6*(59), 273–282. https://doi.org/10.55643/fcaptp.6.59.2024.4575.

7. Rumyk, I., & Puzyrova, P. (2025). Financial security of IT enterprises in the context of digitalization of the smart economy. *Economics, Finance and Management Review*, *1*(21), 85–97. https://doi.org/10.36690/2674-5208-2025-1-85-97.

8. Mekhed, A. M., & Varnalii, Z. S. (2021). Finansova bezpeka pidpryiemstv v umovakh tsyfrovoi ekonomiky [Financial security of enterprises in the conditions of digital economy]. *Sotsialno-ekonomichni vidnosyny v tsyfrovomu suspilstvi – Socio-economic Relations in the Digital Society,* (3), 55–61. https://ser.net.ua/index.php/SER/article/download/440/437.

9. Zakharkin, O. O., Zakharkin, A. A., Boiko, A. V., & Sokol, L. V. (2023). Tsyfrovi tekhnolohii ta instrumenty zabezpechennia finansovoi bezpeky biznesu [Digital technologies and tools for ensuring business financial security]. *Visnyk Sumskoho derzhavnoho universytetu – Sumy State University Bulletin*, (10). https://essuir.sumdu.edu.ua/server/api/core/bitstreams/a0693020-347a-4771-b39b-42e0ea6e04f5/content.

10.Mokhnenko, A. S., & Antonov, R. A. (2025). Kharakterystyka osnovnykh faktoriv konkurentospromozhnosti pidpryiemstv IT sfery v umovakh voiennoho stanu [Characteristics of the main factors of competitiveness of IT enterprises under martial law]. *Problemy suchasnykh transformatsii. Seriia: ekonomika ta upravlinnia – Problems of Modern Transformations. Series: Economics and Management*, (17). https://elibrary.ru/item.asp?id=81524649.

11.Danyliuk, I. (2023). Upravlinnia ryzykamy v IT-biznesi [Risk management in IT business]. *Svit finansiv – The World of Finance*, (3), 105–114. http://sf.wunu.edu.ua/index.php/sf/article/view/1635.

12.Lukianova, V. V., & Malitskyi, R. I. (2025). Yakisnyi analiz ta kilkisne otsiniuvannia ryzyku pidpryiemstv v Ukraini za umov viiny: fokus na IT-sektor [Qualitative analysis and quantitative assessment of enterprise risk in Ukraine under war conditions: Focus on the IT sector]. *Zdobutky ekonomiky: perspektyvy ta innovatsii – Achievements of the Economy: Perspectives and Innovations*, (25). https://econp.com.ua/index.php/journal/article/download/737/694.

13.Panchal, S. S., Ansari, I., Azim, K. S., Bhujel, K., & Ahirrao, Y. S. (2025). Cyber risk and business resilience: A financial perspective on IT security investment decisions. *The American Journal of Engineering and Technology*, *7*(09), 23–48. https://doi.org/10.37547/tajet/Volume07Issue09-04.

14.Shyshkina, O. V. (2020). *Mekhanizm upravlinnia finansovymy ryzykamy promyslovykh pidpryiemstv: teoriia, metodolohiia, praktyka [Mechanism of financial risk management of industrial enterprises: Theory, methodology, practice]*. Chernihivskyi natsionalnyi tekhnolohichnyi universytet.

15.Shyshkina, O. V., Sukhoverskyi, M. Yu., & Dankov, A. Yu. (2025). Otsinka vplyvu finansovykh instrumentiv na ekonomichnu bezpeku pidpryiemstv [Assessment of the impact of financial instruments on the economic security of enterprises]. *Naukovyi visnyk Polissia – Scientific Bulletin of Polissia*, *1*(30), 160–179. https://doi.org/10.25140/2410-9576-2025-1(30)-160-179.

16.Shyshkina, O. V., Boichuk, T. T., & Yevchuk, D. V. (2025). Vplyv tsyfrovykh tekhnolohii na finansovyi ryzyk-menedzhment ta bezpeku transportnykh i ahrarnykh pidpryiemstv [Impact of digital technologies on financial risk management and security of transport and agricultural enterprises]. *Problemy i perspektyvy ekonomiky ta upravlinnia – Problems and Prospects of Economics and Management*, *2*(42), 337–360. https://doi.org/10.25140/2411-5215-2025-2(42)-337-360.

17.Deloitte. (2026). *From reactive compliance to proactive command: How ITAM enables regulatory compliance*. Deloitte UK. https://www.deloitte.com/uk/en/Industries/technology/blogs/how-itam-enables-regulatory-compliance.html.

18.Janas, T. (2025, August 25). Digital risks, real board accountability. *Warsaw Business Journal*. https://wbj.pl/digital-risks-real-board-accountability/post/147006.

19.6Wresearch. (2025). *Ukraine cybersecurity insurance market (2025-2031): Outlook, trends, forecast, growth, size, analysis, industry, value, share, companies & revenue* (Report No. ETC4386018). https://www.6wresearch.com/industry-report/ukraine-cybersecurity-insurance-market.

20.6Wresearch. (2025). *Ukraine cyber (liability) insurance market (2025-2031): Segmentation, forecast, size & revenue, trends, outlook, value, companies, competitive landscape, industry, growth, analysis, share* (Report No. ETC9898907). https://www.6wresearch.com/industry-report/ukraine-cyberliability-insurance-market.

21.GRC PROS Blog. (2025, September 27). *SOC 2 Type 2 vs. ISO 27001: A deep dive comparison for third-party assurance in GRC* [LinkedIn post]. LinkedIn. https://www.linkedin.com/posts/grc-pros-blog_soc-2-type-2-vs-iso-27001-a-deep-dive-comparison-activity-7378141455053316096-9gim.

22.SmartSuite. (2025, December 11). *10 best risk management software & tools in 2026*. SmartSuite Blog. https://www.smartsuite.com/blog/risk-management-software.

23.msg-insurance-suite. (2025, September 12). *New reporting requirements for insurers and IT service providers – Part 2: Emerging obligations for software vendors, managed service providers, and cloud service providers*. msg-insurance-suite Blog. https://msg-insurance-suite.com/blog/rethinking-insurance/new-reporting-requirements-for-insurers-and-it-service-providers-part-2/.

24.Modern Requirements. (2026, January 27). *Modern requirements for AI-driven financial compliance: From obligation to evidence across DORA, NIST, ISO 27001, SOC 2, and PCI DSS*. Modern Requirements Blog. https://www.modernrequirements.com/blogs/ai-driven-financial-compliance/.

25.CyRAACS. (2026, January 8). *How FinTechs can build a future-ready compliance strategy: SOC 2, DPDP Act, RBI & ISO requirements*. CyRAACS Blog. https://cyraacs.com/how-fintechs-can-build-a-future-ready-compliance-strategy/

26.International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001.

27.Secureframe. (n.d.). *What is SOC 2®?* https://secureframe.com/hub/soc-2/what-is-soc-2.

Дата першого надходження статті до видання: 02.02.2026
Дата прийняття статті до друку після рецензування: 09.02.2026

UDC 336.7:004.056

Olena Shyshkina

Doctor of Economic Sciences, Professor,
Professor of the Department of Finance, Banking and Insurance,
Chernihiv Polytechnic National University (Chernihiv, Ukraine).
E-mail: shyshkina.olena.v@gmail.com. ORCID: http://orcid.org/0000-0002-8946-1027
ResearcherID: F-3208-2014. **Scopus Author ID:** 58995081900

FINANCIAL SECURITY INSTRUMENTS FOR IT ENTERPRISES IN THE DIGITAL ENVIRONMENT

The article substantiates the need to revise the theoretical and methodological foundations of ensuring the financial security of IT enterprises in light of rapid digitalization, the growing scale of cyber threats, wartime challenges, and the specific nature of IT-sector activities. It is demonstrated that traditional approaches to financial security – primarily focused on tangible assets and stable cash flows – are insufficiently effective for IT enterprises. The latter are characterized by a set of distinctive features, including the intangible nature of their assets (software code, data, reputation), a high dependence on human capital, a global digital operating model, non-standard cash flow structures (subscriptions, freemium models, royalties), and operation within cyberspace as the primary business environment.

Based on a proposed three-dimensional classification model (source, nature, and impact on financial condition), six qualitatively distinct groups of specific threats to the financial security of IT enterprises are identified and systematized: cyber-financial threats, digital business model threats, intellectual capital threats, contractual and regulatory threats, infrastructural and operational threats, and reputational-digital threats. For each group, the sources of origin, underlying nature, channels of impact (direct, indirect, dual), and priority levels (critical, high, medium) are determined and substantiated.

A critical analysis of existing financial security instruments is conducted using five criteria: alignment with the nature of assets, technological compatibility, response speed, scalability, and accessibility within the Ukrainian context. A systemic gap is identified between the conceptual relevance of certain instruments (such as cyber insurance and RegTech solutions) and their practical accessibility for domestic IT enterprises under martial law conditions. Among the most adaptable instruments are digital solutions, including SIEM systems, cloud-based financial platforms, and contract lifecycle management (CLM) systems.

A functional classification of financial security instruments is developed, encompassing four groups: preventive instruments (aimed at reducing the probability of threat realization), monitoring instruments (ensuring continuous observation and minimizing time lag), protective instruments (localizing losses at the moment of threat realization), and recovery instruments (facilitating a return to a stable state). For each group, the target function, time horizon, performance criteria, and key instruments are defined, taking into account the specific characteristics of IT enterprises.

Differentiated recommendations are formulated for designing a system of financial security instruments depending on enterprise scale (small/startups, medium-sized, large) and business model (outsourcing, product-based IT, SaaS). For each category, a minimum set of instruments is defined across functional groups, along with specific recommendations: a contractual liquidity buffer for outsourcing companies, a technological reserve fund for product-based firms, and an SLA-based reserve fund for SaaS enterprises.

The results obtained have practical value for owners and management of IT enterprises in developing comprehensive financial security systems, as well as for further academic research aimed at quantitatively assessing the effectiveness of the proposed instruments and adapting such systems to the requirements of emerging EU regulatory frameworks (NIS2, EU AI Act) in the context of post-war recovery.

Keywords: *financial security; IT enterprises; digitalization; threats; risks; traditional and digital financial security instruments; cyber-financial threats; digital environment; product-based IT; SaaS; outsourcing.*

Table: 6. References: 27.