Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2026. № 5.
ISSN 2307-2105

DOI: http://doi.org/10.32702/2307-2105.2026.5.203

УДК 330.658.012:004.056

Т. В. Капелюшна,
д. е. н., доцент, професор кафедри управління
кібербезпекою та захистом інформації,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: https://orcid.org/0000-0001-7490-6751
С. В. Легомінова,
д. е. н., професор, завідувач кафедри управління
кібербезпекою та захистом інформації,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: https://orcid.org/0000-0002-1825-0097
М. М. Запорожченко,
доктор філософії з кібербезпеки, доцент кафедри управління
кібербезпекою та захистом інформації,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: https://orcid.org/0000-0003-0182-9497

АНАЛІЗ ЦИФРОВИХ РИЗИКІВ У СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ІНТЕГРАЦІЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

T. Kapeliushna,
Doctor of Economics, Associate Professor, Professor of Departmentof Cybersecurity and Information Protection Management, State University of Information and Communication Technologies
S. Lehominova,
Doctor of Economics, Professor, Head of Departmentof Cybersecurity and Information Protection Management Department, State University of Information and Communication Technologies,
M. Zaporozhchenko,
Ph.D. in Cybersecurity, Associate Professor of Departmentof Cybersecurity and Information Protection Management, State University of Information and Communication Technologies

DIGITAL RISK ANALYSIS IN THE ENTERPRISE ECONOMIC SECURITY SYSTEM: INTEGRATION OF INFORMATION SECURITY AND BUSINESS CONTINUITY

У статті проаналізовано актуальні проблеми забезпечення економічної безпеки підприємства в умовах цифровізації економіки, активного впровадження платформних моделей бізнесу, хмарних технологій та розширення цифрової взаємодії суб'єктів господарювання. Обґрунтовано, що підтримання операційної стійкості та конкурентоспроможності обтяжується без формування комплексної системи захисту інформаційних активів, орієнтованої на резильєнтність та безперервність бізнес-процесів. На основі аналізу провідних міжнародних звітів (Allianz Risk Barometer, Cyber security resilience, Світового економічого форуму) констатовано домінування кіберінцидентів у структурі глобальних бізнес-ризиків для підприємств, які розглядаються не лише як технічна проблема, а як суттєвий фінансовий та стратегічний виклик.

Проведено аналіз структури інформаційних ризиків, який засвідчив критичне домінування загрози фішингу (62%), що підтверджує роль «людського фактора» як вразливої ланки в системі економічної безпеки. Оцінено поширеність шахрайства з платежами (37%), викрадення даних (32%) та внутрішніх загроз (20%). Доведено, цифрові ризики безпосередньо конвертуються у економічний збиток через недоотримання виторгу, зростання вартості залучення нових клієнтів та значні витрати на постфактум-усунення наслідків. Виявлено проблему, яка полягає у відсутності структуризації об'єктів захисту в єдиному фокусі економічної та інформаційної безпеки. З метою вирішення окресленої проблеми запропоновано та деталізовано інтегровану модель управління безпекою, яка системно поєднує бізнес-цілі підприємства, структуровані об'єкти захисту (за стандартом ISO/IEC 27002:2022) та відповідні домени інформаційної безпеки (CRC, IAM, Endpoint Security, захист даних та додатків).

The article analyzes the relevant issues of ensuring the economic security of enterprises in the context of rapid economic digitalization, the active implementation of platform business models, the proliferation of cloud technologies, and the expansion of digital interactions among economic entities. It is substantiated that maintaining operational stability and market competitiveness is impossible without forming a comprehensive system for protecting information assets, specifically focused on resilience and uninterrupted business process continuity. Based on a comprehensive review of leading reports (Allianz Risk Barometer, Cyber Security Resilience, World Economic Forum), the study establishes the absolute dominance of cyber incidents within the structure of global business risks. Consequently, these cyber threats are viewed not merely as technical vulnerabilities, but rather as critical financial and strategic challenges for corporate management. A detailed analysis of the information risk structure was conducted, revealing the prevalence of phishing attacks (62%), which confirms the "human factor" as the most vulnerable link in the overall economic security system. Furthermore, the high frequency of payment fraud

(37%), corporate data theft (32%), and insider threats (20%) was thoroughly evaluated.-A distinct scientific problem was identified regarding of proper structuring and specification of protection objects within the unified conceptual framework of economic and information security. To resolve this outlined problem, an integrated security management model is proposed and detailed. This model systematically aligns the strategic business objectives of the enterprise, structured protection objects (ISO 27002:2022), and their functional information security domains (CRC, IAM, Endpoint, data and application protection). Implementing this holistic model facilitates the transformation of information security from a secondary technical function into a primary strategic instrument for ensuring the economic resilience of the enterprise.

Ключові слова: *безпека підприємства, інформаційна безпека, економічна безпека підприємства, цифрові ризики, інформаційні активи, об'єкти захисту, безперервність бізнесу.*

Keywords: *enterprise security, information security, , economic security of the enterprise, digital risks, information assets, objects of protection, business continuity.*

Постановка проблеми. Підприємства функціонують у середовищі цифрових технологій та потребують використання інформаційних систем, хмарних сервісів, мережевої інфраструктури для автоматизоції бізнес-процесів. У таких умовах інформаційні активи стають важливим ресурсом забезпечення операційної діяльності, управлінських процесів і конкурентоспроможності підприємства. Водночас зростання кількості кіберінцидентів, фішингових атак, витоків даних, інформаційних маніпуляцій та порушень функціонування цифрової інфраструктури формує нові ризики для економічної стійкості підприємств і безперервності їх діяльності. Актуальність зазначеної проблеми посилюється тим, що більшість існуючих підходів до інформаційної безпеки зосереджуються

переважно на технічних аспектах кіберзахисту, не враховуючи їх прямого впливу на стратегічні бізнес-цілі, економічну безпеку та стійкість підприємства. Фрагментарність механізмів захисту, відсутність узгодженості між доменами інформаційної безпеки та бізнес-процесами, а також недостатній рівень інтеграції безпекових рішень у систему корпоративного управління призводять до зниження ефективності реагування на загрози та збільшення потенційних економічних втрат.

Особливої актуальності проблема набуває в умовах цифровізації економіки, розвитку платформних моделей бізнесу, використання хмарних технологій, API-інтеграцій та розширення цифрової взаємодії між суб'єктами господарювання. За таких умов забезпечення економічної безпеки підприємства неможливе без формування комплексної системи захисту інформаційних активів, орієнтованої на підтримку цифрової стійкості, адаптивності та безперервності бізнес-процесів.

Аналіз останніх досліджень та публікацій. Проблематика забезпечення безпеки суб'єктів господарювання, з акцентом на її інформаційну складову, перебуває у фокусі уваги науковців. Значний внесок у теоретико-методологічне обґрунтування засад інформаційної безпеки в загальній системі економічної безпеки підприємства зроблено такими вітчизняними та закордонними вченими, як Ситайло У., Маковець О., Дрозд І, Насіменто Д., Старченко Г., Дячек О.Ю., Рябченко А.М. та Пантос С. Питанням управління безпекою підприємства з детермінацією та комплексним аналізом ризиків за умов активної цифровізації бізнес-процесів та взаємодії суб'єктів господарювання у кіберпросторі ґрунтовно розглянуто у наукових доробках Захарової О., Фернандеса Р., Заблуківського А.В., Віджая Б., Мадіаваті П. та Прадана М.

Окремий напрям досліджень спрямовано на вивчення впливу технічних складових на рівень економічної безпеки. Зокрема, фахівці Центру кібербезпеки О. Скіцько та Р. Ширшов обґрунтовують тезу, що кібербезпека безпосередньо взаємопов'язана з економічною стабільністю через систему

метрик, якими визначається ефективність функціонування систем управління інформаційною безпекою (СУІБ). Також на тісному зв'язку між економічною та інформаційною безпекою й впливі останньої на загальну стійкість підприємства наголошують у своїх працях: Білозерцев В., Проскурович О. та Лисецький М. Однак, прослідковується відсутність однозначної дефініції та структуризації об'єктів захисту в єдиному фокусі економічної та інформаційної безпеки, що ускладнює для підприємств процес формування релевантних стратегій руху до цільових орієнтирів безпеки. Безперечно, наукові результати авторів заслуговують на увагу, проте водночас потребують подальшого розвитку, зокрема у напрямі конкретизації, чіткого окреслення й класифікації об'єктів захисту для підвищення ефективності управління ризиками та забезпечення безперервності бізнесу.

Формулювання цілей статті. Оцінити цифрові ризики підприємств та сформувати інтегровану модель управління безпекою, яка поєднує об'єкти інформаційного захисту, функціональні домени інформаційної безпеки, стандарти забезпечення безперебійного функціонування бізнесу.

Виклад основного матеріалу дослідження. Безпека та захист в умовах невизначеності та глобальних викликів є потребою забезпечення резильєнтості підприємства і є найбільш затребуваною до вирішення серед проблем, перед якими постає суспільство. Потреба у гарантіях безпеки наразі розглядається на всіх рівнях, починаючи від індивіда – до глобального рівня, зважаючи на коваріативні шоки (рідкісні події, що впливають на суспільство), ідіосинкратичні потрясіння (події, що чинять вплив на домогосподарство, сім'ю), політичні та економічні кризи, які виникають на тлі розподілу ресурсів. Інформація, що поширюється загалом у світі стає інструментом впливу на свідомість та світосприйняття, тим самим посилюючи когнітивні викривлення та породжуючи ще більшу невизначеність. Інформаційний актив є повноцінним ресурсом, що відіграє важливу роль в забезпеченні безпеки підприємства, оскільки інформаційна складова остаточно трансформувалася з вузькотехнічної функції у

детермінанту економічної стійкості підприємства, визначаючи здатність організації не лише захищати власні активи, а й підтримувати життєздатність у критичних умовах.

Окрім того, активне використанні штучного інтелекту, водночас із технологічним проривом, спричинило появу нових загроз, а саме: від деградації систем верифікації персоналу та фінансових транзакцій через генеративні фальсифікації до виникнення етичних дилем у стратегіях динамічного ціноутворення. Такі ризики безпосередньо впливають на репутаційний капітал, що є вагомим чинником при прийнятті рішень стейкхолдерами, оскільки будь-яка асиметрія інформації або маніпуляція довірою призводить до варіацій ринкової вартості компанії.

В умовах активної цифровізації бізнес-процесів і суспільних послуг інформаційна складова безперечно займає чільне місце серед складових економічної безпеки. Про інформаційне забезпечення як інструмент моніторингу ринку йдеться у праці Захарова О.І., в якій система інформаційної безпеки підприємства представлена двома взаємозалежними підсистемами, що функціонують у межах єдиного алгоритму: підсистеми інформаційного забезпечення, яка реалізує повний цикл моніторингу ринкового середовища – від легітимного пошуку та систематизації достовірних даних до підготовки аналітичних документів, необхідних для прийняття ефективних управлінських рішень. Водночас підсистема захисту забезпечує збереження інформаційних ресурсів та інтелектуальної власності шляхом інтеграції комплексу організаційних заходів, інженерно-технічних засобів та правових інструментів попередження несанкціонованого доступу. [1].

Забезпечення безперервності бізнесу в Україні розглядається науковицею Ситайло У., якою серед загроз бізнесу виокремлено збої та втручання в інформаційно-технологічні системи, а одним із інструментів вирішення проблеми виступає кібербезпека [2]. Авторами Маковець О., Дрозд І. кібербезпека розглядається як невід’ємна частина забезпечення економічної безпеки підприємства і тлумачиться як специфічний стан

інформаційної системи, за якого ефективно нівелюються загрози для конфіденційності, цілісності та доступності даних, що обробляються суб'єктами господарювання [3]. Забезпечення безпеки корпоративних даних базується на дотриманні принципів тріади CIA, що охоплює конфіденційність, цілісність та доступність інформації. Так науковиці Дячек О. та Рябченко А. розглядають у своїй праці дану модель як дескриптивний стандарт для оцінки ефективності систем захисту від несанкціонованого доступу та витоків конфіденційної інформації, виокремлюючи види ризиків, основні елементи захисту, проте не фіксують їх як об'єкти захисту [4].

У наукових доробках значна увага приділяється ризикам, підкреслюється багатовимірна природа ризиків, асоційованих із втратою цифрових активів, які супроводжують їх протягом усього життєвого циклу – від ініціації до деструкції. Доведено, що на початкових етапах генерації активів домінують ендогенні технологічні вразливості, зокрема архітектурні помилки в проєктуванні систем та недосконаліть криптографічних протоколів, що посилюються кіберзагрозами. У фазах активного зберігання та експлуатації пріоритетними стають організаційно-поведінкові ризик-фактори: неефективне управління ключами доступу, недостатній рівень цифрової компетентності користувачів та нехтування нормами кібергігієни. Фінальні стадії життєвого циклу активу (трансфер, спадкування або ліквідація) характеризуються домінуванням правових та юрисдикційних викликів, обумовлених відсутністю уніфікованих механізмів верифікації прав власності та законодавчими колізіями [5].

Окрему групу ризиків представляють інформаційні, зокрема представлена реактивна модель захисту від ризиків та управління ними задля забезпечення безперервності бізнесу. У праці Фернагдеса Р. [6] запропоновано проводити управління через експозицією загроз TEM (Threat Exposure Management,), за якою, на відміну від традиційних методів, передбачається випереджувальне виявлення потенційних вразливостей ще до моменту їхньої активації зловмисниками для запобігання дороговартісних

інциденті та мінімізації ризиків до їхньої ескалації у масштабні кризи. Сутність ТЕМ полягає у безперервному моніторингу агресивних онлайн-середовищ, зокрема тіньового сегмента інтернету (Dark Web), спеціалізованих хакерських форумів та некоректно конфігурованих хмарних сховищ, що дозволяє вчасно ідентифікувати скомпрометовані облікові дані, відкриті масиви конфіденційної інформації та інші деструктивні фактори.

Не залишається поза увагою питання впливу інформаційної безпеки на безперервність бізнесу та показники ефективності підприємства. Фахівці з Центру кібербезпеки констатують, що управління інформаційною безпекою позначається на економічних ефектах, зокрема зниженні фінансових втрат від інцидентів безпеки (втрати даних, перерв у бізнес-процесах, регуляторних штрафів) та зростання загальної продуктивності праці завдяки надійності інформаційних систем. Окрім економічних аспектів, експерти виділяють метрики, спрямовані на оцінку динаміки зниження ризиків через ідентифікацію та нівелювання загроз, ефективності процедур відновлення роботи після збоїв (часові та ресурсні витрати), а також ступеня забезпечення комплаєнсу відповідно із вимогами законодавства і галузевих стандартів. Інструментарій оцінювання вищезазначених показників ґрунтується на застосуванні методів фінансового та статистичного аналізу, проведенні аудитів безпеки та соціологічних опитуваннях співробітників [7].

Білозерцев В. зазначає, що недоотримання запланованого річного виторгу через відтік клієнтів (у середньому близько 5-8% залежно від галузі), та, по-друге, зростання вартості залучення нових клієнтів. Крім того, іншим важливим чинником є витрати на усунення наслідків та посилення захисту після інциденту. За даними аналізу джерел, понад половина організацій, що пережили витік, змушені збільшити бюджети на кібербезпеку після інциденту, інвестуючи в модернізацію систем безпеки, аудити, навчання персоналу та впровадження засобів виявлення загроз [8]. Науковця Проскурович О. вважає, що економічний аналіз кібербезпеки розглядає цифрові ризики як фінансовий та стратегічний виклик, що вимагає оцінки

захисту бізнесу. Цифрові технології є засобом забезпечення економічної безпеки, оскільки підвищують прозорість та ефективність рішень. Проте, їх впровадження супроводжується кіберзагрозами, що потребують вдосконалення регулювання та забезпечення кіберстійкості [9]. З причин щоденного накопичення масивів даних Лисецький М.Ю. наголошує на важливості захисту корпоративних баз даних як елемента економічної безпеки підприємства. Автор ідентифікує слабо контрольований доступ та зловживання користувачів привілеями доступу як найбільші ризики, пропонує впровадження суворого обліку та принципу мінімально необхідних прав доступу. Для ефективної нейтралізації комплексу загроз, включаючи ін'єкційні атаки та DDoS, дослідник рекомендує застосування спеціалізованих програмно-апаратних комплексів Imperva, що забезпечують повну видимість та контроль використання даних в інфраструктурі [10].

Ефективне управління економічною безпекою потребує переходу до моделі інтегрованої операційної стійкості, де захист інформаційної інфраструктури розглядається в нерозривному зв'язку з планами відновлення після катастроф (DR), безперервністю бізнесу (BCP) та контролем ризиків третіх сторін (TPRM). Центральним елементом цієї стратегії стає впровадження ідіосинкратичних сценаріїв стрес-тестування серйозних, але правдоподібних моделей кризових ситуацій, що дозволяють виявити приховані вразливості в ланцюгах постачання та внутрішніх алгоритмах. Тільки через конвергенцію кіберзахисту, етичного управління даними та жорсткого сценаріального аналізу підприємство здатне забезпечити безперервність бізнес-процесів, мінімізувати інсайдерські загрози та гарантувати фінансову стабільність перед викликами цифрової епохи [11].

Слід також зазначити, що аналіз бізнес-ризиків "Allianz Risk Barometer Identifying the major business risks for 2025" (Барометр ризиків Allianz – визначення головних бізнес-ризиків за 2025 р.) [12] засвідчує, що кіберінциденти укріпили статус головної глобальної загрози, охопивши 38% респондентів (оцінка проводилася 3 700 експертами з управління ризиками з

більш ніж 100 країн світу) та випередивши ризик переривання бізнесу у 7 %. За останнє десятиліття ця категорія ризиків піднялася з восьмого на перше місце, ставши домінуючим фактором у Європі, Америці та Африці, а також у 20 провідних країнах світу (Табл. 1).

Таблиця 1. Глобальні бізнес-ризики для корпоративного сектору за 2024-2025 рр.

Глобальні бізнес-ризики	Рік			
	2024		2025	
	% опитаних	місце	% опитаних	місце
Кіберінциденти (кіберзлочинність, збої в роботі ІТ-мереж та сервісів, шкідливе програмне забезпечення / програми-вимагачі, витоки даних, штрафи та санкції)	36%	1	38%	1
Переривання бізнесу (включаючи розрив ланцюгів постачання)	31%	2	31%	2
Природні катастрофи (бурі, повені, землетруси, лісові пожежі, екстремальні погодні явища)	26%	3	29%	3
Зміни в законодавстві та регулюванні (наприклад, нові директиви, протекціонізм, екологічні, соціальні та управлінські вимоги (ESG), а також вимоги щодо сталого розвитку)	19%	4	25%	4
Макроекономічні зміни (інфляція, дефляція, монетарна політика, програми жорсткої економії)	18%	7	19%	5
Пожежі та вибухи	19%	6	17%	6
Зміни клімату (фізичні, операційні та фінансові ризики внаслідок глобального потепління)	19%	5	15%	7
Ринкові зміни (посилення конкуренції / поява нових гравців, угоди зі злиття та поглинання (M&A), стагнація ринку, ринкові коливання)	13%	9	14%	8
Політичні ризики та насильство (політична нестабільність, війна, тероризм, державні перевороти, громадські заворушення, страйки, бунти, мародерство)	14%	8	14%	9
Нові технології (вплив ризиків штучного інтелекту, мережеві / автономні машини)	0%	NEW	10%	10

Джерело: складено за даними [12]

Наразі кібербезпека визнана критичним викликом для восьми стратегічних галузей економіки, починаючи від фінансових послуг – до авіації. Захист даних також залишається у колі інтересів стейкхолдерів, зважаючи на потребу захисту конфіденційних даних від компрометації, що підкреслює вагу захисту інформаційної складової для підприємств. Найбільші побоювання

суб’єктів господарювання пов’язані з деструктивним впливом витоків даних, що підтверджує безальтернативність інтеграції кіберзахисту в сучасну систему забезпечення економічної безпеки підприємства.

Аналітичні дані звіту Cyber security resilience за 2025 р. свідчать про зниження тяжкості страхових випадків на 50% у першій половині 2025 р. завдяки покращенню інструментів виявлення та реагування на кіберінциденти [13]. Відбувся зсув від простого шифрування до подвійного вимагання (крадіжка даних), що призвело до 40% зростання вартості великих збитків саме через витік даних. Окрім того, 28% від обсягу втрат (збитків великого обсягу) спричинені не атаками, а технічними помилками, збоями в хмарах або порушеннями конфіденційності. Чітко прослідковується тенденція зниження тяжкості фінансових збитків на 50% порівняно з попередніми періодами в організаціях, які впровадили проактивні заходи захисту та стратегії реагування (MDR/EDR). Виявлення та реагування (Detection and Response) можуть зменшити вартість збитків компаній у 1000 разів. Трансформація загроз від простого шифрування даних до складних моделей «подвійного вимагання» та витоків інтелектуальної власності підкреслює, що кібербезпека перестала бути суто технічним питанням, перетворившись на інструмент захисту капіталізації та репутації компанії. Таким чином, здатність підприємства протистояти технологічним збоям та спрямованим атакам стає визначальним фактором при прийнятті рішень, що вимагає інтеграції систем управління кіберризиками в загальну архітектуру операційної та економічної безпеки суб’єктів господарювання».

Аналіз цифрових ризиків та поширення кібершахрайства в організаціях представлено у звіті Світового економічного форуму (складеного за результатами опитування 873 учасників із 99 країн), до фінального аналізу якого було залучено 804 кваліфікованих експерти з 92 країн: 316 директорів з інформаційної безпеки (CISO), що представляють технічну та операційну експертизу; 105 генеральних директорів (CEO), чиї відповіді відображають

загальний управлінський вектор; 123 керівники інших стратегічних напрямків (зокрема директори з ризиків (CRO) та технічні директори (CTO)) [14].

Переважна більшість респондентів стикалися з атаками, що вказує на високу інтенсивність злочинної діяльності в цифровому просторі, при чому найвищий показник (62%) припадає на фішинг, отже «людський фактор» залишається найбільш вразливою ланкою в системі безпеки. Використання генеративного ШІ призводить до технологічної досконалості, що дозволяє зловмисникам ефективно маніпулювати користувачами в масових масштабах (Рис. 1).

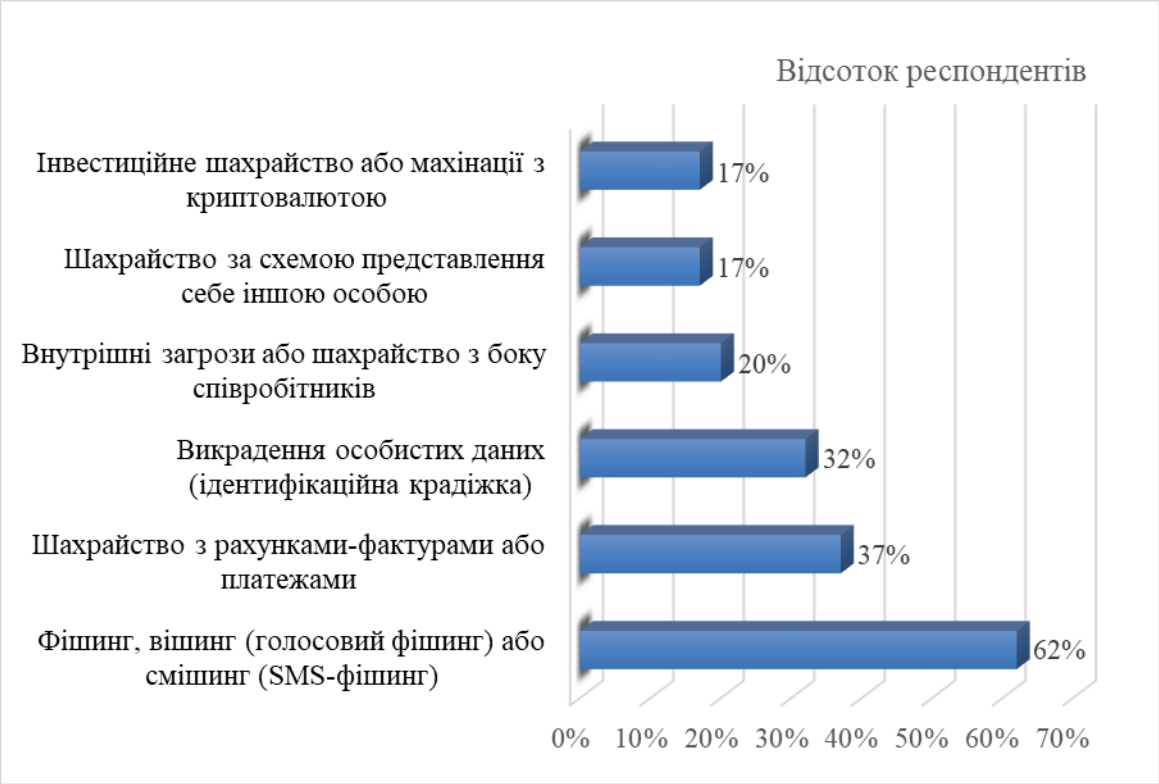

Рис. 1. Поширеність кібершахрайства за даними Global Cybersecurity Outlook 2026 World Economic Forum

Джерело: складено за даними [14]

За даними звіту відзначається високий рівень проникнення кіберзлочинності в професійну та приватну діяльність організацій, кібершахрайство перетворилося на системний фактор ризику.

Доволі висока частка опитаних вказала на шахрайство із платежами (37%) та викрадення даних (32%), наслідком яких є значне навантаження на

фінансові інституції та потребу впровадження більш жорстких протоколів верифікації транзакцій. Корпоративний сектор страждає від внутрішніх загроз (20%), тобто кожна п’ята атака має внутрішнє походження або реалізується через компрометацію облікових записів співробітників, що вимагає зміщення акценту із зовнішнього захисту на модель Zero Trust (нульової довіри). Особистісні, а також крипто-шахрайства (по 17%) вказують на адаптивність зловмисників до нових соціальних та фінансових трендів, використання вподобань користувачів, як слабкостей.

Зростають ризики, пов’язані із використанням ШІ, виникає розрив між технологічними можливостями та кібербезпековою спроможністю організацій, оскільки темпи впровадження інновацій випереджають розвиток відповідних механізмів захисту (87% респондентів щодо зростання вразливостей ШІ) (Рис. 2).

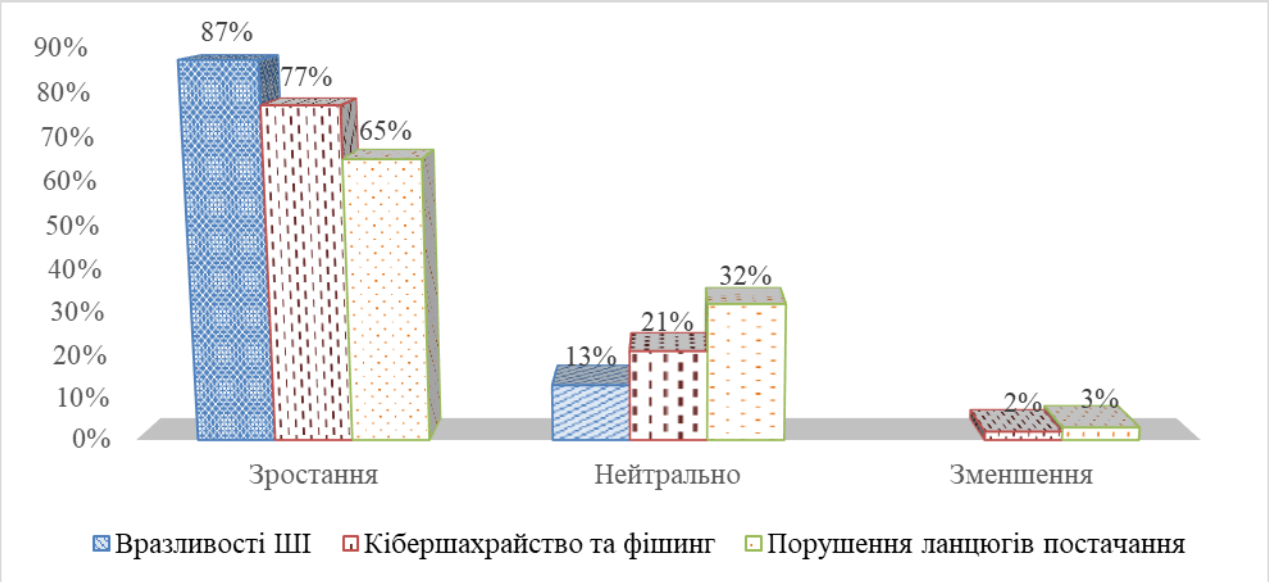

Рис. 2. Тенденції основних кіберризиків впродовж 2025 р. (за результатами опитування керівників організацій)

Джерело: складено за даними [12]

Дослідження щодо управління ризиками закцентовані на необхідності інтеграції цифрових інструментів у стратегії стійкості. Зокрема, наукові [15]

підкреслюють, що для забезпечення операційної стабільності в умовах непередбачуваних дизрупцій необхідний перехід до цифровізованих практик, таких як:

– структура OR (Organizational Resilience), що охоплює прогнозування (Anticipation), готовність до реагування (Readiness to Respond), синхронізацію (Synchronization) та проактивне навчання (Proactive Learning);

– роль цифрових технологій з використанням хмарних обчислень, систем моніторингу в реальному часі та кібербезпеки, що посилює ефективність BCM;

– медіаційний ефект, оскільки BCM стає ланкою, через яку організаційна стійкість трансформується у реальний показник безперервності сервісів (Service Continuity).

Однак, варто врахувати м'які навички щодо забезпечення стійкості, зокрема, організаційну культура та лідерство; управління знаннями в умовах кризи та регуляторну базу та стандарти, що регулюють питання безперервності бізнес-процесів.

Питання регламентування безперервності бізнесу залишаються для українських підприємств відкритими, оскільки законодавчо гармонізується із нормативно-правовими актами країн ЄС. Одним із стандартів, що посилить регуляторну основу забезпечення безперебійного функціонування підприємств – ISO 22301. За даним стандартом безперервність бізнесу визначається як здатність організації продовжувати надавати продукти та послуги під час перерви в прийнятні терміни та з попередньо визначеною потужністю [16].

Стандарт ISO 22301 дозволяє організаціям мінімізувати вплив непередбачених інцидентів, розуміти загрози для бізнесу та захищатися від ризиків, а також сприяє: зміцненню стійкості; покращенню процесів управління ризиками; забезпеченню системи реагування на кризи; зміцненню довіри між усіма залученими сторонами. Для підприємств процес аналізу впливу на бізнес та оцінка ризиків стають узгодженими та зрозумілими,

чіткими, що дозволяє враховувати необхідні внутрішні та зовнішні ресурси, а також розробляти плани та процедури для забезпечення безперервності бізнесу.

Розвиток цифрових ринків також потребує контролю питань кіберзахисту суб'єктів ринку, одним із таких регуляторних актів – Європейський Закон про кіберстійкість (CRA – Cyber Resilience Act), який є інструментом горизонтального регулювання цифрового ринку Європейського Союзу, що встановлює уніфіковані стандарти кібербезпеки для апаратного та програмного забезпечення з цифровими елементами. Актом передбачено імплементацію парадигми «безпека за проєктуванням» (security-by-design) та «безпека за замовчуванням» (security-by-default) та делегування відповідальності за стійкість продуктів із кінцевого споживача на виробника. Закон охоплює повний життєвий цикл продукту – від етапу планування та розробки до експлуатації та технічної підтримки, вимагаючи безперервного усунення виявлених вразливостей [17].

Підсумовуючи, можна стверджувати, що управління економічною безпекою підприємства в умовах цифрової трансформації та зростання кіберзагроз не обмежується суто управлінням економічною стійкістю, оскільки цифровізація бізнесу формує низку викликів, протидія яким – інтеграція доменів інформаційної безпеки у загальну стратегію безпеки підприємства.

Отже, у наукових доробках чітко не окреслено, що саме виступає об'єктом захисту та є цільовим безпековим орієнтиром, окрім того, можна зробити висновок, що визначення об'єктів захисту не є суто технічним етапом, а виступає фундаментальним стратегічним напрямом забезпечення ефективної BCMS та системи безпеки підприємства. Розробка узагальнених цілей захисту є недостатньою, оскільки точні визначення є механізмом досягнення критичних результатів у двох вимірах: проактивному (безпека підприємства) та реактивному (безперервність бізнесу). Дана проблема, обумовлює необхідність розроблення інтегрованої моделі взаємозв'язку

об’єктів захисту, доменів інформаційної безпеки та бізнес-цілей забезпечення цифрової стійкості підприємства, оскільки, як було зазначено, відсутній цілісний науково-методичний підхід до інтеграції механізмів інформаційної безпеки у систему управління економічною безпекою підприємства в умовах цифрової трансформації та зростання гібридних загроз, що підтверджують отримані дані за результатами аналізу міжнародних звітів. Тобто виникає об’єктивна потреба у розробленні інтегрованої моделі, яка б забезпечувала системне поєднання об’єктів захисту, доменів інформаційної безпеки та бізнес-цілей підприємства в єдину концепцію управління безпекою. Такий підхід дозволяє трансформувати інформаційну безпеку з допоміжної технічної функції у стратегічний інструмент забезпечення економічної стійкості підприємства, підвищення його адаптивності до кризових явищ та мінімізації ризиків порушення безперервності діяльності.

Функціональну основу моделі становлять домени інформаційної безпеки, які забезпечують захист інформаційних активів і мінімізацію ризиків порушення безперервності діяльності підприємства. Домени комплаєнсу, управління доступом, мережевої безпеки, захисту кінцевих пристроїв, даних та застосунків, а також протидії дезінформації й фішингу формують інтегровану систему кіберзахисту, орієнтовану на попередження, виявлення та нейтралізацію загроз (Рис. 3).

У моделі об’єкти захисту представлено як сукупність технологічних, основних та допоміжних компонентів цифрового середовища підприємства, що забезпечують функціонування організації та створення бізнес-цінності. До таких об’єктів належать інформаційні системи, дані, бізнес-процеси, програмно-апаратна інфраструктура, мережеві ресурси, персонал, вебресурси та фізичні носії інформації. Вказані елементи формують інформаційні активи підприємства, втрата конфіденційності, цілісності або доступності яких здатна негативно впливати на економічну стійкість, репутацію та операційну діяльність організації.

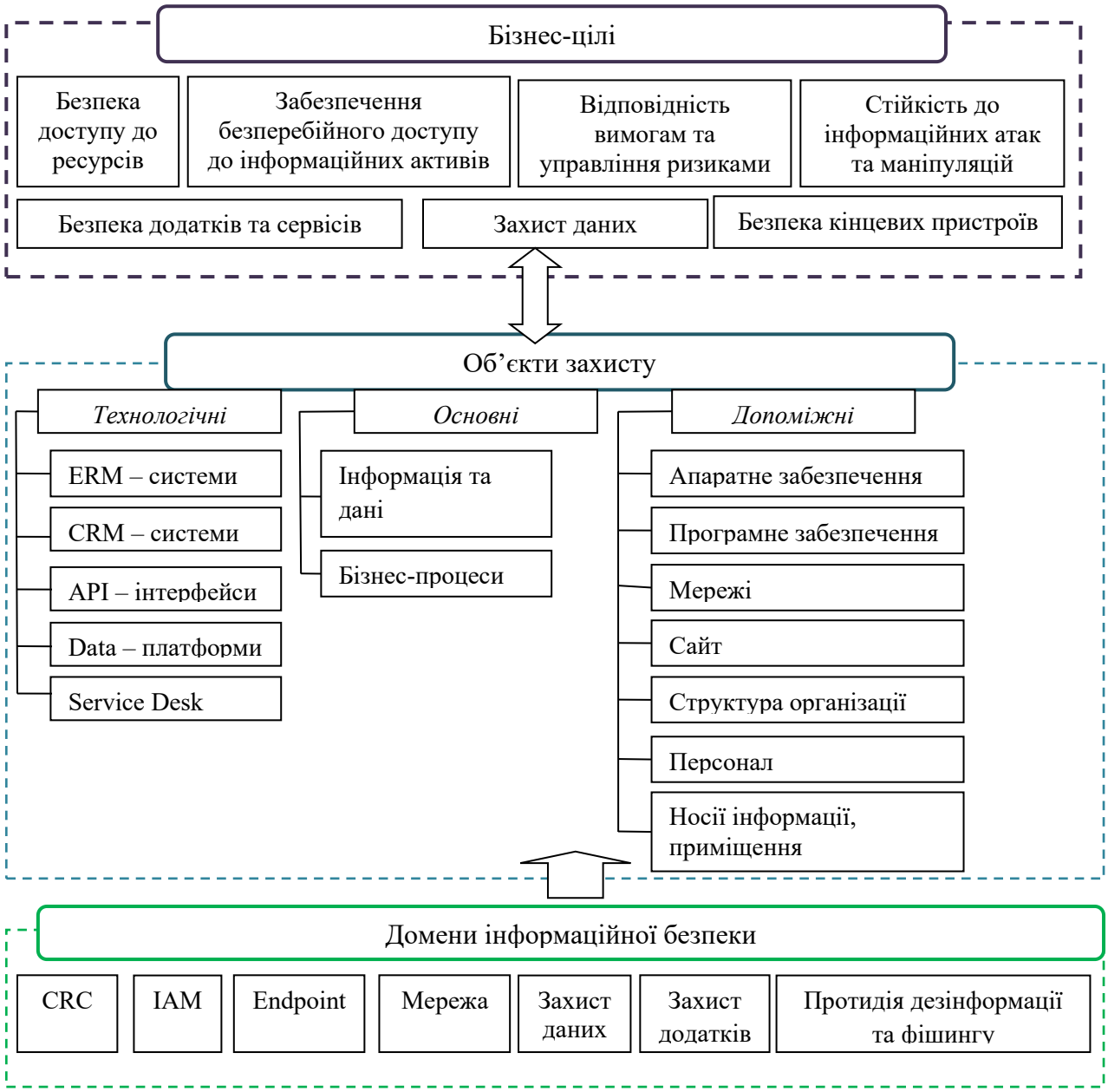

Рис. 3. Інтегрована модель взаємозв'язку об'єктів захисту, доменів інформаційної безпеки та бізнес-цілей забезпечення цифрової стійкості підприємства

Джерело: складено авторами за результатами дослідження

Перший блок схеми демонструє трансформацію функцій інформаційної безпеки у конкретні бізнес-цілі підприємства, що дозволяє розглядати інформаційну безпеку не лише як технічну складову, а як стратегічний

інструмент забезпечення економічної безпеки. Серед основних бізнес-цілей виокремлено:

- забезпечення нормативної відповідності та управління ризиками;
- підтримку безпечного доступу до корпоративних ресурсів;
- забезпечення надійності та відмовостійкості інфраструктури;
- захист кінцевих пристроїв і користувачів;
- гарантування конфіденційності, цілісності та доступності даних;
- підтримку стабільної роботи цифрових сервісів і застосунків;
- забезпечення стійкості до інформаційних атак, маніпуляцій та фішингових загроз.

У другому блоці систематизовано об’єкти захисту, які формують цифрове середовище підприємства, до яких віднесено технологічні компоненти (ERM-, CRM-системи, API-інтерфейси, data-платформи, ServiceDesk), основні об’єкти (інформація, дані та бізнес-процеси), а також допоміжні елементи інфраструктури (апаратне і програмне забезпечення, мережі, вебресурси, організаційна структура, персонал, фізичні носії та приміщення). Об’єкти захисту представляють активи підприємства, які обрано за стандартом ISO 27002:2022 ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls (Інформаційна безпека, кібербезпека та захист конфіденційності – Засоби контролю інформаційної безпеки) [18].

Третій блок відображає корелюючі із об’єктами безпеки домени інформаційної безпеки, що забезпечують захист зазначених активів та підтримують стійкість цифрового середовища підприємства:

- CRC (комплаєнс) – забезпечення відповідності нормативним, правовим та внутрішнім вимогам;
- IAM (Identity and Access Management) – управління цифровими ідентичностями та контролем доступу;

- мережева безпека – захист мережевої інфраструктури та комунікацій;
- Endpoint Security – захист кінцевих пристроїв користувачів;
- захист даних – забезпечення конфіденційності, цілісності та доступності інформації;
- захист додатків – безпека програмного забезпечення та цифрових сервісів;
- протидія дезінформації та фішингу – мінімізація ризиків соціальної інженерії та інформаційного впливу.

У запропонованій моделі домени інформаційної безпеки розглядаються не ізольовано, а як взаємопов'язані елементи єдиної системи управління безпекою підприємства, що формує основу для підтримки безперервності бізнес-процесів, швидкого реагування на інциденти та адаптації підприємства до динамічних умов цифрового середовища.

Таким чином, схема демонструє інтегрований підхід до управління економічною безпекою підприємства, у межах якого інформаційна безпека виступає базовим механізмом забезпечення стабільності функціонування, збереження інформаційних активів та підтримки довгострокової безперервності бізнесу. Сутність моделі полягає у тому, що рівень економічної безпеки підприємства безпосередньо залежить від здатності організації забезпечувати захист інформаційних активів, підтримувати безперервність цифрових процесів та оперативно реагувати на внутрішні й зовнішні загрози. конкурентоспроможність, стійкість та адаптивність підприємства.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Отже, за результатами проведеного дослідження встановлено, що в умовах цифрової трансформації економіки управління економічною безпекою підприємства не може обмежуватися суто фінансово-економічними заходами, а потребує імперативної інтеграції доменів інформаційної безпеки у загальну корпоративну стратегію. Проведений у

статті аналіз структури кіберзагроз на основі емпіричних даних звітів засвідчив домінування методів соціальної інженерії (фішинг – 62%), шахрайства з платежами (37%) та викрадення особистих даних (32%). Це підтверджує, що сучасні цифрові ризики є безпосереднім фінансовим та стратегічним викликом, спрямованим на «людський фактор» та операційні процеси, що є детермінантами економічної стабільності бізнесу. Компанії, що впроваджують проактивні стратегії кіберзахисту (MDR/EDR), здатні вдвічі знизити тяжкість таких фінансових збитків.

Доведено, що методологічно обґрунтоване визначення та специфікація об’єктів захисту в єдиному контурі економічної та інформаційної безпеки виступає стратегічним напрямом забезпечення ефективності системи управління безперервністю бізнесу (BCMS). Виявлено, що у науковій літературі домінує розгляд інформаційних ризиків як технічної проблеми, без чіткого окреслення об’єктів захисту, що ускладнює для підприємств процес формування релевантних стратегій руху до цільових орієнтирів безпеки.

Запропоновано інтегровану модель управління безпекою, яка базується на системному поєднанні бізнес-цілей, систематизованих об’єктів захисту (класифікованих за стандартом ISO/IEC 27002:2022) та функціональних доменів інформаційної безпеки. Застосування даної моделі дозволяє трансформувати інформаційну безпеку з допоміжної функції у стратегічний інструмент забезпечення економічної стійкості підприємства. Це забезпечує підвищення адаптивності організації до кризових явищ, відповідність регуляторним вимогам (ISO 22301, CRA) та мінімізацію ризиків порушення безперервності діяльності за рахунок впровадження принципів Zero Trust та «безпеки за проєктуванням».

Література

1. Захаров О. І. Інформаційне забезпечення управління системою економічної безпеки підприємства. [Електронний ресурс]. URL: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf (дата звернення: 03.04.2026)

2. Ситайло У. Безперервність бізнесу в Україні: виклики та можливості в умовах війни. *Економіка та суспільство.* Вип. 62, 2024. [Електронний ресурс]. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3887/3807 (дата звернення: 17.03.2026)

3. Маковець О., Дрозд І. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право*. № 5/3, 2020. С. 31–35.

4. Дячек О.Ю. Рябченко О.М. ., & Доценко, А. Безпека даних в інформаційно-комунікаційному середовищі та її складність для нових бізнес-моделей. *Економіка та суспільство*. Вип. 38, 2022. [Електронний ресурс]. URL: https://doi.org/10.32782/2524-0072/2022-38-16 (дата звернення: 18.03.2026).

5. Заблуківський А.В. Аналітика ризиків втрати цифрових активів упродовж життєвого циклу власника. *Академічні візії.* Вип. 48, 2025. С.1-12.

6. Fernandes, R. J. Integrating cyber resilience: A critical component of comprehensive business resilience. *Journal of Business Continuity & Emergency Planning*. Vol. 18, No. 4, 2025. Pp. 357-371.

7. Скіцько О., Широшов Р. Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об'єктів критичної інфраструктури. *International Science Journal of Engineering & Agriculture.* Vol. 2 No. 6, 2023. Pp. 12-22.

8. Бєлозерцев В.С. Інформаційна безпека в цифровій економіці: ризики та захисні механізми в бізнес-середовищі. *Інвестиції: практика та досвід.* № 15, 2025. С. 235-241.

9. Проскурович О. Пріоритетні напрямки застосування економічного аналізу за умов діджиталізації. *Modeling the development of the economic systems.* №1, 2026. С. 64–73.

10. Лисецький Ю.М., Калбазов Д.Й. Інформаційна безпека корпоративних баз даних. *Мат. машини і системи.* № 3, 2023. С. 31-37.

11. Pantos, S. Defining resilience: Developing operational risk scenarios for UK insurance companies. *Journal of Risk Management in Financial Institutions*. 2025. vol. 18(3). Pp. 276-288.

12. Allianz Risk Barometer Identifying the major business risks for 2025 [Електронний ресурс]. URL:

https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf (Дата звернення: 09.04.2026).

13. Cyber security resilience 2025. [Електронний ресурс]. URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/commercial-cyber-security-resilience-webinar-2025.pdf (Дата звернення: 02.03.2026).

14. Global Cybersecurity Outlook 2026 Insight Report January 2026. [Електронний ресурс]. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf (Дата звернення: 17.04.2026).

15. Wijaya B., Madiawati P., Pradana M. Strategy to Improve Service Continuity Performance Through Organizational Resilience and Business Continuity Management. Enrichment: *Journal of Multidisciplinary Research and Development.* Vol. 3 No. 7., 2025. Pp. 3262-3278.

16. ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements. ISO 22301:2019. [Електронний ресурс]. URL: https://www.iso.org/standard/75106.html (Дата звернення: 15.03.2026)

17. Official Journal of the European Union. Cyber Resilience Act. [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847 (Дата звернення: 20.03.2026).

18. ISO 27002:2022 ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls. [Електронний ресурс]. URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en (Дата звернення: 25.03.2026).

References

1. Zakharov, O. I. (2015), “Information support for the management of an enterprise’s economic security system”, available at: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf (Accessed 03 April 2026).

2. Sytailo, U. (2024), “Business continuity in Ukraine: challenges and opportunities in the context of the war”, *Ekonomika ta suspilstvo.* [Online], vol.62, available at:

https://economyandsociety.in.ua/index.php/journal/article/view/3887/3807 (Accessed 17 March 2020).

3. Makovets, O. and Drozd, I. (2020), "Cybersecurity as a factor in a company's financial security". *Ekonomika. Finansy. Pravo*, vol. 5/3, pp. 31-35.

4. Diachek, O.Iu. Riabchenko, O.M. ., & Dotsenko, A. (2022), "Data security in the information and communications environment and its implications for new business models". *Ekonomika ta suspilstvo*, [Online], vol. 38, available at: https://doi.org/10.32782/2524-0072/2022-38-16 (Accessed 18 March 2026).

5. Zablukivskyi, A.V. (2025), "Analysis of the risks of losing digital assets throughout the owner's lifecycle". Akademichni vizii , vol. 48, pp. 1-12.

6. Fernandes, R. (2025), "Integrating cyber resilience: A critical component of comprehensive business resilience". *Journal of Business Continuity & Emergency Planning*, vol. 18, No. 4, pp. 357-371.

7. Skitsko, O. and Shyroshov, R. (2023), "An information security management system as a tool for enhancing the security and efficiency of critical infrastructure facilities". *International Science Journal of Engineering & Agriculture,* vol. 2 No. 6, pp. 12-22.

8. Bielozertsev, V.S. (2025), "Information security in the digital economy: risks and protective measures in the business environment". *Investytsii: praktyka ta dosvid,* vol.15, pp. 235-241.

9. Proskurovych, O. (2026), "Key areas of application for economic analysis in the context of digitalization". *Modeling the development of the economic systems,* vol. 1, pp. 64-73.

10. Lysetskyi, Yu.M. and Kalbazov, D.I. (2023), "Information security for corporate databases". *Mat. mashyny i systemy*, vol. 3, pp. 31-37.

11. Pantos, S. (2025), "Defining resilience: Developing operational risk scenarios for UK insurance companies". *Journal of Risk Management in Financial Institutions*. vol. 18(3). Pp. 276-288.

12. Allianz (2025), "Risk Barometer Identifying the major business risks for 2025", available at: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf (Accessed 09 April 2026).

13. Allianz (2025), "Cyber security resilience 2025", available at: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial

/reports/commercial-cyber-security-resilience-webinar-2025.pdf (Accessed 02 March 2026).

14. World Economic Forum (2026), "Global Cybersecurity Outlook 2026 Insight Report January 2026", available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf (Accessed 17 April 2026).

15. Wijaya, B., Madiawati, P. and Pradana, M. (2025), "Strategy to Improve Service Continuity Performance Through Organizational Resilience and Business Continuity Management". *Enrichment: Journal of Multidisciplinary Research and Development.* Vol. 3 No. 7., pp. 3262-3278.

16. ISO (2019), "ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements. ISO 22301:2019", available at: https://www.iso.org/standard/75106.html (Accessed 15 March 2026).

17. Official Journal of the European Union. (2024), "Cyber Resilience Act", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847 (Accessed 20 March 2026).

18. ISO (2022), "ISO 27002:2022 ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls", available at: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en (Accessed 25 March 2026).

Отримано редакцією журналу / Received: 15.05.26
Прорецензовано / Revised: 22.05.26
Дата публікації / Published: 26.05.26