https://doi.org/10.31891/2307-5740-2026-352-75
УДК: 005.922.1:005.334:338.24(477)
JEL classification: M21, L21, D23, G32, K20

САБАДАШ Інна
Національної академії аграрних наук України
https://orcid.org/0009-0001-5267-9153

СИСТЕМНИЙ ПІДХІД ДО ФОРМУВАННЯ МЕХАНІЗМІВ ІНТЕГРАЦІЇ БЕЗПЕКОВИХ КОМПОНЕНТІВ У ЗАГАЛЬНУ СТРАТЕГІЮ ПІДПРИЄМСТВА

У статті досліджено трансформацію системи безпеки підприємства з реактивної функції захисту у фундаментальний елемент корпоративної стратегії та джерело конкурентної переваги. В умовах глобальної цифровізації та геополітичної нестабільності, зокрема триваючої збройної агресії проти України, традиційні підходи до безпеки демонструють обмеженість, що зумовлює необхідність переходу до системного підходу. Обґрунтовано застосування ресурсного підходу (RBV) та теорії випадковості (Contingency Theory) як методологічної основи формування безпекових механізмів, де безпекові активи — технології, знання та культура — розглядаються як стратегічні ресурси, що генерують економічну цінність.

Наукова новизна дослідження полягає у розробці системної моделі інтеграції безпекових компонентів (ESI) у загальну стратегію організації. Проведено порівняльний аналіз патернів інтеграції корпоративних систем, який довів, що перехід від хаотичних з'єднань до сервіс-орієнтованої архітектури (SOA) та корпоративної шини даних (ESB) дозволяє знизити операційні ризики на 45% та прискорити впровадження інновацій. Особливу увагу приділено моделі стратегічного нагляду SIDeARM, яка інтегрує бізнес-аналітику з предиктивним ризик-менеджментом.

У статті деталізовано роль людського фактора крізь призму теорії мотивації захисту (PMT), а також механізми фінансової безпеки, засновані на цифровій економічній форензиці та блокчейн-технологіях. Синтезовано унікальний досвід українських підприємств після 2022 року, що дозволило ідентифікувати ключові фактори стійкості: проєктне управління безпекою, хмарну міграцію («інфраструктурне заплутування») та адаптивну децентралізацію. Статистичні дані підтверджують, що впровадження інтегрованих систем забезпечує підвищення загальної операційної стабільності на 76%. Зроблено висновок, що стратегічна інтеграція безпеки є критичною умовою виживання та сталого відновлення вітчизняного бізнесу у високоризикованому середовищі майбутнього.

Ключові слова: безпека підприємства, системний підхід, стратегічна інтеграція, кібербезпека, операційна стійкість, архітектура ESI, цифрова форензика, воєнна економіка, модель SIDeARM, проєктне управління.

SABADASH INNA
Livestock Farming Institute of the National Academy of Agrarian Sciences of Ukraine

A SYSTEMIC APPROACH TO FORMING MECHANISMS FOR INTEGRATING SECURITY COMPONENTS INTO THE GENERAL ENTERPRISE STRATEGY

The article explores the transformation of enterprise security from a reactive function into a fundamental element of corporate strategy and a source of competitive advantage. In the context of global digitalization and geopolitical instability, particularly the ongoing military aggression in Ukraine, traditional security approaches have demonstrated significant limitations. The study substantiates a systemic approach to the formation of security mechanisms grounded in the Resource-Based View (RBV) and Contingency Theory. The author emphasizes that security assets—technologies, knowledge, and culture—should be treated as strategic resources that generate economic value and foster operational resilience.

The research provides a comparative analysis of enterprise system integration (ESI) patterns, proving that transitioning from point-to-point connections to Service-Oriented Architecture (SOA) and Enterprise Service Bus (ESB) reduces operational risks by up to 45% and increases change implementation speed by 25%. Special attention is paid to boards of directors' strategic oversight of cybersecurity through the SIDeARM (Strategic Intelligence and Decision-centric Adaptive Risk Management) model, which integrates business intelligence with predictive analytics.

The human factor is analyzed through the lens of Protection Motivation Theory (PMT) and Self-Determination Theory (SDT), highlighting that positive incentives and a "culture of error" are more effective than punitive measures. Financial security is addressed via digital economic forensics and blockchain integration, ensuring transaction transparency and anomaly detection. The article synthesizes the unique experience of Ukrainian enterprises post-2022, identifying key resilience factors: project-based management, cloud migration ("infrastructural entanglement"), and decentralized adaptive strategies. Statistical data confirms that integrated security components lead to a 76% improvement in overall operational stability. The findings suggest that for modern enterprises, security integration is a prerequisite for survival and sustainable recovery in a high-risk environment.

Keywords: enterprise security, systemic approach, strategy integration, cybersecurity, operational resilience, ESI, PDCA, SIDeARM, digital forensics, wartime economy.

Стаття надійшла до редакції / Received 17.02.2026
Прийнята до друку / Accepted 11.03.2026
Опубліковано / Published 31.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасному глобалізованому світі, що характеризується експоненціальним зростанням цифрових загроз, економічною нестабільністю та геополітичними трансформаціями, традиційні підходи до

забезпечення безпеки підприємств демонструють свою обмеженість. Безпека більше не може розглядатися як ізольована функція або набір реактивних заходів, спрямованих на купірування вже існуючих інцидентів. Замість цього вона трансформується у фундаментальний елемент загальної стратегії підприємства, стаючи джерелом стратегічної стійкості та конкурентної переваги. Перехід до системного підходу передбачає створення цілісної екосистеми, де інформаційні, фінансові, кадрові та виробничі безпекові компоненти тісно переплетені з бізнес-цілями організації.

Динаміка сучасного бізнес-середовища вимагає від організацій не лише захисту активів, а й здатності швидко адаптуватися до нових викликів, таких як складні кібератаки на базі штучного інтелекту, воєнні конфлікти та розриви логістичних ланцюгів. Інтеграція безпекових компонентів у стратегічне управління дозволяє підприємству діяти проактивно, використовуючи предиктивну аналітику та гнучкі механізми управління ризиками. Зокрема, для українських підприємств у контексті тривалої збройної агресії питання стратегічної інтеграції безпеки набуває екзистенційного значення, вимагаючи нових алгоритмів функціонування, заснованих на цифровій екосистемності та проєктному управлінні.

Системний підхід дозволяє гармонізувати зусилля різних підрозділів, усуваючи фрагментарність захисту та створюючи синергію між технологічними рішеннями та корпоративною культурою. Це передбачає не лише впровадження технічних засобів контролю, а й глибоку трансформацію управлінської парадигми, де безпека стає частиною кожної операції, кожного інвестиційного рішення та кожного кадрового призначення.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Розробка концептуальних засад безпеки підприємства має глибоке коріння в працях українських та закордонних науковців. Фундаментальний внесок у розуміння економічної безпеки як цілісного стану захищеності суб'єкта господарювання зробили Г. В. Козаченко, В. П. Пономарьов та О. М. Ляшенко. У їхніх роботах, зокрема у монографії [1], економічна безпека представлена як стан надійної захищеності від негативного впливу зовнішніх та внутрішніх чинників. О. М. Ляшенко у своїх подальших працях деталізувала дефініції соціально-економічної безпеки, акцентуючи увагу на важливості виробничого потенціалу та стратегії інноваційно-інвестиційного розвитку як засобів протидії глобальним загрозам [2].

Сучасний період (після 2018 року) позначений переходом до системно-процесного аналізу безпеки. С. В. Кавун [4] у своїх дослідженнях обґрунтовує системний підхід як методологічну основу управління проєктними ризиками, що дозволяє визначити чітку послідовність реалізації завдань у механізмах фінансово-економічної безпеки. Аналогічно, К. П. Мисник [5] розглядає механізми цифрової економічної форензики, пропонуючи інтеграцію інструментів блокчейну та штучного інтелекту в загальну систему менеджменту.

Міжнародні дослідники, такі як Koman G. [5] та Tu C. Z. [6] зі співавторами зосереджують увагу на інтеграції систем управління інформаційною безпекою (ISMS) у стратегічне управління через цикл PDCA (Plan-Do-Check-Act). Вони доводять, що ефективна ISMS зміцнює стійкість організації та сприяє впровадженню інновацій. Теоретичні аспекти стратегічного нагляду за кібербезпекою з боку рад директорів були детально опрацьовані в контексті динамічних спроможностей організації.

Внесок Adusumilli T. [7] полягає у глибокому аналізі технічних архітектур інтеграції корпоративних систем (ESI), де безпека розглядається як критичний параметр ефективності. Дослідження мотиваційних аспектів безпеки, проведено О. Герасименко [8], яка підкреслює роль персоналу та мотиваційних ризиків у системі економічної безпеки, вказуючи на необхідність синхронізації HR-політики з безпековою стратегією.

Окремий пласт досліджень присвячений адаптації підприємств до умов війни. Праці Карпенко О., Туровець М.-А. [9], Райтер Н., Мацьків Г. [10], Мицько Р. І., Зачко О. Б. [11] аналізують зміни в операційних алгоритмах українських підприємств, обґрунтовуючи доцільність проєктного підходу та хмарної міграції для забезпечення живучості бізнесу.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Попри значну кількість досліджень окремих видів безпеки, залишається недостатньо вивченим механізм синергетичної взаємодії між цифровою форензикою, мотиваційним менеджментом та стратегічним наглядом в умовах критичної інфраструктурної нестабільності. Потребує деталізації алгоритм швидкої трансформації безпекових бар'єрів у гнучкі інноваційні фільтри під час воєнного стану.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є теоретичне обґрунтування та розробка системної моделі формування механізмів інтеграції безпекових компонентів у загальну стратегію підприємства. Це передбачає аналіз взаємодії інформаційних, фінансових та кадрових підсистем, визначення ключових метрик їх ефективності та обґрунтування ролі безпеки як драйвера стратегічних інновацій та операційної стійкості в умовах цифровізації та воєнних викликів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Системний підхід до формування безпекових механізмів базується на усвідомленні того, що підприємство є складною відкритою системою, де зміни в одному компоненті неминуче впливають на стан

всієї структури. В основі сучасної концепції інтеграції лежать дві фундаментальні теорії: ресурсний підхід (Resource-Based View - RBV) та теорія випадковості (Contingency Theory) [12].

Згідно з ресурсним підходом, безпекові механізми та знання персоналу розглядаються не як витрати, а як стратегічні активи, що володіють характеристиками цінності, рідкісності та складності імітації. Коли система безпеки інтегрована в стратегію, вона створює економічну цінність через підвищення операційної ефективності та зміцнення довіри стейкголдерів. Теоретики стверджують, що проактивна безпека може бути драйвером інновацій, дозволяючи фірмам впроваджувати нові цифрові бізнес-моделі з мінімальним ризиком.

Теорія випадковості, у свою чергу, наголошує, що архітектура безпеки повинна бути адаптивною до зовнішнього середовища. В умовах високої турбулентності, таких як воєнний стан в Україні, механізми безпеки мають трансформуватися з жорстких регуляторних бар'єрів у гнучкі інноваційні фільтри.

У межах системного підходу виділяють два ключові методи управління:

– процесний метод: фокусується на циклічному управлінні діяльністю, включаючи ризик-менеджмент, управління інцидентами та аудит. Ключовим інструментом тут виступає модель PDCA, яка забезпечує безперервність удосконалення;

– системний метод: розглядає організацію як сукупність взаємопов'язаних елементів (люди, технології, процеси), гарантуючи, що нові інструменти безпеки органічно вписуються в існуючі бізнес-процеси.

Інтеграція корпоративних систем (Enterprise System Integration - ESI) є технічним підґрунтям для впровадження безпекових компонентів. Сучасне підприємство оперує великою кількістю розрізнених додатків, що створює проблему "силосів даних" та збільшує поверхню атак. Системна інтеграція дозволяє створити єдину екосистему з централізованим контролем.

Ефективність різних патернів інтеграції суттєво різниться залежно від обраної архітектури. Дослідження показують (таблиця 1), що перехід від хаотичних з'єднань "точка-точка" до структурованих моделей (ESB, SOA) радикально знижує операційні ризики.

Використання сучасних протоколів безпеки, таких як OAuth 2.0 та JWT, у поєднанні з Role-Based Access Control (RBAC), дозволяє досягти значних результатів у захисті даних. Статистичні дані свідчать, що впровадження цих інструментів у межах інтегрованої архітектури знижує кількість успішних спроб несанкціонованого доступу на 67% [7].

Таблиця 1

Порівняльна характеристика патернів інтеграції корпоративних систем та їх впливу на операційні ризики

Параметр порівняння	Точка-точка (Point-to-Point)	Корпоративна шина (ESB)	Сервіс-орієнтована архітектура (SOA)
Складність обслуговування	Зростає на 32% при >10 точках	Знижується на 45%	Оптимізована через сервіси
Повторне використання коду	Мінімальне	Середнє	Покращується на 35%
Моніторинг інцидентів	Ускладнений, фрагментарний	Покращення видимості на 28%	Високий рівень прозорості
Швидкість впровадження змін	Низька	Середня	Збільшується на 25%
Стійкість до відмов	Низька	Висока (централізована)	Найвища (через мікросервіси)

Джерело: розроблено автором за [7].

Інтеграція безпеки в загальну стратегію вимагає активного залучення рад директорів та топ-менеджменту. Стратегічний нагляд за кібербезпекою розглядається як динамічна спроможність організації відчувати загрози, захоплювати можливості для посилення стійкості та трансформувати управління для створення довгострокової цінності.

Ключовим механізмом тут виступає "стратегічний сенсмейкінг" (strategic sensemaking), який включає три субпроцеси: сканування середовища, інтерпретацію сигналів та прийняття дій. У таблиці 2 наведено ролі керівництва на різних етапах управління безпековими подіями.

Таблиця 2

Розподіл стратегічних ролей менеджменту на різних фазах управління безпековими подіями

Фаза управління	Роль контролю та моніторингу	Консультативна та керівна роль
Рутинна фаза	Оцінка позиції безпеки та комплаєнсу. Перевірка розподілу ресурсів.	Визначення апетиту до ризику та стратегічних пріоритетів.
Під час атаки	Нагляд за реагуванням на кризу. Оцінка юридичних та репутаційних ризиків.	Порадництво щодо критичних рішень (зупинка систем, виплата викупу).
Фаза відновлення	Оцінка післяінцидентних звітів та впровадження вивчених уроків.	Формування стратегій стійкості та майбутніх інвестицій.

Джерело: розроблено автором за [7, 13].

Для реалізації такого нагляду часто пропонується модель SIDeARM (Strategic Intelligence and Decision-centric Adaptive Risk Management). Вона інтегрує бізнес-аналітику (BI) з функціями безпеки,

використовуючи OSINT (розвідку на основі відкритих джерел) та предиктивну аналітику для випередження ринкових збоїв та гібридних загроз.

Людський фактор залишається критичним компонентом безпеки. Системний підхід вимагає інтеграції HR-менеджменту в загальний механізм забезпечення безпеки підприємства. Це реалізується через протидію мотиваційним ризикам, які виникають через поведінку персоналу.

Для розуміння того, чому працівники дотримуються або порушують правила безпеки, використовуються теорія мотивації захисту (PMT) та теорія самодетермінації (SDT) [14]:

– оцінка загрози: працівник оцінює серйозність ризику та власну вразливість;

– оцінка відповіді: працівник оцінює, наскільки ефективними є заходи безпеки та чи здатний він їх виконати (self-efficacy).

Дослідження показують, що просте залякування санкціями часто є контрпродуктивним. Натомість, позитивні стимули (ваучери, визнання) та розвиток "культури помилок" (де працівник не боїться повідомити про випадковий інцидент) значно підвищують рівень реальної захищеності [15]. Ефективний мотиваційний механізм дозволяє сформувати лояльну команду, що є особливо важливим в умовах обмежених фінансових ресурсів.

Фінансова компонента є кровоносною системою безпеки підприємства. В умовах цифровізації традиційні методи фінансового контролю доповнюються механізмами цифрової економічної форензики.

Механізм цифрової форензики формалізується як послідовність етапів:

1. Системний збір інформації: агрегація даних про всі транзакції в режимі реального часу.
2. Виявлення аномалій: порівняння поточних операцій з базою даних минулих періодів за допомогою ШІ та машинного навчання.
3. Реагування: автоматизоване оповіщення менеджменту про ризики або блокування сумнівних операцій.

Інтеграція блокчейну у фінансовий менеджмент дозволяє досягти прозорості транзакцій та незмінності записів, що радикально знижує ризики внутрішнього шахрайства та зовнішніх маніпуляцій. Крім того, компанії, які успішно інтегрують безпекові фреймворки (наприклад, ISO/IEC 27001) у фінансове планування, демонструють кращі показники рентабельності та зростання продажів, оскільки безпека стає частиною їхньої ринкової репутації.

Досвід українських підприємств після 2022 року надав унікальний матеріал для переосмислення системного підходу. В умовах фізичного руйнування активів та постійних кібератак стратегія безпеки була вимушена стати максимально гнучкою.

Ключові трансформації включають:

– проєктний підхід: використання гнучких методологій для вирішення стратегічних завдань безпеки в умовах невизначеності;

– цифрова екосистемність: створення розгалужених мереж моніторингу, таких як платформа "Delta", що об'єднують дані від різних сенсорів для забезпечення ситуаційної обізнаності;

– інфраструктурне заплутування (Infrastructural Entanglement): швидка міграція в хмарні середовища глобальних провайдерів (AWS, Microsoft), що дозволило зберегти функціональність бізнесу навіть при знищенні локальних серверів;

– децентралізація: перехід до адаптивних стратегій, заснованих на локальних мережах та автономії підрозділів, що виявилося більш ефективним, ніж жорстка централізована ієрархія.

Статистика впровадження інтегрованих систем під час кризи демонструє вражаючу ефективність у забезпеченні стійкості бізнесу (таблиця 3).

Таблиця 3

Метрики ефективності впровадження інтегрованих безпекових компонентів в умовах кризи

Метрика ефективності інтеграції	Покращення показника (%)
Виявлення загроз у реальному часі	35%
Швидкість вирішення інцидентів безпеки	40%
Зменшення випадків несанкціонованого доступу	25%
Зниження часу простою систем (Downtime)	45%
Загальна операційна стабільність	76%

Джерело: розроблено автором за [7, 13].

Ці дані підтверджують, що інтеграція безпекових компонентів (ESI) не є лише питанням захисту, а й фундаментальним чинником операційної безперервності.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Системний підхід до формування механізмів інтеграції безпекових компонентів у загальну стратегію підприємства дозволяє перетворити функцію захисту на динамічний актив організації. Інтеграція має відбуватися на трьох рівнях: технічному (через архітектури ESI та мікросервіси), управлінському (через

стратегічний нагляд рад директорів та моделі SIDeARM) та ментальному (через формування безпекової культури та мотивацію персоналу).

Дослідження підтверджує, що сучасна безпека підприємства базується на проактивності та предиктивності. Використання штучного інтелекту, блокчейну та великих даних у межах циклу PDCA дозволяє не лише мінімізувати збитки від інцидентів, а й оптимізувати операційні витрати, підвищити довіру інвесторів та забезпечити стійкість в умовах екстремальних викликів, таких як воєнний стан. Для українських підприємств інтеграція безпеки в стратегію є не просто вибором, а необхідною умовою виживання та подальшого відновлення у високотехнологічному та ризикованому середовищі майбутнього. Застосування проєктного підходу та хмарних технологій стає базисом для формування нової моделі безпекоорієнтованого управління, де безпека є невід'ємною частиною інноваційного розвитку.

Література

1. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. Київ : Лібра, 2003. 280 с.
2. Ляшенко О. М. Дефініції соціально-економічної безпеки підприємства. *Економіка. Менеджмент. Підприємництво*. 2007. № 17 (ІІ). С. 179-187.
3. Кавун В. А. Системний підхід як методологічна основа управління проектними ризиками. *Економічний вісник Запорізької державної інженерної академії.* 2018. Вип. 1(13). С. 120-123. URL: https://dspace.znu.edu.ua/jspui/bitstream/12345/863/1/25.pdf
4. Мисник К. П. Інтеграція механізму цифрового економічного форензіку в систему управління підприємствами. *Економіка промисловості*. 2024. № 2 (106). С. 64-76. DOI: http://doi.org/10.15407/econindustry2024.02.064
5. Koman G., Toamn D., Jankal R., Borsos P. Risk management in a human resource information system. *Entrepreneurship and Sustainability Issues*. 2023. Vol. 11(1). pp. 331–352. DOI: http://doi.org/10.9770/jesi.2023.11.1(20)
6. Tu C. Z., Yuan Y., Archer N., Connelly C. E. Strategic value alignment for information security management: A critical success factor analysis. *Information and Computer Security.* 2018. Vol. 26(2), pp. 150–170. DOI: http://doi.org/10.1108/ICS-06-2017-0042
7. Adusumilli T. Enterprise System Integration: A Technical Deep Dive into Modern Business Infrastructure. *European Journal of Computer Science and Information Technology.* 2025. Vol. 13 (14), pp. 198-207. DOI: https://doi.org/10.37745/ejcsit.2013/vol13n14198207
8. Герасименко О. Мотиваційні ризики системи кадрової безпеки підприємства у механізмі управління його економічною безпекою. *Вісник Черкаського національного університету імені Богдана Хмельницького. Серія «Економічні науки».* 2025.Т. 29 № 1. DOI: https://doi.org/10.31651/2076-5843-2025-1-29-38
9. Карпенко О., Туровець М.-А. Особливості управління підприємством в умовах кризи воєнного часу. *Economic Synergy*. 2024. №4. С. 77-89. DOI: https://doi.org/10.53920/ES-2024-4-5
10. Райтер Н., Мацьків Г. Ризики аграрного підприємництва в умовах війни. *Аграрна економіка.* 2023 Т. 16 № 1-2. С. 41-50. DOI: https://doi.org/10.31734/agrarecon2023.01-02.041
11. Мицько Р. І., Зачко О. Б. Генезис управління логістичними проєктами в умовах воєнного стану: від концептуальних до інтелектуальних моделей. *Вісник ЛДУБЖД*. 2024. № 30, С. 250-263. DOI: https://doi.org/10.32447/20784643.30.2024.24
12. Cho H.; Cho K. Impact of Security Management Activities on Corporate Performance. *Systems*. 2025. Vol.13(8) : 633. DOI: https://doi.org/10.3390/systems13080633
13. Staffenova N, Dupakova D, Kubina M. Integration of ISMS into the Organization's Strategy and Its Impact on Security Culture in the Digital Environment. *Administrative Sciences.* 2026. Vol. 16(1) : 26. DOI: https://doi.org/10.3390/admsci16010026
14. Li W, Liu R, Sun L, Guo Z, Gao J. An Investigation of Employees' Intention to Comply with Information Security System-A Mixed Approach Based on Regression Analysis and fsQCA. *Int J Environ Res Public Health*. 2022. Vol. 19(23) : 16038. DOI: https://doi.org/10.3390/ijerph192316038
15. Reittinger T., Glas M., Aminzada S., Pernul G. (). Motivational factors in cybersecurity: linking theory to organizational practice. *Information & Computer Security*. 2025. DOI: https://doi.org/10.1108/ICS-02-2025-0046

References

1. Kozachenko, H. V., Ponomariov, V. P., & Liashenko, O. M. (2003). *Ekonomichna bezpeka pidpryiemstva: sutnist ta mekhanizm zabezpechennia* [Economic security of the enterprise: essence and mechanism of provision]. Kyiv: Libra [in Ukrainian].
2. Liashenko, O. M. (2007). Defunitsii sotsialno-ekonomichnoi bezpeky pidpryiemstva [Definitions of socio-economic security of the enterprise]. *Ekonomika. Menedzhment. Pidpryiemnytstvo – Economics. Management. Entrepreneurship*, 17(II), 179–187 [in Ukrainian].
3. Kavun, V. A. (2018). Systemnyi pidkhid yak metodolohichna osnova upravlinnia proektnymy ryzykamy [System approach as a methodological basis of project risk management]. *Ekonomichnyi visnyk Zaporizkoi derzhavnoi inzhenernoi akademii – Economic Bulletin of Zaporizhzhia State Engineering Academy*, 1(13), 120–123. Retrieved from https://dspace.znu.edu.ua/jspui/bitstream/12345/863/1/25.pdf [in Ukrainian].

4. Mysnyk, K. P. (2024). Intehratsiia mekhanizmu tsyfrovoho ekonomichnoho forenziku v systemu upravlinnia pidpryiemstvamy [Integration of the digital economic forensics mechanism into the enterprise management system]. *Ekonomika promyslovosti – Economy of Industry*, 2(106), 64–76. http://doi.org/10.15407/econindustry2024.02.064 [in Ukrainian].
5. Koman, G., Toamn, D., Jankal, R., & Borsos, P. (2023). Risk management in a human resource information system. *Entrepreneurship and Sustainability Issues*, 11(1), 331–352. http://doi.org/10.9770/jesi.2023.11.1(20)
6. Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information and Computer Security*, 26(2), 150–170. http://doi.org/10.1108/ICS-06-2017-0042
7. Adusumilli, T. (2025). Enterprise System Integration: A Technical Deep Dive into Modern Business Infrastructure. *European Journal of Computer Science and Information Technology*, 13(14), 198–207. https://doi.org/10.37745/ejcsit.2013/vol13n14198207
8. Herasymenko, O. (2025). Motyvatsiini ryzyky systemy kadrovoi bezpeky pidpryiemstva u mekhanizmi upravlinnia yoho ekonomichnoiu bezpekoiu [Motivational risks of the enterprise personnel security system in the mechanism of its economic security management]. *Visnyk Cherkaskoho natsionalnoho universytetu imeni Bohdana Khmelnytskoho. Seriia «Ekonomichni nauky» – Bulletin of Bohdan Khmelnytsky National University of Cherkasy. Economic Sciences Series*, 29(1). https://doi.org/10.31651/2076-5843-2025-1-29-38 [in Ukrainian].
9. Karpenko, O., & Turovets, M.-A. (2024). Osoblyvosti upravlinnia pidpryiemstvom v umovakh kryzy voiennoho chasu [Features of enterprise management in the conditions of wartime crisis]. *Economic Synergy*, 4, 77–89. https://doi.org/10.53920/ES-2024-4-5 [in Ukrainian].
10. Raiter, N., & Matskiv, H. (2023). Ryzyky ahrarnoho pidpryiemnytstva v umovakh viiny [Risks of agricultural entrepreneurship in war conditions]. *Ahrarna ekonomika – Agricultural Economics*, 16(1-2), 41–50. https://doi.org/10.31734/agrarecon2023.01-02.041 [in Ukrainian].
11. Mytsko, R. I., & Zachko, O. B. (2024). Genezys upravlinnia lohistychnymy proiektamy v umovakh voiennoho stanu: vid kontseptualnykh do intelektualnykh modelei [Genesis of logistics project management under martial law: from conceptual to intelligent models]. *Visnyk LDUBSZHD – Bulletin of LSVUBG*, 30, 250–263. https://doi.org/10.32447/20784643.30.2024.24 [in Ukrainian].
12. Cho, H., & Cho, K. (2025). Impact of Security Management Activities on Corporate Performance. *Systems*, 13(8), 633. https://doi.org/10.3390/systems13080633
13. Staffenova, N., Dupakova, D., & Kubina, M. (2026). Integration of ISMS into the Organization's Strategy and Its Impact on Security Culture in the Digital Environment. *Administrative Sciences*, 16(1), 26. https://doi.org/10.3390/admsci16010026
14. Li, W., Liu, R., Sun, L., Guo, Z., & Gao, J. (2022). An Investigation of Employees' Intention to Comply with Information Security System-A Mixed Approach Based on Regression Analysis and fsQCA. *International Journal of Environmental Research and Public Health*, 19(23), 16038. https://doi.org/10.3390/ijerph192316038
15. Reittinger, T., Glas, M., Aminzada, S., & Pernul, G. (2025). Motivational factors in cybersecurity: linking theory to organizational practice. *Information & Computer Security*. https://doi.org/10.1108/ICS-02-2025-0046