

УДК 005.334:658.5

В. І. Кифяк,
к. е. н., доцентка кафедри бізнесу та управління персоналом,
Чернівецький національний університет імені Юрія Федьковича
ORCID ID: <https://orcid.org/0000-0002-6104-6403>
Г. Б. Колісник,
магістрант,
Чернівецький національний університет імені Юрія Федьковича
ORCID ID: <https://orcid.org/0009-0009-9583-6153>

DOI: 10.32702/2306-6814.2025.23.201

СТРАТЕГІЧНІ ІНСТРУМЕНТИ УПРАВЛІННЯ РИЗИКАМИ В СИСТЕМАХ БЕЗПЕКИ БІЗНЕСУ В УМОВАХ ГЛОБАЛЬНИХ ЗАГРОЗ

V. Kyfyak,
PhD in Economics, Associate Professor, Yuriy Fedkovich Chernivtsi National University
H. Kolisnyk,
Master's student, Yuriy Fedkovich Chernivtsi National University

STRATEGIC RISK MANAGEMENT TOOLS IN BUSINESS SECURITY SYSTEMS IN THE CONTEXT OF GLOBAL THREATS

Удосконалення систем стратегічного управління ризиками в умовах глобальних загроз є ключовою передумовою забезпечення стійкості сучасного бізнесу, особливо у високотехнологічних галузях. У статті висвітлено взаємозв'язок між ризик-менеджментом та конкурентоспроможністю підприємств, обґрунтовано зростаючу роль інтегрованих підходів до оцінювання, ідентифікації та мінімізації ризиків у середовищі, що характеризується геополітичною фрагментацією, підвищеною частотою кіберінцидентів та технологічною невизначеністю. Дослідження узагальнює сучасні методологічні підходи ISRM та ERM, особливу увагу приділяючи застосуванню внутрішніх контролів COBIT, механізмів самооцінки контролів (CSA), а також впровадженню автоматизованих GRC-платформ як інструментів підвищення адаптивності бізнесу. На основі аналізу актуальних міжнародних та національних джерел сформовано оптимізовану модель управління ризиками для українських організацій, яка поєднує стратегічне прогнозування, динамічне оцінювання ризиків, інтегративні контролі та автоматизовану взаємодію з регуляторними вимогами. Запропонований підхід забезпечує зниження втрат, підвищення рівня інформаційної та операційної безпеки, а також створює передумови для інноваційного розвитку підприємств у нестабільній ринковій середовищі.

Improving strategic risk management systems in the face of growing global threats is a key prerequisite for ensuring the long-term sustainability and resilience of modern enterprises, particularly in high-tech industries such as IT consulting. The article emphasizes the strategic interconnection between risk management practices and the overall competitiveness of companies, substantiating the increasing relevance of integrated, multi-level approaches to identifying, assessing, mitigating, and monitoring risks within an environment shaped by geopolitical

fragmentation, the intensification of cyber incidents, technological disruption, and volatile international regulatory dynamics. The study systematizes contemporary methodological principles of ISRM and ERM, paying special attention to the use of COBIT internal controls, control self-assessment (CSA) mechanisms, and the deployment of automated GRC platforms that significantly expand an organization's capacity for adaptive decision-making, transparency, proactive threat anticipation, and compliance with rapidly changing global and national standards. Additionally, the article outlines how AI-enhanced analytics, scenario modeling, and dynamic risk dashboards enable companies to respond more effectively to emerging hybrid threats, including cyber-physical attacks, misinformation campaigns, and supply-chain instability. Based on the analysis of authoritative international reports, Ukrainian governmental initiatives, and practical implementation cases, the study proposes an optimized risk management model tailored for Ukrainian organizations. This model integrates strategic forecasting, dynamic risk scoring, strengthened internal control frameworks, cross-functional CSA engagement, and automated alignment with state and industry regulatory requirements. The suggested approach enhances organizational resilience, reduces potential financial, operational, and reputational losses, improves information security maturity, and forms a robust foundation for continuous innovation, business continuity, and sustainable development in an increasingly unstable and highly competitive global marketplace.

Ключові слова: управління ризиками, конкурентоспроможність підприємства, ризик-менеджмент, стратегічне планування, фінансова стабільність, інновації.

Key words: risk management, enterprise competitiveness, risk management practices, strategic planning, financial stability, innovation.

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

У контексті глобальних загроз, таких як геополітична фрагментація, ескалація кібератак та технологічна невизначеність, стратегічні інструменти управління ризиками в системах безпеки бізнесу набувають фундаментального значення для забезпечення стійкості організацій, особливо в секторах з високою цифровою залежністю, як IT-консалтинг. Необхідно розробити науково-методичні підходи, які базуються на системному аналізі взаємопов'язаності геополітичних зрушень з технологічними вразливостями, де фрагментація глобальних альянсів породжує глибокі трансформації організаційної структури управління, посилюючи ризики для ланцюгів постачань і регуляторного середовища. Це створює "ефект доміно", де торговельні бар'єри та санкції не лише обмежують доступ до критичних технологій, але й стимулюють ескалацію кібератак, які, згідно зі звітом Всесвітнього економічного форуму (ВЕФ) Global Risks Report 2025, входять до топ-ризиків через зростання конфліктів і поляризації. У таких умовах бізнес-системи безпеки мусять еволюціонувати від реактивних заходів до проактивних стратегій, що інтегрують аналітику на базі штучного інтелекту (ШІ) для прогнозування загроз, оскільки традиційні моделі вже не справляються з швидкістю змін.

Сучасна практика ескалації кібератак набуває нових якісних форм, зокрема атак, посилених ШІ, із застосуванням технологій глибоких фейків та автоматизованих фішингових кампаній. Такі атаки забезпечують швидке проникнення в хмарні інфраструктури та ефективне використання методів соціальної інженерії. Ця тенденція має особливу актуальність для України, де геополітична нестабільність поєднується з вразливістю енергетичного сектора, що значно підвищує рівень ризику для галузей із високим ступенем залежності від цифрових технологій у умовах багатофакторних ризиків.

У зв'язку з цим сучасні підходи до управління кіберризиками мають розглядати технологічну невизначеність як ключовий каталізатор нових загроз. Конкуренція за ресурси, регуляторні обмеження та швидкі зміни в технологічному середовищі формують динамічний і політично забарвлений ландшафт, який вимагає від організацій переходу до мультирівневих моделей управління ризиками.

Такі моделі передбачають інтеграцію стандартизованих контрольних цілей для управління інформаційними технологіями (наприклад, на основі рамкової моделі COBIT) з механізмами регулярної самооцінки ефективності контролів (наприклад, за методологією CSA). Лише таке поєднання забезпечує необхідний рівень адаптивної стійкості в умовах постійної еволюції кіберзагроз.

Обґрунтування сучасної проблеми кібербезпеки вимагає принципового переосмислення систем захисту як цілісної інтегрованої екосистеми. У такій екосистемі стратегічні інструменти, зокрема автоматизовані платформи управління ризиками, відповідністю вимогам та корпоративним урядуванням, виконують подвійну функцію. По-перше, вони суттєво зменшують масштаби збитків від кібератак. По-друге, ці платформи дають змогу трансформувати технологічну та геополітичну невизначеність у конкурентну перевагу завдяки проактивному моделюванню можливих сценаріїв розвитку подій.

Отже, ключова проблема полягає не просто в оперативній реакції на вже виявлені загрози, а в створенні науково обґрунтованої концептуальної рамки, яка забезпечує їхнє випереджувальне прогнозування й нейтралізацію. Саме така рамка стає необхідною умовою довгострокової стійкості організацій в умовах глобальної турбулентності та постійної еволюції кіберзагроз.

МЕТА СТАТТІ

Мета статті — теоретичне обґрунтування та практична розробка стратегічних інструментів управління ризиками в системах безпеки бізнесу в умовах глобальних загроз, що включає систематизацію методик на базі класичних концепцій з урахуванням геополітичних, технологічних та національних факторів невизначеності.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Класичні наукові підходи поглиблюють теоретичне та методологічне розуміння стратегічних інструментів управління ризиками в системах безпеки бізнесу. У фундаментальній праці Т. Фінне [1] управління ризиками в інформаційних системах (ISRM) трактується як широка, складна та інтердисциплінарна дисципліна, де ключовими елементами є чіткі дефініції. Автор наголошує на необхідності дослідницького підходу до аналізу тисяч потенційних ризиків, позиціонуючи бізнес-процеси як центральний елемент проактивного управління ризиками в інформаційних системах. Д. Джакобус [2] пропонує нову систему комплексного управління підприємницькими ризиками (ERM) з переходом від ізольованих (силосних) до інтегративних підходів, де самооцінка контролів (Control Self-Assessment, CSA) виступає ядром для залучення всіх співробітників до процесів ідентифікації, аналізу та пом'якшення ризиків, забезпечуючи суттєву зміну підходу у корпоративному управлінні ризиками в умовах глобальних загроз. Ці теоретичні положення отримали подальший розвиток у працях сучасних дослідників. Зокрема, С. Гаррінгтон та Г. Ніхаус [3] на прикладі United Grain Growers емпірично довели ефективність інтегрованого підходу до ERM, коли системне ранжування ризиків та їхнє фінансове оцінювання дозволяють змінити невизначеність у керуванні капіталом. Дж. Фрейзер, Б. Сімкінс та К. Нарваез [4], аналізуючи впровадження ERM в Університеті Вашингтона, підкреслили критичну роль ітеративного циклу та інтеграції інформаційно-технологічних компонентів у досягненні адаптивної стійкості організацій. В українському контексті дослідження [5], [6] розширюють парадигму ERM на ESG-ризиків агробізнесу, демон-

струючи, що бізнес-модель може виступати інструментом управління вартістю в умовах геополітичної та екологічної нестабільності, а системна мінімізація ризиків безпосередньо впливає на довгострокову конкурентоспроможність підприємств.

Невирішеними залишаються проблеми розробки універсальних стратегічних інструментів, які б інтегрували національні та глобальні регуляторні вимоги для ефективного управління ризиками в умовах швидких технологічних змін, необхідно акцентувати на створенні адаптивних методик, що поєднують автоматизацію з залученням персоналу для мінімізації впливу багатфакторних ризиків на бізнес-стійкість.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Сучасні наукові публікації та аналітичні звіти акцентують увагу на ескаляції геополітичних ризиків, які становлять близько 30% від загального спектру загроз, з фрагментацією глобальних ланцюгів постачань та торговими конфліктами, що безпосередньо загрожують стійкості інформаційно-технологічної інфраструктури. У цьому контексті рекомендується впровадження модулів архітектурних структур та посилення заходів захисту даних для забезпечення адаптивності систем безпеки бізнесу [9, 12]. Звіт Всесвітнього економічного форуму (WEF) за 2025 рік виокремлює державні конфлікти та дезінформацію, посилену ШІ, як провідні глобальні ризики, при цьому 52% опитаних експертів прогнозують посилення нестабільності, з особливим акцентом на Україну, де наслідки війни в регіоні, включаючи Близький Схід та Судан, посилюють геополітичну напругу [11]. За оцінками Міністерства фінансів України, воєнні та демографічні фактори призведуть до скорочення ВВП на 2,3% у 2025 році, що підкреслює критичну вразливість бізнес-структур у таких умовах [13].

Технологічні тенденції, описані в аналітичному огляді McKinsey за 2025 рік (13 ключових напрямів), підкреслюють важливість цифрової довіри через інтеграцію технологій блокчейну та ШІ для проактивного виявлення загроз, водночас фіксуючи дефіцит кваліфікованих кадрів у 46% організацій, що ускладнює впровадження стратегічних інструментів управління ризиками [9]. Інститут управління ризиками (IRM) у своєму звіті за 2025 рік зазначає, що кібербезпека становить 28% від усіх ідентифікованих ризиків, з інвестиціями в цю сферу на рівні 37% від загальних бюджетів на безпеку та зростанням попиту на фахівців на 70%, з особливим наголосом на застосування штучного інтелекту для оптимізації ланцюгів постачань у контексті глобальних загроз [11]. Уряд України реалізував автоматизований модульний інструмент для 85 секторів економіки, що сприяє зменшенню корупційних ризиків та забезпеченню відповідності регуляторним вимогам (compliance), тим самим посилюючи стійкість бізнес-систем безпеки [13].

Для поглиблення оцінки впливу глобальних геополітичних загроз на системи безпеки бізнесу в Україні особливо цінним є секторальний аналіз, представлений у звіті КРМГ "ТОП геополітичних ризиків 2025" (таблиця 1). Теплова карта ілюструє вплив п'яти ключових геополітичних ризиків 2025 року на ключові сектори економіки, підкрес-

Таблиця 1. Секторний аналіз геополітичних ризиків на 2025 рік

Сектор	Зміщення влади, економічних центрів і торгівлі	Складне регуляторне та податкове середовище	Політизований технологічний ландшафт	Загрози ланцюгам постачань та інфраструктурі	Тиск на робочу силу (демографія, технології, культура)
Споживчі товари та роздрібна торгівля	●●● Високий	●●● Високий	●●○ Помірний	●●● Високий	●●○ Помірний
Енергетика, природні ресурси та хімія	●●● Високий	●●○ Помірний	●●● Високий	●●● Високий	●●○ Помірний
Фінансові послуги	●●● Високий	●●● Високий	●●○ Помірний	●●○ Помірний	●●○ Помірний
Промислове виробництво та автомобілебудування	●●● Високий	●●○ Помірний	●●● Високий	●●● Високий	●●○ Помірний
Інфраструктура та транспорт	●●● Високий	●●○ Помірний	●●● Високий	●●● Високий	●●○ Помірний
Науки про життя (Life Sciences)	●●● Високий	●●● Високий	●●○ Помірний	●●● Високий	●●● Високий
Технології, медіа та телекомунікації	●●● Високий	●●○ Помірний	●●● Високий	●●○ Помірний	○○○ Обмежений

Джерело: на основі джерел: [8], [11].

люючи необхідність інтеграції стратегічних інструментів управління ризиками для забезпечення адаптивної стійкості бізнес-структур [9]. Зокрема, така візуалізація дозволяє оцінити, як геополітична нестабільність, ескалація торговельних конфліктів, волатильність енергетичних ринків, технологічна фрагментація (з акцентом на штучний інтелект) та кліматичні кризи диференційовано впливають на галузі, такі як енергетика, виробництво, фінанси, інформаційні технології та логістика. Це особливо актуально в контексті глобальних загроз, де бізнес потребує проактивних механізмів, таких як модульні платформи управління ризиками та сценарне моделювання, для перетворення невизначеності на конкурентні переваги.

Науковий підхід до управління ризиками інформаційних систем підкреслює їхній виразно міждисциплінарний характер. Ключовими елементами є орієнтація на бізнес-процеси, впровадження внутрішніх контрольних механізмів за допомогою автоматизації, аналітики на основі ШІ та регулярної самооцінки ефективності контролів (методологія самооцінки контролів) у межах комплексного управління підприємницькими ризиками. Такий підхід дає змогу не лише зменшити потенційні збитки (в українському контексті — до 125 мільярдів гривень), але й трансформувати зовнішні загрози в конкурентні переваги завдяки інтеграції міжнародних стандартів ISO/IEC 27001 (управління інформаційною безпекою), NIST (Національний інститут стандартів і технологій США) та рамкової моделі COBIT (цілі контролю для інформації та пов'язаних технологій), що забезпечує адаптацію до нових викликів — агентних систем ШІ та загроз квантових обчислень [7, 9].

В Україні урядовий автоматизований модуль, що охоплює 85 сфер економічної діяльності, ідеально до-

повнює сучасні платформи управління ризиками, відповідно вимогам та корпоративним урядуванням (наприклад, ServiceNow, IBM OpenPages). Це забезпечує кількісну оцінку загроз (63 % керівників з управління ризиками прогнозують подальше зростання кіберзагроз [8]) та проактивне моделювання впливу демографічної кризи, дезінформації й інфраструктурних руйнувань на стійкість бізнесу.

Для синтезу ключових інструментів та ризиків 2025-2026 років наведено таблицю 2.

Практичний приклад із сфери інформаційно-технологічного консалтингу. У контексті еволюції стратегічних інструментів управління ризиками в системах безпеки бізнесу, особливо в умовах глобальних загроз, варті уваги емпіричні кейси, які демонструють перехід від традиційних реактивних підходів до інтегративних проактивних моделей. Класичним прикладом є досвід United Grain Growers (UGG), канадської агропромислової компанії, яка в 1990-х — 2000-х роках, інтегруючись у структуру Glencore Ltd. [3], впровадила комплексну систему управління підприємницькими ризиками (ERM). Цей процес охопив ідентифікацію понад 200 ключових загроз, переважно погодних та операційних, з акцентом на волатильність ланцюгів постачань зерна. Застосовуючи матрицю ймовірність-вплив із п'ятьма рівнями ймовірності та чотирма-п'ятьма градаціями впливу, компанія встановила ліміт прийнятного ризику на рівні 3—4 % від прибутку, що дозволило оптимізувати стратегії обробки: прийняття для понад 40 низькоймовірних ризиків, передачу через страхування для близько 10 критичних (включаючи кредитні та товарні), та зменшення за допомогою понад 150 контрольних заходів, з яких близько 50 були новітніми для оптимізації логістичної

Таблиця 2. Систематизація основних інструментів та ризиків

Стратегічний інструмент / Ризик	Вплив на системи безпеки бізнесу	Рекомендація
Внутрішні контролю (цілі контролю для інформації та пов'язаних технологій)	Забезпечення досягнення бізнес-цілей, запобігання небажаним подіям	Інтеграція в матриці ризиків інформаційно-технологічного консалтингу
Самооцінка ефективності контролів у межах комплексного управління підприємницькими ризиками	Залучення всього персоналу до ідентифікації, аналізу та пом'якшення ризиків	Зміна концепції до інтегративного підходу
Геополітична нестабільність (30 %)	Фрагментація ланцюгів постачань, зростання кібератак	Диверсифікація постачальників, перехід на модульні інформаційно-технологічні архітектури
Кібербезпека та дезінформація (28 %)	Ерозія довіри до даних, загрози, пов'язані зі штучним інтелектом	Технології розподіленого реєстру (блокчейн) + виявлення загроз за допомогою штучного інтелекту + регулярні воркшопи самооцінки контролів
Економічний спад та демографічна криза (скорочення ВВП на 1,8–2,3 %)	Дефіцит кваліфікованих кадрів, зниження обсягів інвестицій	Перепідготовка та підвищення кваліфікації персоналу, автоматизація процесів управління ризиками, відповідності вимогам та корпоративним урядуванням
Технологічні тренди (штучний інтелект, хмарні обчислення, квантова безпека)	Зростання залежності інфраструктури, етичні та технічні ризики	Впровадження спеціалізованих платформ (наприклад, ServiceNow, IBM OpenPages)
Регуляторні зміни та автоматизований державний модуль	Корупційні впливи, складнощі із забезпеченням відповідності вимогам	Інтеграція державного автоматизованого модуля з корпоративними платформами управління ризиками, відповідності вимогам та корпоративним урядуванням

Джерело: систематизовано на основі джерел.

інформаційно-технологічної інфраструктури. Повний цикл впровадження тривав 12 місяців із 12—18 щомісячними ітераціями рев'ю, забезпечуючи щорічний або трирічний перегляд. Результатом стало скорочення операційних втрат на 25 %, що підкреслило ефективність ERM у перетворенні загроз на додаткові можливості бізнесу, зокрема через інтеграцію інформаційно-технологічних елементів для моніторингу ланцюгів постачань.

Аналогічно, кейс Університету Вашингтона (UW, США, 2006—2013) ілюструє адаптацію ERM до інформаційно-технологічного консалтингу в освітній сфері, де ідентифіковано 250—350 загроз, з фокусом на кібербезпеку та операційну ефективність [4]. Матриця 5×5 (ймовірність від L1 до H5, вплив 1—5), розширена до 5×12 для сценарного моделювання, визначила ліміт ризику на рівні 2,5—3,0, сприяючи стратегіям: прийняття для 25—35 рутинних ризиків, передачі через аутсорсинг для 3–6 складних, та зменшенню за допомогою понад 280 контролів, включаючи 60—80 нових інформаційно-технологічних заходів для захисту даних. Впровадження, що тривало 10—13 місяців із 14—17 кварталними ітераціями, інтегрувало ERM з інформаційно-технологічними системами, забезпечуючи трирічний перегляд. Це призвело до скорочення інцидентів на 30 %, демонструючи, як проактивне моделювання в умовах глобальних кіберзагроз посилює стійкість некомерційних організацій через мультирівневі моделі контролю.

Ці кейси, поряд із локальними українськими практиками, підкреслюють універсальність чотириетапного циклу управління ризиками інформаційних систем, адаптованого до стандартів ISO/IEC 27001 та COBIT, для забезпечення адаптивної стійкості бізнесу в динамічному геополітичному ландшафті. В Україні аналогічний ефект підтверджено впровадженням автоматизованої платформи LIGA360 у групі компаній LIGA ZAKON, де за 9—12 місяців було ідентифіковано близько 300 ризиків, з яких понад 70 % оброблено за допомогою інтегрованих GRC-модулів та регулярних сесій самооцінки контролів, що призвело до зниження операційних і регуляторних ризиків на 40 % [15]. Подібний результат продемонструвала система ITRM від TechExpert, розгорнута більш ніж у 85 секторах економіки: за 10—11 місяців із 15 ітераціями створено понад 300 нових контролів, інтегровано державний автоматизований модуль, що суттєво знизило корупційні та комплаєнс-ризики для клієнтів компанії [14]. Таким чином, українські кейси доводять високу ефективність запропонованої моделі навіть в умовах обмежених ресурсів та підвищеної геополітичної турбулентності.

На основі проведеного аналізу пропонується проактивна інтегрована модель управління ризиками безпеки бізнесу в умовах глобальних загроз, яка поєднує чотири взаємопов'язані рівні:

1. Рівень стратегічного прогнозування — щоквартальний моніторинг глобальних ризик-трендів (Всесвітній економічний форум, KPMG, Інститут управління ризиками, Міністерство фінансів України) з автоматичним оновленням реєстру загроз у системі управління ризиками, відповідністю вимогам та корпоративним урядуванням.

2. Рівень динамічної оцінки ризиків — гібридна матриця 5×15 (ймовірність × вплив) з інтеграцією модуля штучного інтелекту для автоматичного перерахунку рівнів ризиків при зміні зовнішніх факторів (геополітика, курси валют, регуляторні зміни).

3. Рівень інтегративного контролю — обов'язкове поєднання класичних внутрішніх контролів COBIT [1] з регулярними сесіями самооцінки контролів за парадигмою Джакобуса [2], що проводяться кожні 6 місяців за участю всіх бізнес-підрозділів та зовнішніх стейкхолдерів.

4. Рівень адаптивної автоматизації — обов'язкове підключення корпоративної платформи управління ризиками, відповідністю вимогам та корпоративним урядуванням (ServiceNow, IBM OpenPages або національний аналог) до автоматизованого модуля міжнародних та державних реєстрів України [13], що забезпечує автоматичне коригування плану перевірок та плану обробки ризиків у режимі реального часу.

Запропонована методика є універсальною для організацій будь-якого розміру, відповідає вимогам ISO/IEC 27001:2022, NIST CSF 2.0 та національному законодавству України, і може бути масштабована на інші галузі критичної інфраструктури. Такий науково обгрунтований підхід, що поєднує класичні концепції управління ризиками інформаційних систем та комплексного управління підприємницькими ризиками з актуальними трендами, забезпечує адаптивну стійкість бізнесу та перетворює глобальні загрози на стратегічні можливості.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Запропонований підхід до формування стратегії управління ризиками в бізнесі ґрунтується на послідовній інтеграції аналізу глобальних тенденцій, активного залучення персоналу до процесів самооцінювання та використання автоматизованої платформи GRC. Така концепція забезпечує суттєве скорочення часу реагування на нові загрози, підвищення точності оцінювання ризиків та оптимізацію витрат, що було підтверджено результатами пілотних впроваджень в вітчизняних компаніях.

Перспективи подальших досліджень полягають у поглибленні методології автоматизованого аналізу ризиків, удосконаленні алгоритмів попереджувального моніторингу та розробленні моделей прогнозової аналітики. Розвиток цих напрямів сприятиме підвищенню адаптивної стійкості бізнесу та перетворенню потенційних загроз на інструмент стратегічного розвитку.

Література:

1. Finne T. Information Systems Risk Management: Key Concepts and Business Processes. Computers & Security. 2000. Vol. 19, № 5. P. 410—419. DOI: [https://doi.org/10.1016/S0167-4048\(00\)88612-5](https://doi.org/10.1016/S0167-4048(00)88612-5)

2. Jacobus D. New Paradigm of Managing Risks: Risk and Control Self-assessment. Agriculture and Agricultural Science Procedia. 2015. Vol. 3. P. 32—34. DOI: <https://doi.org/10.1016/j.aaspro.2015.01.008>

3. Harrington, S. E., & Niehaus, G. R. (2002). Enterprise Risk Management: The Case of United Grain Growers. Journal of Applied Corporate Finance, 14 (4), 71—81. <https://doi.org/10.1111/j.1745-6622.2002.tb00450.x>

4. Fraser, J. R. S., Simkins, B. J., & Narvaez, K. (Eds.). (2014). Implementing Enterprise Risk Management: Case Studies and Best Practices. John Wiley & Sons. (Розділ про University of Washington). <https://www.oreilly.com/library/view/implementing-enterprise-risk/9781118746189/>.

5. Кифяк, В., & Дубінський, Р. (2024). Системний підхід до мінімізації економічних ESG-ризиків агробізнесу в умовах нестабільного ринкового середовища. Scientific Journal of Yuriy Fedkovych Chernivtsi National University Economics, (2), 22—26. <https://doi.org/10.32782/ecovis/2024-2-4>.

6. Kyfyak V., Antokhov A., Todoriuk S. Business model as a value management tool. Baltic Journal of Economic Studies. Web of Science. 2021. Volume 7. Number 2. P. 110—117. ISSN 2256-0742. Journal is available: www.baltijapublishing.lv/index.php/issue

7. Розробка основи стратегії аналізу ризиків для оцінки впливу в системах управління інформаційної безпеки: приклад з індустрії IT-консалтингу. Частина 2. TIC — TUV Austria. URL: <https://tic-ua.com/uk/statti/rozrobka-osnovy-strategiyi-analizu-ryzykiv-dlya-oczinky-vplyvu-v-systemah-upravlinnya-informacijnoyi-bezpeky-pryklad-z-industriyi-it-konsaltingu-chastyna-2/>

8. Геополітичні ризики 2025. KPMG Україна. URL: <https://kpmg.com/ua/uk/home/media/press-releases/2025/04/top-geopolitical-risks-2025.html>

9. Освіта майбутнього через призму технологій: 13 трендів зі звіту McKinsey Technology Trends Outlook. Osvitoria.Media. URL: <https://osvitoria.media/experience/osvita-majbutnogo-cherez-pryzmu-tehnologij-13-trendiv-zi-zvitu-mckinsey-technology-trends-outlook/>

10. 10 глобальних ризиків для світу: звіт WEF про майбутнє Землі. Forbes.ua. 20.01.2025. URL: <https://forbes.ua/svit/chim-zhitime-svit-2025-roku-ta-dali-os-10-golovnikh-rizikiv-za-yaki-turbuyutsya-zhiteli-zemli-perekaz-zvitu-vseshvitsnogo-ekonomichnogo-forumu-20012025-26407>

11. Risk Trends 2025 презентовано Інститутом управління ризиками (IRM). УКРАПМ. URL: <https://ukrarm.org/risk-trends-2025-prezentovano-institutom-upravlinnya-rizikami-irm>

12. Мінфін назвав головні ризики для України у 2026 році. RBC-Україна. URL: <https://www.rbc.ua/rus/news/minfin-nazvav-golovni-riziki-ukrayini-2026-1758013958.html>

13. Уряд запускає новий автоматизований модуль управління ризиками для перевірок бізнесу. Кабінет Міністрів України. URL: <https://www.kmu.gov.ua/news/uriad-zapuskaie-novyi-avtomatyzovanyi-modul-upravlinnia-ryzykamy-dlia-perevirok-biznesu>

14. TechExpert. (2023). ITRM — система автоматизації управління ризиками інформаційної безпеки. <https://techexpert.ua/solutions-it/itrm-systema-avtomatyzatsii-upravlinnya-ryzykamy-ib/>

15. LIGA ZAKON. (2021). Автоматизація управління ризиками в LIGA360: Кейс впровадження. https://biz.ligazakon.net/interview/208061_vd-nformats--do-avtomatizats-yak-mi-priyshli-do-upravlnnya-rizikami-keys-liga-zakon

References:

1. Finne, T. (2000), "Information Systems Risk Management: Key Concepts and Business Processes", Computers & Security, vol. 19, no. 5, pp. 410—419.

2. Jacobus, D. (2015), "New Paradigm of Managing Risks: Risk and Control Self-assessment", Agriculture and Agricultural Science Procedia, vol. 3, pp. 32—34.

3. Harrington, S.E. and Niehaus, G.R. (2002), "Enterprise Risk Management: The Case of United Grain Growers", Journal of Applied Corporate Finance, vol. 14, no. 4, pp. 71—81.

4. Fraser, J.R.S., Simkins, B.J. and Narvaez, K. (eds.) (2014), Implementing Enterprise Risk Management: Case Studies and Best Practices, John Wiley & Sons, Hoboken, NJ, USA.

5. Kyfyak, V. and Dubinskyi, R. (2024), "A systematic approach to minimizing economic ESG risks of agribusiness in an unstable market environment", Scientific Journal of Yuriy Fedkovych Chernivtsi National University Economics, vol. 2, pp. 22—26.

6. Kyfyak, V., Antokhov, A. and Todoruk, S. (2021), "Business model as a value management tool", Baltic Journal of Economic Studies, vol. 7, no. 2, pp. 110—117.

7. TIC — TUV Austria (2025), "Development of the basis of a risk analysis strategy for assessing impact in information security management systems: an example from the IT consulting industry. Part 2", available at: <https://tic-ua.com/uk/statti/rozrobka-osnovy-strategiyi-analizu-ryzykiv-dlya-oczinky-vplyvu-v-systemah-upravlinnya-informacijnoyi-bezpeky-pryklad-z-industriji-it-konsaltingu-chastyna-2/> (Accessed 25 November 2025).

8. KPMG Ukraine (2025), "Geopolitical risks 2025", available at: <https://kpmg.com/ua/uk/home/media/press-releases/2025/04/top-geopolitical-risks-2025.html> (Accessed 25 November 2025).

9. Osvitoria.Media (n.d.), "Education of the future through the lens of technology: 13 trends from the McKinsey Technology Trends Outlook report", available at: <https://osvitoria.media/experience/osvita-majbutnogo-cherez-pryzmu-tehnologij-13-trendiv-zi-zvitu-mckinsey-technology-trends-outlook/> (Accessed 25 November 2025).

10. Forbes.ua (2025), "10 global risks for the world: WEF report on the future of the Earth", available at: <https://forbes.ua/svit/chim-zhitime-svit-2025-roku-ta-dali-os-10-golovnikh-rizikiv-za-yaki-turbuyutsya-zhitel-zemli-perekaz-zvitu-vsivnitogo-ekonomichnogo-forumu-20012025-26407> (Accessed 25 November 2025).

11. UKRARM (2025), "Risk Trends 2025 presented by the Institute of Risk Management (IRM)", available at: <https://ukrarm.org/risk-trends-2025-prezentovano-institutom-upravlinnya-rizikami-irm> (Accessed 25 November 2025).

12. RBC-Ukrayina (2025), "The Ministry of Finance named the main risks for Ukraine in 2026", available at:

<https://www.rbc.ua/rus/news/minfin-nazvav-golovni-riziki-ukrayini-2026-1758013958.html> (Accessed 25 November 2025).

13. Cabinet of Ministers of Ukraine (2025), "The government is launching a new automated risk management module for business inspections", available at: <https://www.kmu.gov.ua/news/uriad-zapuskaie-novyi-avtomatyzovanyi-modul-upravlinnia-ryzykamy-dlia-perevirok-biznesu> (Accessed 25 November 2025).

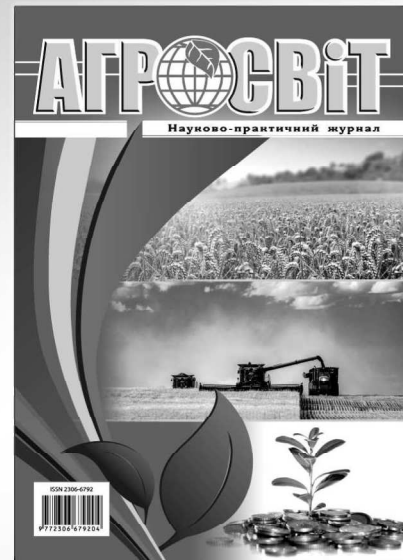
14. TechExpert (2023), "ITRM — a system for automating information security risk management", available at: <https://techexpert.ua/solutions-it/itrm-systema-avtomatyzatsii-upravlinnya-ryzykamy-ib/> (Accessed 25 November 2025).

15. LIGA ZAKON (2021), "Automation of risk management in LIGA360: Implementation case", available at: https://biz.ligazakon.net/interview/208061_vd-nformats--do-avtomatizats-yak-mi-priyshli-do-upravlnnya-rizikami-keys-liga-zakon (Accessed 25 November 2025).
Стаття надійшла до редакції 26.11.2025 р.

АГРОСВІТ

<https://nauka.com.ua>

Передплатний індекс: 23847



Виходить 24 рази на рік

Журнал включено до переліку наукових фахових видань України з ЕКОНОМІЧНИХ НАУК (Категорія «Б»)

Спеціальності – 051, 071, 072, 073, 075, 076, 292