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. № 2.
ISSN 2307-2105

DOI: http://doi.org/10.32702/2307-2105.2026.2.50

УДК 339.9:005.334:004.056

П. Г. Перерва,

д. е. н., професор, професор кафедри економіки бізнесу і міжнародних економічних відносин, Національний технічний університет «ХПІ»

ORCID ID: https://orcid.org/0000-0002-6256-9329

Т. О. Кобєлєва,

д. е. н., професор, професорка кафедри економіки бізнесу і міжнародних економічних відносин, Національний технічний університет «ХПІ»

ORCID ID: https://orcid.org/0000-0001-6618-0380

Р. С. Лепський,

аспірант, Національний технічний університет «ХПІ»

ORCID ID: https://orcid.org/0009-0003-0065-9833

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ РИЗИКАМИ МІЖНАРОДНИХ БІЗНЕС-ПРОЦЕСІВ В УМОВАХ ЦИФРОВОЇ ТА КАДРОВОЇ БЕЗПЕКИ

P. Pererva,
Doctor of Economic Sciences, Professor, Professor of the Department of Business Economics and International Economic Relations,
National Technical University "KhPI"
T. Kobielieva,
Doctor of Economic Sciences, Professor, Professor of the Department of Business Economics and International Economic Relations,
National Technical University "KhPI"
R. Lepskyi,
Postgraduate student, National Technical University "KhPI"

INFORMATION SUPPORT FOR RISK MANAGEMENT OF INTERNATIONAL BUSINESS PROCESSES IN THE CONTEXT OF DIGITAL AND PERSONNEL SECURITY

У статті досліджено теоретико-методологічні засади та практичні аспекти формування системи інформаційного забезпечення управління ризиками міжнародних бізнес-процесів. У контексті глобальної цифровізації обґрунтовано необхідність інтегрованого підходу, що поєднує інструменти цифрової та кадрової безпеки для забезпечення стратегічної стійкості підприємства на світовому ринку. Проаналізував трансформацію профілю ризиків міжнародних компаній, акцентувавши увагу на тому, що в сучасних умовах інформаційний капітал стає основним об'єктом захисту. У роботі деталізовано складові управління ризиками у сфері кадрової безпеки, зокрема через формування корпоративної культури, впровадження систем контролю доступу (UEBA, DLP) та підвищення лояльності персоналу. Систематизовано основні інструменти моніторингу інформаційних потоків у реальному часі. Результати дослідження мають практичне значення для міжнародних компаній при розробці стратегій мінімізації транскордонних ризиків та адаптації до міжнародних стандартів захисту даних.

The article conducts a comprehensive study of the theoretical and applied foundations for developing an information support system for risk management in international business processes. The relevance of the topic is driven by the rapid transformation of the global economic landscape, where digitalization acts not only as a driver of development but also as a source of new systemic threats. It is substantiated that in the transition to the "Enterprise 4.0" model, traditional risk management methods lose their effectiveness, giving way to integrated management systems based on the synergy of digital and personnel security. The purpose of the work is to develop a holistic approach to risk management in international business by optimizing information flows and strengthening the organization's protective circuits. The study employs a complex of methods, including system-structural analysis, logical modeling, and strategic forecasting. Primary attention is paid to the transformation of the risk object: it is proven that in modern international business processes, the object of risk becomes the information potential of the enterprise rather than merely its physical assets. The scientific novelty of the results lies in the detailed specification of risk management components within the sphere of personnel security. The author demonstrates that the human factor remains the most critical link, requiring the implementation of "soft" influence tools — the formation of a corporate security culture and loyalty programs — in combination with "hard" technical monitoring (UEBA analytics, DLP systems). Special emphasis is placed on the digital security component, where the key role is played by the implementation of the "Zero Trust" model and multi-level authentication systems, allowing for the localization of threats in the context of cross-border data transfer. The practical significance of the research lies in the systematization of real-time information flow monitoring tools, which enables international companies to ensure business process continuity and compliance with international standards (GDPR, ISO/IEC 27001). Recommendations are formulated for the adaptation of Ukrainian enterprises to the requirements of the global digital environment in the context of post-war recovery. The conclusions of the article confirm that only the harmonization of high technological standards

with clear regulation of personnel actions allows for the creation of a resilient protection system for the enterprise's information capital in a dynamic global environment.

Ключові слова: *управління ризиками, міжнародний бізнес, кадрова безпека, цифрова безпека, інформаційні технології, управління бізнес-процесами, економічна оцінка, інформаційний потенціал, формування, управління підприємством, світогосподарський розвиток*

Keywords: *risk management, international business, personnel security, digital security, information technology, business process management, economic assessment, information potential, formation, enterprise management, world economic development.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний етап розвитку глобальної економіки характеризується переходом міжнародних компаній до моделі «Enterprise 4.0», де цифрові технології перестають бути лише допоміжним інструментом і стають фундаментом усіх бізнес-процесів [1, 2]. Глобалізація цифрового простору призвела до того, що ланцюги створення вартості тепер мають розгалужений, транскордонний характер, інтегруючи підрозділи, постачальників та клієнтів у єдину інформаційну екосистему [4, 5]. Це створює умови для небаченої раніше операційної ефективності, проте одночасно радикально трансформує профіль ризиків, з якими стикається міжнародне підприємництво. У цих умовах міжнародні бізнес-процеси стають дедалі вразливішими до комплексу ризиків, що мають комплексний характер. Традиційні методи ризик-менеджменту, орієнтовані на статичні моделі аналізу, втрачають свою ефективність, поступаючись місцем системам, що базуються на оперативному та якісному інформаційному забезпеченні [6, 7]. Особливої актуальності набуває питання синхронізації цифрової стійкості підприємства з його кадровою безпекою,

оскільки саме людський чинник залишається найбільш вразливою ланкою в системі кіберзахисту та інтелектуальної безпеки міжнародних корпорацій.

Аналіз останніх досліджень та публікацій. Проблематика інформаційного супроводу управлінських рішень та ризик-орієнтованого підходу в міжнародному бізнесі перебуває у центрі уваги багатьох науковців. Теоретичні засади управління ризиками закладені у фундаментальних працях закордонних [2, 3, 8, 9] та вітчизняних [10-15] вчених. Наукова дискусія щодо формування ефективної системи інформаційного забезпечення управлінських рішень у міжнародному бізнесі триває протягом останніх десятиліть, адаптуючись до викликів глобальної цифровізації. Глибокий аналіз теоретичних засад стратегічного управління ризиками та економічної безпеки підприємства представлений у фундаментальних працях І.М.Посохова [1], який розглядає інформаційний та інтелектуальний потенціал як ключовий драйвер конкурентоспроможності на міжнародних ринках. У його роботах акцентується увага на необхідності комплексного оцінювання ризиків через призму інноваційного розвитку та захисту прав інтелектуальної власності, що є особливо актуальним в умовах транскордонного переміщення капіталу та технологій. Питання трансформації бізнес-моделей під впливом Industry 4.0 та цифровізації підприємницьких структур ґрунтовно досліджено у наукових доробках К.М.Краус та Н.М.Краус [6]. Автори підкреслюють, що перехід до цифрових екосистем не лише створює нові можливості для масштабування бізнесу, а й генерує специфічні ризики, пов'язані з кібербезпекою та надійністю інформаційних каналів. Своєю чергою, İlhan Ümit доповнює цю дискусію вивченням ролі еко-інновацій та цифрової складності, доводячи, що стійкість міжнародних бізнес-процесів прямо залежить від здатності менеджменту інтегрувати цифрові інструменти у загальну стратегію сталого розвитку [2]. Особливе місце в сучасних дослідженнях посідає проблема людського чинника в системі ризик-менеджменту. В дослідженнях [8, 9] кадрова безпека є невід’ємною частиною економічної стійкості, оскільки саме

персонал виступає одночасно і основним ресурсом, і джерелом потенційних загроз інформаційній цілісності корпорації. Дослідження зарубіжних авторів, хоча і зосереджені переважно на циркулярних моделях, опосередковано підтверджують, що будь-яка трансформація бізнес-процесів вимагає радикальної зміни підходів до підготовки та перевірки персоналу [2, 8, 15].

Незважаючи на значний доробок, механізми інтеграції цифрових інструментів контролю із системами забезпечення кадрової безпеки в контексті міжнародної діяльності потребують подальшого детального вивчення.

Формулювання цілей статті (постановка завдання). Метою цієї роботи є теоретичне обґрунтування та розробка методичних підходів до формування системи інформаційного забезпечення управління ризиками міжнародних бізнес-процесів.

Виклад основного матеріалу дослідження. Особливістю сучасної трансформації є детермінація бізнес-процесів через великі масиви даних. Варто акцентувати увагу на тому, що в умовах цифрової трансформації міжнародні бізнес-процеси стають «прозорими» не лише для партнерів, а й для конкурентів та зловмисників.

У системі міжнародного бізнесу кадрова безпека перестає бути суто функцією HR-департаменту і трансформується у стратегічний контур захисту інформаційних та інтелектуальних активів. Людський чинник у цифровому середовищі є найбільш динамічним і водночас найменш прогнозованим джерелом ризиків. Тому управління кадровими ризиками має базуватися на комплексному підході, що поєднує адміністративні, технічні та психологічні інструменти впливу (рис.1).

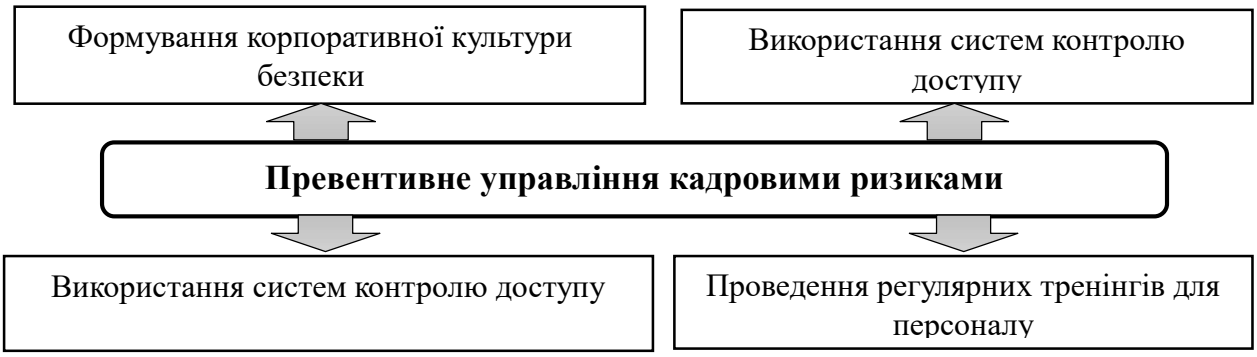

Рис. 1. Складові комплексного підходу до управління кадровими ризиками в міжнародному бізнесі

Джерело: сформовано авторами

Основою превентивного управління ризиками є створення корпоративної культури, де безпека усвідомлюється кожним працівником як спільна цінність, а не як сукупність обмежень. У міжнародних компаніях, де персонал розосереджений між різними країнами та правовими системами, формування єдиного «кодексу цифрової поведінки» є критичним. Корпоративна культура безпеки, на наш погляд, передбачає інтерналізацію стандартів, тобто перетворення зовнішніх вимог на внутрішні переконання співробітників; прозорість політик, коли кожен фахівець має чітко розуміти межі своєї відповідальності та наслідки порушення протоколів роботи з даними; етику повідомлень, яка забезпечується стимулюванням внутрішньої звітності про потенційні вразливості або підозрілу активність без остраху перед санкціями. Пропонований підхід дозволяє мінімізувати ризики, пов’язані з ненавмисними помилками персоналу, які за статистикою складають понад 60% усіх витоків інформації в глобальних мережах. Технічна складова кадрової безпеки в міжнародному бізнесі реалізується через складні ієрархічні системи контролю доступу. В умовах віддаленої роботи та транскордонних операцій традиційних паролів недостатньо. Сучасний інструментарій передбачає надання працівнику доступу лише до тих сегментів бази даних, які необхідні для виконання поточної задачі. Це локалізує ризик у разі компрометації облікового запису. Створення

додаткових бар'єрів для несанкціонованого входу, що є особливо актуальним для топ-менеджменту та системних адміністраторів. Моніторинг вихідного трафіку для запобігання несанкціонованому копіюванню комерційної таємниці. Регулярне навчання є інструментом актуалізації знань у середовищі, де методи соціальної інженерії (фішинг, претекстинг) постійно вдосконалюються. Ефективна програма тренінгів у міжнародному бізнесі має охоплювати проведення «контрольних» фішингових розсилок для перевірки пильності персоналу; ознайомлення працівників із особливостями законодавства про захист персональних даних у різних регіонах присутності компанії; навчання методів шифрування та безпечної передачі інформації через незахищені канали зв'язку. Тренінги повинні проводитися не формально «раз на рік», а бути ітераційним процесом, що супроводжує впровадження будь-якої нової технології в компанії.

Найвищий рівень кадрової безпеки досягається тоді, коли працівник лояльний до організації. Ризик інсайдерської діяльності (свідомого шкідництва чи шпигунства) прямо корелює з рівнем задоволеності персоналу та відчуттям справедливості. У міжнародному бізнес-середовищі програми лояльності мають включати зменшення плинності кадрів автоматично знижує ризик витоку знань до конкурентів; моніторинг професійного вигорання, яке часто стає причиною втрати пильності або виникнення деструктивної поведінки; коли працівник ідентифікує свій успіх із успіхом компанії, він стає природним захисником її інтересів.

Економічне узагальнення складників системи управління ризиками кадрової безпеки в міжнародному бізнесі представлено в табл.1.

Таким чином, кадрова безпека у міжнародних бізнес-процесах є не статичним станом, а безперервним процесом управління ризиками. Тільки синергія жорсткого технічного контролю доступу із «м’яким» впливом через корпоративну культуру та мотивацію дозволяє створити стійку систему захисту інформаційного капіталу підприємства.

Таблиця 1. Складники системи управління ризиками кадрової безпеки в міжнародному бізнесі

Назва складової	Економічна сутність та мета	Інструментарій визначення і управління	Особливості використання
Корпоративна культура безпеки	Превентивне управління через усвідомлення безпеки як спільної цінності; мінімізація ненавмисних помилок (60% витоків)	Інтерналізація стандартів (ISO/IEC 27001), прозорість політик відповідальності, етика повідомлень («no-blame»)	Формування єдиного «кодексу цифрової поведінки» для персоналу в різних країнах та правових системах
Системи контролю доступу	Технічний захист через ієрархічне обмеження прав доступу до інформаційних активів	Принцип найменших привілеїв (Least Privilege), MFA, біометрія, DLP-системи, ШІ-аналітика поведінки (UEBA).	Необхідність виходу за межі традиційних паролів при віддаленій роботі та операціях транскордонності
Регулярні тренінги персоналу	Актуалізація знань і цифрової гігієни для протидії методам соціальної інженерії	Симуляції фішингових атак, крос-культурне навчання (GDPR, CCPA), тренінги з шифрування та конфіденційності	Ітераційний характер навчання, що супроводжує впровадження кожної нової технології
Програми мотивації та лояльності	Зниження ризику свідомого шкідництва через підвищення задоволеності та відчуття справедливості	Конкурентна винагорода, психологічна підтримка (проти вигорання), кар'єрні ліфти, бонуси за безпеку	Пряма кореляція між лояльністю працівника та надійністю захисту інформаційного капіталу підприємства

Джерело: сформовано авторами

Цифрова безпека в контексті міжнародного бізнесу трансформувалася з вузькоспеціалізованого ІТ-питання на фундамент стратегічної стійкості підприємства. Оскільки інформаційні потоки міжнародних компаній перетинають декілька юрисдикцій, управління цифровими ризиками вимагає розробки багаторівневої архітектури захисту, яка здатна адаптуватися до динамічного ландшафту глобальних кіберзагроз.

Захист конфіденційної інформації у транскордонному середовищі ускладнюється диверсифікацією методів кібератак: від цілеспрямованого промислового шпигунства до масового використання програм-вимагачів. У сучасних умовах стратегія захисту базується на концепції «глибокої ешелонованої оборони». Ефективний захист корпоративних даних

передбачає використання наскрізного шифрування для даних як під час їх зберігання, так і в процесі передачі через міжнародні канали зв'язку; розподіл корпоративної IT-інфраструктури на ізольовані сегменти, що дозволяє локалізувати загрозу у разі проникнення в одну з підсистем і запобігти горизонтальному переміщенню зловмисника мережею; створення географічно розподілених копій критично важливих даних, що забезпечує безперервність бізнес-процесів навіть у разі масштабних атак на фізичну або хмарну інфраструктуру компанії.

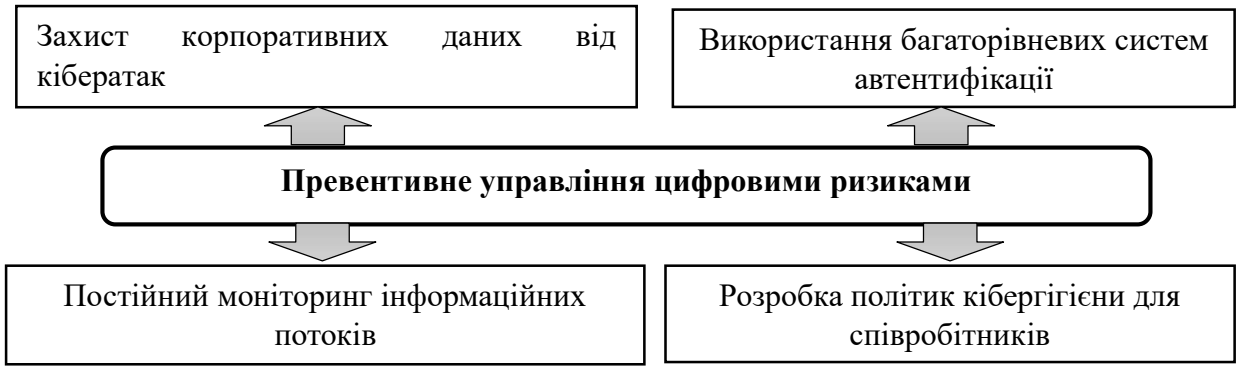

Рис. 2. Складові комплексного підходу до управління цифровими ризиками в міжнародному бізнесі

Джерело: сформовано авторами

В умовах глобалізації бізнесу, де доступ до корпоративних систем здійснюється з різних географічних локацій та пристроїв, традиційна модель ідентифікації за допомогою лише паролів виявилася неефективною. Основою сучасної цифрової безпеки є перехід до моделі Zero Trust («Нульова довіра»), де кожен запит на доступ піддається суворій перевірці. Дана модель передбачає поєднання декількох факторів підтвердження особи; використання алгоритмів, що оцінюють контекст входу; посилений контроль за обліковими записами адміністраторів, які мають доступ до критичної інфраструктури, що мінімізує ризик системного компрометування.

Інформаційне забезпечення ризик-менеджменту в цифровій сфері неможливе без безперервного аналізу мережевої активності. Постійний моніторинг дозволяє ідентифікувати загрози на етапі їх зародження, до

моменту нанесення реальних збитків. Сучасний інструментарій моніторингу охоплює агрегацію та кореляцію логів з усіх корпоративних пристроїв для виявлення підозрілих патернів поведінки; створення спеціалізованих центрів (власних або на аутсорсингу), які в режимі 24/7 відстежують стан безпеки та оперативно реагують на інциденти; використання методів машинного навчання для виявлення прихованих каналів витоку інформації або несанкціонованої передачі великих обсягів даних за межі корпоративного контуру.

Цифрова стійкість міжнародної компанії безпосередньо залежить від поведінкових стандартів її персоналу. Політика кібергігієни — це сукупність регламентованих правил, спрямованих на формування безпечних звичок при роботі з IT-ресурсами. Основними складовими політики кібергігієни є в встановлення чітких вимог до безпеки особистих гаджетів співробітників, які використовуються для доступу до корпоративної пошти або баз даних; вимоги щодо складності та регулярної зміни паролів, а також заборона їх повторного використання на різних сервісах; регламенти щодо перевірки вкладень, посилань та заборони використання незахищених публічних Wi-Fi мереж для виконання службових обов'язків; чіткий алгоритм дій співробітника у разі підозри на злам пристрою або втрату корпоративного носія інформації.

Економічне узагальнення складників системи управління ризиками кадрової безпеки в міжнародному бізнесі представлено в табл.2.

Управління цифровими ризиками у міжнародному бізнесі потребує гармонізації високих технологічних стандартів із чіткою регламентацією дій персоналу. Поєднання систем захисту даних, багаторівневої автентифікації та постійного моніторингу дозволяє створити безпечне середовище для розвитку транскордонних бізнес-процесів, нівелюючи загрози цифрового простору.

Таблиця 2. Складники системи управління ризиками цифрової безпеки в міжнародному бізнесі

Назва складової	Економічна сутність та мета	Інструментарій визначення і управління	Особливості використання в міжнародному бізнесі
Захист корпоративних даних від кібератак	Забезпечення стійкості та цілісності інформаційних активів	Наскрізне шифрування, сегментація мереж, плани аварійного відновлення (DRP)	Реалізація стратегії «глибокої ешелонованої оборони» для захисту розподілених активів
Багаторівнева автентифікація	Мінімізація ризику несанкціонованого доступу через сувору ідентифікацію користувача	Модель Zero Trust, багатофакторна автентифікація (MFA), біометрія, PAM-системи	Використання адаптивних алгоритмів, що оцінюють контекст входу (геолокацію та IP) у реальному часі
Моніторинг інформаційних потоків	Безперервний аудит мережевої активності для раннього виявлення та нейтралізації загроз	SIEM-системи, центри безпеки (SOC 24/7), аналіз аномалій на базі машинного навчання (ML)	Необхідність обробки великих масивів даних (Big Data) для виявлення прихованих каналів витоку інформації
Політики кібергігієни	Формування безпечних поведінкових стандартів персоналу при роботі з IT-інфраструктурою	Регламенти BYOD (власні пристрої), парольні політики, правила роботи з поштою, протоколи звітності про інциденти	Уніфікація правил безпеки для співробітників у різних країнах, незалежно від їхньої технічної грамотності

Джерело: сформовано авторами

Зазначені складові формують цілісну техніко-технологічну вертикаль захисту. Якщо кадрова безпека (попередня таблиця) спрямована на роботу з мотивацією та лояльністю людини, то цифрова безпека створює бар'єри, які мінімізують шкоду навіть у разі помилки або злого умислу персоналу.

Висновки та перспективи подальших розвідок у даному напрямі. У результаті проведеного дослідження здійснено теоретичне узагальнення та розроблено методичні підходи до формування системи інформаційного забезпечення управління ризиками міжнародних бізнес-процесів. Доведено, що в умовах глобальної цифровізації інформаційне забезпечення стає стратегічним ресурсом ризик-менеджменту. Трансформація міжнародних бізнес-процесів у модель «Enterprise 4.0» зумовлює перехід від реактивного захисту до превентивної моделі цифрової стійкості, де ключовим об’єктом захисту виступає інформаційний потенціал підприємства та безперервність його транскордонних потоків даних. Встановлено, що найвищу загрозу для

стабільності міжнародних компаній становить конвергенція цифрових та кадрових ризиків. Технічні вразливості систем часто стають наслідком недостатнього рівня кадрової безпеки, що вимагає інтегрованого підходу до управління. Запропоновано розглядати цифрову безпеку (технічні бар'єри) та кадрову безпеку (лояльність та компетенції) як єдиний захисний контур організації. Обґрунтовано складники управління ризиками у сфері кадрової безпеки. Доведено, що ефективність захисту інформації прямо залежить від синергії «м'яких» інструментів (формування корпоративної культури безпеки, програм лояльності, психологічної підтримки) та «жорстких» методів контролю. Це дозволяє мінімізувати інсайдерські загрози та ненавмисні помилки персоналу, які є причиною більшості витоків даних. Систематизовано ключові інструменти цифрової безпеки в міжнародному середовищі, серед яких особливе місце посідають системи моніторингу інформаційних потоків у реальному часі (SIEM/SOC) та модель «Нульової довіри». Визначено, що практична реалізація запропонованих підходів дозволить міжнародним компаніям не лише знизити ймовірність реалізації ризиків, а й забезпечити відповідність жорстким міжнародним стандартам (GDPR, ISO/IEC 27001). Перспективи подальших досліджень полягають у розробці алгоритмів автоматизованого оцінювання кадрових ризиків із використанням технологій штучного інтелекту та великих даних.

Література

1. Формування механізму управління ризиками переробних підприємств: монографія / За ред. І. М. Посохова. Харків: Видавництво Іванченка І. С., 2022. 278 с.

2. İlhan Ümit (2025). Cybersecurity in Human Resource Management in the Context of Remote Work: Policy, Practice, and Risk Management. DOI: https://doi.org/10.4018/979-8-3693-6417-8.ch007.

3. The Global Risks Report 2024. 19th Edition. *World Economic Forum*. URL: https://www.weforum.org/publications/global-risks-report-2024/ (дата звернення 25.01.2026).

4. Pererva P., Nagy S., Maslak M. (2018) Organization of marketing activities on the intrapreneurship // *MIND Journal*. № 5. 10 p. DOI:10.13140/RG.2.2.17332.10883

5. Старостіна А. О. Маркетинг: теорія, світовий досвід, українська практика: підруч. К.: *Знання*, 2009. 1070 с. 401 с.

6. Краус К. М., Краус Н. М. Цифрова економіка: тренди та перспективи авангардного розвитку. *Ефективна економіка*. 2018. № 1. URL: http://www.economy.nayka.com.ua/?op=1&z=6047 (дата звернення 25.01.2026).

7. Kosenko A. P., Kobielieva T. O., Tkachova N. P. The definition of industry park electrical products // *Scientific bulletin of Polissia.* Part 2. № 3 (11). 2017. P. 43-50. DOI: https://doi.org/10.25140/10.25140/2410-957620173(11)43-50

8. Kocziszky György, Pererva P. G., Szakaly D., Somosi Veres M. (2012) Technology transfer. Kharkiv-Miskolc: NTU «KhPI». 668 p.

9. Перерва П. Г. Управління маркетингом на машинобудівному підприємстві // Навч. посібник для інж.-техн. вузів. Харків: «Основа», 1993. 288с.

10. Перерва П. Г. Управління інноваційною діяльністю підприємства // Маркетинг: підручник / За ред. О. А. Старостіної. К.: Знання, 2009. С. 461-518.

11. Pererva P. G., Kocziszky G., Veres Somosi M. (2019) Compliance program: [tutorial]. Kharkov; Miskolc : NTU "KhPI". 689 p. URL: http://repository.kpi.kharkov.ua/handle/KhPI-Press/48662

12. Борзенко В. І., Перерва П. Г., Кобєлєва Т. О. Інтелектуальна власність: магістерський курс: підручник. Харків: НТУ «ХПІ», 2019. 1002 с.

13. Товажнянський В. Л. Антикризовий механізм сталого розвитку підприємства. Х.: Віровець А. П. : Апостроф, 2012. 703 с.

14. Економіка та організація інноваційної діяльності: підруч. / за ред. П. Г. Перерви, С. А. Меховича, М. І. Погорєлова. Харків: НТУ «ХПІ», 2008. 1080 с.

15. Товажнянський В. Л., Перерва П. Г. Антикризовий моніторинг фінансово-економічних показників роботи машинобудівного підприємства // *Економіка розвитку.* Харків : ХНЕУ. 2010. № 2 (54). С. 46-50. URL: http://repository.kpi.kharkov.ua/handle/KhPI-Press/291 (дата звернення 25.01.2026).

References

1. Posokhov, I.M. (2022), *Formuvannia mekhanizmu upravlinnia ryzykamy pererobnykh pidpryiemstv: monohrafiia* [Formation of the risk management mechanism of processing enterprises: a monograph], Vydavnytstvo Ivanchenka I.S., Kharkiv, Ukraine.

2. İlhan, Ü. (2025), "Cybersecurity in Human Resource Management in the Context of Remote Work: Policy, Practice, and Risk Management", Cybersecurity in the Era of Remote Work. IGI Global. https://doi.org/10.4018/979-8-3693-6417-8.ch007.

3. World Economic Forum (2024), "The Global Risks Report. 19th Edition", available at: https://www.weforum.org/publications/global-risks-report-2024/ (Accessed 25 January 2026).

4. Pererva, P. Nagy, S. and Maslak, M. (2018), "Organization of marketing activities on the intrapreneurship", *MIND Journal*, vol. (5). DOI:10.13140/RG.2.2.17332.10883

5. Starostina, A.O. (2009), *Marketynh: teoriia, svitovyi dosvid, ukrainska praktyka: pidruchnyk* [Marketing: theory, world experience, Ukrainian practice: textbook], Znannia. Kyiv, Ukraine.

6. Kraus, K.M. and Kraus, N.M. (2018), "Digital economy: trends and perspectives of vanguard development", *Efektyvna ekonomika*, vol. 1, available at: http://www.economy.nayka.com.ua/?op=1&z=6047 (Accessed 25 January 2026).

7. Kosenko, A.P. Kobielieva, T.O. and Tkachova, N.P. (2017), "The definition of industry park electrical products", *Scientific Bulletin of Polissia*, vol. 2(3), 43-50. DOI: https://doi.org/10.25140/10.25140/2410-957620173(11)43-50

8. Kocziszky, G. Pererva, P.G. Szakaly, D. and Somosi Veres, M. (2012), *Technology transfer*, NTU "KhPI", Kharkiv-Miskolc.

9. Pererva, P.G. (1993), *Upravlinnia marketynhom na mashynobudivnomu pidpryiemstvi* [Marketing management at a machine-building enterprise], Osnova. Kharkiv, Ukraine.

10. Pererva, P.G. (2009), "Management of innovation activity of the enterprise", *Marketynh* [Marketing], Znannia. Kyiv, Ukraine, pp. 461-518.

11. Pererva, P.G., Kocziszky, G. and Veres Somosi, M. (2019), *Compliance program: tutorial*, NTU "KhPI", Kharkiv, Ukraine, available at: http://repository.kpi.kharkov.ua/handle/KhPI-Press/48662 (Accessed 25 January 2026).

12. Borzenko, V.I. Pererva, P.G. and Kobielieva, T.O. (2019), *Intelektualna vlasnist: mahisterskyi kurs: pidruchnyk* [Intellectual property: master's course: textbook], NTU "KhPI", Kharkiv, Ukraine.

13. Tovazhnianskyi, V.L. (2012), *Antykryzovyi mekhanizm staloho rozvytku pidpryiemstva* [Anti-crisis mechanism of sustainable development of the enterprise], Apostrof, Kharkiv, Ukraine.

14. Pererva, P.G. Mekhovych, S.A. and Pohorelov, M.I. (2008), *Ekonomika ta orhanizatsiia innovatsiinoi diialnosti: pidruchnyk* [Economics and organization of innovation activity: textbook], NTU "KhPI", Kharkiv, Ukraine.

15. Tovazhnianskyi, V.L. and Pererva, P.G. (2010), "Anti-crisis monitoring of financial and economic performance indicators of a machine-building enterprise", *Ekonomika rozvytku*, vol. 2(54), pp. 46-50, available at: http://repository.kpi.kharkov.ua/handle/KhPI-Press/291 (Accessed 25 January 2026).

Отримано редакцією журналу / Received: 28.01.26
Прорецензовано / Revised: 05.02.26
Схвалено до друку / Accepted: 19.02.26