https://doi.org/10.31891/2307-5740-2026-356-21
УДК 338.24:005.334:658.7:004.8
JEL classification: L91, M10, M12, M15, O33

ГАРМАШ Олег
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
https://orcid.org/0000-0003-4324-4411
e-mail: o.harmash.kpi@gmail.com
МАРЧУК Володимир
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
https://orcid.org/0000-0003-0140-5416
e-mail: v.marchuk.kpi@gmail.com
ФЕДОРЕНКО Тетяна
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/ 0000-0002-3447-9078
e-mail: vixen@ukr.net

ФОРМУВАННЯ СИСТЕМИ ІНДИКАТОРІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ІНТЕЛЕКТУАЛІЗАЦІЇ ЛОГІСТИЧНИХ ПОСЛУГ: КОРПОРАТИВНО-УПРАВЛІНСЬКИЙ АСПЕКТ

У статті досліджено теоретико-методичні засади формування системи індикаторів економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг. Обґрунтовано, що цифровізація, використання штучного інтелекту, аналітики великих даних, IoT-рішень, хмарних платформ, електронного документообігу та інтегрованих систем управління ланцюгами постачання трансформують зміст економічної безпеки підприємства. Інтелектуалізацію логістичних послуг операціоналізовано через технологічний, аналітичний, інформаційний, операційний, кадровий, партнерський і корпоративно-управлінський виміри, що дозволяє пов'язати цифрово-логістичні зміни з конкретними індикаторами економічної безпеки підприємства. За таких умов безпека не може оцінюватися лише через фінансові або ресурсні показники, оскільки ризики виникають на перетині операційної безперервності, якості даних, цифрової стійкості, кадрової безпеки, партнерської надійності та корпоративного контролю.

Метою статті є розроблення концептуально-методичного підходу до формування системи індикаторів економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг із виділенням корпоративно-управлінського та кадрового аспектів. Методологічну основу дослідження становлять системний, ризик-орієнтований, функціональний, процесний і корпоративно-управлінський підходи, а також методи порівняльного аналізу, групування, узагальнення та індикаторного моделювання. Запропоновано структуру індикаторів за шістьма блоками: фінансово-економічним, логістично-операційним, цифровим та інформаційним, кадровим, партнерським і корпоративно-управлінським. Для ілюстрації практичної придатності запропонованого підходу подано демонстраційний розрахунок інтегрального індексу економічної безпеки умовного підприємства, що дозволяє показати логіку виявлення попереджувальних зон ризику та формування адресних управлінських дій.

Наукова новизна дослідження полягає в удосконаленні концептуально-методичного підходу до формування системи індикаторів економічної безпеки підприємства, який забезпечує перехід від фрагментарної діагностики окремих ризиків до інтегрованої системи раннього попередження в умовах інтелектуалізації логістичних послуг. Запропонований підхід, на відміну від наявних, поєднує шість блоків безпеки підприємства – фінансово-економічний, логістично-операційний, цифрово-інформаційний, кадровий, партнерсько-мережевий і корпоративно-управлінський – із логікою "ризик – індикатор – джерело даних – порогове значення – власник ризику – управлінська дія", що дозволяє використовувати індикатори не лише для оцінювання стану економічної безпеки, а й для проактивного корпоративного управління ризиками. Практичне значення результатів полягає у можливості використання запропонованої системи для внутрішнього моніторингу, ризик-менеджменту, кадрової політики, аудиту логістичних процесів і підготовки управлінських рішень.

Ключові слова: економічна безпека підприємства, інтелектуалізовані логістичні послуги, індикатори економічної безпеки, цифрові ризики ланцюгів постачання, логістична стійкість, показники раннього попередження, корпоративне ризик-управління, кадрова безпека, Логістика 4.0, безперервність бізнесу.

HARMASH Oleh, MARCHUK volodymyr
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
FEDORENKO Tetiana
HEI "Open International University of Human Development "Ukraine"

DEVELOPING ENTERPRISE ECONOMIC SECURITY INDICATORS IN THE CONTEXT OF INTELLIGENT LOGISTICS SERVICES: A CORPORATE GOVERNANCE PERSPECTIVE

The article examines the theoretical and methodological foundations for developing a system of enterprise economic security indicators in the context of intelligent logistics services. It is substantiated that artificial intelligence, big data analytics, IoT technologies, cloud platforms, electronic document management and integrated supply chain systems transform logistics from an operational support function into a digitally integrated risk-sensitive management environment. The intellectualization of logistics services is operationalized through technological, analytical, informational, operational, personnel, partner-network and corporate governance dimensions, which makes it possible to link digital logistics transformation with measurable enterprise economic security indicators.

Under these conditions, enterprise economic security cannot be assessed only through financial or resource-based indicators, as risks arise at the intersection of operational continuity, data quality, digital resilience, personnel security, partner reliability and corporate control. The purpose of the article is to develop a conceptual and methodological approach to forming a system of economic security indicators for enterprises operating in intelligent logistics environments, with special attention to corporate governance and personnel security. The study is based on systemic, risk-oriented, functional, process and corporate governance approaches, as well as methods of comparative analysis, grouping, generalization and indicator modelling.

A six-block indicator structure is proposed: financial-economic, logistics-operational, digital-information, personnel, partner-network and corporate governance indicators. To illustrate the practical applicability of the proposed approach, a demonstrative calculation of the integral economic security index for a hypothetical enterprise is provided, showing how warning risk zones can be identified and translated into targeted managerial actions. The scientific novelty of the study lies in improving a conceptual and methodological approach that ensures the transition from fragmented diagnostics of individual risks to an integrated early-warning system under the intellectualization of logistics services. The proposed approach links enterprise security blocks with the logic of "risk — indicator — data source — threshold value — risk owner — managerial action", which allows indicators to be used not only for assessing the state of economic security, but also for proactive corporate risk governance. The practical value of the results lies in their applicability for internal monitoring, risk management, personnel policy, logistics audit, business continuity control and managerial decision-making in digitally integrated logistics environments.

Keywords: enterprise economic security, intelligent logistics services, economic security indicators, digital supply chain risk, logistics resilience, early-warning indicators, corporate risk governance, personnel security, Logistics 4.0, business continuity

Стаття надійшла до редакції / Received 07.07.2026
Прийнята до друку / Accepted 04.08.2026
Опубліковано / Published 27.08.2026

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

Інтелектуалізація логістичних послуг є одним із найбільш помітних проявів цифрової трансформації підприємств. Вона охоплює використання штучного інтелекту для прогнозування попиту й оптимізації маршрутів, застосування IoT-сенсорів для моніторингу руху вантажів, автоматизацію складських операцій, електронний документообіг, хмарні платформи для координації партнерів, аналітику великих даних і цифрові канали взаємодії з клієнтами. У результаті логістика перетворюється з допоміжної функції на інформаційно насичений управлінський контур, від якого залежать швидкість обороту ресурсів, якість обслуговування, репутація підприємства та стабільність його доходів [8; 11; 12].

У цьому дослідженні інтелектуалізація логістичних послуг розглядається не як загальний синонім цифровізації, а як якісна зміна логістичного управління, за якої дані, алгоритми, цифрові платформи, автоматизовані рішення та компетентність персоналу стають безпосередніми чинниками економічної безпеки підприємства.

У міжнародному науковому дискурсі ця проблематика дедалі частіше розглядається не лише крізь призму ефективності цифрової логістики, а й у контексті стійкості підприємств, безперервності ланцюгів постачання, цифрових ризиків і корпоративного ризик-управління. Глобальні збої ланцюгів постачання, воєнно-політична нестабільність, кіберзагрози, залежність від платформних рішень, дефіцит критичних компетентностей і висока динаміка ринкового середовища формують умови, за яких логістичні послуги стають не лише операційним сервісом, а й елементом забезпечення економічної стійкості підприємства. Тому питання економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг доцільно розглядати як складову ширшої наукової проблеми забезпечення безпеки, стійкості та безперервності функціонування підприємств у цифрово інтегрованому логістичному середовищі. [13].

Разом із позитивними ефектами інтелектуалізація створює новий профіль ризиків. Підприємство стає залежним від якості даних, працездатності цифрової платформи, кіберзахисту, цифрової компетентності персоналу, надійності постачальників IT-сервісів і синхронності партнерської мережі. Збій алгоритму прогнозування, компрометація даних, помилки персоналу при роботі з цифровими системами або порушення SLA з боку партнера можуть швидко трансформуватися у фінансові втрати, зриви поставок, штрафні санкції, втрату клієнтів і погіршення ділової репутації [8; 13].

За таких умов класичні підходи до оцінювання економічної безпеки підприємства, орієнтовані передусім на фінансові коефіцієнти, ресурсний потенціал або загальну діагностику стану підприємства, потребують доповнення. Система індикаторів має фіксувати не лише поточний рівень захищеності, а й ранні сигнали ризиків, які виникають у цифрово-логістичному середовищі. Особливої ваги набуває кадрова безпека, оскільки саме персонал забезпечує коректне використання цифрових систем, дотримання процедур, захист інформації, якість операційних рішень і здатність підприємства адаптуватися до технологічних змін [1; 2; 3; 7].

Практичне значення проблеми полягає в необхідності створення такої системи індикаторів, яка буде зрозумілою для органів корпоративного управління, власників ризиків, керівників логістичних підрозділів, HR-служби, IT-блоку, служби безпеки та внутрішнього аудиту. Індикатор у цій логіці має бути не лише статистичною характеристикою, а й управлінським сигналом: він повинен мати джерело даних, порогове

значення, відповідального суб'єкта, сценарій реагування та зв'язок із конкретною складовою економічної безпеки [4; 5].

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Теоретичний фундамент дослідження економічної безпеки підприємства сформовано у працях Г. Козаченко, В. Пономарьова та О. Ляшенко, де економічна безпека розглядається через сутність, механізми забезпечення та гармонізацію інтересів підприємства із зовнішнім середовищем [1]. Подальший розвиток цього напряму пов'язаний із роботами О. Ляшенко, З. Живко, Т. Васильціва, Н. Єршової, О. Ареф'євої та інших дослідників, які розкривали функціональні складові, механізми управління, інформаційно-аналітичне забезпечення та методи діагностики економічної безпеки підприємства.

Проблематика індикаторного та інтегрального оцінювання економічної безпеки висвітлена у працях С. Ілляшенка, С. Пілецької, Т. Коритько, Є. Ткаченко, О. Шуміло, В. Бабенко, Л. Любохинець, І. Воловельської та О. Ареф'євої. У цих дослідженнях важливим є підхід до формування сукупності показників, їх нормування, визначення ваг і побудови інтегрального індексу [5]. Разом з тим інтегральна оцінка, якщо вона не доповнюється динамічними індикаторами ризику, може фіксувати стан безпеки із запізненням.

Кадрова безпека як складова економічної безпеки підприємства досліджувалася Т. Зубко, В. Лаптєвою, Т. Момот, Х. Чжан, Н. Логіновою, І. Швець, О. Кавтиш, О. Ареф'євою та О. Литовченко. Зокрема, Т. Зубко і В. Лаптєва обґрунтовують систему показників для експрес-оцінки кадрової безпеки, акцентуючи увагу на загрозах, структурі, принципах і ролі персоналу в забезпеченні економічної безпеки [2]. Для теми цієї статті важливо розширити кадрову безпеку за рахунок цифрової грамотності, готовності до технологічних змін, кібергігієни, ризиків інсайдерської поведінки та помилок персоналу в інтелектуалізованому логістичному середовищі.

Цифровий вимір економічної безпеки підприємства набув активного розвитку в сучасних українських дослідженнях. В. Проскура, Т. Черничко та Д. Верецький запропонували підхід до визначення рівня економічної безпеки підприємства в умовах цифровізації, включивши кадрову, виробничо-технологічну, фінансову, екологічну та цифрову складові [3]. М. Кравченко і Ф. Немировський розглянули інтегровану методику CRITIC-DEMATEL для оцінювання економічної безпеки підприємств в умовах цифрової трансформації, що дає змогу не тільки визначати ваги показників, а й аналізувати причинно-наслідкові зв'язки між компонентами безпеки [4]. О. Правдивець досліджує інструментарій оцінювання цифрової трансформації та інноваційного розвитку системи економічної безпеки підприємств [6].

Найближчим до теми цієї статті є дослідження В. Андрєєвої та Є. Невмержицького, присвячене формуванню адаптивної системи економічної безпеки логістичного підприємства в умовах цифровізації та кризових явищ [7]. Автори акцентують увагу на фінансовій, техніко-технологічній, кадровій, цифровій і репутаційній складових, а також на необхідності адаптивного управління. Водночас потребує подальшого розвитку саме система індикаторів, прив'язана до корпоративного управління, власників ризиків, кадрової безпеки та інтелектуалізованих логістичних послуг.

Міжнародні дослідження Logistics 4.0 розкривають технологічні, організаційні та людські аспекти цифрової логістики. V. Dixit і P. Verma обґрунтували необхідність ідентифікації, оцінювання та кількісного вимірювання нових ризиків Logistics 4.0, показавши вагомість технологічної інфраструктури для різних технологій Industry 4.0 у логістиці [8]. C. Cimini, A. Lagorio, F. Pirola та R. Pinto дослідили людські фактори в Logistics 4.0 і довели, що цифрові технології змінюють роль логістичних операторів, створюючи потребу в нових компетентностях, сценаріях взаємодії людини й технології та системах управління змінами [9; 10]. S. Winkelhaus і E. Grosse систематизували Logistics 4.0 як нову логістичну систему [11], а G. Frederico, J. Garza-Reyes, A. Anosike і V. Kumar розкрили концепти, зрілість і дослідницький порядок денний Supply Chain 4.0 [12].

Окремого значення для даного дослідження набуває міжнародний напрям, пов’язаний із цифровою стійкістю ланцюгів постачання та управлінням ризиками в умовах турбулентності. У сучасних наукових дослідженнях цифровізація розглядається як чинник підвищення стійкості, надійності та здатності ланцюгів постачання зберігати функціональність в умовах збоїв, оскільки вона посилює інформаційну прозорість, координацію між учасниками, швидкість реагування на відхилення та адаптивність підприємств до порушень у логістичному середовищі. Водночас цифрова інтеграція не усуває ризики автоматично, а змінює їхню природу: ризики дедалі частіше виникають у сфері якості даних, алгоритмічної підтримки рішень, кібербезпеки, платформної залежності, партнерської синхронізації та людсько-машинної взаємодії [13].

У цьому контексті економічна безпека підприємства має розглядатися не лише як стан захищеності його ресурсів та інтересів, а як здатність підтримувати безперервність критичних процесів, своєчасно ідентифікувати слабкі сигнали ризику та трансформувати їх у корпоративні управлінські дії. Саме тому індикатори економічної безпеки в цифрово інтегрованому логістичному середовищі мають виконувати функцію показників раннього попередження, які забезпечують своєчасне виявлення слабких сигналів ризику та пов’язуються з конкретними джерелами даних, пороговими значеннями, відповідальними власниками ризиків і сценаріями управлінського реагування [1; 4; 7].

Таблиця 1

Узагальнення наукових підходів до теми дослідження

Напрям	Представники	Внесок у дослідження	Потреба в розвитку
Економічна безпека підприємства	Г. Козаченко, В. Пономарьов, О. Ляшенко; З. Живко; Т. Васильців; Н. Єршова; О. Ареф'єва	Визначено сутність, складові, механізми та управлінську природу економічної безпеки.	Адаптація до інтелектуалізованої логістики, цифрових платформ і партнерських екосистем.
Кадрова безпека	Т. Зубко, В. Лаптєва; Т. Момот, Х. Чжан; Н. Логінова; І. Швець; О. Кавтиш	Розкрито сутність кадрової безпеки, загрози та показники оцінювання.	Урахування цифрової грамотності, кібергігієни, інсайдерських ризиків і готовності до змін.
Цифровізація економічної безпеки	В. Проскура, Т. Черничко, Д. Верецький; М. Кравченко, Ф. Немировський; О. Правдивець	Запропоновано цифрові складові, інтегральні та MCDM-підходи до оцінювання.	Галузева деталізація для логістичних послуг і прив'язка показників до корпоративних рішень.
Logistics 4.0 / Supply Chain 4.0	V. Dixit, P. Verma; C. Cimini, A. Lagorio, F. Pirola, R. Pinto; S. Winkelhaus, E. Grosse; G. Frederico et al.	Виявлено технології, ризики, людський фактор, зрілість і бар'єри цифрової логістики.	Поєднання технологічних ризиків із системою економічної та кадрової безпеки підприємства.
Цифрова стійкість ланцюгів постачання та корпоративне ризик-управління	Y. Li, D. Li, Y. Liu, Y. Shou; дослідники проблематики цифрової стійкості ланцюгів постачання, управління ризиками в ланцюгах постачання та корпоративного ризик-управління	Обґрунтовано роль цифровізації, співпраці, формалізованих контрактів, інформаційної прозорості та координації у підвищенні стійкості й робастності ланцюгів постачання.	Інтеграція підходів до забезпечення стійкості, робастності та раннього попередження ризиків у систему економічної безпеки підприємства, орієнтовану на потреби корпоративного управління.

Джерело: складено автором за результатами узагальнення [1; 2; 3; 7; 8; 11; 12; 13].

Отже, аналіз останніх досліджень і публікацій свідчить, що наукова база для вивчення економічної безпеки підприємства, кадрової безпеки, цифровізації, Logistics 4.0, Supply Chain 4.0 та цифрової стійкості ланцюгів постачання є достатньо розвиненою. Водночас у наявних підходах ці напрями здебільшого розглядаються відокремлено. Дослідження з економічної безпеки підприємства переважно зосереджуються на фінансових, ресурсних, кадрових або функціональних складових; праці з Logistics 4.0 – на технологіях, автоматизації, цифровій зрілості та людському факторі; дослідження цифрової стійкості ланцюгів постачання зосереджуються на здатності ланцюгів постачання протидіяти збоям, адаптуватися до порушень і відновлювати функціональність після кризових впливів [1; 2; 3; 7; 8; 11; 12; 13].

Недостатньо розробленим залишається питання побудови системи індикаторів, яка б поєднувала ці напрями в єдину корпоративно-управлінську логіку. Така система має не лише діагностувати стан економічної безпеки підприємства, а й виконувати функцію раннього попередження: виявляти слабкі сигнали цифрових, логістичних, кадрових, партнерських та управлінських ризиків до того, як вони трансформуються у фінансові втрати, порушення безперервності діяльності, зниження якості сервісу або втрату довіри з боку клієнтів і партнерів [4; 8; 13].

Саме ця наукова прогалина визначає спрямованість даного дослідження: формування системи індикаторів економічної безпеки підприємства, що враховує ризики інтелектуалізованих логістичних послуг і може бути використана в системі корпоративного управління як інструмент моніторингу, раннього попередження та управлінського реагування.

Наявні методики часто розглядають індикатори як елементи діагностики, тоді як для корпоративного управління вони мають виконувати роль ранніх сигналів ризику. Кожний показник повинен бути пов'язаний із конкретною загрозою, джерелом даних, порогом реагування, відповідальним власником і управлінською дією. Також потребує поглиблення кадровий аспект, адже в умовах цифрової логістики персонал одночасно є носієм компетентностей, суб'єктом прийняття рішень і потенційним джерелом операційних, інформаційних та інсайдерських ризиків [2; 4; 8].

ФОРМУЛЮВАННЯ МЕТИ СТАТТІ

Метою статті є розроблення концептуально-методичного підходу до формування системи індикаторів економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг із урахуванням корпоративно-управлінського аспекту та кадрової безпеки.

Для досягнення поставленої мети визначено такі завдання: уточнити зміст економічної безпеки підприємства в умовах інтелектуалізованої логістики; систематизувати ризики, що виникають у логістичних цифрових сервісах; сформулювати принципи добору індикаторів; запропонувати структуру показників за функціональними блоками; розкрити роль кадрової безпеки у системі індикаторів; обґрунтувати корпоративно-управлінський механізм використання індикаторів для раннього попередження ризиків.

У такій постановці дослідження орієнтоване не лише на уточнення внутрішньої системи показників економічної безпеки підприємства, а й на включення цієї проблематики до ширшого міжнародного наукового дискурсу, пов’язаного зі стійкістю цифрово інтегрованих ланцюгів постачання, управлінням ризиками

інтелектуалізованих логістичних сервісів та застосуванням показників раннього попередження в системі корпоративного управління. Це дозволяє розглядати запропоновану систему індикаторів як інструмент не тільки внутрішньої діагностики, а й забезпечення організаційної стійкості, безперервності діяльності та контрольованості ризиків у цифровому логістичному середовищі [8; 13].

Подальше розкриття заявленої мети потребує уточнення змісту базового для статті поняття – інтелектуалізації логістичних послуг. Без його операціоналізації система індикаторів економічної безпеки може залишатися надто загальною, оскільки не буде зрозуміло, які саме технологічні, аналітичні, організаційні та управлінські зміни створюють новий профіль ризиків для підприємства. Тому перед розглядом економічної безпеки доцільно визначити ознаки, прояви та вимірювані параметри інтелектуалізації логістичних послуг.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

1. Операціоналізація поняття інтелектуалізації логістичних послуг

У цьому дослідженні інтелектуалізацію логістичних послуг розглянуто як перехід від переважно традиційного виконання логістичних функцій до використання цифрових, аналітичних, автоматизованих та алгоритмічних інструментів планування, моніторингу, прогнозування, координації, контролю й оптимізації логістичних процесів. Йдеться не про механічне додавання окремих цифрових технологій, а про зміну управлінської логіки: рішення дедалі більше спираються на дані, алгоритми, інтегровані платформи та швидку міжфункціональну взаємодію [8; 11; 12].

Основними проявами інтелектуалізації логістичних послуг є використання штучного інтелекту та машинного навчання для прогнозування попиту, оцінювання ризиків і оптимізації маршрутів; застосування TMS, WMS, ERP, CRM та BI-систем для інтегрованого управління логістичними процесами; IoT-сенсори й GPS-моніторинг для відстеження вантажів, транспортних засобів і умов перевезення; електронний документообіг та цифрові платформи для взаємодії з клієнтами, перевізниками, складами й постачальниками [8; 11; 12].

Таблиця 2

Операціоналізація поняття інтелектуалізації логістичних послуг

Вимір інтелектуалізації	Зміст прояву	Приклади технологій та інструментів	Потенційний вплив на економічну безпеку підприємства
Технологічний	Автоматизація та цифрова підтримка логістичних операцій	TMS, WMS, ERP, CRM, IoT, GPS-моніторинг, електронний документообіг	Зниження операційних витрат, підвищення контрольованості процесів, але посилення залежності від цифрової інфраструктури
Аналітичний	Використання даних для прогнозування, планування та прийняття рішень	BI-системи, Big Data, AI-прогнозування, машинне навчання, аналітичні панелі	Підвищення якості управлінських рішень, але ризик помилкових прогнозів і викривлення рішень через низьку якість даних
Інформаційний	Забезпечення прозорості, доступності та цілісності логістичних даних	Інтегровані бази даних, API-інтеграції, цифрові кабінети клієнтів і партнерів, системи моніторингу подій	Підвищення прозорості логістики, але виникнення ризиків витоку, втрати, дублювання або спотворення даних
Операційний	Скорочення часу виконання логістичних операцій і підвищення точності сервісу	Автоматизоване управління маршрутами, контроль SLA, цифрове управління складом, автоматичне сповіщення про відхилення	Підвищення рівня сервісу та безперервності процесів, але ризик масштабного збою у разі відмови системи
Кадровий	Зміна вимог до компетентностей персоналу та характеру взаємодії людини з цифровими системами	LMS, цифрове навчання, кібергігієна, рольове управління доступом, інструкції роботи з TMS/WMS/BI	Підвищення продуктивності персоналу, але ризик помилок, опору змінам, інсайдерських загроз і залежності від ключових фахівців
Партнерський	Цифрова координація з перевізниками, постачальниками, клієнтами та IT-провайдерами	Партнерські платформи, електронний обмін даними, цифровий аудит контрагентів, SLA-моніторинг	Посилення синхронізації ланцюга постачання, але зростання ризику партнерської незрілості та залежності від зовнішніх провайдерів
Корпоративно-управлінський	Використання цифрових даних для контролю, аудиту, ескалації та стратегічного управління ризиками	Ризик-реєстри, dashboards, внутрішній аудит, звітність перед ризик-комітетом, BCP/DRP	Перехід до проактивного управління ризиками, але потреба у чітких власниках ризику, порогах реагування та процедурах контролю

Джерело: складено автором на основі [8; 11; 12].

Операціоналізація цього поняття передбачає виокремлення таких вимірюваних ознак інтелектуалізації логістичних послуг: рівень цифрової інтеграції логістичних процесів; частка автоматизованих управлінських рішень; наявність прогнозної аналітики; якість і повнота логістичних даних; доступність цифрових платформ; швидкість виявлення відхилень; рівень прозорості операцій у реальному часі; ступінь автоматизації контролю SLA; цифрова зрілість партнерів; рівень цифрових компетентностей

персоналу; наявність процедур кіберзахисту та контролю доступів. Саме ці ознаки дозволяють перейти від загального опису цифрової трансформації логістики до побудови конкретних індикаторів економічної безпеки підприємства [3; 4; 7].

З позиції економічної безпеки підприємства інтелектуалізація логістичних послуг має подвійний вплив. З одного боку, вона підвищує швидкість, точність, прозорість і керованість логістичних процесів, сприяє зниженню витрат, підвищенню якості сервісу, покращенню прогнозування та посиленню контролю за виконанням договірних зобов'язань. З іншого боку, вона формує нові джерела ризиків, пов'язані з якістю даних, алгоритмічними помилками, кіберзагрозами, залежністю від цифрових платформ, недостатньою цифровою компетентністю персоналу, ненадійністю IT- або логістичних партнерів, а також непрозорістю автоматизованих рішень [3; 8; 13].

Отже, інтелектуалізація логістичних послуг у цій статті трактується як багатовимірний процес, що має технологічний, інформаційний, аналітичний, кадровий, партнерський та корпоративно-управлінський виміри. Саме тому її вплив на економічну безпеку підприємства не варто зводити до одного узагальненого показника. Потрібна система індикаторів, здатна показувати як позитивні ефекти цифрової логістики, так і ризики, що виникають у цифрово інтегрованому логістичному середовищі [7; 8; 11; 12].

Наведена операціоналізація дозволяє розглядати інтелектуалізацію логістичних послуг не як абстрактну характеристику цифрової трансформації, а як сукупність вимірюваних змін у технологічній, аналітичній, інформаційній, операційній, кадровій, партнерській та корпоративно-управлінській площинах. У межах запропонованого підходу ці зміни трансформуються в новий профіль ризиків, відповідні блоки економічної безпеки, індикатори моніторингу, порогові значення та корпоративні управлінські дії. Узагальнену логіку такого переходу подано на рис. 1 [7; 8; 11; 12].

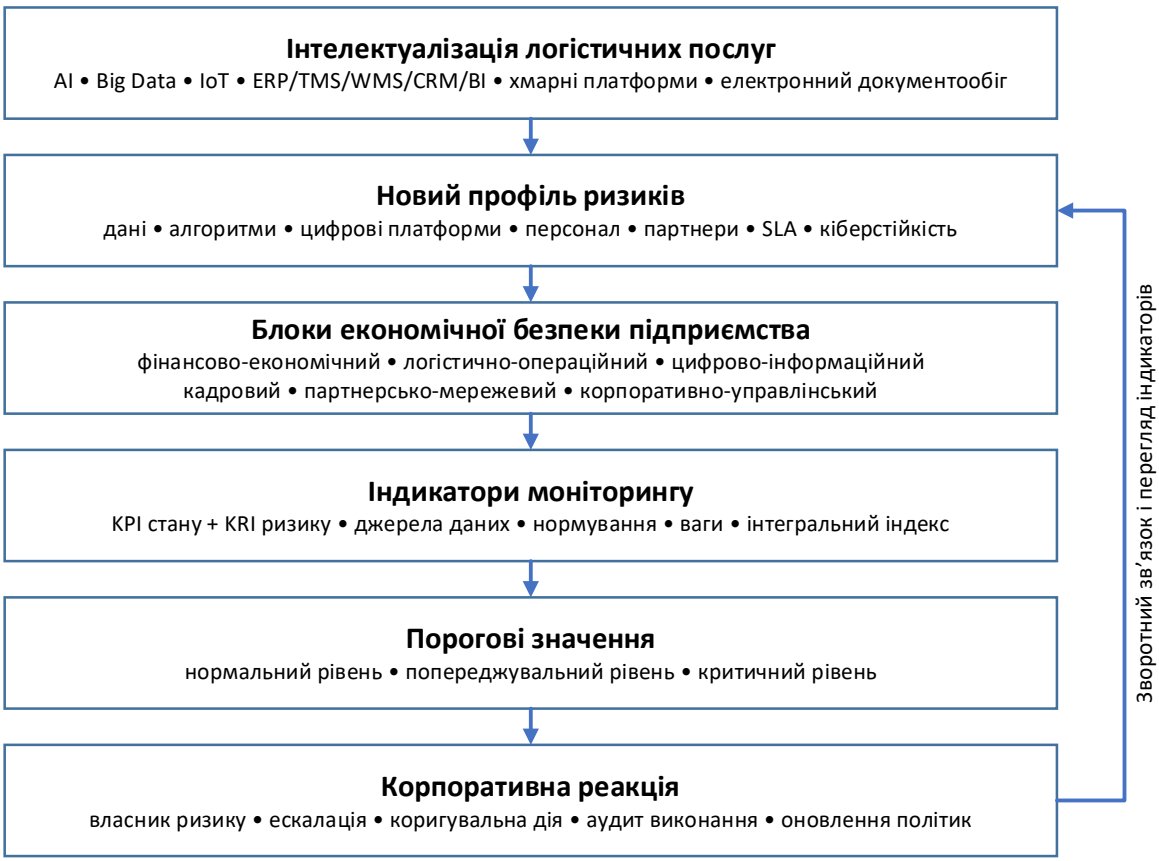


Рис. 1. Концептуальна модель формування системи індикаторів економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг

Джерело: розроблено автором.

Рис. 1 показує, що формування системи індикаторів економічної безпеки підприємства варто розглядати як послідовну трансляцію змін у логістичному середовищі в управлінські сигнали. Спочатку інтелектуалізація логістичних послуг змінює технологічну та інформаційну основу процесів. Далі ці зміни формують новий профіль ризиків, пов'язаний із даними, алгоритмами, цифровими платформами, персоналом, партнерами, SLA та кіберстійкістю [8; 13].

Подальша логіка моделі передбачає перехід від блоків безпеки до конкретних індикаторів моніторингу, серед яких доцільно розмежовувати KPI стану та KRI ризику. Кожен індикатор має бути пов'язаний із джерелом даних, способом нормування, ваговим коефіцієнтом та місцем у загальному

інтегральному індексі економічної безпеки. Управлінська цінність такої системи розкривається через встановлення порогових значень – нормального, попереджувального та критичного рівнів, після досягнення яких запускається відповідна корпоративна реакція: визначення власника ризику, ескалація, коригувальна дія, аудит виконання та оновлення внутрішніх політик [4; 5].

Отже, запропонована концептуальна модель підкреслює превентивну роль індикаторів економічної безпеки. Вони мають не лише описувати поточний стан підприємства, а й виявляти слабкі сигнали ризику, достатньо ранні для корпоративного реагування [4; 7].

2. Економічна безпека підприємства в умовах інтелектуалізації логістичних послуг

Економічну безпеку підприємства в умовах інтелектуалізації логістичних послуг пропонується визначати як здатність підприємства забезпечувати стійке функціонування, захист економічних інтересів, безперервність логістичних процесів, збереження даних, результативне використання кадрового та цифрового потенціалу, а також своєчасне виявлення й нейтралізацію ризиків, що виникають у цифрово інтегрованому логістичному середовищі [1; 3; 7].

Таке трактування узгоджується з міжнародним підходом до розуміння стійкості підприємств і ланцюгів постачання, у межах якого безпека розглядається не лише як здатність уникати загроз, а як здатність зберігати функціональність, адаптуватися до порушень, відновлювати критичні процеси та підтримувати контрольованість рішень в умовах невизначеності. У цифрово інтегрованому логістичному середовищі ця здатність залежить від якості даних, прозорості процесів, узгодженості партнерських дій, надійності цифрових платформ, компетентності персоналу та ефективності корпоративного ризик-управління [13].

Таке визначення важливе тим, що в сучасному підприємстві логістична функція вже не є лише операційною. Вона входить до корпоративної архітектури безпеки, адже через логістичні процеси проходять дані про клієнтів, маршрути, вантажі, контрагентів, платежі, складські залишки, строки поставки та якість виконання договорів. Від точності й захищеності цих даних залежить не тільки ефективність логістики, а й фінансовий результат підприємства [1; 7].

Інтелектуалізація логістичних послуг змінює саму природу ризику. Якщо для традиційної логістики типовими були втрата вантажу, транспортні затримки, нераціональні маршрути або складські помилки, то для Logistics 4.0 до цього переліку додаються алгоритмічні рішення, інтеграційні збої, залежність від цифрових провайдерів, порушення доступності даних, недостатня цифрова компетентність персоналу та непрозорість автоматизованих управлінських рішень [8; 11].

3. Ризики інтелектуалізованих логістичних послуг

Таблиця 3

Ризики інтелектуалізованих логістичних послуг та їх економічні наслідки

Група ризиків	Типові прояви	Потенційні наслідки для економічної безпеки
Цифрово-технологічні	збої платформи; вразливості IT-інфраструктури; помилки інтеграції; залежність від хмарних сервісів	втрата доступності сервісу; додаткові витрати на відновлення; зниження довіри клієнтів
Дані та алгоритми	низька якість даних; викривлення прогнозів; непрозорість AI-рішень; некоректні маршрути	перевитрати; порушення строків; помилки планування; зростання операційних ризиків
Логістично-операційні	зрив SLA; затримки доставки; складські помилки; недостатня пропускна здатність	штрафи; втрата клієнтів; зниження оборотності активів; репутаційні втрати
Кадрові	дефіцит цифрових компетентностей; помилки операторів; опір змінам; інсайдерські ризики	збої процесів; витік інформації; зниження продуктивності; залежність від ключових працівників
Партнерські	цифрова незрілість постачальників; невиконання договірних умов; слабка кібербезпека контрагентів	ланцюгові збої; додаткові витрати; юридичні ризики; втрата контролю над сервісом
Корпоративно-управлінські	відсутність власників ризику; слабка ескалація; нерегулярний аудит; нечіткі пороги реагування	реактивне управління; запізнілі рішення; накопичення прихованих загроз

Джерело: складено автором на основі [7; 8; 13].

4. Принципи та архітектура формування системи індикаторів

Систему індикаторів економічної безпеки підприємства слід формувати з урахуванням специфіки логістичних послуг, цифрової залежності процесів і потреб корпоративного управління. Її основними принципами є системність, вимірюваність, ризик-орієнтованість, динамічність, пороговість, управлінська адресність, інтегрованість із корпоративним контролем, релевантність джерел даних і регулярний перегляд показників [3; 4; 5].

Принцип системності означає, що індикатори повинні охоплювати не один функціональний блок, а всю логіку створення логістичної цінності: фінанси, операції, цифрові системи, персонал, партнерів і управлінські механізми. Принцип вимірюваності передбачає наявність чіткої формули або процедури визначення показника. Принцип ризик-орієнтованості вимагає, щоб кожен індикатор був пов'язаний із конкретним ризиком або групою ризиків [1; 5].

Пороговість означає встановлення допустимих, попереджувальних і критичних значень. Управлінська адресність передбачає закріплення відповідального суб'єкта за кожним показником. Інтегрованість із корпоративним контролем означає включення індикаторів до регулярної звітності, внутрішнього аудиту, засідань ризик-комітету та процесу прийняття управлінських рішень [4; 5].

Водночас добір окремих показників ще не створює повноцінної системи. Потрібна узгоджена архітектура індикаторів, яка відображає багатовимірний характер економічної безпеки підприємства та поєднує фінансово-економічні, логістично-операційні, цифрово-інформаційні, кадрові, партнерсько-мережеві й корпоративно-управлінські параметри. Такий підхід не дозволяє звузити безпеку до одного фінансового або технологічного виміру [3; 4; 7].

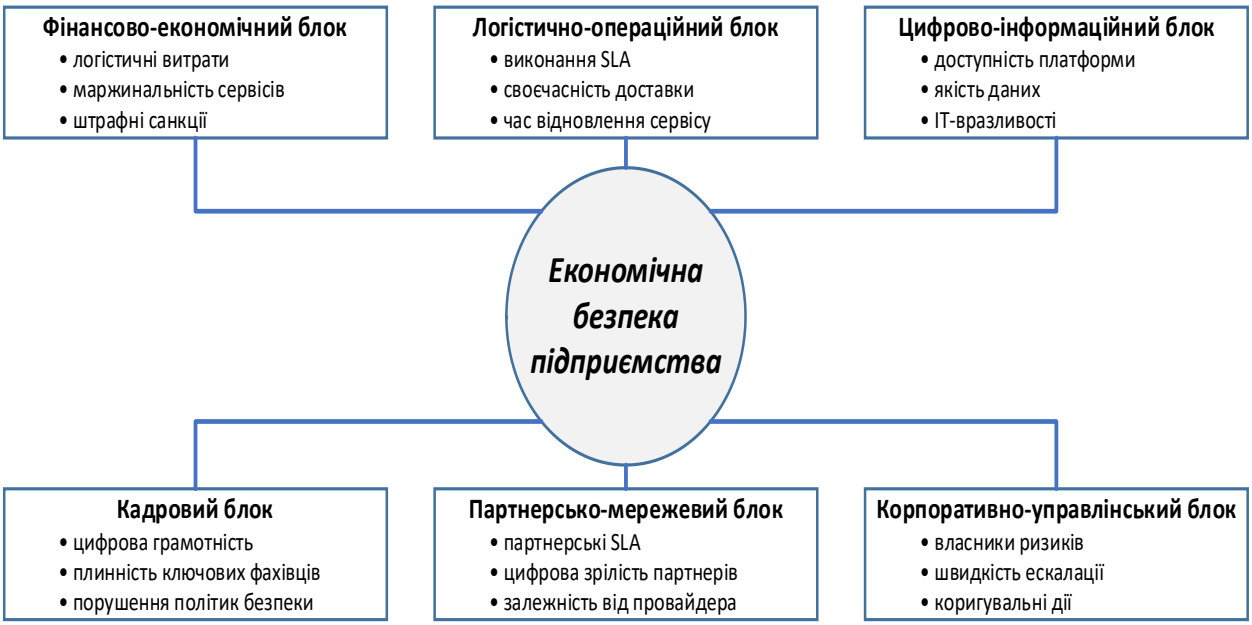


Рис. 2. Архітектура системи індикаторів економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг
Джерело: розроблено автором.

Архітектура, подана на рис. 2, спирається на шість взаємопов'язаних блоків економічної безпеки підприємства. Фінансово-економічний блок показує вплив логістичних процесів на витрати, маржинальність, штрафні санкції та фінансову стійкість. Логістично-операційний блок характеризує безперервність і надійність сервісу через виконання SLA, своєчасність доставки та здатність відновлювати роботу після збоїв. Цифрово-інформаційний блок фіксує доступність платформ, якість даних, рівень інтеграції систем і кіберризики [7; 8; 13].

Кадровий блок відображає здатність персоналу працювати в умовах цифрово інтегрованої логістики, дотримуватися процедур безпеки та своєчасно реагувати на ризикові відхилення. Партнерсько-мережевий блок характеризує надійність контрагентів, цифрову зрілість партнерів, виконання партнерських SLA та рівень залежності від окремих провайдерів. Корпоративно-управлінський блок забезпечує зв'язок індикаторів із власниками ризиків, процедурами ескалації, коригувальними діями та контролем виконання рішень [2; 9; 10].

Особливість цієї архітектури полягає в тому, що кожен блок є не ізольованим переліком показників, а окремим контуром раннього попередження. У такому контурі індикатор пов'язується з джерелом даних, пороговим значенням, відповідальним власником ризику та управлінською дією. Деталізований склад індикаторів, джерел даних і напрямів управлінського використання наведено в табл. 4 [4; 5].

5. Система індикаторів економічної безпеки підприємства

Запропонована система є відкритою: конкретний набір показників може змінюватися залежно від масштабу підприємства, рівня цифрової зрілості, виду логістичних послуг, структури партнерської мережі та доступності даних. Водночас принциповим є збереження балансу між фінансовими, операційними, цифровими, кадровими та управлінськими індикаторами [3; 7].

Для практичного застосування доцільно розмежовувати показники стану та показники ризику. Показники стану характеризують поточний рівень безпеки, наприклад ліквідність, цифрову доступність платформи чи рівень виконання SLA. Показники ризику, або KRI, сигналізують про наближення небезпечної події: зростання кількості критичних вразливостей, збільшення частки помилкових даних, підвищення плинності ключових фахівців або погіршення виконання партнерських SLA [4; 8].

Таблиця 4

Система індикаторів економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг

Блок	Індикатори	Джерела даних	Управлінське використання
Фінансово-економічний	коефіцієнт поточної ліквідності; частка логістичних витрат у доході; маржинальність логістичних сервісів; частка витрат на відновлення після збоїв; рівень штрафних санкцій	фінансова звітність; управлінський облік; договори	аналіз фінансової стійкості, бюджетування ризиків, перегляд тарифів і резервів
Логістично-операційний	рівень виконання SLA; своєчасність доставки; кількість критичних збоїв; точність складського обліку; середній час відновлення сервісу; відхилення маршрутів	TMS/WMS/ERP; CRM; звіти операційного блоку	корекція процесів, резервування потужностей, перегляд маршрутів і операційних стандартів
Цифровий та інформаційний	доступність цифрової платформи; кількість критичних вразливостей; частота інцидентів доступу; частка помилкових даних; відсоток інтегрованих процесів; кількість помилок AI-прогнозу	IT-моніторинг; журнали подій; аудит даних; BI-системи	посилення кіберзахисту, аудит даних, тестування алгоритмів, модернізація IT-архітектури
Кадрова безпека	плинність ключових фахівців; вакансії критичних ролей; рівень цифрової грамотності; охоплення навчанням; порушення політик безпеки; інциденти інсайдерського ризику	HRM-система; LMS; служба безпеки; внутрішні розслідування	навчання, утримання персоналу, кадровий резерв, контроль доступів, формування культури безпеки
Партнерський і мережевий	частка критичних партнерів із підтвердженою цифровою зрілістю; виконання партнерських SLA; залежність від одного провайдера; кількість партнерських інцидентів	договори; анкети постачальників; аудит контрагентів; SLA-звіти	диверсифікація постачальників, перегляд договорів, встановлення вимог безпеки
Корпоративно-управлінський	регулярність перегляду KRI; частка ризиків із визначеним власником; швидкість ескалації; частка виконаних коригувальних дій; результати внутрішнього аудиту	протоколи комітетів; ризик-реєстр; аудиторські звіти	ескалація на рівень правління, оновлення політик, контроль виконання рішень

Джерело: складено автором з урахуванням [2; 3; 4; 5; 7; 8].

6. Кадрова безпека як критичний блок системи індикаторів

Кадрова безпека в умовах інтелектуалізації логістичних послуг має подвійний зміст. З одного боку, персонал є об'єктом захисту: підприємство має забезпечити безпечні умови праці, прийнятне навантаження, навчання, мотивацію та можливості професійного розвитку. З іншого боку, персонал може бути джерелом ризику, оскільки помилки, недбалість, опір змінам, порушення політик доступу або інсайдерська поведінка здатні спричинити відчутні економічні втрати [2; 9; 10].

У логістичному середовищі значення кадрової безпеки посилюється через високу швидкість процесів. Неправильно введені дані, хибна інтерпретація системного попередження, несвоєчасна реакція на збій маршруту або недотримання правил інформаційної безпеки можуть швидко вплинути на сотні операцій. Тому кадрові індикатори мають бути пов'язані не тільки з HR-статистикою, а й з операційними та цифровими показниками [9; 10].

До спеціальних кадрових індикаторів для інтелектуалізованої логістики варто віднести рівень цифрової грамотності персоналу, частку працівників, які пройшли навчання з кібергігієни та роботи з логістичними платформами, кількість помилок у критичних операціях, частоту порушень політик доступу, плинність працівників на критичних ролях, наявність кадрового резерву, участь персоналу в програмах удосконалення процесів і кількість інцидентів, пов'язаних із людським фактором [2; 9; 10].

Наведена система індикаторів створює змістову основу для моніторингу економічної безпеки, однак її практична цінність з'являється лише після методичного впорядкування. Потрібно визначити тип кожного індикатора, спосіб нормування, вагу в межах відповідного блоку, порогові значення та зв'язок із управлінською реакцією. Тому подальший виклад зосереджено на формалізації методичного підходу до оцінювання економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг [4; 5].

7. Методичний підхід до оцінювання економічної безпеки підприємства на основі системи індикаторів

Запропонована система індикаторів має не лише описове, а й прикладне значення: вона дає змогу перейти від якісної ідентифікації ризиків до кількісної діагностики, порівняння та управлінської інтерпретації. Для цього використовується блочний підхід, за якого кожна група індикаторів описує окремий вимір економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг [5].

Методичний підхід охоплює такі етапи: формування переліку індикаторів за функціональними блоками; визначення джерел даних; класифікацію показників на стимулятори та дестимулятори; встановлення нормативних, попереджувальних і критичних значень; нормування показників; визначення вагових коефіцієнтів; розрахунок часткових індексів; формування інтегрального індексу економічної безпеки; інтерпретацію результатів і запуск управлінських дій [5].

Окреме значення має поділ індикаторів на стимулятори та дестимулятори. До стимуляторів належать показники, зростання яких посилює економічну безпеку: рівень виконання SLA, доступність цифрової платформи, частка інтегрованих процесів, цифрова грамотність персоналу, частка ризиків із визначеним власником, частка виконаних коригувальних дій. Дестимулятори, навпаки, сигналізують про посилення ризиків: частка помилкових даних, кількість критичних IT-вразливостей, рівень штрафних санкцій, кількість критичних логістичних збоїв, плинність ключових фахівців [5].

Для забезпечення порівнянності різнорідних показників необхідним є їх нормування в інтервалі від 0 до 1. Для індикаторів-стимуляторів, зростання яких позитивно впливає на рівень економічної безпеки підприємства, нормоване значення доцільно визначати за формулою [5]:

$$Z_{ij} = \frac{x_{ij} - \min(x_{ij})}{\max(x_{ij}) - \min(x_{ij})},$$

де Z_{ij} – нормоване значення *j*-го індикатора *i*-го блоку; x_{ij} – фактичне значення відповідного показника; $\min(x_{ij})$ – мінімальне допустиме або критичне значення показника; $\max(x_{ij})$ – максимальне, цільове або нормативне значення показника.

Для індикаторів-дестимуляторів, зростання яких свідчить про посилення ризику, доцільно застосовувати обернену формулу нормування:

$$Z_{ij} = \frac{\max(x_{ij}) - x_{ij}}{\max(x_{ij}) - \min(x_{ij})}.$$

У такому разі всі нормовані значення перебувають у межах від 0 до 1, де значення, наближене до 1, свідчить про вищий рівень безпеки за відповідним індикатором, а значення, наближене до 0 – про критичне посилення ризику. Якщо підприємство не має достатнього масиву історичних даних для визначення мінімальних і максимальних значень, можуть використовуватися експертно встановлені пороги, галузеві орієнтири, договірні SLA, внутрішні нормативи або цільові значення корпоративної стратегії [5].

Частковий індекс за кожним блоком економічної безпеки доцільно розраховувати як зважену суму нормованих індикаторів [5]:

$$I_i = \sum_i (a_{ij} \cdot z_{ij}),$$

де I_i – частковий індекс *i*-го блоку економічної безпеки; a_{ij} – вага *j*-го індикатора в межах *i*-го блоку; z_{ij} – нормоване значення *j*-го індикатора *i*-го блоку. Сума ваг індикаторів у межах кожного блоку має дорівнювати 1.

Загальний інтегральний індекс економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг може бути представлений у вигляді блочної моделі [5]:

$$I_{\text{ЕБ}} = \omega_1 F + \omega_2 L + \omega_3 D + \omega_4 P + \omega_5 N + \omega_6 G,$$

де $I_{\text{ЕБ}}$ – інтегральний індекс економічної безпеки підприємства;
F – частковий індекс фінансово-економічного блоку;
L – частковий індекс логістично-операційного блоку;
D – частковий індекс цифрово-інформаційного блоку;
P – частковий індекс кадрової безпеки;
N – частковий індекс партнерсько-мережевого блоку;
G – частковий індекс корпоративно-управлінського блоку;
$\omega_1 - \omega_6$ – вагові коефіцієнти відповідних блоків, сума яких дорівнює 1.

Вагові коефіцієнти можуть визначатися кількома способами. На початковому етапі впровадження системи доцільним є використання експертного оцінювання із залученням представників фінансового,

логістичного, IT-, HR-, безпекового та управлінського блоків. За наявності достатньої кількості даних можуть застосовуватися метод аналізу ієрархій, CRITIC, DEMATEL або їх комбінація. Експертний підхід дозволяє врахувати стратегічні пріоритети підприємства, тоді як CRITIC і DEMATEL забезпечують більш формалізоване визначення ваг з урахуванням варіативності показників, взаємозв'язків між ними та сили причинно-наслідкового впливу окремих компонентів системи [4; 14; 15].

Для практичного використання інтегрального індексу необхідною є шкала інтерпретації, яка пов'язує кількісний результат із рівнем управлінського реагування. Доцільно виділяти чотири рівні економічної безпеки підприємства: стабільний, допустимий, попереджувальний і критичний [5].

Таблиця 5

Шкала інтерпретації інтегрального індексу економічної безпеки підприємства

Значення інтегрального індексу	Рівень економічної безпеки	Управлінська інтерпретація	Рекомендована реакція
0,80–1,00	Стабільний	Система економічної безпеки функціонує в межах допустимих параметрів; ризики контрольовані	Стандартний моніторинг, плановий аудит, підтримання наявних процедур
0,60–0,79	Допустимий	Загальний стан є прийнятним, але окремі блоки можуть містити ризикові відхилення	Посилений контроль слабких блоків, уточнення порогів, локальні коригувальні дії
0,40–0,59	Попереджувальний	Накопичуються ризики, які можуть перейти у фінансові втрати, збої сервісу або управлінські порушення	Розроблення плану коригувальних дій, ескалація на рівень відповідальних керівників, позаплановий аудит
Менше 0,40	Критичний	Економічна безпека перебуває під загрозою; існує ризик втрати безперервності, даних, клієнтів або фінансової стійкості	Негайна ескалація на рівень правління або ризик-комітету, активація кризового плану, перегляд ресурсів і відповідальних осіб

Джерело: складено автором з урахуванням підходів до інтегрального оцінювання [5; 14; 15].

Запропонована шкала має орієнтовний характер і може уточнюватися залежно від галузевої специфіки, рівня цифрової зрілості підприємства, критичності логістичних процесів, ризик-апетиту власників і вимог корпоративного управління. Водночас її використання дозволяє перетворити інтегральний індекс із суто аналітичного показника на інструмент управлінського реагування [5].

Особливе значення має не лише загальне значення інтегрального індексу, а й профіль часткових індексів за окремими блоками. Наприклад, підприємство може мати допустимий загальний рівень економічної безпеки, але водночас перебувати в зоні попереджувального ризику за цифрово-інформаційним або кадровим блоком. У такому разі управлінська реакція має спрямовуватися не на всю систему загалом, а на конкретний проблемний контур: якість даних, кіберзахист, цифрові компетентності персоналу, партнерські SLA або корпоративну ескалацію ризиків [4; 5].

Таким чином, методичний підхід до оцінювання економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг передбачає не лише розрахунок інтегрального показника, а й побудову системи раннього попередження. Її сутність полягає у зв'язку між індикатором, джерелом даних, пороговим значенням, власником ризику та управлінською дією. Саме цей зв'язок забезпечує перехід від реактивної діагностики економічної безпеки до проактивного корпоративного управління ризиками.

Запропонована формалізована модель дає змогу оцінювати економічну безпеку підприємства як багатовимірну систему, у якій фінансово-економічні, логістично-операційні, цифрово-інформаційні, кадрові, партнерські та корпоративно-управлінські індикатори взаємодіють між собою. Перевага такого підходу полягає в тому, що він показує не тільки загальний індекс, а й конкретні контури, де накопичуються ризики [4; 5].

Наведені етапи задають загальну послідовність використання індикаторів, але для практики цього недостатньо. Процедура оцінювання має забезпечити зіставність різнорідних показників, розрахунок часткових індексів за блоками, формування інтегрального індексу та його подальшу інтерпретацію в логіці корпоративного управлінського реагування [4; 5].

Для посилення прикладної спрямованості запропонованого підходу доцільно доповнити методичний блок демонстраційним розрахунком інтегрального індексу економічної безпеки підприємства. Такий приклад має умовний характер і не є емпіричною апробацією на даних конкретного підприємства. Його призначення полягає в ілюстрації логіки використання часткових індексів, вагових коефіцієнтів, інтегрального показника та управлінської інтерпретації результатів у системі раннього попередження ризиків.

8. Демонстраційне застосування запропонованого підходу

Для демонстрації логіки використання запропонованої системи індикаторів розглянуто умовне підприємство з розвиненою логістичною функцією, яке використовує TMS, WMS, ERP, CRM, BI-систему, електронний документообіг і цифрові канали взаємодії з партнерами. Припустимо, що за результатами внутрішнього моніторингу розраховано часткові індекси за шістьма блоками економічної безпеки. Значення

подано в нормованому вигляді в інтервалі від 0 до 1, де 1 відповідає найвищому рівню безпеки, а 0 - критичному стану відповідного блоку [5].

Таблиця 6

Демонстраційний розрахунок інтегрального індексу економічної безпеки підприємства

Блок економічної безпеки	Частковий індекс	Вага блоку	Зважене значення	Управлінська інтерпретація
Фінансово-економічний	0,72	0,20	0,144	Допустимий рівень; фінансові ризики загалом контрольовані
Логістично-операційний	0,61	0,20	0,122	Допустимий рівень із ризиковими відхиленнями у виконанні SLA та відновленні сервісу
Цифрово-інформаційний	0,48	0,20	0,096	Попереджувальний рівень; підвищені ризики якості даних, цифрової доступності та IT-вразливостей
Кадровий	0,55	0,15	0,083	Попереджувальний рівень; потреба в посиленні цифрових компетентностей і утриманні критичних фахівців
Партнерсько-мережевий	0,67	0,15	0,101	Допустимий рівень; необхідний подальший моніторинг партнерських SLA та залежності від провайдерів
Корпоративно-управлінський	0,58	0,10	0,058	Попереджувальний рівень; потреба в посиленні ескалації, контролю виконання рішень і закріплення власників ризиків
Інтегральний індекс економічної безпеки	—	**1**	**0,604**	**Допустимий рівень із наявністю попереджувальних зон ризику**

Джерело: складено автором на основі умовного прикладу.

Отримане значення інтегрального індексу економічної безпеки становить 0,604, що відповідно до запропонованої шкали інтерпретації належить до допустимого рівня. Водночас такий результат не може трактуватися як повністю стабільний стан економічної безпеки підприємства, оскільки частина блоків уже перебуває в попереджувальній зоні. Найбільш проблемними є цифрово-інформаційний, кадровий і корпоративно-управлінський блоки. Саме вони формують ранні сигнали ризику, які за відсутності своєчасного реагування можуть трансформуватися у збої логістичного сервісу, втрату якості даних, зростання кадрової залежності, затримку управлінських рішень або фінансові втрати [5].

З управлінської точки зору результати демонстраційного розрахунку свідчать про необхідність адресного реагування не на всю систему економічної безпеки загалом, а на конкретні проблемні контури. Для цифрово-інформаційного блоку першочерговими діями можуть бути аудит якості логістичних даних, перевірка доступності TMS/WMS/ERP-систем, оцінювання кіберризиків, тестування інтеграцій і перегляд політик доступу. Для кадрового блоку доцільними є оцінювання цифрових компетентностей персоналу, посилення навчання щодо роботи з логістичними платформами, формування кадрового резерву для критичних ролей і зменшення залежності від окремих фахівців. Для корпоративно-управлінського блоку необхідними є уточнення власників ризиків, запровадження регулярної звітності щодо KRI, підвищення швидкості ескалації критичних відхилень і контроль виконання коригувальних дій [4; 7].

Таким чином, демонстраційний приклад підтверджує, що інтегральний індекс економічної безпеки має використовуватися не як ізольований числовий результат, а як інструмент виявлення проблемних блоків і запуску адресних управлінських дій. Його практична цінність полягає в тому, що навіть за допустимого загального рівня безпеки підприємство може виявити слабкі сигнали ризику в окремих блоках і своєчасно активувати механізм раннього попередження [4; 5].

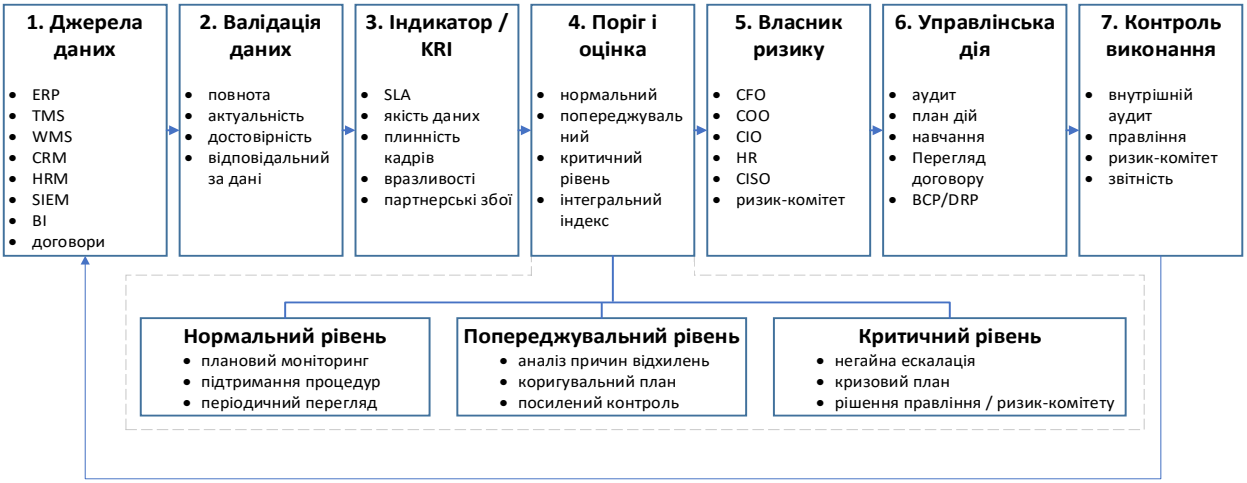
Демонстраційний розрахунок додатково підтверджує, що навіть прийнятне інтегральне значення не усуває потреби аналізувати окремі блоки. Якщо кадровий або цифрово-інформаційний блок перебуває в попереджувальній зоні, підприємство вже має підстави для управлінського втручання, не очікуючи фінансових втрат чи зриву логістичного сервісу [2; 4; 9].

9. Корпоративно-управлінський механізм використання індикаторів

Корпоративно-управлінський аспект використання індикаторів означає, що система економічної безпеки має бути вбудована в реальну управлінську архітектуру підприємства. На стратегічному рівні власники, наглядова рада або правління визначають політику економічної безпеки, допустимий рівень ризику та вимоги до звітності. На функціональному рівні керівники фінансового, логістичного, IT-, HR-, безпекового та партнерського контурів забезпечують моніторинг показників, аналіз причин відхилень і підготовку рішень. На операційному рівні власники процесів відповідають за коригувальні дії та документування інцидентів [1; 4; 7].

Управлінська цінність системи індикаторів розкривається лише тоді, коли кожен показник має джерело даних, порогове значення, відповідального власника ризику, процедуру реагування та контроль виконання. Без цього індикатори залишаються статистичною звітністю. В умовах інтелектуалізації

логістичних послуг вони мають працювати як механізм раннього попередження, що переводить цифрові, логістичні, кадрові, партнерські й управлінські сигнали в конкретні корпоративні рішення [4; 8; 13].



Зворотний зв'язок: оновлення джерел даних, уточнення індикаторів, перегляд порогів, відповідальних осіб і коригувальних дій.

Рис. 3. Удосконалений механізм раннього попередження ризиків економічної безпеки підприємства
Джерело: розроблено автором.

Як видно з рис. 3, механізм раннього попередження починається з визначення джерел даних, до яких можуть належати ERP, TMS, WMS, CRM, HRM, SIEM, BI-системи, договори, ризик-реєстри та звіти внутрішнього аудиту. На основі цих джерел формуються індикатори, що відображають стан або ризикові відхилення у відповідних блоках економічної безпеки: виконання SLA, якість логістичних даних, рівень плинності ключових фахівців, кількість критичних IT-вразливостей, партнерські збої або швидкість ескалації управлінських рішень [4; 7; 8].

Наступним елементом механізму є встановлення порогових значень, які дозволяють відрізняти нормальний, попереджувальний і критичний рівні ризику. Досягнення попереджувального рівня має ініціювати аналіз причин відхилень, підготовку коригувальних дій і посилений моніторинг. Досягнення критичного рівня потребує негайної ескалації на рівень правління, ризик-комітету або іншого уповноваженого органу корпоративного управління. Таким чином, поріг виконує роль не лише аналітичного орієнтира, а й управлінського тригера [4; 5].

Ключовою умовою дієвості механізму є закріплення власника ризику за кожним індикатором або групою індикаторів. Залежно від природи ризику такими власниками можуть бути фінансовий директор, операційний директор, IT-директор, HR-директор, CISO, керівник логістики, служба внутрішнього аудиту або ризик-комітет. Після реалізації управлінської дії необхідним є контроль виконання, що забезпечує зворотний зв'язок: уточнення порогових значень, перегляд відповідальних осіб, оновлення процедур, коригування індикаторів і посилення внутрішніх політик [4].

Для конкретизації запропонованого механізму доцільно показати, як окремі сигнали індикаторів можуть інтерпретуватися з позиції економічної безпеки підприємства, хто має бути власником реагування та які управлінські дії можуть застосовуватися залежно від характеру ризику. Приклади такої трансляції подано в табл. 7 [4; 7].

Таблиця 7

Трансляція індикаторів у корпоративні управлінські дії

Сигнал індикатора	Економічна інтерпретація	Власник реагування	Управлінська дія
Зростання плинності ключових фахівців логістики та IT	Ризик втрати компетентностей і знань про критичні процеси	HR-директор, операційний директор	програма утримання, кадровий резерв, перегляд мотивації
Підвищення частки помилкових даних у TMS/WMS	Ризик некоректних маршрутів, складських помилок і зриву SLA	CIO, керівник логістики	аудит даних, очищення довідників, перевірка інтеграцій
Збільшення критичних IT-вразливостей	Ризик кіберінциденту та зупинки логістичного сервісу	CISO, ризик-комітет	патч-менеджмент, тестування захисту, перегляд доступів
Погіршення партнерського SLA	Ризик ланцюгового збою та втрати клієнтської довіри	закупівлі, комплаєнс, операційний директор	перегляд договору, резервний партнер, штрафні механізми
Збільшення часу відновлення після збоїв	Ризик операційної нестійкості та фінансових втрат	правління, керівник безперервності бізнесу	оновлення BCP/DRP, навчання, резервування інфраструктури

Джерело: складено автором з урахуванням логіки ризик-орієнтованого управління [4; 7; 8; 13].

10. Практична логіка впровадження системи індикаторів

Впровадження системи індикаторів варто починати з аудиту джерел даних. Підприємство має визначити, які показники вже доступні в ERP, TMS, WMS, CRM, HRM, SIEM, LMS, фінансовій звітності та договорах із партнерами. Після цього формується карта ризиків інтелектуалізованої логістики й обираються індикатори, які можна вимірювати без надмірного адміністративного навантаження [4; 7].

На другому етапі встановлюються порогові значення. Їх можна визначати на основі історичних даних, галузевих орієнтирів, експертних оцінок, умов договорів або внутрішніх стандартів. На третьому етапі створюється регламент моніторингу: періодичність, відповідальні особи, порядок ескалації, формат звіту та вимоги до коригувальних дій [5].

На четвертому етапі система інтегрується в корпоративну звітність. Доцільною є панель індикаторів, у якій показники згруповано за блоками, а відхилення позначено за принципом світлофора: нормальний, попереджувальний і критичний рівні. На п'ятому етапі проводиться аудит ефективності: перевіряється, чи справді індикатори дають змогу виявляти ризики раніше, ніж вони перетворюються на фінансові втрати [4; 5].

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті обґрунтовано, що інтелектуалізація логістичних послуг змінює зміст економічної безпеки підприємства. У цифрово інтегрованому логістичному середовищі джерелами загроз стають не лише фінансові дисбаланси чи традиційні операційні ризики, а й якість даних, доступність цифрових платформ, надійність алгоритмічних рішень, кіберстійкість, цифрова зрілість партнерів і кадрова безпека.

У межах дослідження інтелектуалізацію логістичних послуг операціоналізовано як багатовимірний процес, що охоплює технологічний, аналітичний, інформаційний, операційний, кадровий, партнерський і корпоративно-управлінський виміри. Такий підхід дозволив уникнути надмірно загального трактування цифрової трансформації логістики та сформувати підґрунтя для побудови системи індикаторів, придатної для моніторингу економічної безпеки підприємства.

Отримані результати розширюють традиційне розуміння економічної безпеки підприємства через включення цифрової стійкості, логістичної безперервності, раннього попередження ризиків і корпоративної керованості. У цьому контексті запропонована система індикаторів поєднує підходи до забезпечення економічної безпеки підприємства, підвищення цифрової стійкості ланцюгів постачання та формування корпоративного ризик-управління, що дозволяє розглядати її як інструмент не лише діагностики, а й раннього попередження та управлінського реагування на ризики. Її особливість полягає в тому, що індикатори не обмежуються фіксацією поточного стану підприємства, а орієнтовані на виявлення слабких сигналів ризику, їх інтерпретацію та трансляцію в управлінські дії.

Запропоновано систему індикаторів економічної безпеки підприємства за шістьма блоками: фінансово-економічним, логістично-операційним, цифровим та інформаційним, кадровим, партнерським і корпоративно-управлінським. Така структура дозволяє оцінювати не лише поточний стан підприємства, а й ранні сигнали ризиків, які можуть вплинути на стійкість логістичних процесів, фінансовий результат, репутацію та якість корпоративного управління.

Особливу увагу приділено кадровій безпеці, яка в умовах інтелектуалізованої логістики охоплює цифрову грамотність, кібергігієну, готовність до змін, надійність персоналу, наявність кадрового резерву та здатність працівників коректно взаємодіяти з цифровими системами. Доведено, що кадрові індикатори мають бути пов'язані з операційними та цифровими показниками, оскільки людський фактор може як зменшувати, так і посилювати ризики економічної безпеки.

Наукова новизна дослідження полягає у формуванні корпоративно-управлінської логіки використання індикаторів: кожен показник пов'язано з ризиком, джерелом даних, пороговим значенням, відповідальним суб'єктом і сценарієм управлінської реакції. Практичне значення запропонованого підходу полягає в можливості його використання для системи раннього попередження, внутрішнього аудиту, HR-політики, управління логістичними ризиками та підготовки рішень ризик-комітету або правління підприємства.

Демонстраційний розрахунок інтегрального індексу економічної безпеки умовного підприємства показав, що навіть за допустимого загального рівня безпеки окремі блоки можуть формувати попереджувальні зони ризику. Зокрема, цифрово-інформаційний, кадровий і корпоративно-управлінський блоки потребують пріоритетної управлінської уваги, оскільки саме вони можуть виступати джерелами слабких сигналів майбутніх фінансових, операційних або репутаційних втрат. Це підтверджує доцільність використання запропонованої системи не лише для інтегрального оцінювання, а й для адресного управління ризиками.

Разом з тим дослідження має певні обмеження. Запропонований підхід має концептуально-методичний характер і спрямований на формування логіки побудови системи індикаторів, а не на повну емпіричну перевірку її результативності на масиві даних конкретних підприємств. Демонстраційний розрахунок інтегрального індексу має ілюстративне значення та використовується для пояснення логіки

застосування підходу. Це зумовлює необхідність подальшої апробації запропонованої системи в різних галузевих, організаційних і цифрових контекстах.

Перспективами подальших досліджень є емпірична апробація запропонованої системи на прикладі логістичних підприємств або підприємств із розвиненою логістичною функцією, визначення ваг індикаторів за допомогою експертних і MCDM-методів, установлення галузевих порогових значень, тестування чутливості інтегрального індексу до зміни окремих блоків, а також розроблення цифрової панелі моніторингу економічної безпеки підприємства.

Література

1. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення. Київ: Лібра, 2003. 280 с.

2. Зубко Т., Лаптєва В. Індикатори кадрової безпеки підприємства. *Scientia Fructuosa*. 2018. Т. 120, N 4. С. 57-67. DOI: https://doi.org/10.31617/visnik.knute.2018(120)06

3. Проскура В. Ф., Черничко Т. В., Верецький Д. Є. Сучасні підходи до визначення рівня економічної безпеки підприємства в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2024. DOI: https://doi.org/10.32782/dees.13-9

4. Кравченко М. О., Немировський Ф. В. Оцінювання економічної безпеки підприємств в умовах цифрової трансформації: інтегрована методика CRITIC-DEMATEL. *Економічний вісник НТУУ «КПІ»*. 2025. URL: https://ev.fmm.kpi.ua/article/view/353992

5. Пілецька С. Т., Коритько Т. Ю., Ткаченко Є. В. Модель інтегральної оцінки економічної безпеки підприємства. *Економічний вісник Донбасу*. 2021. N 3(65). С. 56-65.

6. Правдивець О. Науково-практичний інструментарій оцінювання рівня цифрової трансформації, інноваційного розвитку системи економічної безпеки підприємств сфери інформаційних технологій. *Вчені записки Університету «КРОК»*. 2023. DOI: https://doi.org/10.31732/2663-2209-2022-71-92-102

7. Андрєєва В., Невмержицький Є. Формування адаптивної системи економічної безпеки логістичного підприємства в умовах цифровізації та кризових явищ. *Вчені записки Університету «КРОК»*. 2026. DOI: https://doi.org/10.31732/2663-2209-2026-81-105-115

8. Dixit V., Verma P. Identification, assessment, and quantification of new risks for Logistics 4.0. *International Journal of Logistics Research and Applications.* 2022. DOI: https://doi.org/10.1080/13675567.2022.2100331

9. Cimini C., Lagorio A., Pirola F., Pinto R. Exploring human factors in Logistics 4.0: empirical evidence from a case study. *IFAC-PapersOnLine*. 2019. DOI: https://doi.org/10.1016/j.ifacol.2019.11.529

10. Cimini C., Lagorio A., Pirola F., Pinto R. How human factors affect operators' task evolution in Logistics 4.0. *Human Factors and Ergonomics in Manufacturing & Service Industries*. 2020. DOI: https://doi.org/10.1002/hfm.20872

11. Winkelhaus S., Grosse E. H. Logistics 4.0: a systematic review towards a new logistics system. *International Journal of Production Research*. 2019. DOI: https://doi.org/10.1080/00207543.2019.1612964

12. Frederico G. F., Garza-Reyes J. A., Anosike A., Kumar V. Supply Chain 4.0: concepts, maturity and research agenda. *Supply Chain Management: An International Journal*. 2019. DOI: https://doi.org/10.1108/SCM-09-2018-0339

13. Li Y., Li D., Liu Y., Shou Y. Digitalisation for supply chain resilience and robustness: The roles of collaboration and formal contracts. *Frontiers of Engineering Management*. 2023. DOI: https://doi.org/10.1007/s42524-022-0229-x

14. Diakoulaki D., Mavrotas G., Papayannakis L. Determining objective weights in multiple criteria problems: The CRITIC method. *Computers & Operations Research*. 1995. DOI: https://doi.org/10.1016/0305-0548(94)00059-H

15. Seyed-Hosseini S. M., Safaei N., Asgharpour M. J. Reprioritization of failures in system FMEA using the DEMATEL technique. *Reliability Engineering & System Safety*. 2006. DOI: https://doi.org/10.1016/j.ress.2005.09.005

References

1. Kozachenko, H. V., Ponomarov, V. P., & Liashenko, O. M. (2003). Economic security of the enterprise: essence and mechanism of provision. Kyiv: Libra.

2. Zubko, T., & Laptieva, V. (2018). Indicators of enterprise personnel security. *Scientia Fructuosa*, 120(4), 57-67. https://doi.org/10.31617/visnik.knute.2018(120)06

3. Proskura, V. F., Chernychko, T. V., & Veretskyi, D. Ye. (2024). Modern approaches to determining the level of enterprise economic security in the conditions of digitalization. *Digital Economy and Economic Security*. https://doi.org/10.32782/dees.13-9

4. Kravchenko, M. O., & Nemirovskyi, F. V. (2025). Assessment of enterprise economic security in the conditions of digital transformation: integrated CRITIC-DEMATEL methodology. *Economic Bulletin of NTUU KPI*. https://ev.fmm.kpi.ua/article/view/353992

5. Piletska, S. T., Korytko, T. Yu., & Tkachenko, Ye. V. (2021). Model of integrated assessment of enterprise economic security. *Economic Herald of the Donbas*, 3(65), 56-65.

6. Pravdyvets, O. (2023). Scientific and practical toolkit for assessing digital transformation and innovative development of the enterprise economic security system. *Vcheni zapysky Universytetu KROK*. https://doi.org/10.31732/2663-2209-2022-71-92-102

7. Andreieva, V., & Nevmerzhytskyi, Ye. (2026). Formation of an adaptive system of economic security of a logistics enterprise under digitalization and crisis phenomena. *Vcheni zapysky Universytetu KROK*. https://doi.org/10.31732/2663-2209-2026-81-105-115

8. Dixit, V., & Verma, P. (2022). Identification, assessment, and quantification of new risks for Logistics 4.0. *International Journal of Logistics Research and Applications*. https://doi.org/10.1080/13675567.2022.2100331

9. Cimini, C., Lagorio, A., Pirola, F., & Pinto, R. (2019). Exploring human factors in Logistics 4.0: empirical evidence from a case study. *IFAC-PapersOnLine*. https://doi.org/10.1016/j.ifacol.2019.11.529

10. Cimini, C., Lagorio, A., Pirola, F., & Pinto, R. (2020). How human factors affect operators' task evolution in Logistics 4.0. *Human Factors and Ergonomics in Manufacturing & Service Industries*. https://doi.org/10.1002/hfm.20872

11. Winkelhaus, S., & Grosse, E. H. (2019). Logistics 4.0: a systematic review towards a new logistics system. *International Journal of Production Research*. https://doi.org/10.1080/00207543.2019.1612964

12. Frederico, G. F., Garza-Reyes, J. A., Anosike, A., & Kumar, V. (2019). Supply Chain 4.0: concepts, maturity and research agenda. *Supply Chain Management: An International Journal*. https://doi.org/10.1108/SCM-09-2018-0339

13. Li, Y., Li, D., Liu, Y., & Shou, Y. (2023). Digitalisation for supply chain resilience and robustness: The roles of collaboration and formal contracts. *Frontiers of Engineering Management*. https://doi.org/10.1007/s42524-022-0229-x

14. Diakoulaki, D., Mavrotas, G., & Papayannakis, L. (1995). Determining objective weights in multiple criteria problems: *The CRITIC method. Computers & Operations Research*. https://doi.org/10.1016/0305-0548(94)00059-H

15. Seyed-Hosseini, S. M., Safaei, N., & Asgharpour, M. J. (2006). Reprioritization of failures in system FMEA using the DEMATEL technique. *Reliability Engineering & System Safety*. https://doi.org/10.1016/j.ress.2005.09.005