

Кривещенко Вікторія Віталіївна

к. е. н, доцент, доцент кафедри комерційної діяльності і логістики
Київський національний економічний університет імені Вадима Гетьмана
ORCID: 0000-0002-2375-9664
kryveshchenko.viktoriia@kneu.edu.ua

Хмурковський Геннадій Володимирович

к. е. н, доцент, доцент кафедри комерційної діяльності і логістики
Київський національний економічний університет імені Вадима Гетьмана
ORCID: 0000-0002-8421-0675
khmurkovskiy@kneu.edu.ua

ІНТЕГРАЦІЯ РИЗИКОЛОГІЇ В СИСТЕМУ УПРАВЛІННЯ СКЛАДСЬКОЮ ЛОГІСТИКОЮ ПІДПРИЄМСТВА

Kryveshchenko Viktoriia

Candidate of Economic Sciences, Associate Professor
Associate Professor of the Department of Commercial Activity and Logistics
Kyiv National Economic University named after Vadym Hetman
ORCID: 0000-0002-2375-9664

Khmurkovskiy Hennadii

Candidate of Economic Sciences, Associate Professor
Associate Professor of the Department of Commercial Activity and Logistics
Kyiv National Economic University named after Vadym Hetman
ORCID: 0000-0002-8421-0675

INTEGRATION OF RISK MANAGEMENT INTO THE ENTERPRISE WAREHOUSE LOGISTICS MANAGEMENT SYSTEM

Анотація. У статті обґрунтовано необхідність інтеграції ризикології в систему управління складською логістикою підприємства в умовах прискореної цифровізації, воєнної та геополітичної нестабільності, посилення вимог до кібербезпеки й сталого розвитку в сучасному бізнес-середовищі. Актуальність теми зумовлена трансформацією складів із пасивних зон зберігання на високоінтегровані операційні хаби, керовані даними, автоматизованими засобами переміщення та WMS-платформами, що посилює вразливість підприємств до операційних, кіберфізичних, ергономічних та партнерських загроз, а традиційний підхід до ризиків як ізольованих подій уже не забезпечує достатньої стійкості. Узагальнено сучасні підходи до управління складськими ризиками: розглянуто концепцію Warehousing 5.0, що поєднує автоматизацію з людиноцентричністю та стійкістю процесів; SCRM-фреймворки для побудови планів безперервності бізнесу; методи кількісного оцінювання небезпек FMECA, ALARP і Risk Priority Number; архітектуру Zero Trust та

трирівневу структуру стандарту NIST SP 800-161 для захисту WMS. Систематизовано індикатори безпеки та випереджальні показники складських ризиків. Запропоновано комбіновану матрицю математичних і процедурних інструментів ризик-менеджменту на основі мереж Петрі, дискретно-подієвої симуляції, формалізованого підходу до інтеграції логістичних процесів та експертного методу MACTOR. Обґрунтовано системну логіку переходу від фрагментарного страхування ризиків до проактивного управління ними через вимірювані показники стійкості, безпеки, ергономіки та інформаційного захисту, а також через інтеграцію принципів циркулярної економіки й ESG у зворотну логістику. Практична цінність результатів полягає у формуванні орієнтирів для модернізації складських процесів, удосконалення WMS і підвищення безперервності бізнесу підприємства.

Ключові слова: складська логістика; ризикологія; управління ризиками; Warehousing 5.0; WMS; Zero Trust; SCRM; FMECA; ALARP; стійкість ланцюгів постачання.

Abstract. The article substantiates the need to integrate riskology into enterprise warehouse logistics management under conditions of accelerated digitalisation, martial-law and geopolitical instability, and growing requirements for cybersecurity and sustainable development. The relevance of the topic stems from the transformation of warehouses from passive storage facilities into data-driven operational hubs combining automated equipment, WMS platforms and cyber-physical systems, which increases enterprise exposure to operational, cyber-physical, ergonomic and partner-related risks, while the traditional treatment of risks as isolated events no longer ensures adequate resilience. The article summarises current approaches to warehouse risk management: the Warehousing 5.0 concept, which combines automation with human-centredness and process resilience; SCRM frameworks for business-continuity planning; quantitative hazard-assessment methods FMECA, ALARP and Risk Priority Number; Zero Trust architecture; and the three-tier NIST SP 800-161 standard for protecting WMS infrastructure. Safety indicators and leading indicators of warehouse risk are systematised. A combined matrix of mathematical and procedural risk-management tools is proposed, built on Petri nets, discrete-event simulation, a formalised approach to integrating logistics processes, and the MACTOR expert method. The systemic logic of shifting from fragmented risk insurance to proactive risk management is substantiated through measurable indicators of resilience, safety, ergonomics and information security, alongside the integration of circular-economy and ESG principles into reverse logistics. The practical value lies in a set of benchmarks for modernising warehouse processes, improving WMS and increasing enterprise business continuity.

Keywords: warehouse logistics; riskology; risk management; Warehousing 5.0; WMS; Zero Trust; SCRM; FMECA; ALARP; supply chain resilience.

Постановка проблеми та актуальність теми. Сучасні тенденції розвитку логістичних систем демонструють трансформацію складських комплексів із пасивних зон зберігання вантажів на високоінтегровані операційні хаби, керовані даними, автоматизованими засобами переміщення, WMS-платформами та цифровими сервісами моніторингу [1, 2]. Такий перехід посилює залежність підприємств від якості даних, кіберстійкості, безперервності енергопостачання, готовності персоналу та надійності зовнішніх партнерів.

Актуальність теми зумовлена тим, що складська логістика дедалі частіше функціонує в умовах одночасної дії кількох груп ризиків: воєнних і геополітичних, операційних, технологічних, ергономічних, екологічних та інформаційних. У таких умовах традиційний підхід, за якого ризики розглядають як ізольовані події або перекладають на страхові механізми, не забезпечує достатнього рівня стійкості підприємства [3–5]. Виникає потреба в інтеграції ризикології в повсякденне управління складом: від планування маршрутів і запасів до організації безпечних робочих місць, захисту WMS та оцінювання ESG-наслідків.

Аналіз останніх досліджень і публікацій. У науковій літературі останніх років активно розвивається концепція Warehousing 5.0, яка розширює засади Industry 4.0 через акцент на людиноцентричності, стійкості та екологічній відповідальності [2, 6]. Дослідники підкреслюють, що надмірна концентрація лише на технологічній ефективності є стратегічно обмеженою, якщо вона не враховує добробут працівників, автономію персоналу, когнітивне навантаження та здатність складської системи відновлюватися після збоїв [2, 6].

Окремий напрям досліджень присвячений поєднанню WMS, lean warehousing та розвитку компетентностей персоналу. У цих працях доведено, що продуктивність складу залежить не тільки від алгоритмів розміщення вантажів, а й від організаційної готовності працівників застосовувати цифрові інструменти [7]. Паралельно розвиваються підходи циркулярної економіки, які змінюють складські процеси через зворотну логістику, перероблення пакування та управління вторинними потоками матеріалів [8, 9].

У сфері управління ризиками ланцюгів постачання дослідники та практики пропонують SCRM-фреймворки, плани безперервності бізнесу, матриці відповідальності, сценарне моделювання та кількісні методи оцінювання небезпек [3–5, 10, 11]. Для складських систем особливо важливими є FMEDA, ALARP, аналіз вартості заходів безпеки, дискретно-подієва симуляція та кібербезпекові стандарти NIST [12–17]. Водночас не вирішеною частиною проблеми залишається недостатня інтеграція цих підходів у єдину управлінську логіку, придатну для складської логістики підприємства в умовах воєнної, цифрової та ESG-невизначеності.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значний обсяг наукових напрацювань у сфері управління ризиками складської логістики, окремі аспекти цієї проблематики залишаються недостатньо розкритими.

Більшість наявних досліджень зосереджена на окремих інструментах ризик-менеджменту — SCRM-фреймворках, кількісних методах FMEDA та ALARP, архітектурі Zero Trust, стандартах NIST [3–5, 10–12, 15–17] — розглядаючи їх здебільшого ізольовано один від одного. Питання їх системної інтеграції в єдину управлінську логіку, придатну для практичного впровадження на конкретному складському підприємстві, дослідники розкривають фрагментарно.

Недостатньо вивченим залишається й питання адаптації міжнародних регуляторних вимог, зокрема стандарту NIST SP 800-161 та фармацевтичних вимог GDP і DSCSA [15, 19] — до умов українських підприємств, які функціонують за одночасної дії воєнних, інфраструктурних та енергетичних обмежень [3, 20, 21]. Наявні джерела здебільшого орієнтовані на стабільні економічні умови й не враховують специфіку функціонування складів в умовах збройного конфлікту.

Також відкритим залишається питання емпіричної верифікації кількісних інструментів — дискретно-подієвої симуляції, показника RPN, методу MASTOR — на даних реальних складських комплексів, оскільки більшість публікацій обмежується теоретичним чи методичним обґрунтуванням підходів без практичної апробації [5, 18, 22, 23].

Мета і завдання дослідження. Метою статті є обґрунтування інтегрованого ризик-орієнтованого підходу до управління складською логістикою підприємс-

тва на основі поєднання концепції Warehousing 5.0, SCRM, цифрової безпеки, кількісного оцінювання операційних небезпек та принципів сталого розвитку.

Для досягнення мети поставлено такі завдання: узагальнити сучасні підходи до управління ризиками складської логістики; визначити вплив воєнної та геополітичної нестабільності на логістичну стійкість; систематизувати індикатори складських ризиків; охарактеризувати роль Zero Trust, IoT та ШІ у захисті WMS; сформувані практичні рекомендації для підприємств.

Методи дослідження. У статті застосовано методи критичного аналізу наукових і практичних джерел, порівняльного аналізу логістичних моделей, систематизації індикаторів ризику, табличного узагальнення, логічного синтезу та концептуального моделювання. Для опису інструментарію управління ризиками використано положення SCRM, FMECA, ALARP, ABC-аналізу витрат, дискретно-подієвого моделювання, Zero Trust Architecture та оцінювання зрілості процесів кібербезпеки ланцюгів постачання [14, 17, 18, 27, 28].

Основні результати дослідження. Функціонування логістичних систем у кризових умовах вимагає переосмислення класичних моделей управління ризиками. Для українських підприємств особливо відчутними є руйнування інфраструктури, зростання страхових тарифів, дефіцит транспорту, обмеження руху складу та перебої в енергопостачанні [6–8]. Це змушує підприємства відмовлятися від одного «оптимального» маршруту на користь динамічного балансування потоків між залізничними вузлами, автомобільними коридорами та альтернативними портами, а також коридорами міжнародної консолідаційної логістики [26].

Порівняння традиційної та адаптивної логістичної моделей наведено в табл. 1.

ТАБЛИЦЯ 1 — ПОРІВНЯЛЬНИЙ АНАЛІЗ ЛОГІСТИЧНИХ МОДЕЛЕЙ В УМОВАХ КРИЗИ ТА НЕВИЗНАЧЕНОСТІ

Параметр порівняння	Традиційна оптимізаційна модель	Адаптивна модель Складу 5.0
Критерій ефективності	Мінімізація операційних витрат і максимізація швидкості обороту	Баланс між витратами, соціальною відповідальністю та гнучкістю
Географія маршрутів	Орієнтація на один оптимальний і стабільний транспортний коридор	Балансування потоків між альтернативними портами та наземними вузлами
Управління запасами	Модель «точно в строк» (Just-in-Time) з мінімальними страховими буферами	Динамічний розрахунок запасів з оцінкою часу виживання та відновлення
Реагування на збої	Реактивне усунення наслідків відхилень після їх фізичного виникнення	Проактивне імітаційне моделювання та автоматичне перенаправлення потоків
Джерело стійкості	Фінансові інструменти та класичні програми страхування ризиків	Технологічна гнучкість, цифрові двійники та інтеграція персоналу

Джерело: узагальнено автором на основі [6, 8, 13].

У табл. 1 показано, що джерелом стійкості в сучасних умовах стає не мінімізація запасів будь-якою ціною, а поєднання резервування, цифрового моніторингу, сценарного планування й міжфункціональної взаємодії.

На глобальному рівні на складську логістику впливають інфляція, валютні коливання, регуляторні бар'єри, дефіцит комплектувальних і зміна вимог до простежуваності товарів, зокрема в чутливих до температури ланцюгах поставання [9–11, 22]. У випадках екстремальних природних або воєнних катастроф доцільним є використання математичного програмування для переміщення небезпечних вантажів і цінних активів у безпечні локації за умов дефіциту часу та транспортного флоту [12, 23].

Сучасний аудит складських ризиків вийшов за рамки формальних щорічних перевірок, перетворившись на основу операційної програми підприємства. Кількісний аналіз факторів ризику, проведений дослідниками на основі методів Cronbach's Alpha та дисперсійного аналізу (ANOVA), підтверджує, що найвищий рівень згоди експертів щодо критичності загроз стосується якості управління процесами (83 %) і внутрішніх крадіжок (83 %) [15]. Для побудови надійного захисного контуру провідні оператори використовують комплексний інструментарій оцінки операційних загроз. На етапі концептуального проектування застосовується якісна ідентифікація небезпек (HAID), яка на етапі детального проектування доповнюється структурованим аналізом небезпек та працездатності (HAZOP). Кількісна оцінка систем захисту здійснюється через аналіз рівнів безпеки (LOPA) для визначення вимог до систем протиаварійного захисту (SIL), тоді як для моделювання великих аварійних подій використовується метод «краватка-метелик» (bowtie) [14].

Важливе місце у системі управління ризиками посідає запобігання фізичному травматизму та пошкодженню інфраструктури. Статистичні дані свідчать про стійку структуру причин важкого травматизму в складському секторі. Це вимагає суворого дотримання галузевих регламентів, таких як OSHA 1910.178 для промислового транспорту, NFPA 13 для проектування систем пожежогасіння висотних складів та FEM 10.2.08 для інспектування стелажних систем [14].

Особливу увагу приділяють так званим «зонам взаємодії» (Interaction Zones), насамперед вантажним докам та проїздам з високою інтенсивністю руху. Останні дослідження рекомендують проектувати схеми руху транспорту з урахуванням «природних ліній поведінки» персоналу (desire lines), оскільки занадто довгі або незручні безпечні обхідні шляхи ігноруються працівниками, що створює додаткові некеровані ризики. Також доведено перевагу світлодіодних та лазерних проекторів дорожньої розмітки над звичайними фарбами, які швидко зтираються пилом або перекриваються піддонами [16].

Кількісна оцінка та моніторинг операційних ризиків вимагають інтеграції динамічних випереджальних показників (leading indicators) у панель управління WMS. Це дозволяє здійснювати проактивний контроль відхилень до моменту виникнення критичної події.

Інтеграція ризикології потребує переходу від загальних описів небезпек до вимірюваних індикаторів. У складській логістиці такими індикаторами можуть бути частота пошкоджень стелажів, кількість травм під час ручного переміщення вантажів, час закриття дефектів, результати перевірок розподілу небезпечних речовин і стан систем пожежогасіння та результати загальної оцінки складських операційних ризиків [15, 16]. Узагальнення цих показників подано в табл. 2.

**ТАБЛИЦЯ 2 — ПОКАЗНИКИ БЕЗПЕКИ
ТА ВИПЕРЕДЖАЛЬНІ ІНДИКАТОРИ СКЛАДСЬКИХ РИЗИКІВ**

Метрика ризику (KPI)	Сфера застосування та стандарт	Цільове призначення індикатора
Частота інцидентів з навантажувачами	OSHA 1910.178 / На 10 000 годин роботи	Контроль безпеки руху та оцінка кваліфікації водіїв складської техніки
Показник небезпечного зближення (Near-Miss)	ISO 3691-1 / Конфлікти пішохід-техніка	Виявлення слабких місць у фізичній схемі зонування та бар'єрах
Час закриття звітів про пошкодження стелажів	FEM 10.2.08 / Період усунення дефектів	Запобігання прогресуючому обваленню конструкцій через механічні удари
Частота травм від ручного оброблення вантажів	Методики MAC, REBA / На 100 FTE	Оцінка ергономічної відповідності робочих станцій комплектування
Показник успішності перевірок розподілу вантажів	Регламенти ADR, IMDG / Відсоток проходжень	Контроль дотримання правил сумісності зберігання небезпечних речовин
Compliance-показник систем пожежогасіння	NFPA 13 / Спринклерні тести та профілактика	Мінімізація ризику відмови автоматичних систем під час займання

Джерело: систематизовано автором на основі [14].

Зближення фізичних і цифрових ланцюгів постачань призводить до розширення поверхні кібератак, коли сенсори та хмарні платформи WMS стають вхідними точками для зловмисників. Сучасні дослідження вказують на те, що загрози дедалі частіше криються в інфраструктурі третіх сторін (Nth-tier ecosystems) та транзитивних залежностях програмного забезпечення, що вимагає впровадження обов'язкових специфікацій програмних компонентів (SBOM) та ретельної перевірки походження всіх компонентів коду [17].

Для пріоритизації інвестицій у безпеку доцільно застосовувати FMECA та показник Risk Priority Number, який поєднує ймовірність події, тяжкість наслідків і здатність системи виявити відхилення до настання збитків [28]. Поєднання RPN з Activity-Based Costing дає змогу обґрунтувати витрати на модернізацію не як формальне дотримання вимог, а як інвестицію в безперервність бізнесу.

Цифровізація складської логістики розширює поверхню кібератак, оскільки сенсори, RFID, мобільні термінали, хмарні сервіси та API зовнішніх партнерів стають потенційними точками проникнення [1, 17]. Для нейтралізації цих загроз складські комплекси мають впроваджувати архітектуру Zero Trust, яка передбачає багатофакторну автентифікацію, сегментування мереж, контроль доступу на основі ролей і перевірку кожної транзакції незалежно від її походження [17, 18].

Вразливості процесу приймання вантажів і технологічні засоби їх нівелювання наведено в табл. 3. Ця таблиця демонструє, що контроль ризику має починатися ще до фізичного прибуття вантажу на склад і продовжуватися під час приймання, ідентифікації, звіряння кількості та розміщення.

**ТАБЛИЦЯ 3 — ВРАЗЛИВОСТІ ПРОЦЕСУ ПРИЙМАННЯ ВАНТАЖУ
ТА ТЕХНОЛОГІЧНІ ЗАСОБИ ЇХ НІВЕЛЮВАННЯ**

Етап процесу та ризик	Вразливість системи	Технологічне рішення (Zero Trust / IoT)
Транспортування від відправника	Механічні пошкодження, підміна товарів, несанкціоноване відкриття транспортного засобу	Використання інтелектуального індикаторного пакування, датчиків розкриття та безперервного GPS-моніторингу
Відправка з пункту походження	Навмисне розкрадання частини партії до моменту опломбування та фіксації вантажу	Обов'язкове вагове маркування, RFID-ідентифікація кожної палети при виїзді зі складу постачальника
Декларування постачальником	Маніпуляція документами, невідповідність фактичної кількості задекларованим даним	Автоматичне звірення накладних через блокчейн-реєстри, виявлення аномалій алгоритмами машинного навчання
Транзитне перевезення	Крадіжки на проміжних стоянках за участю персоналу перевізника або третіх осіб	IoT-телеметрія замків вантажного відсіку, інтегрована з тривожною сигналізацією та геозонуванням
Розвантаження на складі призначення	Приховане вилучення високоціквдних одиниць персоналом під час розвантаження та сортування	Запис розкриття коробок камерами CCTV високої роздільної здатності із хмарним шифруванням та ШІ-аналізом дій
Розміщення в зоні зберігання	Помилки адресації, втрата палет в проходах, несанкціоноване списання залишків	Автоматичне підтвердження локації сканерами навантажувачів, логування змін у центральних аудит-таблицях WMS

Джерело: узагальнено автором на основі [1, 17, 18].

Штучний інтелект може виконувати роль превентивного інструмента реагування: виявляти аномалії в поведінці постачальників, прогнозувати відмови обладнання, рекомендувати альтернативні маршрути та ескалувати інциденти відповідальним особам [19–21]. Водночас використання ШІ потребує прозорого контролю якості даних, журналювання рішень і розмежування відповідальності між алгоритмом та управлінцем.

Особливо жорсткі вимоги до ризик-менеджменту висуваються в логістиці чутливих до температурних коливань товарів, зокрема у фармацевтичній галузі. Недотримання стандартів Належної практики дистрибуції (GDP) призводить до масштабних фінансових та репутаційних втрат. Запровадження вимог закону DSCSA (Drug Supply Chain Security Act) передбачає обов'язкову серіалізацію та пакетну верифікацію кожної товарної одиниці за кодами GTIN, лоту та терміну придатності. Будь-які невідповідності між електронними файлами даних (EPCIS) та фізичним вантажем ведуть до миттєвого карантину та штрафів, що загалом генерує для американського ринку до 6 мільярдів доларів додаткових витрат на рік [22].

Для кількісного прогнозування стійкості складських систем до зовнішніх шоків дедалі частіше застосовується імітаційне моделювання. Дискретно-подієві симуляції дозволяють стрес-тестувати систему за різними сценаріями катастрофічних збоїв (CRDs), оцінюючи чутливість ланцюга через метрики часу до виживання (TTS) та часу до відновлення (TTR) [13, 23]. Симуляційні експе-

рименти довели, що повне перекриття маршрутів між постачальниками та складами має значно більший деструктивний вплив на рівень сервісу, ніж різкі коливання попиту. Це обґрунтовує необхідність точного розрахунку страхових запасів (safety stock) та точок перезаамовлення (ROP) на основі балансування витрат на утримання запасів і вартості потенційних втрачених продажів [18, 24].

Інтегральний підхід до управління логістикою постачання, виробництва та дистрибуції, заснований на глибокій формалізації бізнес-процесів (як описують сучасні дослідження, наприклад, інтегральні моделі процесного керування Іваненка), дозволяє зв'язати оперативне планування з контролем відхилень у єдиний замкнений контур [25]. Останні напрацювання в галузі транскордонної електронної комерції пропонують використання OEM-моделей (Operational E-commerce Model) для досягнення стабільного зростання і мінімізації дисперсії часу доставки в умовах слабкої інфраструктури коридорів [26].

Для систематизації підходів до впровадження SCRM-практик у логістичну систему доцільно використовувати трирівневу структуру стандартів NIST SP 800-161, яка поєднує базові, підтримуючі та покращені заходи [27]. Додатково, логічна спроможність і несуперечність нових складських регламентів перед їх безпосереднім розгортанням верифікується математичним моделюванням за допомогою мереж Петрі, що унеможлиблює виникнення логічних колізій або блокувань процесів [4].

Ризики складської логістики неможливо ефективно контролювати одним методом. Для операційних, кібернетичних, інфраструктурних і партнерських загроз доцільно формувати комбіновану матрицю процедурних і математичних інструментів. Такий підхід подано в табл. 4, на яку слід спиратися під час побудови внутрішнього регламенту ризик-менеджменту складу.

**ТАБЛИЦЯ 4 — КОМПЛЕКС МАТЕМАТИЧНИХ
ТА ПРОЦЕДУРНИХ МОДЕЛЕЙ УПРАВЛІННЯ РИЗИКАМИ**

Модель / Стандарт	Сфера застосування в логістиці	Логістичний ефект
Мережі Петрі (Petri Nets)	Перевірка логічної узгодженості складських та виробничих процедур	Виявлення тупикових станів (deadlocks), циклічних блокувань та помилок адресації до розгортання WMS
Специфікація NIST SP 800-161	Трирівневе оцінювання зрілості процесів кібербезпеки ланцюгів постачань	Формування дорожньої карти від початкового контролю до прогностичного реагування на кіберзагрози
Формалізований підхід за Іваненко Л. М., Смерічевською С. В., Іваненко В. І.	Інтеграція логістики постачання, виробництва та збуту на підприємстві	Побудова замкненого контуру планування, обліку та координації бізнес-процесів середнього рівня
Модель дискретно-подієвої симуляції	Оцінка наслідків великих техногенних чи природних катастроф (CRDs)	Отримання точних значень TTS і TTR для критичних категорій товарних груп
Експертний метод MACTOR	Аналіз взаємодії та координації зацікавлених сторін складської мережі	Оптимізація взаємовідносин, усунення конфліктів та узгодження ризикових політик партнерів

Джерело: узагальнено автором на основі [4, 17, 25, 27].

У табл. 4 показано, що ризики складської логістики мають комплексний характер, тому їх неможливо усунути одним інструментом — необхідна комбінована матриця, яка поєднає математичне моделювання з процедурними стандартами й експертними методами. Такий інтегрований підхід дає змогу одночасно контролювати операційні, кібернетичні, інфраструктурні та партнерські загрози, що робить його доцільною основою для побудови внутрішнього регламенту ризик-менеджменту складу.

Дискусія. Розвиток наукових підходів до управління ризиками складської логістики свідчить про поступовий перехід від фрагментарного, здебільшого реактивного реагування на окремі види загроз до системних, процедурно-математичних моделей ризик-менеджменту. Класичні концепції SCRM, FMECA та ALARP заклали фундамент для кількісного оцінювання складських небезпек, однак в умовах воєнної та геополітичної нестабільності вони потребують подальшого методологічного переосмислення. Дискусійним залишається питання універсальності запропонованого комплексу інструментів — мереж Петрі, стандарту NIST SP 800-161, дискретно-подієвої симуляції та методу MASTOR, — оскільки її практична застосовність істотно залежить від рівня цифрової зрілості конкретного складського підприємства та доступності якісних історичних даних. Водночас актуалізується проблема адаптації міжнародних регуляторних стандартів до умов українських підприємств, які функціонують за одночасної дії інфраструктурних, енергетичних та воєнних обмежень. Окремої уваги потребує баланс між техноцентричною автоматизацією в межах Warehousing 5.0 і людиноцентричністю, оскільки надмірна орієнтація на швидку окупність технологічних рішень може нівелювати ергономічну й соціальну складову моделі. У цьому контексті постає необхідність розроблення інструментальних підходів, які поєднували б процедурне регламентування з економічним обґрунтуванням інвестицій у ризик-орієнтоване управління складською логістикою підприємства.

Висновки. Інтеграція ризикології в систему управління складською логістикою є необхідною передумовою конкурентоспроможності підприємства в умовах високої волатильності.

По-перше, підприємствам доцільно переходити до Warehousing 5.0, де автоматизація поєднується з людиноцентричністю, ергономікою та стійкістю процесів [2, 3]. По-друге, фрагментарний ризик-менеджмент має бути замінений інтегрованою системою SCRM із чіткими ролями, планами безперервності бізнесу та сценарним плануванням [6, 10, 13]. По-третє, оцінювання складських небезпек повинно мати кількісний характер через FMECA, ALARP, RPN та вартісне обґрунтування заходів безпеки [14, 28]. По-четверте, цифровий склад потребує Zero Trust, RBAC, MFA, журналювання подій та ШІ-інструментів виявлення аномалій [1, 17, 18]. По-п'яте, ESG та циркулярна логістика мають бути вбудовані в управління запасами, пакуванням і зворотними потоками [4, 29].

Практичне значення отриманих результатів полягає у можливості використання запропонованих таблиць і рекомендацій як основи для внутрішнього аудиту складської логістики, формування реєстру ризиків, вибору КРІ стійкості та визначення пріоритетів цифрової модернізації. Подальші дослідження доцільно спрямувати на емпіричну перевірку запропонованого комплексу на даних конкретних підприємств і розрахунок економічного ефекту від впровадження ризик-орієнтованих складських технологій.

Література

1. Sari A., Butun I. A security-centric warehouse management framework for mitigating product abuse and cybersecurity risks. *Computers*. 2026. Vol. 15. Article 348. doi: <https://doi.org/10.3390/computers15060348>.
2. Ekren B. Y., Venkatadri U., Sgarbossa F., Grosse E. H. Warehousing 5.0 for the future of the logistics industry. *International Journal of Production Research*. 2026. Vol. 64, No. 5. P. 1587-1597. doi: <https://doi.org/10.1080/00207543.2026.2617791>.
3. Mohammed A., Rahman M., Demir G., Shah B., Alaya A. When warehouses dream: a systems-informed exploration of Industry 5.0 principles in warehousing performance management. *International Journal of Systems Science: Operations & Logistics*. 2025. Vol. 12, No. 1. doi: <https://doi.org/10.1080/23302674.2025.2559257>.
4. Sánchez Suárez Y., Samá Muñoz D., Pancorbo Sandoval J. A., Domínguez Díaz L. E., Hernández Nariño A., Marqués León M., Espinosa Blanco M. A. Sustainable sugar agro-industrial value chain: an integrated lean framework for risk management, circularity, and artificial intelligence. *Sustainability*. 2026. Vol. 18. Article 6389. doi: <https://doi.org/10.3390/su18136389>.
5. Ghaddafi M., Fatimah S., Soekirman A., Agusinta L., Arubusman D. A. Analysis of the effect of warehousing management system and employee ability on work productivity through lean warehousing in the warehouses of the National Disaster Management Agency (BNPB) and the Regional Disaster Management Agency (BPBD). *TRANSEKONOMIKA: Akuntansi, Bisnis dan Keuangan*. 2025. Vol. 5, No. 4. P. 926-944. doi: <https://doi.org/10.55047/transekonomika.v5i4.971>.
6. Вакулєнко В., Лю Ю., Лю С. Система ризик-менеджменту логістичних систем в умовах воєнного стану України. Сталий розвиток економіки. 2025. № 3(54). С. 296-300. doi: <https://doi.org/10.32782/2308-1988/2025-54-45>.
7. Виклики, ризики та тренди логістики у 2026 році. Бліц-інтерв'ю з Global Ocean Link. *Ukrainian Shipping Magazine*. URL: <https://usm.media/gol-about-logistics-2026/>.
8. Як бізнесу знизити логістичні ризики у 2026 році: виклики та рішення. *Liga.net*. URL: https://blog.liga.net/user/peres_baro/article/58931.
9. Economic risk to supply chain up significantly over last quarter. *Lehigh University News*. URL: <https://news.lehigh.edu/economic-risk-to-supply-chain-up-significantly-over-last-quarter>.
10. Supply chain risk management (SCRM) in 2026: the process and policy template you need. *Secureframe*. URL: <https://secureframe.com/blog/supply-chain-risk-management>.
11. What is a supply chain risk management framework? *Z2Data*. URL: <https://www.z2data.com/insights/what-is-supply-chain-risk-management-framework>.
12. Zaid A. A., Jum'a L. The role of AI-driven supply chains in shaping agility, adaptability, and technology adoption under market turbulence. *Logistics*. 2026. Vol. 10. Article 49. doi: <https://doi.org/10.3390/logistics10020049>.
13. Supply chain risk management: complete guide 2026. *Ivalua*. URL: <https://www.ivalua.com/blog/supply-chain-risk-management/>.
14. Warehousing and logistics risk assessment 2026: methodologies, frameworks and KPIs. *SmartQHSE*. URL: <https://www.smartqhse.com/safety-blog/risk-assessment-warehousing-logistics-2026>.
15. Osa P. O., Kingsley-Omoyibo Q. A. Analysis of factors contributing to warehousing risk management and operations: a quantitative assessment. *World Journal of Advanced Engineering Technology and Sciences*. 2025. Vol. 16, No. 2. P. 223–233. doi: <https://doi.org/10.30574/wjaets.2025.16.2.1268>.
16. Warehouse risk assessment: a guide with free checklists. *GoAudits*. URL: <https://goaudits.com/blog/warehouse-risk-assessment/>.

17. Boyens J., Smith A., Bartol N., Winkler K., Holbrook A., Fallon M. Cybersecurity supply chain risk management practices for systems and organizations. NIST Special Publication 800-161r1-upd1. 2024. doi: <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>.
18. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. doi: <https://doi.org/10.6028/NIST.SP.800-207>.
19. AI, sustainability and traceability: 2026 trends in warehouse management. Asset Management Professionals. URL: <https://assetmanagementprofessionals.org/news-articles/ai-sustainability-and-traceability-2026>.
20. How to operationalize supply chain risk management. Hyperproof. URL: <https://hyperproof.io/resource/how-to-operationalize-supply-chain-risk-management>.
21. 2026 warehouse technology trends operations leaders should watch. MHS Lift. URL: <https://mhslift.com/2026-warehouse-technology-trends-operations-leaders-should-watch/>.
22. Pharma cold chain logistics standards & compliance guide 2025. Tempcon. URL: <https://www.tempcontrolpack.com/knowledge/pharma-cold-chain-logistics-standards-compliance-guide-2025/>.
23. Mharzi R., Ben Kacem A., Elouadi A. Catastrophe-related disruptions' preparedness and emergency management in Morocco: a proactive risks and resilience digital twin-based analysis. Journal of Modelling in Management. 2025. Vol. 20, No. 3. P. 825-845. doi: <https://doi.org/10.1108/JM2-02-2024-0050>.
24. Supply chain risk management: a consolidated framework. Pathlock. URL: <https://pathlock.com/blog/risk-mitigation/supply-chain-risk-management>.
25. Іваненко Л. М., Смерічевська С. В., Іваненко В. І. Інтегральний підхід до логістики постачання, виробництва та дистрибуції на основі формалізації логістичних бізнес-процесів. Бізнес Інформ. 2024. № 4. С. 315–325. doi: <https://doi.org/10.32983/2222-4459-2024-4-315-325>.
26. Jurayev K. Operational model of e-commerce consolidation logistics on emerging markets: methodology and effectiveness factors on the USA / Europe / South Korea — Central Asia corridors. The American Journal of Engineering and Technology. 2026. doi: <https://doi.org/10.37547/tajet/book-26-02>. URL: <https://www.theamericanjournals.com/index.php/tajet/article/download/8112/7405/12179>.
27. Julião B. J. B., Reis M. S., Duarte B. P. M. A systematic lean-driven framework for warehouse optimization. Systems. 2025. Vol. 13. Article 813. doi: <https://doi.org/10.3390/systems13090813>.
28. Supply chain risk management: best practices. Drata. URL: <https://drata.com/learn/tpm/supply-chain-best-practices>.
29. Panigrahi S. S., Bahinipati B., Jain V. Sustainable supply chain management: a review of literature and implications for future research. Management of Environmental Quality. 2019. Vol. 30, No. 5. P. 1001-1049. doi: <https://doi.org/10.1108/MEQ-01-2018-0003>.

References

1. Sari, A., & Butun, I. (2026). A security-centric warehouse management framework for mitigating product abuse and cybersecurity risks. Computers, 15, 348. <https://doi.org/10.3390/computers15060348>
2. Ekren, B. Y., Venkatadri, U., Sgarbossa, F., & Grosse, E. H. (2026). Warehousing 5.0 for the future of the logistics industry. International Journal of Production Research, 64(5), 1587-1597. <https://doi.org/10.1080/00207543.2026.2617791>
3. Mohammed, A., Rahman, M., Demir, G., Shah, B., & Alaya, A. (2025). When warehouses dream: A systems-informed exploration of Industry 5.0 principles in warehousing

performance management. *International Journal of Systems Science: Operations & Logistics*, 12(1). <https://doi.org/10.1080/23302674.2025.2559257>

4. Sánchez Suárez, Y., Samá Muñoz, D., Pancorbo Sandoval, J. A., Domínguez Díaz, L. E., Hernández Nariño, A., Marqués León, M., & Espinosa Blanco, M. A. (2026). Sustainable sugar agro-industrial value chain: An integrated lean framework for risk management, circularity, and artificial intelligence. *Sustainability*, 18, 6389. <https://doi.org/10.3390/su18136389>

5. Ghaddafi, M., Fatimah, S., Soekirman, A., Agusinta, L., & Arubusman, D. A. (2025). Analysis of the effect of warehousing management system and employee ability on work productivity through lean warehousing in the warehouses of the National Disaster Management Agency (BNPB) and the Regional Disaster Management Agency (BPBD). *TRANSEKONOMIKA: Akuntansi, Bisnis dan Keuangan*, 5(4), 926-944. <https://doi.org/10.55047/transekonomika.v5i4.971>

6. Vakulenko, V., Liu, Y., & Liu, S. (2025). Systema ryzyk-menedzhmentu lohistychnykh system v umovakh voiennoho stanu Ukrainy [Risk management system of logistics systems under martial law in Ukraine]. *Stalyi rozvytok ekonomiky*, 3(54), 296-300. <https://doi.org/10.32782/2308-1988/2025-54-45> [In Ukrainian]

7. Ukrainian Shipping Magazine. (2026). Vyklyky, ryzyky ta trendy lohistyky u 2026 rotsi: Blits-interviu z Global Ocean Link. <https://usm.media/gol-about-logistics-2026/> [In Ukrainian]

8. Liga.net. (2026). Yak biznesu znyzhyty lohistychni ryzyky u 2026 rotsi: Vyklyky ta rishennia. https://blog.liga.net/user/peres_baro/article/58931 [In Ukrainian]

9. Lehigh University News. (2026). Economic risk to supply chain up significantly over last quarter. <https://news.lehigh.edu/economic-risk-to-supply-chain-up-significantly-over-last-quarter>

10. Secureframe. (2026). Supply chain risk management (SCRM) in 2026: The process and policy template you need. <https://secureframe.com/blog/supply-chain-risk-management>

11. Z2Data. (2026). What is a supply chain risk management framework? <https://www.z2data.com/insights/what-is-supply-chain-risk-management-framework>

12. Zaid, A. A., & Jum'a, L. (2026). The role of AI-driven supply chains in shaping agility, adaptability, and technology adoption under market turbulence. *Logistics*, 10, 49. <https://doi.org/10.3390/logistics10020049>

13. Ivalua. (2026). Supply chain risk management: Complete guide 2026. <https://www.ivalua.com/blog/supply-chain-risk-management/>

14. SmartQHSE. (2026). Warehousing and logistics risk assessment 2026: Methodologies, frameworks and KPIs. <https://www.smartqhse.com/safety-blog/risk-assessment-warehousing-logistics-2026>

15. Osa, P. O., & Kingsley-Omoyibo, Q. A. (2025). Analysis of factors contributing to warehousing risk management and operations: A quantitative assessment. *World Journal of Advanced Engineering Technology and Sciences*, 16(2), 223–233. <https://doi.org/10.30574/wjaets.2025.16.2.1268>

16. GoAudits. (2026). Warehouse risk assessment: A guide with free checklists. <https://goaudits.com/blog/warehouse-risk-assessment/>

17. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2024). Cybersecurity supply chain risk management practices for systems and organizations (NIST SP 800-161r1-upd1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>

18. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>

19. Asset Management Professionals. (2026). AI, sustainability and traceability: 2026 trends in warehouse management. <https://assetmanagementprofessionals.org/news-articles/ai-sustainability-and-traceability-2026>
20. Hyperproof. (2026). How to operationalize supply chain risk management. <https://hyperproof.io/resource/how-to-operationalize-supply-chain-risk-management>
21. MHS Lift. (2026). 2026 warehouse technology trends operations leaders should watch. <https://mhslift.com/2026-warehouse-technology-trends-operations-leaders-should-watch/>
22. Tempcon. (2025). Pharma cold chain logistics standards & compliance guide 2025. <https://www.tempcontrolpack.com/knowledge/pharma-cold-chain-logistics-standards-compliance-guide-2025/>
23. Mharzi, R., Ben Kacem, A., & Elouadi, A. (2025). Catastrophe-related disruptions' preparedness and emergency management in Morocco: A proactive risks and resilience digital twin-based analysis. *Journal of Modelling in Management*, 20(3), 825-845. <https://doi.org/10.1108/JM2-02-2024-0050>
24. Pathlock. (2026). Supply chain risk management: A consolidated framework. <https://pathlock.com/blog/risk-mitigation/supply-chain-risk-management>
25. Ivanenko, L. M., Smerichevska, S. V., & Ivanenko, V. I. (2024). Intehralnyi pidkhid do lohistyky postachannia, vyrobnytstva ta dystrybutsii na osnovi formalizatsii lohistychnykh biznes-protsesiv [An integrated approach to the logistics of supply, production and distribution based on the formalization of logistic business processes]. *Biznes Inform*, (4), 315–325. <https://doi.org/10.32983/2222-4459-2024-4-315-325> [In Ukrainian]
26. Jurayev, K. (2026). Operational model of e-commerce consolidation logistics on emerging markets: Methodology and effectiveness factors on the USA / Europe / South Korea — Central Asia corridors. *The American Journal of Engineering and Technology*. <https://doi.org/10.37547/tajet/book-26-02>
27. Julião, B. J. B., Reis, M. S., & Duarte, B. P. M. (2025). A systematic lean-driven framework for warehouse optimization. *Systems*, 13, 813. <https://doi.org/10.3390/systems13090813>
28. Drata. (2026). Supply chain risk management: Best practices. <https://drata.com/learn/tprm/supply-chain-best-practices>
29. Panigrahi, S. S., Bahinipati, B., & Jain, V. (2019). Sustainable supply chain management: A review of literature and implications for future research. *Management of Environmental Quality*, 30(5), 1001-1049. <https://doi.org/10.1108/MEQ-01-2018-0003>