

УДК656.07:338.47

Г. Я. Левків,**д. е. н., Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Гжицького, м. Львів, Україна****ORCIDID: <https://orcid.org/0000-0002-5909-3390>****Г. З. Леськів,****к. т. н., Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Гжицького, м. Львів, Україна,****Івано-Франківський національний технічний університет нафти і газу м. Івано-Франківськ, Україна****ORCIDID: <https://orcid.org/0000-0002-4900-9466>****М. О. Хаврел,****магістр, Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Гжицького, м. Львів, Україна****ORCIDID: <https://orcid.org/0009-0004-4972-1113>**

DOI: 10.32702/2306-6792.2026.3.108

ФАКТОР БЕЗПЕКИ ПРИ РОЗВИТКУ ЛОГІСТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ СЬОГОДЕННЯ

Н. Levkiv,**Doctor of Economic Sciences, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies, Lviv, Ukraine****Н. Leskiv,****PhD in Technical Sciences,****Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies, Ivano-Frankivsk National Technical University of Oil and Gas, Ukraine****М. Khavrel,****Master, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies, Lviv, Ukraine**

THE SAFETY FACTOR IN THE DEVELOPMENT OF UKRAINE'S LOGISTICS INFRASTRUCTURE IN TODAY'S CONDITIONS

Мета дослідження полягає у розкритті ролі фактора безпеки як визначального елементу планування, проектування та управління розвитком логістичної інфраструктури у нашій країні в умовах сьогодення та у формуванні практичних рекомендацій щодо підвищення її стійкості. Об'єктом дослідження є процес розвитку логістичної інфраструктури у нашій країні в умовах підвищених безпекових ризиків. Умови сьогодення у нашій країні характеризуються високою мінливістю логістичних потоків, нерівномірним навантаженням на транспортні коридори, обмеженнями пропускної спроможності окремих вузлів і зростанням частоти інцидентів, що впливають на швидкість, вартість і прогнозованість доставки. За таких обставин розвиток логістичної інфраструктури має спиратися не лише на економічні критерії ефективності, а й на системне врахування безпеки як ключової умови функціональної стійкості. У межах теми безпека розглядається як інтегрований підхід, що охоплює фізичний захист критичних об'єктів, організаційну готовність до кризових сценаріїв, кібербезпеку цифрових систем логістики та захист інформації про маршрути і вантажі. Показано, що домінування точкових рішень, наприклад посилення охорони окремого складу без резервування маршрутів або без відпрацьованих процедур відновлення, не забезпечує належної безперервності постачання. Обґрунтовано доцільність підходу, за якого безпекові вимоги закладаються ще на стадії вибору локації, технічного завдання і проектування, а також підтримуються на етапі експлуатації через моніторинг стану інфраструктури, регламенти доступу, резервне електроживлення, дублювання критичних сервісів і регулярні навчання персоналу.

Акцентовано, що цифровізація логістики одночасно підвищує керованість процесів і посилює вразливість до кібератак, тому потрібні сегментація мереж, багатофакторна автентифікація, резервне копіювання з перевіркою відновлення, а також контроль прав доступу до даних. Окремо підкреслено перспективність застосування технологій на базі штучного інтелекту для раннього виявлення аномалій у потоках, прогнозування заторів і підтримки диспетчеризації за умови належного захисту даних і чіткої відповідальності за управлінські рішення.

The purpose of the study is to reveal the role of the security factor as a determining element of planning, designing and managing the development of logistics infrastructure in our country in the current conditions and in the formation of practical recommendations for increasing its stability. The object of the study is the process of developing logistics infrastructure in our country in conditions of increased security risks. Current conditions in our country are characterized by high variability of logistics flows, uneven load on transport corridors, limitations in the capacity of individual nodes and an increase in the frequency of incidents that affect the speed, cost and predictability of delivery. Under such circumstances, the development of logistics infrastructure should be based not only on economic efficiency criteria, but also on the systematic consideration of security as a key condition for functional stability. Within the framework of the topic, security is considered as an integrated approach that includes physical protection of critical facilities, organizational preparedness for crisis scenarios, cybersecurity of digital logistics systems and protection of information about routes and cargo. It is shown that the dominance of point solutions, for example, strengthening the security of a separate warehouse without route reservation or without proven recovery procedures, does not ensure proper continuity of supply. The feasibility of an approach is substantiated, in which security requirements are laid down at the stage of location selection, technical specifications and design, and are also supported at the operation stage through monitoring the state of the infrastructure, access regulations, backup power supply, duplication of critical services and regular personnel training. It is emphasized that the digitalization of logistics simultaneously increases the manageability of processes and increases vulnerability to cyberattacks, which is why network segmentation, multi-factor authentication, backup with recovery verification, and control of data access rights are required. The prospects for the use of technologies based on artificial intelligence for early detection of anomalies in flows, forecasting congestion and supporting dispatching, provided that data is properly protected and clear responsibility for management decisions is emphasized.

Ключові слова: логістична інфраструктура, безпековий фактор, стійкість ланцюгів постачання, управління ризиками, критична інфраструктура, кібербезпека, фізичний захист, резервування маршрутів, відновлення після пошкоджень, інвестиційне планування.

Key words: logistics infrastructure, security factor, supply chain resilience, risk management, critical infrastructure, cybersecurity, physical protection, route redundancy, disaster recovery, investment planning.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

В сучасному науковому дискурсі проблема розвитку логістичної інфраструктури та керування логістичними процесами розкривається переважно крізь призму оцінювання ефективності діяльності підприємств, забезпечення якості ланцюгів постачання, аналізу організаційних моделей логістичних центрів і загального стану інфраструктурної бази [1—10]. До прикладу, Н. Чернописька [1] акцентує увагу на методичних підходах до оцінювання логістичної діяльності підприємства, що є важливим для нашого дослідження з огляду на потребу формалізувати критерії, індикатори та логіку оцінювання результативності логістичних рішень. В. Хаврук [2] розглядає основні ас-

пекти якості ланцюга постачання, підкреслюючи, що якість у логістиці не зводиться лише до характеристик продукту, а формується на рівні процесів, взаємодії учасників та керованості потоків. В. Мандра [3] аналізує світовий досвід управління транспортно-логістичним центром, зосереджуючись на організаційних підходах, функціональній структурі та ролі управлінських механізмів у забезпеченні ефективності роботи таких центрів. О. Карий [4] досліджує логістичну інфраструктуру у нашій країні через співставлення наявних кількісних показників і практичних реалій її функціонування, привертаючи увагу до розривів між потребами економіки та фактичним станом інфраструктурних елементів.

Таблиця 1. Роль фактора безпеки у розвитку логістичної інфраструктури

Складова	Характеристика
Стійкість логістичних коридорів і вузлів	Безпека визначає, чи здатні транспортні коридори, мости, залізничні вузли, термінали й склади працювати без довгих зупинок під час загроз. У сучасних умовах важливо не лише мати маршрут, а й мати можливість швидко перейти на альтернативний, зберігши строки доставки та мінімізувавши втрати від простоїв.
Безперервність постачання критичних ресурсів	Логістика забезпечує постачання пального, медикаментів, продовольства, комплектуючих для виробництва та інших ресурсів, які не можуть чекати. Безпечові рішення, зокрема резервні потужності, дублювання складів і альтернативні схеми перевезень, знижують ризик дефіциту та хаотичних перебоїв.
Економічна стабільність і контрактна надійність	Коли інфраструктура захищена, бізнес може планувати виробництво й експорт, а партнери отримують прогнозовані строки та умови. Це впливає на репутацію, здатність виконувати довгострокові контракти, рівень логістичних витрат і фінансові результати підприємств.
Інвестиційна привабливість і довіра	Інвестори й міжнародні партнери оцінюють не лише технічні параметри об'єктів, а й ризик їх втрати або простою. Якщо безпека закладена у проєкти з самого початку, зростає готовність вкладати кошти в хаби, термінали, склади й цифрові системи, тому що правила захисту стають зрозумілими та перевірюваними.

Джерело: сформовано авторами.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Мета дослідження полягає у розкритті ролі фактора безпеки як визначального елементу планування, проєктування та управління розвитком логістичної інфраструктури у нашій країні в умовах сьогодення та у формуванні практичних рекомендацій щодо підвищення її стійкості. Об'єктом дослідження є процес розвитку логістичної інфраструктури у нашій країні в умовах підвищених безпекових ризиків.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Фактор безпеки при розвитку логістичної інфраструктури у нашій країні в умовах сьогодення слід розуміти як сукупність рішень, правил і практик, які забезпечують безперервність руху вантажів, людей і критично важливих ресурсів навіть тоді, коли середовище є нестабільним і ворожим. Логістична інфраструктура включає транспортні коридори, автодороги, залізничні колії, мости, тунелі, порти, річкові термінали, аеропорти, прикордонні переходи, логістичні хаби, склади, митні та сервісні зони, а також цифрові системи, через які плануються маршрути, оформлюються документи, відстежуються вантажі й координується робота операторів. У реальності сьогодення ця інфраструктура працює під тиском одночасно кількох чинників, це фізичні пошкодження об'єктів, обмеження пропускної спроможності, зміна географії потоків, зростання ролі

західних кордонів, підвищений попит на швидкі перевезення для оборони, гуманітарних потреб і підтримки економіки. Тому безпека перестає бути окремим напрямом охорони і перетворюється на принцип проєктування та управління, який визначає, де будувати, як будувати, як експлуатувати і як відновлювати (табл. 1).

Ризики для логістичної інфраструктури мають багатшаровий характер, і саме тому тема безпеки потребує комплексного розкриття. Фізичні загрози включають ракетні удари, атаки безпілотних літальних апаратів, диверсії, підпали, крадіжки вантажів, мінування окремих ділянок, а також навмисне пошкодження засобів зв'язку й енергоживлення. Окремий пласт становлять кіберризики, тому що сучасна логістика залежить від електронного документообігу, систем керування складом, систем керування транспортом, навігації, диспетчеризації, митних і банківських сервісів. Атака на сервери або на робочі станції може паралізувати оформлення, зробити неможливим планування маршрутів, призвести до витоку даних про критичні вантажі та їх переміщення, а це вже не лише економічна проблема, а й пряма загроза життю та національній стійкості. Є також організаційні ризики, це помилки в координації між перевізниками, адміністрацією інфраструктури, місцевою владою, митницею, силовими структурами, а також дефіцит персоналу й перевтома працівників у пікові періоди. Додаються фінансові ризики, це подорожчання страхування, обмежений доступ до дов-

Таблиця 2. Ключові групи ризиків для логістичної інфраструктури та їх наслідки

Група ризиків	Типові прояви	Наслідки для логістики й економіки
Фізичні загрози об'єктам і маршрутам	Пошкодження транспортних вузлів, руйнування мостів і під'їзних шляхів, атаки на склади та термінали, диверсії, підпали, мінування окремих ділянок, крадіжки вантажів, порушення енергоживлення й зв'язку на критичних точках	Зупинка або різке уповільнення руху вантажів, накопичення черг, зриви строків, подорожчання доставки, зростання втрат від псування товарів і простоїв транспорту, зниження довіри партнерів до стабільності ланцюга постачання
Кіберризики та інформаційні загрози	Атаки на системи керування складом і транспортом, втручання в електронний документообіг, блокування сервісів відстеження, фішингові кампанії проти персоналу, витік даних про маршрути й номенклатуру вантажів, шкідливе програмне забезпечення в корпоративних мережах	Параліч оформлення та координації перевезень, неможливість планувати маршрути, ризик компрометації критичних даних, помилки в обліку й відвантаженнях, затримки на кордонах, фінансові втрати та підвищення операційних ризиків
Організаційні та кадрові ризики	Нестача персоналу, перевтома та помилки через інтенсивний режим, слабка координація між операторами, митницею, адміністрацією інфраструктури й силовими структурами, відсутність тренувань реагування, неузгоджені протоколи дій під час загроз	Збої в управлінні потоками, хаотичні перенаправлення, дублювання або провали відповідальності, зростання часу простою, підвищення аварійності, збільшення витрат через неефективні рішення та втрату керованості в кризових ситуаціях
Фінансові та регуляторні ризики	Подорожчання страхування, обмежений доступ до кредитів, нестабільність тарифів, підвищення вартості охорони й ремонту, затримки погоджень, складні або непередбачувані процедури контролю, ризики невиконання умов договорів	Погіршення окупності інфраструктурних проєктів, відтермінування модернізації, скорочення інвестицій, зростання логістичних витрат для бізнесу й кінцевих споживачів, зменшення конкурентоспроможності експорту та уповільнення відновлення економіки

Джерело: сформовано авторами.

гих кредитів, нестабільність попиту, високі витрати на охорону, ремонт і резервування (табл. 2).

Практичне втілення фактора безпеки починається з підходу "безпека за задумом", коли захисні рішення закладаються ще на стадії вибору місця, технічного завдання і проектування. Для транспортних вузлів і логістичних хабів це означає правильну просторову структуру, розосередження критичних функцій, наявність альтернативних під'їзних шляхів, можливість швидко перенаправляти потоки, а також інженерні рішення, що зменшують наслідки ураження. Для складів і терміналів важливо мати зонування, контроль доступу, відеоспостереження, захист периметра, протипожежні системи, резервне електроживлення, запаси пального, захищені місця для зберігання критичних вантажів і засоби швидкої евакуації персоналу. Для залізничної й автомобільної інфраструктури безпека включає технічний моніторинг стану мостів і колій, своєчасні

ремонти, контроль перевантаження, обмеження руху в небезпечних зонах, а також організацію режимів руху під час повітряних тривог і загроз. Для цифрової частини це означає сегментацію мереж, багатофакторну автентифікацію, шифрування, резервне копіювання, план відновлення після інциденту, контроль прав доступу, регулярні оновлення та навчання працівників кібергігієні. Окремо важливі питання інформаційної безпеки, коли дані про маршрути, графіки та номенклатуру вантажів мають обмежений доступ і не потрапляють у відкриті канали (табл. 3).

Щоб фактор безпеки реально працював, потрібна зрозуміла система управління, фінансування та стандартів, яка поєднує державні пріоритети й можливості приватного сектору. На рівні держави ключовим є визначення критично важливих логістичних об'єктів і коридорів, встановлення мінімальних вимог до їх захисту, створення єдиних протоколів реагування на інциденти, а також

Таблиця 3. Практичні рішення безпеки, які закладаються у розвиток логістичної інфраструктури на етапі проєктування та експлуатації

Напрямок безпеки	Що саме роблять у проєкті або в роботі об'єкта	Приклад реалізації у логістичному хабі, складі або на маршруті	Який ефект для стійкості та безперервності постачання це дає
Просторова та інженерна стійкість об'єкта	Проєктують так, щоб критичні функції не були зосереджені в одному місці, передбачають зонування, резервні під'їзди, безпечні коридори руху персоналу, а також конструктивні рішення, що зменшують наслідки локальних пошкоджень	Розміщення складу з поділом на незалежні секції, окремі зони приймання й відвантаження, можливість працювати хоча б частиною потужностей при пошкодженні однієї ділянки, наявність другого в'їзду для вантажного транспорту	Знижується ризик повної зупинки роботи, збільшується швидкість відновлення після інциденту, скорочуються втрати від простоїв, підвищується прогнозованість строків доставки
Резервування ресурсів і сценарії безперервності	Завчасно готують резервне електроживлення, автономні засоби зв'язку, запаси пального, аварійні комплекти для ремонту, а також прописують сценарії роботи під час загрози і правила швидкого перенаправлення потоків	Дизельний генератор або акумуляторні системи для підтримки ключових процесів, дублювання каналів зв'язку, попередньо погоджені альтернативні маршрути для критичних вантажів, інструкції для персоналу на випадок повітряної тривоги	Підприємство не втрачає керування у кризі, зберігає мінімально необхідний рівень роботи, швидше переходить на альтернативні схеми, зменшує ризик дефіциту критичних ресурсів
Контроль доступу і фізичний захист	Впроваджують багаторівневий контроль доступу, відеоспостереження, охорону периметра, перевірки вантажів і транспорту, протипожежні системи, а також процедури реагування на підозрілі події	Перепусткова система з обмеженням доступу до зон з критичними вантажами, відеоаналітика для фіксації нетипових дій, датчики пожежі й задимлення, регулярні огляди території й пломбування вантажних відсіків	Зменшується ймовірність диверсій і крадіжок, підвищується дисципліна на об'єкті, скорочується час виявлення загрози, а наслідки інциденту стають локальнішими
Кібербезпека і захист логістичних даних	Захищають системи керування складом і транспортом, обмежують права доступу, застосовують багатофакторну автентифікацію, резервне копіювання, сегментацію мережі, регулярні оновлення, навчання персоналу розпізнавати атаки	Окрема мережа для критичних сервісів, щоденне резервне копіювання з перевіркою відновлення, журнали доступу, навчальні фішингові симуляції для працівників, заборона зберігати маршрути й номенклатуру вантажів у відкритих каналах	Знижується ризик паралічу оформлення й диспетчеризації, зменшується ймовірність витоку даних про переміщення вантажів, підвищується надійність електронного документообігу й координації

Джерело: сформовано авторами.

механізмів обміну інформацією між транспортними операторами, силовими структурами, митницею та місцевою владою. На рівні бізнесу потрібні політики безпеки, аудит підрядників, контроль ланцюга постачання, перевірка персоналу на критичних ділянках, корпоративні плани безперервності, а також договори, які чітко розподіляють відповідальність за охорону, кіберзахист і відновлення. Окрема тема це фінансова архітектура безпеки, де важливі страхування, гарантії, фонди відновлення, механізми співфінан-

сування і проєкти державно-приватного партнерства, коли частина витрат на захисні рішення підтримується державою або міжнародними партнерами, а частина вкладається оператором, який отримує стабільні правила гри та прогнозований попит.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отже, слід зазначити, що сам фактор безпеки при розвитку логістичної інфраструкту-

ри у нашій країні в умовах сьогодення являється базовою умовою життєздатності всієї системи перевезень і постачання, тому що саме він визначає безперервність роботи маршрутів, стійкість критичних вузлів, надійність цифрових процесів і швидкість відновлення після інцидентів. Коли безпека закладена в проектування, експлуатацію та управління ризиками одночасно, логістика зменшує втрати від простоїв, краще витримує зовнішні удари, підтримує експорт і забезпечує критичні потреби держави та бізнесу, а також формує довіру інвесторів і партнерів, що в підсумку створює реальну основу для відбудови та довгострокового економічного розвитку.

Література:

1. Чернописка Н. В. Методичні підходи до оцінювання логістичної діяльності підприємства. Вісник НУ "Львівська політехніка". 2015. № 608. С. 265—271.
2. Хаврук В. О. Основні аспекти якості ланцюга постачання. Управління проектами, системний аналіз і логістика. Технічна серія. 2012. Вип. 9. С. 223—228.
3. Мандра В. В. Аналіз світового досвіду управління транспортно-логістичним центром. Економічний аналіз. 2016. № 2. С. 92—97.
4. Карий О. І. Логістична інфраструктура в Україні: цифри і реальність. Вісник Національного університету "Львівська політехніка". Логістика. 2013. № 762. С. 73—79.
5. Благун І. С., Ничик О. Я. Напрями розвитку логістичної інфраструктури регіону, промисловий сектор. Причорноморські економічні студії. 2017. Вип. 18. С. 215—218.
6. Маматова Т. В., Назар С. К. Забезпечення стійкості транспортно-логістичної інфраструктури в Україні: нормативне підґрунтя, виклики та перспективи. Дніпровський науковий часопис публічного управління, психології, права. 2024. № 3. С. 59—6.
7. Зибарева О. В., Кравчук І. П. Формування механізму мережевої економіки на підприємствах: монографія. Чернівці: Технодруk, 2020. 276 с.
8. Зибарева О. В. Управління ризиками бізнес-проектів в умовах цифровізації. Проблеми сучасних трансформацій. Серія: економіка та управління, 2023, (10). <https://doi.org/10.54929/2786-5738-2023-10-04-09>
9. Штангрет А., Силкін О., Шляхетко В. Трудова міграція як зовнішня загроза для кадрової безпеки підприємства. № 10 (38), 2024. Наукові інновації та передові технології. С. 190—201. DOI: [https://doi.org/10.52058/2786-5274-2024-10\(38\)-190-20](https://doi.org/10.52058/2786-5274-2024-10(38)-190-20) (дата звернення: 11/06/2025).
10. Штангрет А., Силкін О. Безпекові аспекти управління персоналом в умовах гіпердинамічного зовнішнього середовища. № 9 (Вип. 37), 2024. Наукові інновації та передові технології. С. 227—237. DOI: [https://doi.org/10.52058/2786-5274-2024-9\(37\)-227-237](https://doi.org/10.52058/2786-5274-2024-9(37)-227-237) (дата звернення: 11/06/2025)

References:

1. Chornopyska, N. V. (2015), "Methodological approaches to assessing enterprise logistics activity", Visnyk Natsionalnoho universytetu "Lvivska politekhnika", vol. 608, pp. 265—271.
2. Khavruk, V. O. (2012), "Key aspects of supply chain quality", Upravlinnia proektamy, systemnyi analiz i lohistyka, tekhnichna seriia, vol. 9, pp. 223—228.
3. Mandra, V. V. (2016), "Analysis of global experience in managing a transport and logistics center", Ekonomichnyi analiz, vol. 2, pp. 92—97.
4. Karyi, O. I. (2013), "Logistics infrastructure in Ukraine, figures and reality", Visnyk Natsionalnoho universytetu "Lvivska politekhnika", Lohistyka, vol. 762, pp. 73—79.
5. Blahun, I. S., & Nychyk, O. Ya. (2017), "Directions for development of regional logistics infrastructure, industrial sector", Prychornomorski ekonomichni studii, vol. 18, pp. 215—218.
6. Mamatova, T. V., & Nazar, S. K. (2024), "Ensuring the resilience of transport and logistics infrastructure in Ukraine, regulatory framework, challenges and prospects", Dniprovskiyi naukovyi chasopys publicnogo upravlinnia, psykhologii, prava, vol. 3, pp. 59-6.
7. Zybareva, O. V., & Kravchuk, I. P. (2020), Formuvannia mekhanizmu merezhevoi ekonomiky na pidpriemstvakh [Formation of a network economy mechanism at enterprises], Tekhnodruk, Chernivtsi, Ukraine.
8. Zybareva, O. V. (2023), "Risk management of business projects under digitalization", Problemy suchasnykh transformatsii, seriia ekonomika ta upravlinnia, vol. (10). DOI <https://doi.org/10.54929/2786-5738-2023-10-04-09>
9. Shtangret, A., Silkin, O., & Shliakhetko, V. (2024), "Labor migration as an external threat to enterprise personnel security", Naukovi innovatsii ta peredovi tekhnologii, vol. 10 (38), pp. 190—201, DOI 10.52058/2786-5274-2024-10(38)-190-201.
10. Shtangret, A., & Silkin, O. (2024), "Security aspects of personnel management in a hyperdynamic external environment", Naukovi innovatsii ta peredovi tekhnologii, vol. 9 (37), pp. 227—237. *Стаття надійшла до редакції 25.01.2026 р.*