Ми висвітлимо ваші професійні здобутки
Успіхи і досягнення у науці
№ 1(23)
2026

УДК 656.078:004.056

https://doi.org/10.52058/3041-1254-2026-1(23)-1060-1069

Сеньків Андрій Тарасович аспірант кафедри маркетингу і логістики Інституту економіки і менеджменту, Національний університет «Львівська полі техніка», https://orcid.org/0009-0009-4203-9046

ТРАНСФОРМАЦІЯ БЕЗПЕКОВОСТІ ПРИ РОЗВИТКУ ЛОГІСТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Мета дослідження полягає у формуванні та обгрунтуванні комплексних підходів до трансформації безпековості під час розвитку логістичної інфраструктури для підвищення стійкості й безперервності логістичних процесів. Об'єкт дослідження є логістична інфраструктура та пов'язані з нею процеси перевезення, складування і цифрового супроводу вантажопотоків у частині їх безпекового забезпечення. Визначено сутність трансформації безпековості при розвитку логістичної інфраструктури як переходу від фрагментарних охоронних і контрольних процедур до інтегрованого управління ризиками, стійкістю та безперервністю логістичних процесів. Охарактеризовано логістичну інфраструктуру як взаємопов'язану систему транспортних коридорів, терміналів, складських комплексів, вузлів обробки вантажів, пунктів пропуску, енергетичних і комунікаційних компонентів, а також цифрових платформ планування, диспетчеризації, трекінгу та електронного документообігу. Встановлено, що зростання взаємозалежності фізичних об'єктів і цифрових сервісів формує ефект доміно, коли інцидент у критичному вузлі спричиняє каскад затримок, фінансові втрати та падіння довіри контрагентів. Обґрунтовано необхідність поєднаного розгляду груп загроз, серед яких фізичні впливи на інфраструктурні об'єкти та вантажі, кіберзагрози до систем керування перевезеннями і складськими операціями, уразливості навігації та зв'язку, інсайдерські дії і ризики ланцюга постачання підрядників, а також природні й техногенні чинники, що загрожують безперервності роботи. Доведено, що ефективне зниження вразливостей потребує закладання вимог безпековості на етапі проєктування, коли здійснюється оцінювання критичності активів, сценарне моделювання відмов, планування резервування маршрутів і потужностей, дублювання енергоживлення та визначення прийнятних показників часу відновлення.

Охарактеризовано операційний рівень трансформації як впровадження постійного моніторингу, управління доступом, перевірки контрагентів, стандартизації процедур, навчання персоналу, регулярних аудитів і відпрацьованих планів реагування на інциденти з відновленням даних і комунікацій.

Ключові слова: трансформація безпековості, логістична інфраструктура, управління ризиками, стійкість, безперервність діяльності, кібербезпека, фізична безпека, моніторинг, резервування, ланцюги постачання.

Senkiv Andriy Tarasovych Postgraduate student of the Department of Marketing and Logistics, Institute of Economics and Management, Lviv Polytechnic National University, https://orcid.org/0009-0009-4203-9046

TRANSFORMATION OF SECURITY IN THE DEVELOPMENT OF LOGISTICS INFRASTRUCTURE

Abstract. The purpose of the study is to form and substantiate comprehensive approaches to the transformation of security during the development of logistics infrastructure to increase the stability and continuity of logistics processes. The object of the study is the logistics infrastructure and the related processes of transportation, warehousing and digital support of cargo flows in terms of their security. The essence of the transformation of security in the development of logistics infrastructure is determined as a transition from fragmented security and control procedures to integrated risk management, stability and continuity of logistics processes. The logistics infrastructure is characterized as an interconnected system of transport corridors, terminals, warehouse complexes, cargo processing nodes, checkpoints, energy and communication components, as well as digital platforms for planning, dispatching, tracking and electronic document management. It is established that the growth of interdependence of physical objects and digital services creates a domino effect, when an incident at a critical node causes a cascade of delays, financial losses and a decline in the trust of counterparties. The need for a combined consideration of threat groups is justified, including physical impacts on infrastructure facilities and cargo, cyber threats to transportation and warehouse management systems, navigation and communication vulnerabilities, insider actions and risks of the contractor supply chain, as well as natural and man-made factors that threaten the continuity of work. It is proven that effective vulnerability reduction requires the establishment of security requirements at the design stage, when asset criticality assessment, failure scenario modeling, route and capacity reservation planning, power supply redundancy and determination of acceptable recovery time indicators are carried out.

The operational level of transformation is characterized as the implementation of continuous monitoring, access control, counterparty verification, standardization of procedures, personnel training, regular audits and proven incident response plans with data and communications recovery.

Keywords: security transformation, logistics infrastructure, risk management, resilience, business continuity, cybersecurity, physical security, monitoring, redundancy, supply chains.

Постановка проблеми. Сучасні ланцюги постачання дедалі більше залежать від складних мереж транспортних коридорів, терміналів, складів, цифрових платформ і постачальників послуг, а будь-який збій у цій системі швидко перетворюється на економічні втрати, дефіцит ресурсів, зриви виробничих графіків і зниження конкурентоспроможності територій та підприємств. Розвиток інфраструктури, який традиційно оцінювали через пропускну спроможність, швидкість і собівартість, тепер неможливо відокремити від нових профілів загроз, серед яких фізичні пошкодження об'єктів, терористичні й диверсійні ризики, зростання кіберзагроз для систем управління транспортом і складською логістикою, вразливості супутникової навігації та зв'язку, маніпуляції даними у цифрових документах, а також ризики, пов'язані з організованою злочинністю й контрабандними потоками.

Аналіз останніх досліджень і публікацій. В наукових публікаціях, присвячених логістичній інфраструктурі, домінує підхід, за якого інфраструктура розглядається як один з ключових чинників конкурентоспроможності підприємств і територій. Так, С. М. Ортнік [1] акцентує увагу на тому, що формування і розвиток логістичної інфраструктури підсилює конкурентні позиції через підвищення якості логістичного сервісу, скорочення витрат і покращення керованості потоків ресурсів. О. І. Карий і Г. В. Подвальна [2] аналізують місце логістичної інфраструктури України у світових рейтингах, підкреслюючи значущість індикаторів якості інфраструктури, ефективності митних процедур і надійності логістичних послуг.О. В. Зибарева та І. Л. Гольцова [8] виокремлюють ключові аспекти і сучасні тренди розвитку цифрових технологій у діяльності підприємств, що релевантно для логістики через поширення цифрових платформ, електронного документообігу, систем управління перевезеннями та аналітики даних, які стають новими об'єктами захисту. А. Штангрет і О. Силкін [9] розкривають безпекові аспекти управління персоналом в умовах гіпердинамічного зовнішнього середовища, що важливо для логістичної інфраструктури, де значна частина інцидентів пов'язана з помилками, інсайдерськими ризиками, культурою дотримання процедур і готовністю персоналу діяти за протоколами реагування.

Мета дослідження полягає у формуванні та обгрунтуванні комплексних підходів до трансформації безпековості під час розвитку логістичної інфраструктури для підвищення стійкості й безперервності логістичних процесів. Об'єкт дослідження є логістична інфраструктура та пов'язані з нею процеси перевезення, складування і цифрового супроводу вантажопотоків у частині їх безпекового забезпечення.

Виклад основного матеріалу. Трансформація безпековості при розвитку логістичної інфраструктури означає перехід від вузького уявлення про охорону об'єктів і контроль доступу до комплексної системи управління ризиками,

стійкістю та безперервністю логістичних процесів. Логістична інфраструктура сьогодні є не лише дорогами, залізницею, портами, аеропортами, терміналами, складами й митними переходами, а й цифровими контурами, серед яких системи управління перевезеннями, складські системи, електронний документообіг, платформи бронювання, трекінг вантажів, системи керування рухом і критичні комунікації. Саме ця взаємопов'язаність створює ефект доміно, коли інцидент на одному вузлі, наприклад відмова енергоживлення на сортувальному хабі або збій у системі планування маршрутів, швидко викликає затримки в суміжних секторах, порушення контрактних зобов'язань, втрати якості товарів, збільшення витрат і падіння довіри клієнтів. Тому безпековість у логістиці потрібно розуміти як здатність системи запобігати загрозам, витримувати удари, адаптуватися до змін і швидко відновлювати функціонування, зберігаючи прийнятний рівень сервісу, передбачуваності та контролю (табл.1).

Таблиця 1

Трансформація безпековості у логістичній інфраструктурі

Категорія загроз і вразливостей	Як має змінюватися безпековість під час розвитку інфраструктури
Фізичні загрози для вузлів інфраструктури, складів, терміналів, транспортних коридорів, вантажів, персоналу, а також ризики крадіжок і навмисного втручання	Безпековість переходить від охорони периметра до керованої багаторівневої системи, де поєднані інженерний захист, контроль доступу, зонування території, правила роботи з критичними зонами, перевірка маршрутів підвищеного ризику та постійний моніторинг подій. У проєктних рішеннях з'являються вимоги до резервних під'їздів, безпечних майданчиків для простою, посилення конструкцій, протипожежних рішень, а також до планів реагування, які визначають дії персоналу, логіку евакуації і порядок відновлення робіт
Кіберзагрози для систем управління перевезеннями, складськими операціями, електронним документообігом, трекінгом, платіжними процесами, а також ризики підміни даних і компрометації облікових записів	Безпековість доповнюється кіберстійкістю, де ключовими стають сегментація доступів, багатофакторна автентифікація, принцип найменших привілеїв, контроль змін, журналювання, резервне копіювання та перевірене відновлення. Додатково змінюється ставлення до даних, оскільки цілісність електронних документів і трекінгу визначає правильність маршрутизації та пріоритетів обробки, тому вводяться процедури валідації, контролю аномалій і розмежування відповідальності. Технології на базі штучного інтелекту можуть підтримувати раннє виявлення підозрілих патернів, але лише за умови надійного захисту даних і контролю помилок автоматизації

Категорія загроз і вразливостей	Як має змінюватися безпековість під час розвитку інфраструктури
Природні й техногенні чинники, перебої енергопостачання, пожежі, аварії, екстремальні погодні явища, що зупиняють роботу вузлів і порушують строки постачання	Безпековість стає орієнтованою на безперервність діяльності, тому з'являються вимоги до дублювання критичних сервісів, автономних джерел живлення, резервних каналів зв'язку, запасних майданчиків і альтернативних маршрутів. Розвиток інфраструктури передбачає створення буферів потужностей, гнучкі сценарії перенаправлення потоків, а також регламенти швидкого переходу на ручні процедури, коли цифрові сервіси тимчасово недоступні. Важливим результатом є скорочення часу простою, стабільність температурних режимів для чутливих вантажів і прогнозована швидкість відновлення операцій

Джерело: сформовано автором

Коло загроз для логістичної інфраструктури стало ширшим і складнішим, тому що одночасно зростають фізичні, цифрові, організаційні та природні ризики. До фізичних належать пошкодження транспортних шляхів, мостів, тунелів, терміналів, складів, об'єктів енергетики та зв'язку, а також крадіжки, втручання в вантаж, підроблення пломб, інсайдерські дії, блокування маршрутів і вплив організованої злочинності. До цифрових належать атаки на системи управління перевезеннями і складськими операціями, шифрування даних з вимогою викупу, компрометація облікових записів, підміна реквізитів у платіжних дорученнях, фішинг для доступу до документів, атаки на промислові системи керування, а також маніпуляції даними трекінгу, що може створити помилкову картину місцезнаходження вантажу. Окрему групу становлять ризики уразливості навігації та зв'язку, коли перешкоди або спотворення сигналів порушують маршрутизацію, координацію руху та безпеку перевезень. Додаються природні та техногенні чинники, серед яких повені, сильні вітри, спека, обмерзання, пожежі, аварії на небезпечних об'єктах, дефіцит води для портових операцій, а також перебої постачання електроенергії, що критично для холодильних складів і автоматизованих комплексів. Усе це посилюється глобальною нестабільністю ринків, змінами регулювання, дефіцитом кадрів, зростанням витрат на страхування й необхідністю дотримання вимог до прозорості походження товарів, що підвищує ціну помилки у кожному вузлі логістичного ланцюга (табл.2).

Таблиця 2

Безпековість у життєвому циклі інфраструктурного проєкту

Етап розвитку логістичної інфраструктури	Ключові рішення безпековості, які треба закласти	Показники результату, за якими видно ефект
Передпроєктна підготовка	Визначення критичних вузлів і залежностей між ними, формування карти ризиків з урахуванням фізичних і цифрових загроз, вибір сценаріїв, які мають найбільші наслідки для безперервності. Планування резервних маршрутів і потужностей, підготовка вимог до енергоживлення і зв'язку, первинні вимоги до перевірки контрагентів	Зниження частки непередбачених витрат у проєкті, наявність погоджених сценаріїв реагування, розрахований допустимий час простою і відновлення, визначені пріоритети захисту для найбільш критичних активів
Проєктування і закупівлі	Проєктування з урахуванням зонування, контролю доступу, протипожежних і інженерних рішень, а також вимог кіберстійкості для цифрових систем. Вимоги до постачальників щодо безпечної конфігурації, оновлень, журналювання, резервного копіювання, а також до сумісності з моніторинговими системами	Відсутність критичних уразливостей у проєктних рішеннях, готовність інфраструктури до резервування, наявність формалізованих вимог до підрядників, підтверджена можливість відновлення даних і сервісів за регламентом
Будівництво і введення в експлуатацію	Контроль фізичної безпеки майданчика, управління доступом підрядників, перевірка відповідності фактичних рішень проєктним вимогам, тестування планів реагування і процедур відновлення. Налаштування кіберзахисту, розмежування ролей, навчання персоналу, запуск моніторингу інцидентів і аномалій	Зменшення інцидентів на майданчику, успішне проходження тестів відновлення, зниження кількості помилок під час запуску, стабільна робота критичних сервісів у тестових стресових режимах

Джерело: сформовано автором

Управлінська трансформація безпековості полягає в тому, що безпека перестає бути функцією окремого підрозділу і стає наскрізною відповідальністю проєктування, експлуатації та партнерської взаємодії. Для інфраструктурних проєктів ключовим є принцип закладання безпековості на етапі проєктування, коли визначають критичні активи, аналізують сценарії загроз, моделюють наслідки відмов і планують резервування, тобто альтернативні маршрути, дублювання енергоживлення, запасні майданчики, буферні запаси і процедури переведення операцій у ручний режим. На операційному рівні формується логіка

безперервного управління ризиками, де поєднуються оцінювання вразливостей, контроль доступу, перевірка контрагентів, стандарти роботи з підрядниками, навчання персоналу, аудит процедур, а також чіткі плани реагування на інциденти, включно з комунікаціями, взаємодією з регуляторами і відновленням даних. Важливою стає інтеграція публічних і приватних суб'єктів, оскільки об'єкти логістики часто належать бізнесу, але працюють у просторі критичної інфраструктури, де потрібні спільні протоколи, обмін інформацією, узгоджені стандарти і спільні навчання. Окремої уваги потребує баланс між швидкістю логістики та контрольними процедурами, тому що надмірні перевірки можуть паралізувати потоки, а недостатні створюють ризики, отже завданням є розумне, ризик-орієнтоване керування, яке концентрує ресурси на найбільш уразливих ділянках і найнебезпечніших сценаріях (рис.1).

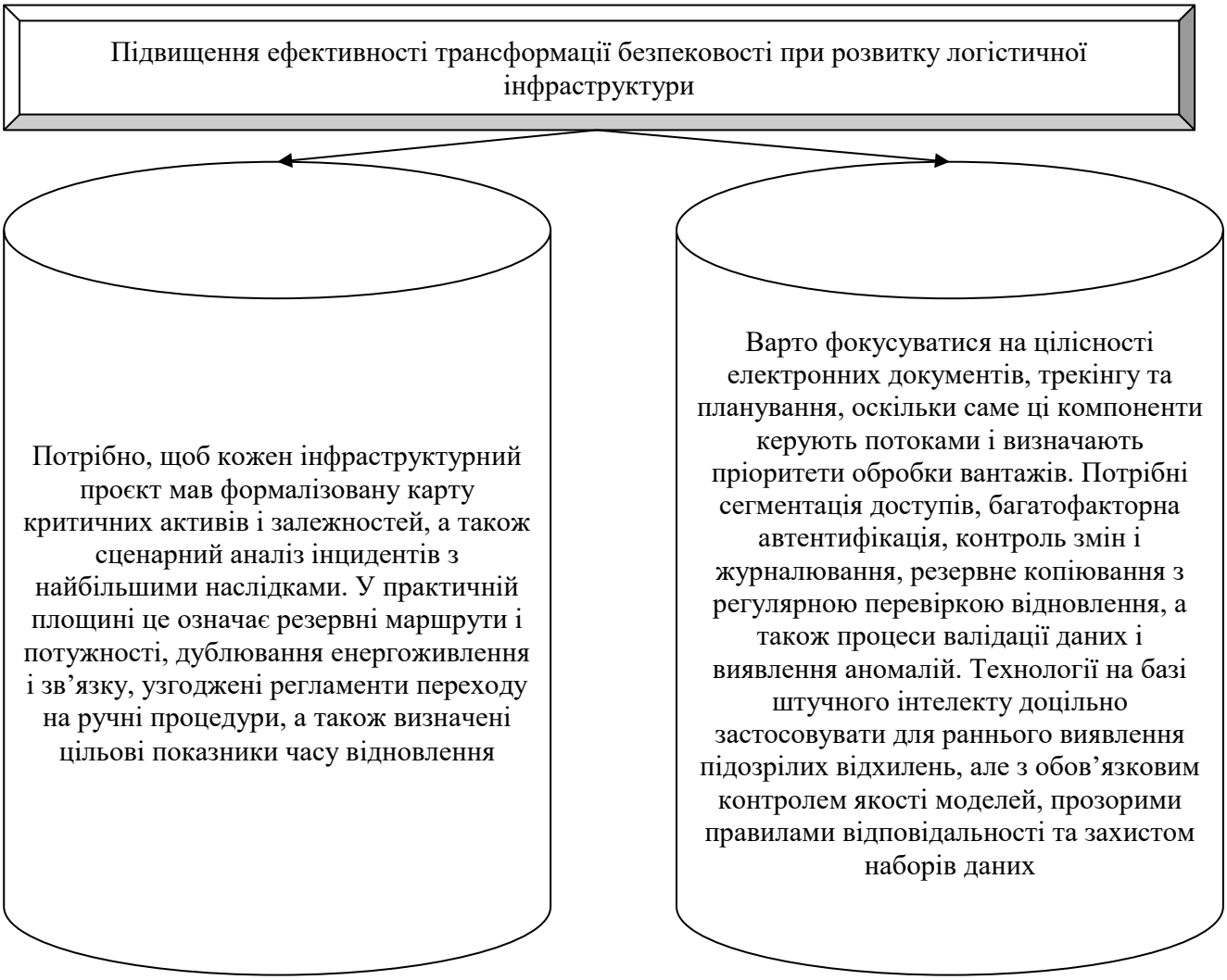

Рис.1. Підвищення ефективності трансформації безпековості при розвитку логістичної інфраструктури

Технологічний аспект є одним з головних драйверів змін, оскільки цифровізація одночасно підвищує ефективність і створює нові уразливості, а отже потребує захисту не лише фізичних об'єктів, а й даних, алгоритмів і каналів зв'язку. На практиці це означає розвиток систем моніторингу, датчиків, відеоаналітики, контролю стану інфраструктури, кіберзахисту мереж і сегментації доступів, багатофакторної автентифікації, резервного копіювання та швидкого відновлення, а також контроль цілісності електронних документів. Технології на базі штучного інтелекту можуть підсилювати безпековість через раннє виявлення аномалій у потоках вантажів, прогнозування ризикових зон, аналіз поведінки на периметрі, оптимізацію маршрутів з урахуванням загроз і погодних чинників, а також підтримку диспетчерів у кризових ситуаціях. Водночас ці технології вимагають відповідальної експлуатації, якісних даних, захисту моделей і контролю помилок, тому що неправильні рішення автоматизації можуть створити нові ризики. Для розвитку інфраструктури практичним результатом теми є набір підходів, які можна закладати в інвестиційні рішення, серед них оцінювання критичності вузлів, вимоги до резервування, стандарти кіберстійкості, показники часу відновлення, вимоги до надійності постачальників, протоколи обміну інформацією, регулярні навчання персоналу та тестування планів реагування. У підсумку трансформація безпековості стає необхідною умовою конкурентоспроможної логістики, тому що без гарантій стійкості, передбачуваності та довіри інфраструктурні інвестиції не забезпечують очікуваного ефекту для бізнесу й суспільства.

Висновки. Підсумовуючи, зазначимо, шо саме трансформація безпековості при розвитку логістичної інфраструктури є переходом до комплексного, ризик-орієнтованого управління, де фізичний захист, кіберстійкість, організаційні процедури, надійність партнерів і готовність до відновлення розглядаються як єдина система забезпечення безперервності логістики. З огляду на взаємопов'язаність транспортних, складських і цифрових елементів, зростання фізичних і цифрових загроз, а також вплив кліматичних і техногенних чинників, безпековість має закладатися вже на етапі проєктування, підкріплюватися резервуванням критичних вузлів, регулярним оцінюванням вразливостей, підготовкою персоналу та узгодженими протоколами взаємодії держави і бізнесу. Технології на базі штучного інтелекту можуть посилювати здатність до раннього виявлення інцидентів і прогнозування ризиків, але потребують відповідального використання та захисту даних. Саме тому інвестиції в інфраструктуру мають супроводжуватися інвестиціями в безпековість, оскільки лише поєднання ефективності й стійкості забезпечує довіру, передбачуваність і конкурентоспроможність логістичних ланцюгів у середовищі постійних змін.

Література:

1. Бортнік С. М. Формування та розвиток логістичної інфраструктури як фактор забезпечення конкурентоспроможності підприємств. № 3(81), 2019. Вісник Сумського національного аграрного університету. Серія Економіка і менеджмент. С. 45–50.
2. Карий О. І., Подвальна Г. В. Логістична інфраструктура України у світових рейтингах. № 873, 2017. Вісник Національного університету «Львівська політехніка». Серія Проблеми економіки та управління. С. 41–49.
3. Харченко М. В. Транспортно-логістична інфраструктура та її місце в соціально-економічній системі підприємств України. № 153, 2020. Економічний простір. С. 83–88.
4. Ільченко Н. Б., Кулік А. В. Розвиток транспортно-логістичної системи в Україні. Том 30(69). № 5(2), 2019. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія Економіка і управління. С. 42–50.
5. Іщенко О. А. Методичні підходи до оцінювання інфраструктурного забезпечення транспортно-логістичних систем. Том 28. № 4, 2018. Економічний аналіз. С. 313–320.
6. Корнієцький О. В., Орел В. М. Моделі відновлення транспортно-логістичної інфраструктури скотарства на деокупованих територіях України. Том 9. № 3, 2024. Український журнал прикладної економіки та техніки. С. 144–149.
7. Гнєдіна К., Нагорний В. Сучасний стан та проблеми розвитку логістичної інфраструктури України. № 65, 2024. Економіка та суспільство. С. 18–27.
8. Зибарева О.В., Гольцова І.Л. Ключові аспекти та сучасні тренди розвитку цифрових технологій в діяльності підприємств України. Ефективна економіка. 2020. №12. URL: http://www.economy.nayka.com.ua/?op=1&z=8444
9. Штангрет А., Силкін О. Безпекові аспекти управління персоналом в умовах гіпердинамічного зовнішнього середовища. № 9(37), 2024. Наукові інновації та передові технології. С. 227-237. https://doi.org/10.52058/2786-5274-2024-9(37)-227-237
10. Криштанович, М., & Силкін, О. Оцінювання стратегічних напрямів реалізації державно-приватного партнерства в царині безпекового розвитку агропромислового сектора. Socio-Economic Relations in the Digital Society, 1(55), 2025, 44-55. https://doi.org/10.55643/ser.5.55.2025.587
11. 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. https://doi.org/10.52058/2786-5274-2024-10(38)-190-201
12. Криштанович, М., Богоніс А. Інформаційне забезпечення роботи системи публічного управління. Актуальні питання у сучасній науці, 4(22), 2024, 359-368.
13. Криштанович М.Ф., Богоніс А.Р. Інформаційна безпека в умовах цифровізації: виклики сучасності. Журнал «Наукові перспективи», № 3(45) 2024. - С. 214-223. https://doi.org/10.52058/2708-7530-2024-3(45)-214-223

References:

1. Bortnik, S. M. (2019). Formuvannia ta rozvytok lohistychnoi infrastruktury yak faktor zabezpechennia konkurentospromozhnosti pidpryiemstv [Formation and development of logistics infrastructure as a factor in ensuring enterprise competitiveness]. Visnyk Sumskoho natsionalnoho ahrarnoho universytetu. Seriia Ekonomika i menedzhment – Bulletin of Sumy National Agrarian University. Series Economics and Management, 3(81), 45–50. [in Ukrainian].
2. Karyi, O. I., & Podvalna, H. V. (2017). Lohistychna infrastruktura Ukrainy u svitovykh reitynhakh [Ukraine's logistics infrastructure in global rankings]. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia Problemy ekonomiky ta upravlinnia – Bulletin of Lviv Polytechnic National University. Series Problems of Economics and Management, 873, 41–49. [in Ukrainian].

3. Kharchenko, M. V. (2020). Transportno-lohistychna infrastruktura ta yii mistse v sotsialno-ekonomichnii systemi pidpryiemstv Ukrainy [Transport and logistics infrastructure and its place in the socio-economic system of Ukrainian enterprises]. Ekonomichnyi prostir – Economic Space, 153, 83–88. [in Ukrainian].

4. Ilchenko, N. B., & Kulik, A. V. (2019). Rozvytok transportno-lohistychnoi systemy v Ukraini [Development of the transport and logistics system in Ukraine]. Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia Ekonomika i upravlinnia – Scientific Notes of V. I. Vernadsky Taurida National University. Series Economics and Management, 30(69), 5(2), 42–50. [in Ukrainian].

5. Ishchenko, O. A. (2018). Metodychni pidkhody do otsiniuvannia infrastrukturnoho zabezpechennia transportno-lohistychnykh system [Methodological approaches to assessing infrastructure support of transport and logistics systems]. Ekonomichnyi analiz – Economic Analysis, 28(4), 313–320. [in Ukrainian].

6. Korniietskyi, O. V., & Orel, V. M. (2024). Modeli vidnovlennia transportno-lohistychnoi infrastruktury skotarstva na deokupovanykh terytoriiakh Ukrainy [Models for restoring the transport and logistics infrastructure of cattle breeding in de-occupied territories of Ukraine]. Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky – Ukrainian Journal of Applied Economics and Technology, 9(3), 144–149. [in Ukrainian].

7. Hniedina, K., & Nahornyi, V. (2024). Suchasnyi stan ta problemy rozvytku lohistychnoi infrastruktury Ukrainy [Current state and problems of logistics infrastructure development in Ukraine]. Ekonomika ta suspilstvo – Economy and Society, 65, 18–27. [in Ukrainian].

8. Zybareva, O. V., & Holtsova, I. L. (2020). Kliuchovi aspekty ta suchasni trendy rozvytku tsyfrovykh tekhnolohii v diialnosti pidpryiemstv Ukrainy [Key aspects and current trends in the development of digital technologies in the activities of Ukrainian enterprises]. Efektyvna ekonomika – Efficient Economy, 12. http://www.economy.nayka.com.ua/?op=1&z=8444[in Ukrainian].

9. Shtangret, A., & Sylkin, O. (2024). Bezpekovi aspekty upravlinnia personalom v umovakh hiperdynamichnoho zovnishnoho seredovyshcha [Security aspects of personnel management under hyperdynamic external environment]. Naukovi innovatsii ta peredovi tekhnolohii – Scientific Innovations and Advanced Technologies, 9(37), 227–237. https://doi.org/10.52058/2786-5274-2024-9(37)-227-237 [in Ukrainian].

10. Kryshtanovych, M., & Sylkin, O. (2025). Otsiniuvannia stratehichnykh napriamiv realizatsii derzhavno-pryvatnoho partnerstva v tsaruni bezpekovoho rozvytku ahropromyslovoho sektora [Assessment of strategic directions for implementing public-private partnership in the field of security development of the agro-industrial sector]. Socio-Economic Relations in the Digital Society, 1(55), 44–55. https://doi.org/10.55643/ser.5.55.2025.587 [in Ukrainian].

11. Shtangret, A., Sylkin, O., & Shliakhetko, V. (2024). Trudova mihratsiia yak zovnishnia zahroza dlia kadrovoi bezpeky pidpryiemstva [Labor migration as an external threat to enterprise's personnel security]. Naukovi innovatsii ta peredovi tekhnolohii – Scientific Innovations and Advanced Technologies, 10(38), 190–201. https://doi.org/10.52058/2786-5274-2024-10(38)-190-201 [in Ukrainian].

12. Kryshtanovych, M., & Bohonis, A. (2024). Informatsiine zabezpechennia roboty systemy publichnoho upravlinnia [Information support for the functioning of the public administration system]. Aktualni pytannia u suchasnii nautsi – Current Issues in Modern Science, 4(22), 359–368. [in Ukrainian].

13. Kryshtanovych M.F., Bogonis A.R. Information security in the context of digitalization: challenges of the present. Journal "Scientific Perspectives", No. 3(45) 2024. pp. 214-223. [in Ukrainian].