



УДК 658.012.8: 658.7: 338.24(477)(045):004.9

[https://doi.org/10.52058/3041-1254-2025-11\(21\)-494-510](https://doi.org/10.52058/3041-1254-2025-11(21)-494-510)

Волкова Неля Василівна кандидат економічних наук, доцент, доцент кафедри підприємництва і права Полтавського державного аграрного університету, м. Полтава, <https://orcid.org/0000-0002-8374-1546>

Світлична Алла Василівна кандидат економічних наук, доцент, професор кафедри підприємництва і права Полтавського державного аграрного університету, м. Полтава, <https://orcid.org/0000-0003-3674-5787>

Кирпота Альона Геннадіївна здобувачка другого (магістерського) рівня вищої освіти, Полтавський державний аграрний університет, м. Полтава, <https://orcid.org/0009-0008-1176-3691>

Гаркуша Антон Сергійович здобувач другого (магістерського) рівня вищої освіти, Полтавський державний аграрний університет, м. Полтава, <https://orcid.org/0009-0004-6306-7218>

Мирошніченко Роман Вікторович здобувач другого (магістерського) рівня вищої освіти, Полтавський державний аграрний університет, м. Полтава, <https://orcid.org/0009-0002-1604-6516>

ІННОВАЦІЙНІ ЛОГІСТИЧНІ РІШЕННЯ У ЗМІЦНЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ БІЗНЕСУ В УМОВАХ ВІЙНИ

Анотація. У статті розглянуто трансформацію логістичних систем України в умовах воєнної нестабільності та зростання загроз економічній безпеці. Досліджено, як логістика поступово перетворюється з традиційної функції постачання на стратегічний елемент виживання підприємств у кризових ситуаціях. Адже у мирні часи вона лишалася невидимою основою виробничої системи, однак війна суттєво змінила її роль. Руйнування транспортних коридорів, кібератаки та нестача ресурсів зробили логістику вразливою, але водночас перетворили і на центральну ланку адаптації бізнесу.

Проаналізовано основні фактори дестабілізації логістичних систем серед яких руйнування інфраструктури, порушення ланцюгів постачань, кібератаки на цифрові платформи, обмеження доступу до міжнародних маршрутів. Тому підприємства змушені переглядати управлінські підходи, створювати резерви, диверсифікувати канали постачання й активніше інтегрувати цифрові технології для зменшення ризиків. Особливу увагу приділено концепції Smart Adaptive





Logistics, тобто системі, яка поєднує штучний інтелект, автоматизоване планування, блокчейн і безпілотні технології. Завдяки цим технологіям компанії можуть швидше реагувати на зміни, заздалегідь оцінювати ризики і зберігати постачання навіть тоді, коли умови роботи стають критичними. Розкрито роль безпілотних систем як нового елемента логістичної інфраструктури, який дозволяє здійснювати доставку навіть за умов руйнування традиційних транспортних шляхів.

Також у роботі наведено приклади українських практик, зокрема використання AI-агентів для оптимізації маршрутів, впровадження платформ військово-логістичної взаємодії, що базуються на децентралізованих моделях управління (DAO) та Web3-рішеннях. Такі технології разом із цифровими паспортами вантажів формують нову логіку довіри між державою, бізнесом і партнерами постачання, зменшують вплив людського фактору та підвищують прозорість процесів. Водночас розвиток адаптивних систем кіберзахисту і застосування моделі Zero Trust забезпечують цифрову стійкість та контроль над критичною інформацією.

Зроблено висновок, що сучасна логістика в умовах війни виходить за межі економічного інструменту і та перетворюється на комплексну систему управління ризиками і ресурсами, у якій поєднуються технологічний, організаційний і безпековий виміри. Саме така розумна адаптивна логістика здатна стати основою для відновлення економічної стійкості держави у післявоєнний період.

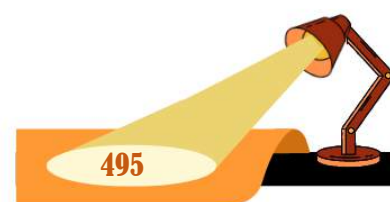
Ключові слова: логістика, адаптивна логістика, економічна безпека, бізнес, штучний інтелект, блокчейн, дрони, кіберстійкість, децентралізоване управління, Smart Adaptive Logistics.

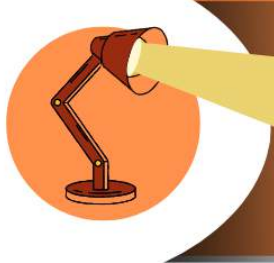
Volkova Nelia Vasylivna PhD in Economics, Associate Professor, Associate Professor of the Department of Entrepreneurship and Law, Poltava State Agrarian University, Poltava, <https://orcid.org/0000-0002-8374-1546>

Svitlychna Alla Vasylivna PhD in Economics, Associate Professor, Professor of the Department of Entrepreneurship and Law, Poltava State Agrarian University, Poltava, <https://orcid.org/0000-0003-3674-5787>

Kyrpota Aliona Hennadiyivna Master's degree student (second level of higher education), Poltava State Agrarian University, Poltava, <https://orcid.org/0009-0008-1176-3691>

Harkusha Anton Serhiyovych Master's degree student (second level of higher education), Poltava State Agrarian University, Poltava, <https://orcid.org/0009-0004-6306-7218>





Myroshnychenko Roman Viktorovych Master's degree student (second level of higher education), Poltava State Agrarian University, Poltava, <https://orcid.org/0009-0002-1604-6516>

INNOVATIVE LOGISTICS SOLUTIONS FOR STRENGTHENING BUSINESS ECONOMIC SECURITY UNDER WAR CONDITIONS

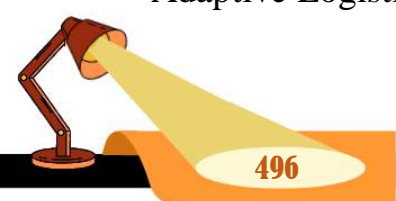
Abstract. The article examines the transformation of Ukraine's logistics systems under conditions of wartime instability and increasing threats to economic security. It explores how logistics is gradually evolving from a traditional supply function into a strategic element of enterprise survival in crisis situations. In peacetime, logistics remained an invisible foundation of the production system; however, the war has significantly changed its role. The destruction of transport corridors, cyberattacks, and resource shortages have made logistics vulnerable, while simultaneously turning it into a central link in business adaptation.

The main destabilizing factors are analyzed, including the destruction of infrastructure, disruption of supply chains, cyberattacks on digital platforms, and restricted access to international routes. As a result, enterprises are forced to reconsider management approaches, create reserves, diversify supply channels, and actively integrate digital technologies to reduce risks. Particular attention is given to the concept of Smart Adaptive Logistics, a system that combines artificial intelligence, automated planning, blockchain, and unmanned technologies. Such solutions enable rapid responses to environmental changes, facilitate risk forecasting, and ensure the continuity of supply even under critical conditions.

The role of unmanned systems is revealed as a new component of the logistics infrastructure capable of compensating for the destruction of ground routes. The study also presents examples of Ukrainian practices, including the use of AI agents for route optimization and the implementation of military-logistics interaction platforms based on decentralized governance models (DAO) and Web3 solutions. These technologies, together with digital cargo passports, establish a new framework of trust between the state, business, and supply partners, reduce human factor influence, and enhance process transparency. Meanwhile, the development of adaptive cybersecurity systems and the application of the Zero Trust model strengthen digital resilience and ensure control over critical information.

It is concluded that modern logistics in wartime conditions transcends its traditional economic function and transforms into a comprehensive system for managing risks and resources, integrating technological, organizational, and security dimensions. Such intelligent adaptive logistics can form the foundation for restoring the country's economic resilience in the post-war period.

Keywords: logistics, adaptive logistics, economic security, biznes, artificial intelligence, blockchain, drones, cyber resilience, decentralized management, Smart Adaptive Logistics.



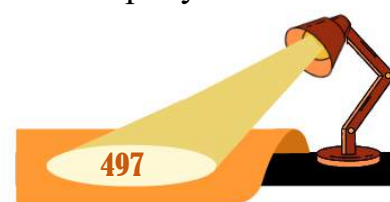


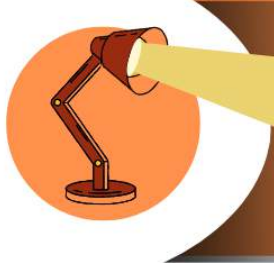
Постановка проблеми. В умовах сучасної економіки безпека бізнесу вже не сприймається як абстрактне поняття. Вона має цілком практичний вимір для кожної компанії, незалежно від її масштабу чи форми власності. Ринкове середовище надзвичайно мінливе: коливання валют, перебої у постачанні, непостійність попиту, – миттєво і відчутно впливають на стабільність підприємства. У такій ситуації визначальним стає не стільки розмір прибутку, скільки здатність підтримувати безперервність операцій, адже будь-яка зупинка може поставити під сумнів саме існування бізнесу. Саме тому логістика поступово виходить за межі традиційного уявлення про транспортування та зберігання. Вона перетворюється на гнучкий інструмент управління ризиками, витратами і часом. Тому технічні рішення, як-то вибір маршруту, організація складів або інтеграція цифрових платформ, на нашу думку, визначають, наскільки підприємство здатне протистояти зовнішнім викликам і зберігати стійкість до потрясінь.

Сучасні інновації в логістиці не обмежуються лише технологіями. Вони змінюють і способи взаємодії між партнерами, і підходи до управління запасами. Як відомо, використання великих даних для прогнозування попиту, швидке переналаштування ланцюгів постачання, гнучкість у прийнятті рішень забезпечують реальні конкурентні переваги. Це допомагає не тільки зменшити витрати, а й знизити ризики. Однак, варто пам'ятати, що будь-яке впровадження інновацій завжди пов'язане з невизначеністю. Якщо підприємство не має чіткої логістичної стратегії, навіть значні інвестиції в автоматизацію чи цифрові системи не забезпечать очікуваного результату. Баланс між технологічним оновленням та ризиком стає ключовим завданням кожного сучасного бізнесу.

Логістика є складною і водночас вразливою системою, у якій навіть невелика зміна одного вузла може вплинути на всю систему. Затримки транспортування, нестача запасів, перебої у постачанні часто призводять до наслідків, що виходять за межі фінансових втрат. Як свідчать сучасні дослідження, інноваційні підходи дозволяють передбачати подібні ситуації та реагувати на них швидше. Аналітичні інструменти, автоматизовані платформи управління запасами і системи моніторингу допомагають прогнозувати ризики, підвищують рівень передбачуваності та зміцнюють економічну безпеку. Завдяки цьому підприємство стає більш стійким і здатним діяти навіть за непередбачуваних обставин [1].

Сьогодні логістика вже не є лише операційним процесом. Вона перетворюється на простір для стратегічних рішень. Нові технології, цифрові платформи та сучасні моделі співпраці змінюють структуру ланцюгів постачання. Такі рішення, як блокчейн, штучний інтелект, інтернет речей та автоматизація складів, дають змогу контролювати процеси у реальному часі, підвищують точність і роблять бізнес гнучкішим. Проте вирішальним усе одно залишається людський фактор. Адже інновації не працюють самостійно, вони потребують





продуманої інтеграції у бізнес-процеси й адаптації організаційних структур. Без цього навіть найсучасніші технології не принесуть очікуваної користі і залишаться лише дорогим інструментом.

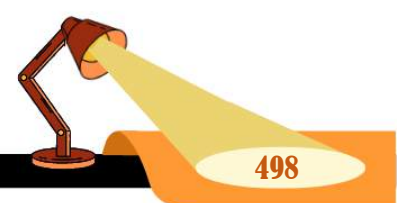
Аналіз останніх досліджень і публікацій. Наукова увага дослідників у сфері логістики та економічної безпеці нині зосереджена на підвищенні адаптивності ланцюгів постачання і цифровій трансформації управлінських процесів в умовах воєнного конфлікту. Так, Волкова Н. та її співавтори у своїй публікації [1] акцентували увагу на ролі інформаційного забезпечення логістичних процесів у мінімізації економічних ризиків під час воєнних дій. Кирилюк І. і Сокур П. [2] досліджували проблеми організації логістики в умовах війни та підкреслили потребу в пошуку альтернативних маршрутів через руйнування транспортної інфраструктури. Дроздова В., Шаповалова О., Лагно Д. [3] підкреслюють, що перебудова логістичних маршрутів потребує залучення додаткових організаційних зусиль і часу, що ускладнює забезпечення стабільності логістичних процесів підприємств. Рейкін В., Романець А. і Рак Б. [4] досліджували адаптацію логістичних систем оборонної промисловості, підкреслюючи стратегічне значення цифрових рішень для забезпечення стійкості постачань. Інші наковці [5] доводять, що цифрові технології дозволяють оптимізувати ланцюги постачання та підвищити ефективність прийняття рішень, зокрема завдяки аналітиці даних та алгоритмам штучного інтелекту.

З недавнього часу почав активно розвиватися напрям використання безпілотних систем і блокчейну. І автори Лещенко Ю., Мороз І. і Юхимчук М. [6] вивчали використання UAV (дронів) у якості засобу для доставки критичних вантажів у зонах зруйнованої інфраструктури. Ліваковський В. і Римар П. [7] зосередили увагу на мобільних дронах-складах як рішення для оперативності. Савченко Л. [8] було запропоновано алгоритми «мурашиної логістики», які допомагають адаптивно розподіляти потоки. На противагу цьому інші дослідники [9, 10] підкреслюють роль блокчейн-технологій і смарт-контрактів у забезпеченні прозорості та зниженні ризику шахрайства. А деякі наковці [11, 12] вбачають перспективу в DAO-моделях, тобто формах децентралізованої взаємодії, що зміцнюють довіру між учасниками логістичних кластерів. Інші автори [13; 14] додають, що цифровізація підсилює економічну безпеку й конкурентні позиції бізнесу навіть під час війни.

Звідси, сучасні дослідження наголошують на комплексності підходу до адаптивної логістики. Цифровізація, автономні рішення, прозорість, безпека, проактивне управління ризиками - усе це формує нову архітектуру стійкості. І дає змогу підприємствам і державі витримувати навіть турбулентні періоди.

Метою даної статті є дослідження впливу інноваційних логістичних рішень і на підвищення економічної безпеки бізнесу та визначення ефективних стратегій їх впровадження.

Виклад основного матеріалу дослідження. Ефективна логістика є однією з ключових складових економічної безпеки підприємств. Зрозуміло, що у



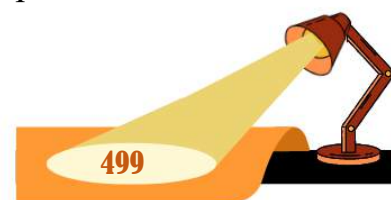


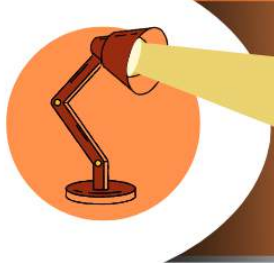
стабільних умовах вона функціонує як невидимий фундамент виробничої системи: забезпечує постачання сировини, координує переміщення матеріалів, мінімізує витрати та підтримує конкурентоспроможність бізнесу. Проте війна радикально змінює логіку цього процесу. Те, що раніше сприймалося як налагоджене й передбачуване, сьогодні стикається з численними перешкодами. Як свідчать події останніх років, руйнування транспортної інфраструктури, перебої у комунікаціях, обмеження доступу до маршрутів і кібератаки перетворюють логістику на зону постійного ризику. Від її ефективності безпосередньо залежить стійкість підприємства до зовнішніх загроз, а отже і його і здатність адаптуватися до постійно змінюваного середовища [1; 19; 21].

Для українських підприємств ці виклики набувають особливої гостроти. Не секрет, що вітчизняний бізнес стикається з постійним зростанням витрат на транспортування, нестачею ресурсів та ризиком зриву поставок. Кожне порушення в ланцюзі постачання породжує хвилю наслідків: від затримки виробництва до втрати ринку збуту. Бізнес більше не може діяти за старими схемами, розрахованими на стабільність. Тому доводиться переосмислювати логістичні стратегії, формувати резерви, диверсифікувати канали постачання. Як наслідок, компанії все активніше впроваджують цифрові інструменти, автоматизують планування маршрутів і шукають способи зробити ланцюги постачання гнучкими [5; 8; 24]. Зважаючи на це, така трансформація не відбувається миттєво, однак саме вона визначає, чи зможе підприємство вистояти в умовах невизначеності. А отже, від цього залежить і здатність держави зберегти економічну стійкість [14].

Одним із найсерйозніших викликів є руйнування транспортної інфраструктури. Пошкоджені дороги, зруйновані мости, заблоковані залізничні вузли – все це створює додаткові логістичні розриви. Як зазначають Кирилюк І. та Сокур П. [2], «збитки логістичної інфраструктури прямо впливають на вартість поставок та змушують підприємства шукати альтернативні маршрути». Однак ці шляхи часто виявляються довгими, дорожчими і менш безпечними. Втрата стабільності транспортування веде до підвищення собівартості продукції, що знижує конкурентоспроможність на внутрішньому та зовнішньому ринках. Крім того, відновлення інфраструктури потребує часу та ресурсів, яких у воєнний період завжди бракує. Тому порушення фізичних ланцюгів постачання безпосередньо загрожує економічній безпеці підприємств і змушує бізнес будувати системи, здатні функціонувати навіть у нестандартних умовах [3; 4; 23].

Не менш небезпечним фактором є кібератаки на цифрові логістичні платформи. Оскільки сучасні підприємства дедалі більше залежать від інформаційних систем, що координують рух товарів, управління складом і фінансові потоки, то це створює спокусю для зловмисників і підвищує вразливість бізнесу. І, як зауважують деякі науковці [1], «інформаційне забезпечення логістичного обслуговування в умовах воєнних дій потребує підвищеної кіберзахисності».



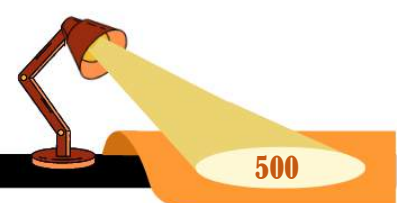


Зокрема, злами таких систем можуть паралізувати процес постачання без фізичного втручання. Втрата даних або блокування доступу до них миттєво дезорганізує роботу підприємства. А отже, кібербезпека стає не технічним, а стратегічним аспектом економічної безпеки. Ігнорування цього фактору вже не просто ризик – це вже потенційна загроза існуванню бізнесу [19; 21; 22].

Ще однією проблемою є втрата доступу до традиційних міжнародних маршрутів. Закриття портів, обмеження авіасполучення, ускладнення перетину кордонів знижують ефективність зовнішньоекономічної діяльності. Підприємства змушені шукати нові, часто непрямі шляхи доставки. Однак ми погоджуємося із думкою Дроздова В.А., Шаповалова О.В. і Лагно Д.В. [3] про те, що «адаптація до нових логістичних маршрутів потребує додаткових ресурсів і часу». І у деяких випадках зміна маршруту означає перебудову всього процесу: починаючи від закупівлі й до збуту. Особливо болісно це для експортерів, де навіть коротка затримка призводить до втрати контрактів. У таких умовах виникає новий вид ризику, пов'язаний зі стратегічною нестабільністю логістики [13; 14]. І бізнес має навчитися діяти в умовах, де постійна зміна стає нормою.

Окремим аспектом постає нестабільність постачання як системне явище. Не секрет, що кожна перерва у ланцюгу викликає каскадний ефект, що може паралізувати виробництво. Як наголошено у науковій роботі [13]: «нестабільність постачання прямо впливає на конкурентоспроможність і якість продукції аграрних підприємств». Це справедливо і для багатьох інших галузей, зокрема промисловості та харчової сфери. У таких умовах підприємства просто змушені створювати резерви, перерозподіляти ресурси і автоматизувати планування. Гнучкість при цьому стає ключовою перевагою, а здатність швидко реагувати визначає рівень ефективності [5; 8]. Логістика більше не є допоміжною функцією бізнесу, перетворюється на його нервову систему, що визначає життєздатність економіки під час війни [14].

На цьому тлі формується концепція «розумної адаптивної логістики» (Smart Adaptive Logistics) (рис. 1). Вона виникає як відповідь на потребу працювати у середовищі, де стабільності немає і не буде найближчим часом. Її суть полягає у використанні систем штучного інтелекту, здатних у реальному часі аналізувати ризики, прогнозувати ситуації та пропонувати альтернативні маршрути. Такі алгоритми дозволяють скоротити час реакції на зміни та мінімізувати втрати від затримок [1]. Яскравим прикладом є український freight-tech Cargoфу, який впроваджує AI-агентів для автоматичного пошуку вантажів, підбору водіїв і динамічного маршруту в реальному часі [15]. Саме такі рішення демонструють, як технології можуть забезпечити безперервність логістики навіть у зонах підвищених ризиків [16; 20]. Іншими словами, «розумна адаптивна логістика» – це вже не просто ідея, а практична відповідь на виклики воєнної економіки.



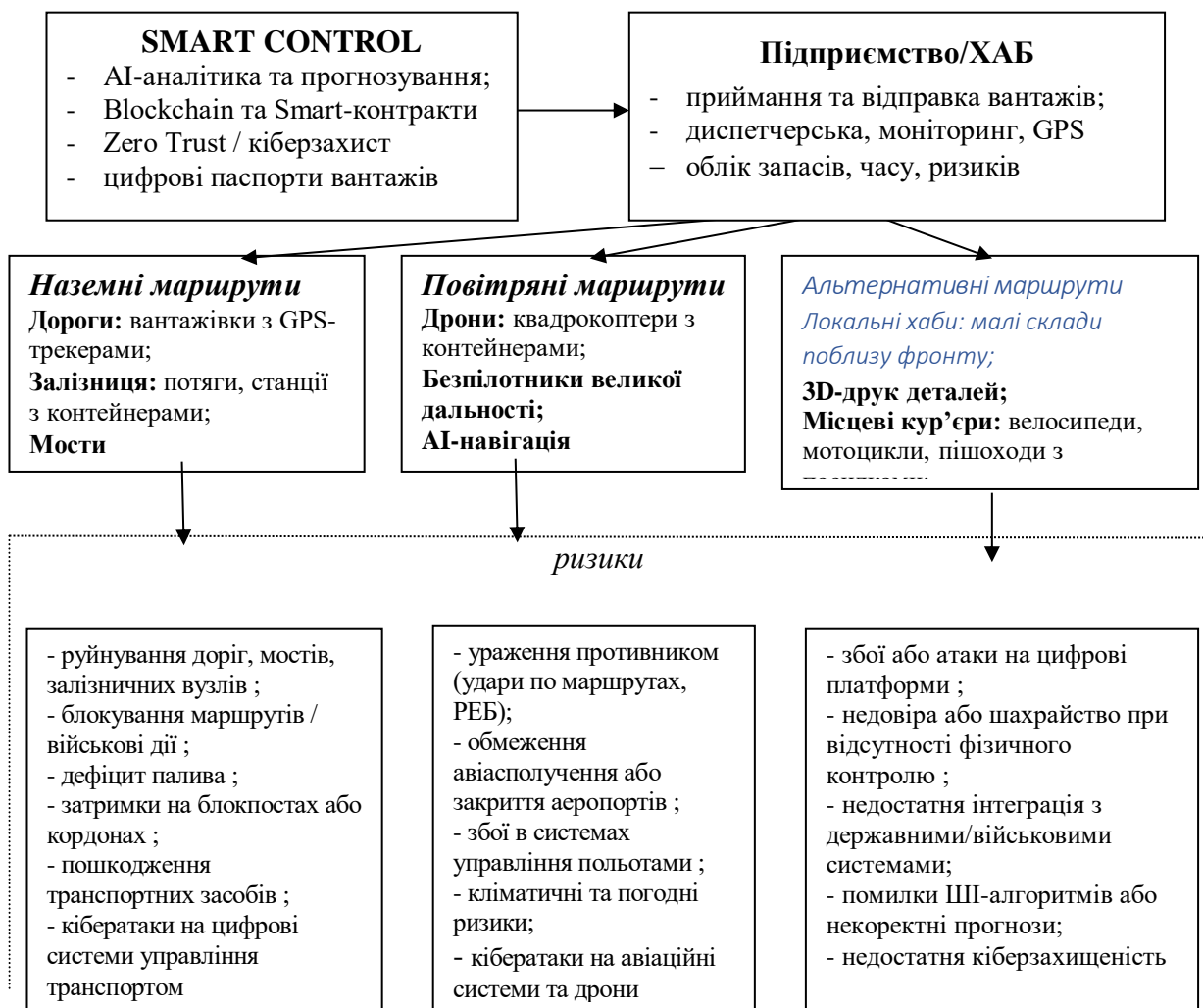
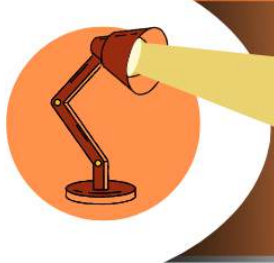


Рис. 1. Smart Adaptive Logistics в умовах війни [розроблено на основі 1, 15, 16]

Інтеграція таких систем з державними та військовими платформами моніторингу забезпечує ефективну взаємодію між учасниками логістичних процесів. Підприємства отримують можливість уникати небезпечних зон, координувати маршрути між собою, планувати постачання у складних умовах. І як зазначають Рейкін В. С., Романець, А. О. і Рак Б. І. технології на базі штучного інтелекту дозволяють прогнозувати потенційні ризики ще до того, як вони реалізуються [4]. Це створює простір для превентивних дій: формування резервів, корекції маршрутів, оптимізації графіків. І, як результат, логістика перестає бути реактивною системою, яка просто долає проблеми. Вона стає активним інструментом управління ризиками [17; 18; 19]. І, можливо, саме така логістика стане фундаментом післявоєнної відбудови України [24].

Зауважимо, що концепція Smart Adaptive Logistics не зводиться лише до технологічного виміру. На нашу думку, вона охоплює саму суть управлінських процесів, зокрема: організацію, дисципліну, координацію та прийняття рішень у

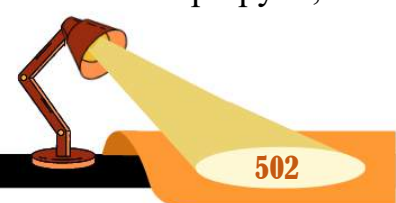


реальному часі. Оскільки безперервність постачань залежить від структури складських систем і швидкості обміну даними між підрозділами, підприємствам доводиться переосмислювати внутрішні процедури. Без надійної інформаційної інфраструктури жодні дрони чи аналітичні системи не здатні забезпечити стійкість ланцюгів постачання. Інтеграція технологій із управлінськими процедурами формує «живу» структуру, здатну реагувати на зміни середовища. Це вже не класична логістика, а адаптивна система прийняття рішень, котра працює з фізичними, економічними та інфраструктурними ризиками [19; 20]. Коли штучний інтелект починає відстежувати ціни на паливо, стан транспортних шляхів або соціальні коливання попиту, він фактично стає частиною стратегічного управління постачаннями. Зважаючи на це, у воєнний час логістика перестає бути лише інструментом підвищення ефективності й набуває критичного значення для збереження діяльності бізнесу [14; 17].

Зараз в Україні формується ще одна гілка цієї адаптивної системи, яка пов'язана з логістикою безпілотних систем. Після 2022 року сектор дронів зріс вибухово. Компанії Ukrspecsystems, TAF Drones, 3DTech та інші створили модульні платформи для бойових, розвідувальних і транспортних завдань. Вони відпрацювали виробничі рішення, що дозволяють оперативно масштабувати випуск, завдяки стандартизації компонентів і застосуванню вітчизняних технологій. Зокрема нові моделі стійкі до впливу РЕБ, використовують fiber-optic (волоконно оптичний) зв'язок, а елементи штучного інтелекту дозволяють керувати групами дронів у майже автономному режимі. Такі рішення вже виходять за межі чисто бойового призначення і перетворюють безпілотники на мобільну логістику для доставки критичних ресурсів та створення автономних польових складів [5; 16]. А отже інтеграція подібних технологій у цивільні логістичні ланцюги може значно підвищити швидкість реагування і надійність постачань.

Використання автономних літальних роботів дозволяє доставляти критично важливі вантажі у зони, куди не дістатися колоною. Це не гіпотетична перспектива, а щоденна практика. Медичні комплекти, продовольство, батареї та деталі до техніки доставляються швидко і безпечно. Погоджуємося і твердженням, що дрони скорочують час доставки і мінімізують людські втрати [5]. Новий тип мобільності проявляється через децентралізацію та гнучкість. У разі якщо одна точка втрачена, маршрут перебудовується миттєво. Логістика аероботів стає окремою стратегічною інфраструктурою, де сила системи проявляється у здатності адаптуватися. Групи безпілотників, що діють як рій, вже тестуються для транспортування невеликих партій одночасно у кілька напрямків [6; 7].

Як зазначено у дослідженні [6] координована робота груп безпілотних літальних апаратів підвищує ефективність постачання у складних умовах, де швидкість і надійність критично важливі. К зв'язку із цим з'являються нові маршрути, які не залежать від доріг або мостів. Повітряна логістика перестає





бути другорядною і стає головною там, де наземні транспортні коридори постійно під обстрілом. Деякі розробки йдуть ще далі: з'являються енергоефективні безпілотні склади, що можуть утримувати вантаж у повітрі, створюючи буфер часу. Ліваковський В.К. та Римар П.В. [7] наголошують, що мобільні безпілотні склади відкривають новий рівень управління запасами і забезпечують швидке перенаправлення вантажів залежно від обстановки. Це експериментальні рішення з великим потенціалом, адже зменшують залежність від пошкоджених логістичних центрів і підтримують безперервність постачання.

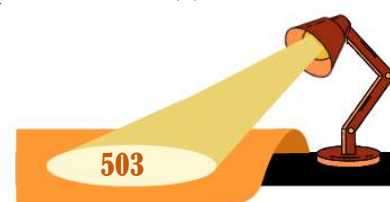
Проте будь-яка технологія має тіньову сторону. Противник активно використовує дрони не лише для розвідки, а й для ударів по логістичних маршрутах. Прикладами слугують бої у районі Покровська, де безпілотники паралізували постачання [20]. Це змушує розробників і логістів думати не тільки про ефективність, а й про захищеність маршрутів. Логістика із вбудованими елементами кібер- та РЕБ-захисту стає нормою. Системи маскування, фальшиві сигнали та маршрути-заміни стають частиною логістичного мислення. Адаптивна логістика майбутнього – це симбіоз штучного інтелекту, кіберзахисту, виробництва і стратегії.

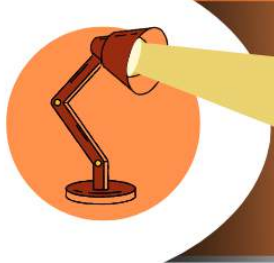
Цифрові технології у вигляді літальних роботів підтримують безперервність постачання і формують нову логістичну культуру [5]. Гнучкість важливіша за масштаби, а швидкість реакції – за звичну стабільність. Українські виробники безпілотних систем довели, що інновації можуть виникати не з комфортних лабораторій, іноді вони народжуються у хаосі війни. Smart Adaptive Logistics стає реальним інструментом виживання для держави та бізнесу.

У сучасних умовах воєнної нестабільності логістика перестає бути лише питанням транспорту. Вона стала питанням довіри. Бізнес і держава шукають способи зробити ланцюги постачання не лише гнучкими, а й перевіреними у кожній дії та в кожній транзакції. Блокчейн і Web3 відкрили двері до нової моделі контролю, прозорості та водночас стійкої. Смарт-контракти автоматизують перерозподіл ресурсів у критичні моменти [9; 11]. І, як зауважує Благун І., автоматизація через смарт-контракти скорочує вплив людського фактору та пришвидшує реакцію системи в кризових умовах [9].

Цифрові паспорти вантажів додають порядку там, де фізичний контроль неможливий. Кожен контейнер або партія отримує власний цифровий слід, унікальний, непідробний і зафіксований у блокчейні назавжди. Оскільки непідробні цифрові ідентифікатори формують механізм довіри там, де вона зруйнована обставинами [10]. Такий підхід мінімізує шахрайство, підміну або втручання у маршрут, адже вантажі рухаються не лише фізично, а й із цифровим доказом існування.

Також варто згадати що один окремий напрям – DAO-моделі для управління логістичними кластерами. На думку авторів, це не модний тренд, а логічна еволюція децентралізованого управління. DAO дозволяє підприємствам діяти





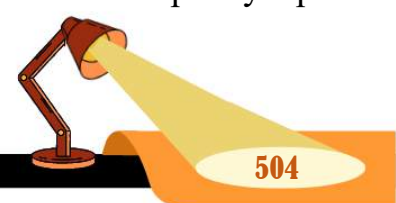
спільно без жорсткої ієрархії, але з високим рівнем координації. Учасники одночасно приймають рішення і несуть колективну відповідальність. Так Ткач Л. [11] підкреслює, що децентралізоване управління підвищує стійкість до зовнішніх шоків і зменшує ризики надмірної централізації. Так виникають логістичні мережі нового типу, де швидкість реакції перевищує бюрократичні обмеження.

В Україні вже є практичні приклади таких підходів. Платформа DOT-Chain Defence, спільний проєкт Міністерства оборони та команди DOT, дозволяє здійснювати швидкі закупівлі військових товарів: від FPV-дронів до засобів РЕБ. Система скорочує бюрократію, автоматизує перевірку походження товарів і прискорює поставки. Кповноважені особи Міністерства оборони України [17] зазначають, що платформа фактично імітує функції блокчейну, забезпечуючи доказ походження та прозорість транзакцій. Це державна версія Web3, адаптована до реалій війни. Вона показує, що цифрова довіра може існувати не лише в бізнесі, а й у військових процесах. Саме через такі приклади виникає нова модель постачання, де швидкість не суперечить відповідальності.

Інтеграція блокчейну з системами моніторингу створює ефект прозорої логістики. Кожен етап постачання може відображатися у режимі реального часу. Не зважаючи на те, що це виглядає як просте спостереження, насправді мова йде про спосіб ухвалення рішень на підставі точних даних. Досвід провідних міжнародних компаній демонструє ефективність blockchain у умовах невизначеності [12]. В українських реаліях прозорість набуває особливого значення. Вона є умовою виживання, бо будь-яка затримка чи помилка може мати не економічні, а людські наслідки.

Тому разом із зростанням цифрових потоків постає новий фронт – кіберзагрози. Логістичні платформи накопичують надто багато чутливої інформації, включно з маршрутами, запасами та даними про контрагентів. Один збій здатний паралізувати всю мережу. Звідси впровадження концепції Zero Trust перестало бути опцією. Це не просто рекомендація, а необхідність, вимога сучасності. Модель базується на простому принципі, що нікому не можна довіряти за замовчуванням, а кожен доступ перевіряється повторно. І як відзначається дослідниками [5], Zero Trust зменшує ризики маніпуляцій і витоків даних у цифровій логістиці, особливо під час військових або стратегічних постачань. Іншими словами, цей підхід змінює традиційне, класичне уявлення про безпеку, перетворюючи контроль у постійний і системний процес, доповнюючи інші механізми захисту.

Українські IT-компанії активно реалізують підходи кібербезпеки у логістиці. Модель Zero Trust [18] застосовується для постійного контролю доступу, що мінімізує ризики витоків та маніпуляцій із даними. Крім того, автоматизоване навчання та AI-моделі для безпечного управління ланцюгами постачання [19] дозволяють виявляти аномалії та потенційні загрози ще до прояву проблем. Завдяки цьому організації переходять від реактивних дій до





проактивного прогнозування загроз. І такі рішення особливо важливі для критично значущих ланцюгів, де будь-який збій може впливати на безперервність постачань.

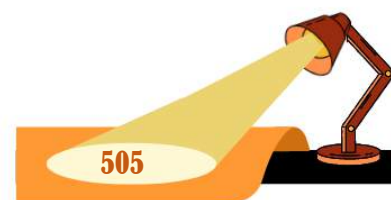
Штучний інтелект, що працює на цих системах, додає ще один рівень безпеки. Він не лише фіксує аномалії, а й навчається їх передбачати. Алгоритми можуть виявити зміну маршруту, яка на перший погляд здається незначною, але фактично сигналізує про потенційне втручання. Як свідчать дані Міністерства фінансів України [21], інтелектуальні алгоритми дозволяють локалізувати загрози до їхнього прояву. Це вже не контроль, а проактивна оборона даних. Такий підхід важливий не менше, ніж фізичний захист складів або техніки.

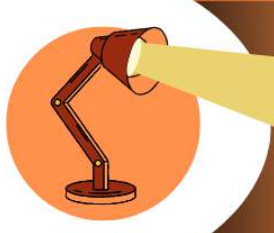
Паралельно формується концепція кібер-безпечних коридорів. Це реальні канали зв'язку, створені спеціально для передачі критично важливих логістичних даних. Вони шифруються, проходять кілька рівнів автентифікації і залишають цифровий слід кожного обміну. Зважаючи на умови війни, їхня роль стає особливо помітною під час транспортування стратегічних або гуманітарних вантажів. Коли інші канали виходять з ладу, ці коридори дозволяють зберегти безперервність інформаційного потоку [22].

Стійкі логістичні рішення для економічної безпеки стають ключовим чинником виживання бізнесу в умовах тривалої воєнної нестабільності. Порушення маршрутів, дефіцит палива, затримки на кордонах змушують підприємства шукати автономні моделі. Одним із таких напрямів є розвиток мікрологістики, що спирається на локальні ресурси. Малий масштаб стає перевагою, коли великі системи не витримують. Виробництво деталей на 3D-принтерах і невеликі склади зменшують залежність від зовнішніх постачальників. Як зазначають наковці, що оперативне виготовлення запасних частин і швидка дистрибуція створюють стабільність навіть у кризових умовах [13].

Одночасно розвивається напрям альтернативного транспорту, що знижує ризики, пов'язані з нестачею традиційних енергоресурсів. Електровантажівки, водневі системи, локальні джерела енергії забезпечують більшу автономність логістичних процесів. Використання енергетично незалежного транспорту – безперервність постачань навіть за обмеженого доступу до нафтопродуктів [5]. Зростає і значення енергетичної автономності складів та логістичних центрів, адже енергетична самодостатність є передумовою стабільності бізнесу [14].

Яскравим прикладом практичного застосування принципів стійкої логістики стала діяльність компанії Nova Poshta. Її широка мережа відділень і автоматизованих хабів продемонструвала здатність працювати навіть у прифронтових регіонах. Як бачимо, досвід компанії став показовим для гнучкості й технологічної зрілості в умовах воєнного часу [23]. З іншого боку, цифровізація логістики переходить у фазу глибшого аналізу та прогнозування. Моделі цифрових двійників транспортних коридорів дозволяють виявити слабкі місця ще до фактичних збоїв [24].





Симуляції воєнної економіки допомагають підприємствам підготуватися до непередбачуваних сценаріїв, адже моделювання кризових ситуацій сприяє виробленню стійких управлінських рішень [14]. Загальна тенденція рухається у напрямі розподілених логістичних мереж, де великі склади поступаються місцем дрібним, але мобільним вузлам. А отже, деконцентрація потоків підвищує здатність бізнесу до саморегуляції [13]. У поєднанні з цифровими двійниками й аналітичними платформами це формує новий тип логістики, який не боїться змін оточуючого середовища.

Висновки. Отже, сучасна логістика перестала бути лише допоміжною функцією бізнесу і поступово перетворилася на ключовий елемент економічної безпеки підприємств. Інноваційні технології, такі як штучний інтелект, безпілотні системи, блокчейн і цифрові платформи, допомагають і компаніям адаптуватися до нестабільного середовища, зменшувати ризики та підтримувати безперервність постачань навіть в умовах зовнішніх загроз. Як свідчать сучасні тенденції, впровадження таких рішень створює новий тип логістики, у якому швидкість реагування, автономність і здатність передбачати проблеми стають стратегічними конкурентними перевагами. Зважаючи на це, поєднання технологій із управлінськими й організаційними процесами створює гнучку і стійку систему, здатну протистояти фізичним, економічним та кіберзагрозамі. В результаті бізнес отримує не лише інструменти ефективного управління ресурсами, а й міцну основу для довгострокової стабільності, а держава, в свою чергу, додаткові механізми підтримки економічної стійкості у кризових умовах. Тому сучасна інноваційна логістика перетворюється із технічного засобу доставки на стратегічний фактор виживання і розвитку економіки.

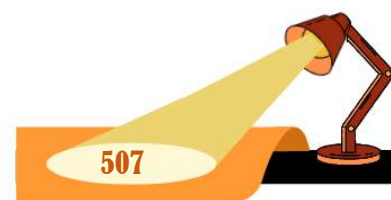
Література:

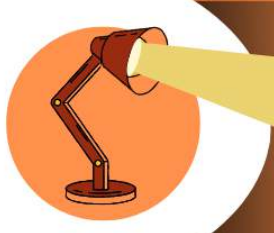
1. Волкова Н. В., Світлична А., Іващенко О., Супрун В. Інформаційне забезпечення процесу логістичного обслуговування торговельних підприємств в умовах воєнних дій. *Успіхи і досягнення у науці. Серія «Соціальні та поведінкові науки»*. 2024. № 9(9). С. 1028–1040. URL: <http://perspectives.pp.ua/index.php/sas/article/view/16872> (дата звернення: 27.09.2025).
2. Кирилюк І., Сокур П. Організація логістичних процесів підприємства в умовах війни: проблеми та рішення. *Економіка та суспільство*. Вип. 61. 2024. DOI: <https://doi.org/10.32782/2524-0072/2024-61-54> (дата звернення: 27.09.2025).
3. Дроздова В. А., Шаповалова О. В., Лагно Д. В. Виклики логістичної діяльності виробничих підприємств в умовах воєнного стану: кадрові, адміністративні та операційні аспекти. *Економічний простір*. № 196. 2024. С. 3–9. DOI: <https://doi.org/10.30838/EP.196.3-9> (дата звернення: 30.09.2025).
4. Рейкін В. С., Романець А. О., Рак Б. І. Адаптація логістичних систем до умов війни на прикладі оборонної промисловості України. *Актуальні питання економічних наук*. 2025. № 10. DOI: <https://doi.org/10.5281/zenodo.15196373> (дата звернення: 01.10.2025).
5. Михаць А. Р., Михаць С. Р., Гринів Н. Т., Гринів Т. Т. Цифрові технології як інструмент оптимізації ланцюга поставок: впровадження та перспективи. *Актуальні проблеми сталого розвитку*. 2025. Т. 2, № 1. С. 22–30. DOI: [https://doi.org/10.60022/2\(1\)-3S](https://doi.org/10.60022/2(1)-3S) (дата звернення: 30.09.2025).





6. Лещенко Ю., Мороз І., Юхимчук М. Використання UAV (дронів) для оптимізації доставки останньої милі. *Measuring and Computing Devices in Technological Processes*. 2024. № 4. С. 425–432. DOI: <https://doi.org/10.31891/2219-9365-2024-80-53> (дата звернення: 30.09.2025).
7. Лівачковський В. К., Римар П. В. Роль дронів у технологічних процесах для логістики. *Прикладні аспекти сучасних міждисциплінарних досліджень*. 2024. С. 186–187. URL: <https://jpasmd.donnu.edu.ua/article/view/16752> (дата звернення: 02.10.2025).
8. Савченко Л. А. Дигіталізація в логістиці за рахунок введення алгоритму мурашиної логістики. *Machinery & Energetics. Journal of Rural Production Research*. Київ, 2019. Т. 10, № 3. С. 119–125.
9. Благун І. Дослідження факторів впливу на впровадження технологій блокчейн в логістичному секторі. *Економіка та суспільство*. 2024. № 70. DOI: <https://doi.org/10.32782/2524-0072/2024-70-135> (дата звернення: 02.10.2025).
10. Юрченко О. А., Савченко Р. В. Роль і місце блокчейн-технологій для ведення бухгалтерського обліку та складання фінансової звітності. *Економічний простір*. № 198. 2025. С. 269–274. URL: <https://economic-prostir.com.ua/wp-content/uploads/2025/03/198-269-274-yurchenko.pdf> (дата звернення: 05.10.2025).
11. Ткач Л. Стан впровадження блокчейн технології в економіку України, враховуючи виклики сьогодення. *Економіка та суспільство*. 2024. № 69. DOI: <https://doi.org/10.32782/2524-0072/2024-69-79> (дата звернення: 03.10.2025).
12. Шльончак І. А., Солтус А. П., Рудь М. П. Аналіз можливостей застосування технології блокчейн у сфері управління ланцюгами постачань. *Центральноукраїнський науковий вісник. Технічні науки*. Кропивницький: ЦНТУ, 2023. Вип. 7(38), ч. 2. С. 231–236.
13. Волкова Н., Мехтієв Р., Попадін Є. Ключові аспекти конкурентоспроможності та якості продукції аграрних підприємств в умовах воєнної агресії. *Економіка та суспільство*. 2023. № 54. DOI: <https://doi.org/10.32782/2524-0072/2023-54-10> (дата звернення: 27.09.2025).
14. Волкова Н. В., Кононенко О. І., Кравченко Т. В. Сутність та особливості формування конкурентоспроможності та економічної безпеки сільськогосподарських підприємств. *Інфраструктура ринку*. 2022. № 68. С. 89–94. URL: <http://www.market-infr.od.ua/uk/68-2022> (дата звернення: 27.09.2025).
15. Сайт LIGA Tech+1. Як штучний інтелект допомагає скорочувати витрати на перевезення: реальні кейси. URL: <https://blog.liga.net/user/sguzenko/article/51274> (дата звернення: 04.10.2025).
16. Сайт Financial Times. Сайт Patriot-nrg. Дрони як новітній засіб отримання інформації та перевезення вантажу. URL: <https://patriot-nrg.com/uk/povitriana-logistyka> (дата звернення: 02.10.2025).
17. Сайт Міністерства оборони України. Міноборони масштабує маркетплейс DOT-Chain Defence: у жовтні доступ отримають 130 бригад. 2024. URL: <https://mod.gov.ua/news/minoboroni-masshtabuye-marketplejs-dot-chain-defence-u-zhovtni-dostup-otrimayut-130-brigad> (дата звернення: 04.10.2025).
18. Сайт SoftServe (Itspecialist). Zero Trust: Модель кібербезпеки, яка не вірить нікому - і саме тому рятує бізнес. URL: <https://itspecialist.com.ua/articles/zero-trust-model> (дата звернення: 07.10.2025).
19. Wang H., Sua L. S., Alidaee B. Enhancing supply chain security with automated machine learning. arXiv preprint. arXiv:2406.13166. 2024. 36 p. DOI: <https://doi.org/10.48550/arXiv.2406.13166> (дата звернення: 02.10.2025).
20. Маркулич П. На Покровському напрямку російські дрони мають змогу бити по логістиці ЗСУ в тилу. Вільне радіо. 2025. URL: <https://freeradio.com.ua/na-pokrovskomu-napriamku-rosiiski-drony-maiut-zmohu-byty-po-lohistytsi-zsu-v-tylu-ofitser-59-i-bryhady/> (дата звернення: 01.10.2025).





21. Сайт Міністерства фінансів України. Кібербезпека бізнесу під час війни. URL: <https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny> (дата звернення: 03.10.2025).
22. Сайт Громадське радіо. Кібер-безпечні коридори для логістики. Сайт компанії Trade Master Group. У 2025 році почнуть діяти нові регламенти кібербезпеки у логістиці. URL: <https://trademaster.ua/news/35614> (дата звернення: 05.10.2025).
23. Сайт NV. Завтра буде. Як працюють прифронтові відділення Нової пошти. URL: <https://nv.ua/ukr/ukraine/events/zavtra-bude-yak-pracyuyut-prifrontovi-viddilennya-novoji-poshti-fotoreportazh-50530842.html> (дата звернення: 02.10.2025).
24. Інтернет-портал PaySpace Magazine. Цифрові двійники: що це за технологія і як вона допоможе відновити Україну - аналітика. URL: <https://psm7.com/uk/technology/cifrovye-dvojniki-chto-eto-za-technologie-i-kak-ona-pomozhet-vosstanovit-ukrainu-analitika.html> (дата звернення: 06.10.2025).

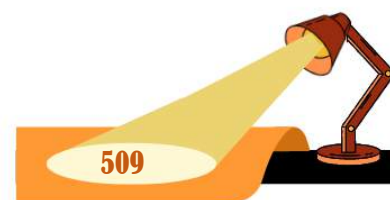
References:

1. Volkova, N.V., Svitlychna, A., Ivashchenko, O., Suprun, V. (2024) Informatsiine zabezpechennia protsesu lohistychnoho obsluhovuvannia torhovelnykh pidpryiemstv v umovakh voyennykh dii [Information Support of the Logistics Service Process of Trade Enterprises under Martial Conditions]. *Uspikhy i dosiahnennia u nauksi*. Series "Sotsialni ta povedinkovi nauky", No. 9(9), pp. 1028–1040. Available at: <http://perspectives.pp.ua/index.php/sas/article/view/16872> (Accessed: 07 Oct. 2025). [in Ukrainian]
2. Kyryliuk, I., Sokur, P. (2024) Orhanizatsiia lohistychnykh protsesiv pidpryiemstva v umovakh viiny: problemy ta rishennia [Organization of Enterprise Logistics Processes under War Conditions: Problems and Solutions]. *Ekonomika ta suspilstvo*, Issue 61. DOI: <https://doi.org/10.32782/2524-0072/2024-61-54> (Accessed: 07 Oct. 2025). [in Ukrainian]
3. Drozdova, V.A., Shapovalova, O.V., Lahno, D.V. (2024) Vyklyky lohistychnoi diialnosti vyrobnychykh pidpryiemstv v umovakh voyennoho stanu: kadrovi, administratyvni ta operatsiini aspekty [Challenges of Logistics Activities of Manufacturing Enterprises under Martial Law: Personnel, Administrative and Operational Aspects]. *Ekonomichnyi prostir*, No. 196, pp. 3–9. DOI: <https://doi.org/10.30838/EP.196.3-9> (Accessed: 07 Oct. 2025). [in Ukrainian]
4. Reykin, V.S., Romanets, A.O., Rak, B.I. (2025) Adaptatsiia lohistychnykh system do umov viiny na prykladi oboronnoi promyslovosti Ukrainy [Adaptation of Logistic Systems to War Conditions: Case of Ukraine's Defense Industry]. *Aktualni pytannia ekonomichnykh nauk*, No. 10. DOI: <https://doi.org/10.5281/zenodo.15196373> (Accessed: 07 Oct. 2025). [in Ukrainian]
5. Mykhats, A.R., Mykhats, S.R., Hryniv, N.T., Hryniv, T.T. (2025) Tsifrovi tekhnolohii yak instrument optymizatsii lantsiuha postavok: vprovadzhennia ta perspektyvy [Digital Technologies as a Tool for Supply Chain Optimization: Implementation and Prospects]. *Актуальні проблеми сталого розвитку*, Vol. 2, No. 1, pp. 22–30. DOI: [https://doi.org/10.60022/2\(1\)-3S](https://doi.org/10.60022/2(1)-3S) (Accessed: 07 Oct. 2025). [in Ukrainian]
6. Leshchenko, Y., Moroz, I., Yukhymchuk, M. (2024) Vykorystannia UAV (droniv) dlia optymizatsii dostavky ostannoï myli [Using UAVs (Drones) for Last-Mile Delivery Optimization]. *Measuring and Computing Devices in Technological Processes*, No. 4, pp. 425–432. DOI: <https://doi.org/10.31891/2219-9365-2024-80-53> (Accessed: 07 Oct. 2025). [in Ukrainian]
7. Livakovskiy, V.K., Rymar, P.V. (2024) Rol droniv u tekhnolohichnykh protsesakh dlia lohistyky [The Role of Drones in Technological Processes for Logistics]. *Prykladni aspekty suchasnykh mizhdysyplinarnykh doslidzhen*, pp. 186–187. Available at: <https://jpasmd.donnu.edu.ua/article/view/16752> (Accessed: 07 Oct. 2025). [in Ukrainian]
8. Savchenko, L.A. (2019) Dyhitalizatsiia v lohistytsi za rakhunok vvedennia alhorytmu murashynoi lohistyky [Digitalization in Logistics through the Implementation of Ant Logistics Algorithm]. *Machinery & Energetics. Journal of Rural Production Research*, Vol. 10, No. 3, pp. 119–125.





9. Blahun, I. (2024) Doslidzhennia faktoriv vplyvu na vprovadzhennia tekhnolohii blokchein v lohistrychnomu sektori [Study of Factors Affecting the Implementation of Blockchain Technologies in the Logistics Sector]. *Ekonomika ta suspilstvo*, No. 70. DOI: <https://doi.org/10.32782/2524-0072/2024-70-135> (Accessed: 07 Oct. 2025). [in Ukrainian]
10. Yurchenko, O.A., Savchenko, R.V. (2025) Rol i mistse blokchein-tekhnolohii dlia vedennia bukhhalterskoho obliku ta skladannia finansovoi zvitnosti [The Role and Place of Blockchain Technologies in Accounting and Financial Reporting]. *Ekonomichnyi prostir*, No. 198, pp. 269–274. Available at: <https://economic-prostir.com.ua/wp-content/uploads/2025/03/198-269-274-yurchenko.pdf> (Accessed: 07 Oct. 2025). [in Ukrainian]
11. Tkach, L. (2024) Stan vprovadzhennia blokchein tekhnolohii v ekonomiku Ukrainy, vrakhuvaiuchy vyklyky siohodennia [The State of Blockchain Implementation in Ukraine's Economy, Considering Current Challenges]. *Ekonomika ta suspilstvo*, No. 69. DOI: <https://doi.org/10.32782/2524-0072/2024-69-79> (Accessed: 07 Oct. 2025). [in Ukrainian]
12. Shlonchak, I.A., Soltus, A.P., Rud, M.P. (2023) Analiz mozhlyvostei zastosuvannia tekhnolohii blokchein u sferi upravlinnia lantsiamy postachan [Analysis of Blockchain Technology Application in Supply Chain Management]. *Tsentrlnoukraiynskiyi naukovyi visnyk. Tekhnichni nauky*, Vol. 7(38), Part 2, pp. 231–236.
13. Volkova, N., Mekhtiev, R., Popadin, Ye. (2023) Kliuchovi aspekty konkurentospro-mozhnosti ta yakosti produktsii ahrarnykh pidpryiemstv v umovakh voyennoi ahresii [Key Aspects of Competitiveness and Product Quality of Agricultural Enterprises under Martial Aggression]. *Ekonomika ta suspilstvo*, No. 54. DOI: <https://doi.org/10.32782/2524-0072/2023-54-10> (Accessed: 07 Oct. 2025). [in Ukrainian]
14. Volkova, N.V., Kononenko, O.I., Kravchenko, T.V. (2022) Sutnist ta osoblyvosti formuvannia konkurentospro-mozhnosti ta ekonomichnoi bezpeky silskohospodarskykh pidpryiemstv [Essence and Features of Formation of Competitiveness and Economic Security of Agricultural Enterprises]. *Infrastruktura rynku*, No. 68, pp. 89–94. Available at: <http://www.market-infr.od.ua/uk/68-2022> (Accessed: 07 Oct. 2025). [in Ukrainian]
15. LIGA Tech+ (2025) Yak shtuchnyi intelekt dopomahaye skorchuvaty vytraty na perevezennia: realni keysy [How AI Helps Reduce Transport Costs: Real Cases]. Available at: <https://blog.liga.net/user/sguzenko/article/51274> (Accessed: 07 Oct. 2025). [in Ukrainian]
16. Financial Times. Patriot-nrg (2025) Drony yak novitnii zasib otrymannia informatsii ta perevezennia vantrazu [Drones as a New Tool for Data Collection and Cargo Delivery]. Available at: <https://patriot-nrg.com/uk/povitriana-logistyka> (Accessed: 07 Oct. 2025). [in Ukrainian]
17. Ministerstvo oborony Ukrainy (2024) Minoborony masshtabuie marketplace DOT-Chain Defence: u zhovtni dostup otrimayut 130 bryhad [The Ministry of Defense Scales DOT-Chain Defence Marketplace: 130 Brigades to Get Access in October]. Available at: <https://mod.gov.ua/news/minoboroni-masshtabuie-marketplejs-dot-chain-defence-u-zhovtni-dostup-otrimayut-130-brigad> (Accessed: 07 Oct. 2025). [in Ukrainian]
18. SoftServe (Itspecialist) (2025) Zero Trust: Model kiberbezpeky, iaka ne viryt nikomu - i same tomu riatuie biznes [Zero Trust: Cybersecurity Model That Trusts No One - and Saves Business]. Available at: <https://itspecialist.com.ua/articles/zero-trust-model> (Accessed: 07 Oct. 2025). [in Ukrainian]
19. Wang, H., Sua, L.S., Alidaee, B. (2024) Enhancing supply chain security with automated machine learning. arXiv preprint. arXiv:2406.13166, 36 pp. DOI: <https://doi.org/10.48550/arXiv.2406.13166> (Accessed: 07 Oct. 2025).
20. Markulych, P. (2025) Na Pokrovskomu napriamku rosiiski drony maiut zmohu byty po lohistrytsi ZSU v tylu [Russian Drones Can Strike Ukrainian Logistics in the Rear on the Pokrovsk Direction]. *Vilne radio*. Available at: <https://freeradio.com.ua/na-pokrovskomu-napriamku-rosiiski-drony-maiut-zmohu-byty-po-lohistrytsi-zsu-v-tylu-ofitser-59-i-bryhady/> (Accessed: 07 Oct. 2025). [in Ukrainian]





21. Ministerstvo finansiv Ukrainy (2025) Kiberbezpeka biznesu pid chas viiny [Business Cybersecurity during War]. Available at: <https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny> (Accessed: 07 Oct. 2025). [in Ukrainian]

22. Hromadske radio / Trade Master Group (2025) Kiber-bezpechni koridory dlia lohistyky: u 2025 rotsi pochnut diiaty novi rehlementy kiberbezpeky u lohistytsi [Cyber-Safe Corridors for Logistics: New Cybersecurity Regulations to Take Effect in 2025]. Available at: <https://trademaster.ua/news/35614> (Accessed: 07 Oct. 2025). [in Ukrainian]

23. NV (2025) Zavtra bude. Yak pratsuiut prifrontovi viddilennia Novoi poshty [Tomorrow Will Be: How Frontline Nova Poshta Branches Operate]. Available at: <https://nv.ua/ukr/ukraine/events/zavtra-bude-yak-pracyuyut-prifrontovi-viddilennya-novoji-poshti-fotoreportazh-50530842.html> (Accessed: 07 Oct. 2025). [in Ukrainian]

24. PaySpace Magazine (2025) Tsifrovi dviinyky: shcho tse za tekhnolohiia i yak vona dopomozhe vidnovyty Ukrainu - analityka [Digital Twins: What This Technology Is and How It Will Help Rebuild Ukraine - Analytics]. Available at: <https://psm7.com/uk/technology/cifrovye-dvojniki-chto-eto-za-tekhnologiya-i-kak-ona-pomozhet-vosstanovit-ukrainu-analitika.html> (Accessed: 07 Oct. 2025). [in Ukrainian]

