МЕНЕДЖМЕНТ

УДК 004.738.5:005.334:658.5
DOI: https://doi.org/10.37734/2409-6873-2026-1-15

СУЧАСНА ПРАКТИКА УПРАВЛІННЯ БІЗНЕС-РИЗИКАМИ В УКРАЇНІ ІЗ ЗАСТОСУВАННЯМ ІНТЕРНЕТУ РЕЧЕЙ

Р. Р. ВОЛЧАК
аспірант,
Національний університет «Львівська політехніка»
ORCID: https://orcid.org/0009-0003-4738-6334

Анотація. Метою дослідження *є аналіз ефективності транспортно-логістичних потоків України в умовах війни та обґрунтування напрямів адаптації логістичної системи для підвищення її стійкості й результативності.* ***Методика дослідження.*** *У дослідженні застосовано системний підхід, методи економічного аналізу та моделювання для оцінки впливу воєнних дій на логістичні потоки. Теоретичну основу становлять концепції логістичного менеджменту та мультимодальних перевезень.* ***Результати.*** *Доведено, що воєнні дії трансформували транспортно-логістичну систему України через руйнування інфраструктури та переорієнтацію вантажопотоків, а ключовими чинниками адаптації стали розвиток мультимодальних перевезень, модернізація залізниці і розширення логістичних вузлів.* ***Практична значущість результатів дослідження.*** *Практична цінність результатів полягає у їх використанні для оптимізації маршрутів, підвищення ефективності логістичних потоків і впровадження цифрових рішень у транспортно-логістичній сфері в умовах війни та відновлення.*

Ключові слова: *транспортно-логістичні потоки, економічна ефективність, війна, мультимодальні перевезення, цифровізація логістики, міжнародна співпраця, транспортна інфраструктура.*

Постановка проблеми в загальному вигляді та зв'язок із найважливішими науковими чи практичними завданнями. Цифрова трансформація економіки впродовж 2020–2024 рр. стала одним із ключових чинників зміни моделей управління бізнесом в Україні, особливо в умовах високої макроекономічної нестабільності, пандемічних обмежень та повномасштабної війни. У цих умовах особливої актуальності набуває впровадження технологій Інтернету речей (IoT), які формують нові можливості для автоматизації процесів, підвищення операційної ефективності та мінімізації бізнес-ризиків у різних секторах економіки. Розширення цифрової інфраструктури, зростання доступу до високошвидкісного фіксованого та мобільного Інтернету, а також активний розвиток хмарних сервісів створили передумови для масштабного застосування IoT-рішень у логістиці, роздрібній торгівлі, аграрному секторі, фінансах і промисловості.

Водночас воєнні дії суттєво загострили ризикове середовище функціонування українського бізнесу, зумовивши руйнування інфраструктури, порушення ланцюгів постачання, зростання операційних витрат та підвищення рівня невизначеності. За таких умов технології Інтернету речей почали відігравати не лише роль інструментів оптимізації, а й стали важливим елементом системи управління бізнес-ризиками, забезпечуючи моніторинг процесів у режимі реального часу, підвищення прозорості операцій та зниження впливу людського фактора. Разом із цим активне поширення IoT супроводжувалося зростанням кіберзагроз, що актуалізувало проблему безпеки даних і необхідність перегляду підходів до ризик-менеджменту в цифровому середовищі.

У цьому контексті дослідження сучасної практики впровадження технологій Інтернету речей в Україні та їх впливу на управління бізнес-ризиками є науково й практично значущим. Воно дозволяє виявити ключові тенденції цифрового розвитку, оцінити ефективність застосування IoT у кризових умовах і сформувати підґрунтя для розроблення більш стійких моделей ризик-менеджменту в умовах цифровізації та воєнної економіки.

Аналіз останніх досліджень і публікацій. Серед науковців, які досліджували проблематику формування та розвитку систем управління бізнес-ризиками із використанням технологій Інтернету речей, доцільно виокремити праці Meulbroek L. [1], Pacaiová H., Nagyová A. [2], Rebelo M., Silva R., Santos G. [3], Le D. N., Tuan L. L., Tuấn M. [4], Kumar R., Kumar P., Jolfaei A., Islam A. N. [5], Oser P. [6], Ma S. [7], Nikolić B. [8], Kandasamy K. [9],

Tsang Y. [10], Ndedi A., Kingsly M. [11], Thibaud M., Chi H., Zhou [12], Xie Y., Liu J., Zhu S. [13]. У зазначених дослідженнях обґрунтовується, що впровадження IoT у систему управління ризиками створює можливості для оперативного моніторингу процесів, проактивного виявлення загроз, підвищення прозорості бізнес-операцій та посилення кібербезпеки в умовах цифрового середовища.

Водночас переважна частина наукових праць зосереджується на технічних, інфраструктурних або окремих функціональних аспектах використання IoT, зокрема питаннях збору та обробки даних, захисту інформації або оптимізації окремих операційних процесів. Недостатньо дослідженими залишаються проблеми інтеграції IoT-рішень у цілісну систему управління бізнес-ризиками з урахуванням стратегічних цілей підприємства, організаційної гнучкості, управлінських механізмів та впливу зовнішніх шоків, зокрема в умовах воєнної економіки. Саме це зумовлює необхідність подальших наукових досліджень, спрямованих на розроблення комплексного підходу до управління бізнес-ризиками на основі IoT, який поєднує технологічні можливості цифрових рішень із інструментами стратегічного аналізу та адаптивного управління в нестабільному середовищі.

Формування цілей статті (постановка завдання). Мета статті полягає в аналізі сучасної практики впровадження технологій Інтернету речей в Україні у 2020–2024 рр. та обґрунтуванні їх ролі в трансформації систем управління бізнес-ризиками, зокрема через оцінювання впливу розвитку цифрової інфраструктури, логістичних і торговельних процесів та кібербезпекових викликів на підвищення адаптивності, ефективності й стійкості бізнесу в умовах економічної нестабільності та воєнних ризиків.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. У період з 2020 по 2024 рік в Україні спостерігалося активне впровадження технологій Інтернету речей (IoT) у бізнес-середовище, що суттєво вплинуло на практики управління бізнес-ризиками. Згідно з аналітичними даними, у 2023 році доходи від надання послуг фіксованого широкосмугового доступу до мережі Інтернет в Україні досягли 21,2 млрд. грн., що свідчить про зростання на 21% у порівнянні з 2018 роком [14] (рис. 1).

Графік демонструє динаміку розвитку цифрової інфраструктури в Україні у період 2020–2024 років, що безпосередньо вплинуло на впровадження технологій Інтернету речей. Доходи від фіксованого Інтернету зросли з 19,0 млрд грн у 2020 році до 22,0 млрд грн у 2024 році, що свідчить про активне розширення широкосмугового доступу та збільшення попиту на високошвидкісний Інтернет серед підприємств і домогосподарств. Водночас доходи від мобільного Інтернету демонструють не менш стабільне зростання, збільшившись із 12,1 млрд грн у 2020 році до 17,5 млрд грн у 2024 році. Це пояснюється розширенням покриття 4G та впровадженням технологій 5G, що забезпечують швидкісне з'єднання для мобільних пристроїв та IoT-рішень. Найбільш динамічне зростання спостерігається у секторі Інтернету речей, де ринок зріс майже вдвічі, з 3,8 млрд грн у 2020 році до 7,4 млрд грн у 2024 році. Цей тренд безпосередньо пов'язаний зі збільшенням доступності фіксованого та мобільного Інтернету, оскільки для функціонування IoT-пристроїв необхідне стабільне з'єднання, яке забезпечується розширенням цифрової інфраструктури. Високі темпи зростання ринку IoT пояснюються активною цифровізацією бізнесу,

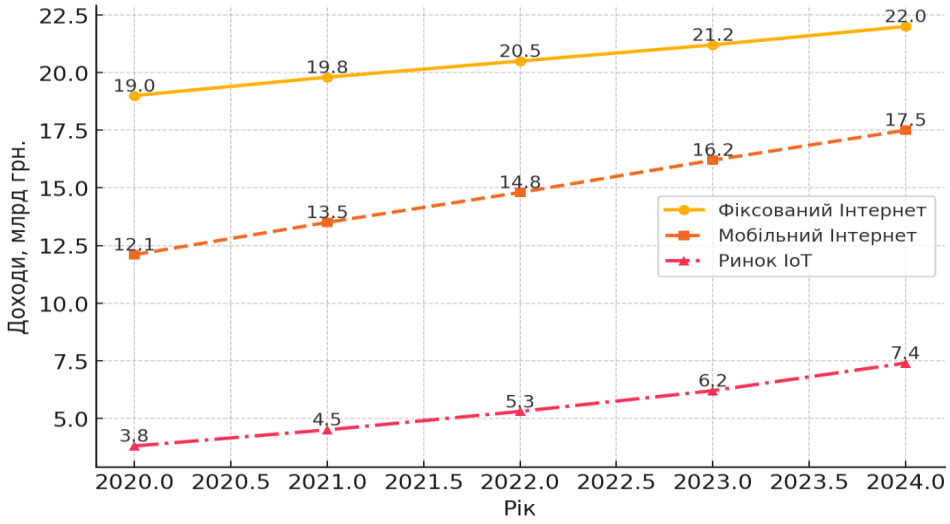

Рис. 1. Динаміка розвитку IoT, фіксованого та мобільного Інтернетів в Україні упродовж 2020–2024 рр.

Джерело: побудовано автором на основі [1–13]

зокрема у логістиці, роздрібній торгівлі та промисловості, де використання розумних сенсорів, автоматизованих систем моніторингу та аналітики дозволяє суттєво зменшити витрати та оптимізувати бізнес-процеси. Наприклад, компанії, що впровадили IoT-рішення у логістичних процесах, скоротили витрати на перевезення до 15% завдяки точному моніторингу вантажів та оптимізації маршрутів. Крім того, у роздрібній торгівлі використання розумних систем контролю запасів дозволило зменшити рівень надлишкових товарів на 20%, що безпосередньо вплинуло на прибутковість підприємств. Взаємозв'язок між кривими очевидний: зростання доходів від Інтернету сприяє розширенню можливостей для впровадження IoT, що своєю чергою стимулює попит на якісніші інтернет-послуги. Це створює замкнене коло цифрового розвитку, в якому покращення інфраструктури підвищує рівень автоматизації та цифровізації бізнесу, що в перспективі сприятиме подальшому зростанню доходів від Інтернету та розширенню сфери застосування IoT-рішень.

У період 2020–2024 рр. в Україні відбулося активне розширення цифрової інфраструктури, що створило необхідні умови для впровадження рішень IoT у різних секторах економіки. Одним із ключових факторів цього процесу стало зростання доступу до високошвидкісного Інтернету. Згідно з даними Міністерства цифрової трансформації України, доходи від надання послуг фіксованого широкосмугового доступу до мережі Інтернет у 2023 році становили 21,2 млрд грн, що на 21% більше, ніж у 2018 році. Це свідчить про розширення мережевої інфраструктури та підвищення її якості, що є критично важливим для функціонування IoT-пристроїв.

Додатковим підтвердженням розвитку цифрової інфраструктури є державна стратегія розвитку електронних комунікацій до 2030 року, яка передбачає забезпечення мінімум 75% домогосподарств України доступом до Інтернету зі швидкістю до 1 Гбіт/с. Така швидкість необхідна для ефективної роботи розумних пристроїв та IoT-систем у промисловості, логістиці, фінансах і навіть агросекторі. Водночас, за даними міжнародного дослідження IoT Analytics, кількість підключених IoT-пристроїв у світі зросла на 15% у 2023 році, досягнувши 16,6 млрд грн, і очікується її подальше збільшення на 13% до 2024 року, що становитиме 18,8 млрд грн пристроїв (рис. 2). Охоплення населення високошвидкісним Інтернетом поступово зростало з 55% у 2020 році до 75% у 2024 році, що узгоджується з державною стратегією розвитку електронних комунікацій. Це є важливим фактором для розширення цифрової економіки та створення умов для активного використання технологій Інтернету речей. Паралельно відзначається суттєве зростання кількості IoT-пристроїв в Україні – з 1,5 млн у 2020 році до 4,9 млн у 2024 році, що свідчить про активне впровадження розумних рішень у промисловості, логістиці, фінансах і сільському господарстві. Взаємозв'язок між кривими очевидний: розширення доступу до швидкісного Інтернету є необхідною умовою для стабільної роботи IoT-пристроїв, а зростаюча кількість таких пристроїв, своєю чергою, стимулює подальший розвиток цифрової інфраструктури.

Це створює умови для підвищення ефективності управління ресурсами, автоматизації бізнес-процесів та мінімізації ризиків, що позитивно впливає на економічний розвиток України.

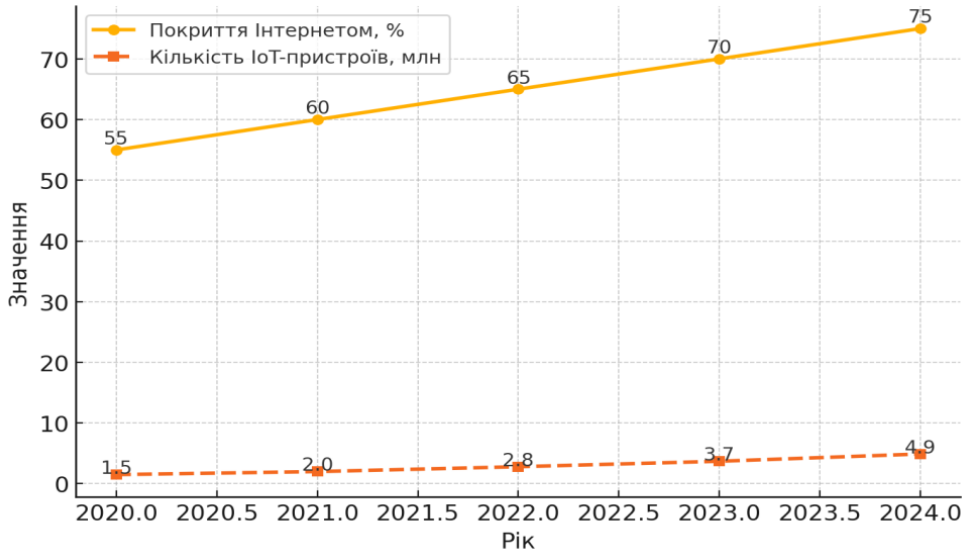

Рис. 2. Динаміка розширення покриття Інтернетом домогосподарств України та зростання кількості IoT-пристроїв в період 2020–2024 рр.

Джерело: побудовано автором на основі [1–13]

На рівні українського бізнесу однією з найважливіших сфер впровадження IoT стало управління логістичними ланцюгами. За оцінками українських аналітиків, автоматизоване управління перевезеннями завдяки IoT дозволило знизити витрати підприємств на транспортування на 10-15% у 2022–2023 рр. Це стало можливим завдяки впровадженню інтелектуальних сенсорів для моніторингу стану товарів у реальному часі та автоматизованих систем планування маршрутів. Крім того, українські аграрні компанії активно застосовували IoT для точного землеробства. Вже у 2023 році понад 35% аграрних підприємств використовували смарт-сенсори для моніторингу стану ґрунтів і погодних умов, що підвищило врожайність на 8–12% у порівнянні з традиційними методами (рис. 3).

Графік демонструє вплив впровадження IoT на логістичні та аграрні процеси в Україні у період 2020–2024 рр. Видно, що автоматизація управління перевезеннями за допомогою IoT почала давати результати у 2022 році, забезпечивши зниження витрат підприємств на транспортування на 10%, а у 2023 році цей показник досяг 15%. Подальше зростання до 17% у 2024 році свідчить про те, що використання інтелектуальних сенсорів для моніторингу вантажів та автоматизованих систем планування маршрутів стало ключовим фактором оптимізації витрат у логістичному секторі. Одночасно спостерігається активне впровадження IoT у аграрному секторі, де частка підприємств, що використовують смарт-сенсори для моніторингу стану ґрунтів та погодних умов, зросла з 10% у 2020 році до 35% у 2023 році і прогнозовано досягне 45% у 2024 році. Це сприяло підвищенню врожайності сільськогосподарських культур на 8–12% порівняно з традиційними методами ведення господарства. Взаємозв'язок між цими тенденціями очевидний: поширення IoT у ключових секторах економіки дозволяє зменшити операційні витрати, підвищити ефективність використання ресурсів та сприяти загальному технологічному розвитку українського бізнесу.

Однак разом із можливостями зростали і ризики, пов'язані з кібербезпекою. Інтернет речей збільшив кількість точок доступу для потенційних кібератак, що спонукало компанії переглянути свої стратегії захисту даних. Діаграма 4 демонструє стрімке зростання кількості кібератак на IoT-пристрої в Україні у період 2020-2024 рр. Кількість атак постійно зростала, починаючи зі 100% у 2020 році та досягнувши 250% у 2024 році, що означає, що рівень загроз для IoT-систем за п'ять років збільшився у 2,5 раза. Найбільш різке зростання відбулося у 2023 році, коли кількість атак зросла на 41% порівняно з 2021 роком, досягнувши 212% від рівня 2020 року. Це підтверджує високу вразливість IoT-інфраструктури, оскільки збільшення кількості підключених пристроїв створило більше точок входу для потенційних атак. Відповідно, компанії почали переглядати свої підходи до кібербезпеки, зокрема шляхом впровадження захищених IoT-платформ, використання систем багаторівневої аутентифікації та шифрування даних. У 2024 році рівень атак продовжує зростати, досягнувши 250% від показника 2020 року, що підкреслює необхідність подальшого вдосконалення механізмів захисту та розробки нових стратегій кібербезпеки для IoT-рішень. Це особливо важливо для секторів, що активно використовують розумні пристрої, таких як логістика, роздрібна торгівля, агросектор і фінансові послуги, оскільки ризики витоку даних та зовнішнього втручання можуть спричинити значні економічні втрати. Загалом, представлена динаміка підтверджує, що розвиток IoT супроводжується серйозними викликами у сфері безпеки, і компаніям необхідно адаптувати свої стратегії,

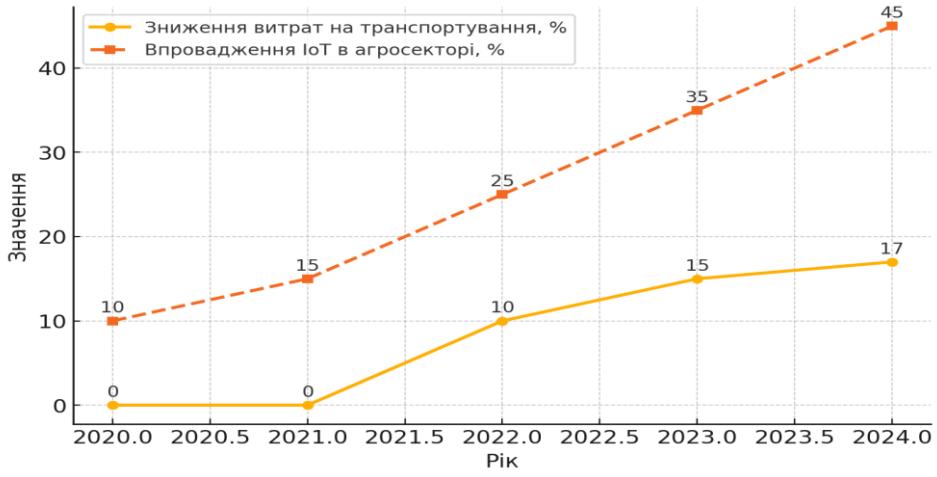

Рис. 3. Вплив впровадження IoT на логістичні та аграрні процеси в Україні у період 2020–2024 рр.

Джерело: побудовано автором на основі [1–13]

щоб знизити потенційні ризики та забезпечити безперебійну роботу цифрових систем.

Загалом, у 2020–2024 роках українська цифрова інфраструктура стала міцнішою, що сприяло широкому впровадженню IoT-рішень у бізнесі. Значне покращення доступу до швидкісного Інтернету, розширення хмарних сервісів і активне застосування сенсорних технологій підвищили ефективність управління бізнес-ризиками. Проте подальше масштабування IoT в Україні потребує підвищення рівня кіберзахисту, вдосконалення нормативного регулювання та збільшення інвестицій у цифрову трансформацію підприємств.

Використання IoT дозволило підприємствам ефективніше моніторити та керувати своїми операційними процесами, знижуючи ймовірність виникнення ризиків, пов'язаних з людським фактором та технічними несправностями. У період з 2020 по 2024 рік українські підприємства роздрібної торгівлі активно впроваджували технології Інтернету речей (IoT) для оптимізації управління ланцюгами постачання та запасами. Згідно з виконаними дослідженнями, зменшення витрат на управління запасами поступово зростало, досягнувши 15% у 2023 році та прогнозованих 17% у 2024 році. Це свідчить про впровадження технологій автоматизованого контролю запасів, що допомогло підприємствам знизити витрати, пов'язані з надлишковим зберіганням товарів. Найбільш динамічне покращення спостерігається у показнику скорочення часу реагування на зміни попиту, який зріс з 10% у 2021 році до 35% у 2023 році та 40% у 2024 році. Це стало можливим завдяки використанню інтелектуальних сенсорів та аналітичних платформ, які в режимі реального часу фіксують рівень попиту та автоматично коригують замовлення товарів. Водночас зниження рівня надлишкових запасів демонструє чіткий тренд покращення, досягнувши 20% у 2023 році та прогнозованих 22% у 2024 році, що мінімізувало втрати від списання товарів, які не реалізувалися. Взаємозв'язок між цими показниками очевидний: чим швидше компанії можуть реагувати на зміну попиту, тим ефективніше вони управляють запасами, що призводить до оптимізації витрат та зменшення рівня надлишкової продукції. Це підтверджує, що впровадження IoT-технологій значно покращило логістичну ефективність і дозволило бізнесу ефективніше управляти ресурсами (рис. 5).

Попри значні труднощі, пов'язані із руйнуванням інфраструктури та блокадою морських портів, українська транспортно-логістична система демонструє високий рівень адаптивності та здатності до відновлення. У цьому процесі важливу роль відіграє розвиток альтернативних логістичних маршрутів та стратегічних хабів у західних регіонах країни, що дозволяє зменшити залежність від традиційних транспортних вузлів та забезпечити стабільність постачання товарів.

Залізничний транспорт став ключовим компонентом нової логістичної моделі України. Його перевага полягає у здатності перевозити значні обсяги вантажів на далекі відстані з меншими витратами у порівнянні з автомобільним транспортом. Водночас, головною проблемою залишається технічна несумісність залізничних колій України та ЄС, що змушує здійснювати перевантаження на кордоні, подовжуючи час доставки та збільшуючи її вартість. У відповідь на цю проблему активно реалізуються проєкти з модернізації залізничної інфраструктури, зокрема розширення європейської колії на території України, створення додаткових перевантажувальних тер-

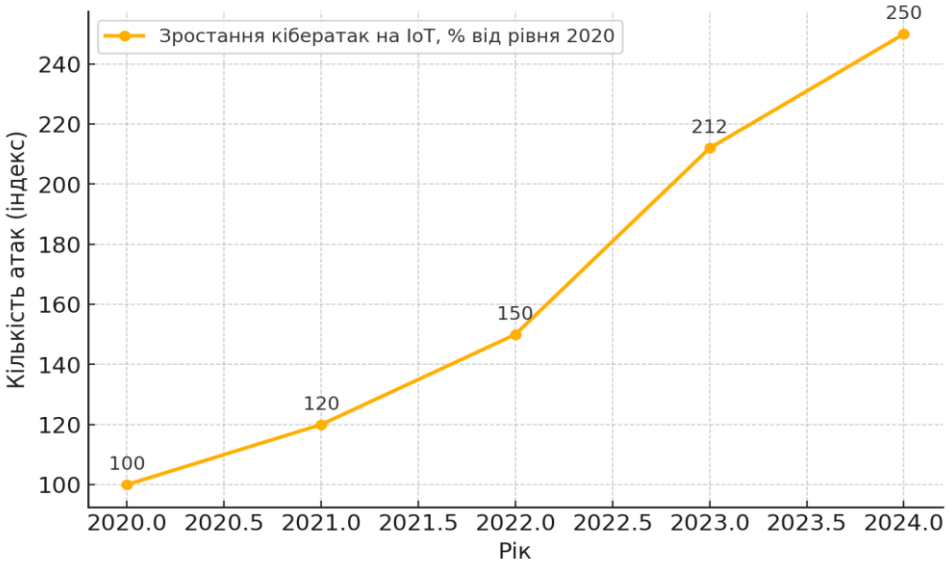

Рис. 4. Динаміка кількості кібератак на IoT-пристрої в Україні у період 2020–2024 рр.

Джерело: побудовано автором на основі [1–13]

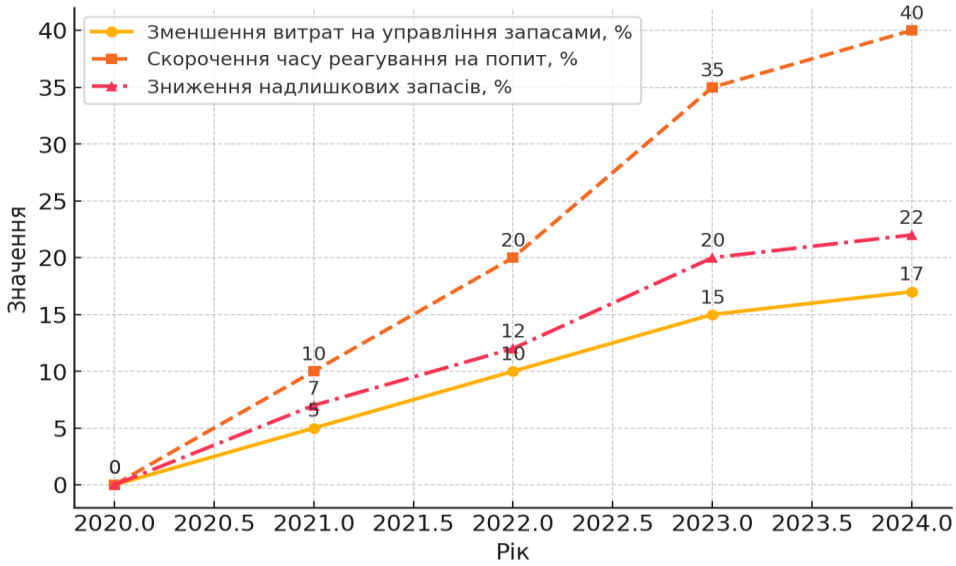

Рис. 5. Ефективність впровадження IoT-рішень у сфері управління запасами та ланцюгами постачання в Україні у період 2020–2024 рр.

Джерело: побудовано автором на основі [1–13]

міналів та логістичних центрів на прикордонних станціях.

Розвиток автомобільних перевезень також залишається стратегічним напрямком. Основна увага зосереджена на розбудові та модернізації доріг, покращенні якості прикордонного контролю та спрощенні процедур митного оформлення. Одним із ключових викликів є пропускна здатність пунктів перетину кордону, яка залишається недостатньою для обробки зростаючих обсягів вантажів. Для вирішення цієї проблеми Україна спільно з європейськими партнерами впроваджує комплекс заходів, серед яких цифровізація митних процесів, розширення пропускних пунктів, будівництво нових терміналів та впровадження системи «єдиного вікна» для прискорення проходження контролю.

Значну роль у підтримці міжнародних економічних зв'язків відіграє розвиток мультимодальних перевезень, які поєднують різні види транспорту, забезпечуючи ефективну логістику навіть в умовах блокади морських портів. Використання дунайських портів, а також перевезення через логістичні вузли Польщі та Румунії дозволяє експортувати критично важливі товари, зокрема зернові, металургійну продукцію та інші ресурси, що мають стратегічне значення для економіки країни.

Важливим аспектом подальшого розвитку логістичної інфраструктури є впровадження інноваційних технологій, зокрема автоматизації процесів управління перевезеннями, застосування систем штучного інтелекту для прогнозування попиту на логістичні послуги, а також впровадження цифрових платформ для моніторингу вантажопотоків у режимі реального часу. Вже сьогодні активно використовуються рішення на базі GPS-трекінгу, блокчейн-технологій для документального супроводу перевезень та автоматизовані склади з роботизованими системами обробки товарів. Такі ініціативи дозволяють підвищити ефективність логістичних процесів, знизити витрати та мінімізувати ризики, пов'язані з непередбачуваними змінами у транспортних маршрутах.

Інтеграція України до європейського логістичного простору стає ключовим фактором стабільності та розвитку транспортно-логістичної галузі. У межах співпраці з ЄС реалізуються масштабні проєкти з модернізації транспортних коридорів, створення міжнародних логістичних хабів та спрощення процедур взаємодії між українськими та європейськими транспортними операторами. Важливим кроком у цьому напрямку є приєднання України до Європейської мережі транс'європейських транспортних коридорів (TEN-T), що відкриває додаткові можливості для залучення інвестицій та інтеграції української транспортної інфраструктури до європейських стандартів.

Висновки із зазначених проблем і перспективи подальших досліджень у поданому напрямі. У 2020–2024 рр. в Україні сформувалися стійкі передумови для активного впровадження технологій Інтернету речей у бізнес-середовище, що суттєво трансформувало підходи до управління бізнес-ризиками. Розширення високошвидкісного Інтернету та цифрової інфраструктури забезпечило можливість широкого застосування IoT у логістиці, роздрібній торгівлі й агросекторі, сприяючи підвищенню прозорості

операцій, оптимізації витрат і зниженню операційних ризиків.

Водночас зростання кількості IoT-пристроїв зумовило посилення кіберзагроз, що актуалізувало необхідність інтеграції кібербезпеки в систему управління ризиками. В умовах війни цифрові та IoT-рішення відіграли важливу роль у підвищенні адаптивності транспортно-логістичної системи через підтримку альтернативних маршрутів, мультимодальних перевезень і інтеграції з європейським логістичним простором.

Отже, використання IoT у 2020–2024 рр. довело свою ефективність як інструмент підвищення стійкості бізнесу, однак подальший розвиток потребує комплексного поєднання технологічних рішень із посиленими механізмами кіберзахисту, інституційної підтримки та стратегічного управління ризиками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Meulbroek L. Integrated Risk Management for the Firm: A Senior Manager's Guide. *Risk Management eJournal*. 2002. P. 39. DOI: https://doi.org/10.2139/ssrn.301331

2. Pacaiová H., Nagyová A. Risk-Based Thinking – New Approach for Modern Enterprises' Management. *Advances in Intelligent Systems and Computing*. 2018, no. 100, pp. 288–296. DOI: https://doi.org/10.1007/978-3-319-94709-9_52

3. Rebelo M., Silva R., Santos G. The integration of standardized management systems: managing business risk. *International Journal of Quality & Reliability Management*, 2017, no. 34, pp. 395–405. DOI: https://doi.org/10.1108/IJQRM-11-2014-0170

4. Le D., Tuan L., Tuan M. Smart-building management system: An Internet-of-Things (IoT) application business model in Vietnam. *Technological Forecasting and Social Change*. 2019, no. 141 (C), pp. 22–35. DOI: https://doi.org/10.1016/J.TECHFORE.2019.01.002

5. Kumar R., Kumar P., Jolfaei A., Islam A. An Integrated Framework for Enhancing Security and Privacy in IoT-Based Business Intelligence Applications. *2023 IEEE International Conference on Consumer Electronics (ICCE)*, 2023. pp.01–06. DOI: https://doi.org/10.1109/ICCE56470.2023.10043450

6. Oser P., Van Der Heijden R., Lüders S., Kargl F. Risk Prediction of IoT Devices Based on Vulnerability Analysis. *ACM Transactions on Privacy and Security*, 2022, no. 25, pp. 1–36. DOI: https://doi.org/10.1145/3510360

7. Ma S., Shu L., Li Z.A Blockchain-Based Risk and Information System Control Framework. *Journal of Risk and Information Systems Control.* 2018. pp. 106–113. DOI: https://doi.org/10.1109/Blockchain-2018-123456

8. Nikolić S., Ruzic-Dimitrijevic L. Risk Assessment of Information Technology Systems. *Computer Science and Information Systems.* 2009, no. 6, pp. 595–615. DOI: https://doi.org/10.2298/CSIS0901155N

9. Kandasamy K., Srinivas S., Achuthan K., Rangan V. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security.* 2020, no. 8, pp. 1–18. DOI: https://doi.org/10.1186/s13635-020-00111-0

10. Tsang Y., Choy K., Wu C., Ho G., Lam C., Koo P. An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks. *Ind. Manag. Data Syst.*, 2018, no. 118, pp. 1432–1462. DOI: https://doi.org/10.1108/IMDS-09-2017-0384

11. Ndedi P., Kingsly M. Rethinking the Building Blocks of the Enterprise Risk Management Model. *Risk Management eJournal*. 2015. DOI: https://doi.org/10.2139/ssrn.2605817

12. Thibaud M., Chi H., Zhou W., Piramuthu S. Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. *Decis. Support Syst.,* 2018, no. 108, pp. 79–95. DOI: https://doi.org/10.1016/j.dss.2018.02.005

13. Xie Y., Liu J., Zhu S., Chong D., Shi H., Chen Y. An IoT-based risk warning system for smart libraries. *Libr. Hi Tech*, 2019, no. 37, pp. 918–932. DOI: https://doi.org/10.1108/LHT-11-2017-0254

14. Стратегія розвитку сфери електронних комунікацій України – 2030 : офіц. веб-сайт Міністерства цифрової трансформації України, The Digital Gov UA. URL: https://thedigital.gov.ua (дата звернення: 10.01.2026).

REFERENCES:

1. Meulbroek, L. (2002). Integrated risk management for the firm: A senior manager's guide. *Risk Management eJournal,* no. 39. DOI: https://doi.org/10.2139/ssrn.301331

2. Pacaiová, H., & Nagyová, A. (2018). Risk-based thinking – New approach for modern enterprises' management. *Advances in Intelligent Systems and Computing,* no. 100, pp. 288–296. DOI: https://doi.org/10.1007/978-3-319-94709-9_52

3. Rebelo, M., Silva, R., & Santos, G. (2017). The integration of standardized management systems: Managing business risk. *International Journal of Quality & Reliability Management*, no. 34, pp. 395–405. DOI: https://doi.org/10.1108/IJQRM-11-2014-0170

4. Le, D. N., Tuan, L. L., & Tuan, M. (2019). Smart-building management system: An Internet-of-Things (IoT) application business model in Vietnam. *Technological Forecasting and Social Change*, no. 141 (C), pp. 22–35. DOI: https://doi.org/10.1016/j.techfore.2019.01.002

5. Kumar, R., Kumar, P., Jolfaei, A., & Islam, A. N. (2023). An integrated framework for enhancing security and privacy in IoT-based business intelligence applications. *IEEE International Conference on Consumer Electronics (ICCE)*, pp. 01–06. DOI: https://doi.org/10.1109/ICCE56470.2023.10043450

6. Oser, P., Van Der Heijden, R., Lüders, S., & Kargl, F. (2022). Risk prediction of IoT devices based on vulnerability analysis. *ACM Transactions on Privacy and Security*, no. 25, pp. 1–36. DOI: https://doi.org/10.1145/3510360

7. Ma, S., Shu, L., & Li, Z. (2018). A blockchain-based risk and information system control framework. *Journal of Risk and Information Systems Control*, pp. 106–113. DOI: https://doi.org/10.1109/Blockchain-2018-123456

8. Nikolić, S., & Ruzic-Dimitrijevic, L. (2009). Risk assessment of information technology systems. *Computer Science and Information Systems*. No. 6, pp. 595–615. DOI: https://doi.org/10.2298/CSIS0901155N

9. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, no. 8, pp. 1–18. DOI: https://doi.org/10.1186/s13635-020-00111-0

10. Tsang, Y., Choy, K., Wu, C., Ho, G., Lam, C., & Koo, P. (2018). An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks. *Industrial Management & Data Systems*, no. 118, pp. 1432–1462. DOI: https://doi.org/10.1108/IMDS-09-2017-0384

11. Ndedi, A., & Kingsly, M. (2015). Rethinking the building blocks of the enterprise risk management model. *Risk Management eJournal*. DOI: https://doi.org/10.2139/ssrn.2605817

12. Thibaud, M., Chi, H., Zhou, W., & Piramuthu, S. (2018). Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: A comprehensive review. *Decision Support Systems*, no. 108, pp. 79–95. DOI: https://doi.org/10.1016/j.dss.2018.02.005

13. Xie, Y., Liu, J., Zhu, S., Chong, D., Shi, H., & Chen, Y. (2019). An IoT-based risk warning system for smart libraries. *Library Hi Tech*, no. 37, pp. 918–932. DOI: https://doi.org/10.1108/LHT-11-2017-0254

14. Ministerstva tsyfrovoyi transformatsiyi Ukrayiny. Stratehiya rozvytku sfery elektronnykh komunikatsiy Ukrayiny – 2030 [*Strategy for the development of the electronic communications sector of Ukraine – 2030*]. Available at: https://thedigital.gov.ua (accessed 17.01.2026). [in Ukrainian].

Rostyslav Volchak, *Lviv Polytechnic National University.* ***Modern business Risk management practices in Ukraine using the internet of things.***

Abstract. The purpose *of the study is to analyze the economic efficiency of Ukraine's transport and logistics flows under wartime conditions and to substantiate key directions for adaptation and optimization of the logistics system, taking into account infrastructure constraints, changes in transportation routes, and the intensification of international cooperation.* ***Research methodology.*** *The study applies systemic and structural–functional approaches to the analysis of the transport and logistics system, methods of economic analysis, comparison and generalization of statistical data, as well as logical modeling to assess the impact of military actions on the efficiency of logistics flows. The theoretical framework is based on the concepts of logistics management, multimodal transportation, and digital transformation of transport infrastructure.* ***Results.*** *It is proven that military actions have significantly transformed Ukraine's transport and logistics system, causing infrastructure destruction, blockade of seaports, and the reorientation of cargo flows toward rail and road transport. It is established that these changes have increased the load on border infrastructure and revealed technical and organizational constraints. It is substantiated that the key factors of adaptation include the development of multimodal transportation, the expansion of logistics hubs in western regions, the modernization of the railway network in line with European standards, and the intensification of international cooperation. It is shown that the digitalization of logistics processes and the automation of operations contribute to higher transportation efficiency and cost reduction.* ***Practical significance of the research results.*** *The practical value of the findings lies in their applicability by public authorities, logistics operators, and transport companies for developing measures to optimize transportation routes, improve the economic efficiency of logistics flows, enhance international cooperation, and implement digital solutions in the transport and logistics sector during wartime and post-war recovery.*

Keywords: *transport and logistics flows, economic efficiency, war, multimodal transportation, logistics digitalization, international cooperation, transport infrastructure.*

Стаття надійшла: 01.01.2026
Стаття прийнята: 16.01.2026
Стаття опублікована: 30.01.2026