ШАХРАЙСТВО В ЛОГІСТИЧНІЙ ДІЯЛЬНОСТІ ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВ

FRAUD IN LOGISTICS ACTIVITIES AS A THREAT TO THE ECONOMIC SECURITY OF ENTERPRISES

Систематизовано основні шахрайські схеми в логістичній діяльності та визначено напрями їх впливу на економічну безпеку підприємств. Проаналізовано судову та правоохоронну практику України, Німеччини та Сполучних Штатів Америки, а також узагальнено інструменти запобігання шахрайству в логістичних процесах. Запропоновано методику комплексної верифікації учасників логістичної операції, яка передбачає послідовну перевірку юридичних, контактних, фінансових, документальних, транспортних, репутаційних та операційних аспектів співпраці. Практична цінність одержаних результатів полягає у можливості їх використання логістичними підприємствами для вдосконалення системи економічної безпеки, управління ризиками та запровадження превентивних заходів щодо запобігання шахрайським проявам.

Ключові слова: *ланцюги постачання, внутрішній контроль, кіберризики, контрагенти, цифрові платформи, інформаційний захист, перевезення, комплаєнс.*

The increasing complexity of supply chains, the active implementation of digital technologies, and the expanding use of electronic platforms in transportation activities by business entities are accompanied by the emergence of new risks associated with fraudulent actions and cyber threats. Under such conditions, ensuring the economic security of enterprises engaged in the organization and management of logistics processes becomes particularly important. The purpose of the article is to investigate manifestations of fraud in logistics activities and determine their impact on the economic security of enterprises, as well as to substantiate tools for counteracting relevant threats. The study employed methods of analysis, synthesis, comparison, systematization, and generalization, which made it possible to identify the characteristics of common fraudulent schemes in logistics, assess the nature of their impact on individual components of economic security, and analyze judicial practice related to such cases in Ukraine, Germany, and the United States of America. It has been determined that the most common threats include the activities of fictitious carriers and freight forwarding companies, document forgery, manipulation of bank details, unlawful appropriation of cargo, hacking of accounts on digital platforms, and the use of artificial intelligence technologies for fraudulent purposes. The findings indicate that the consequences of such violations affect the financial, property, contractual, operational, informational, legal, personnel, and reputational components of enterprise activities. An integrated anti-fraud approach involving counterparty verification procedures, electronic document management, internal control, protection of information resources, and enhancement of personnel awareness regarding contemporary risks has been substantiated. A methodology for the comprehensive verification of participants in logistics operations has been proposed, providing for the consistent assessment of legal, contact, financial, documentary, transport, reputational, and operational aspects of cooperation. The proposed methodology can be adapted to enterprises of different sizes and used as a preventive tool to strengthen economic security and reduce the likelihood of fraudulent activities.

Key words: *supply chains, internal control, cyber risks, counterparties, digital platforms, information security, transportation, compliance.*

УДК 338.47:658.012.8:343.72
DOI: https://doi.org/10.32782/dees.24-15

Лега О.В.[1]
к.е.н., доцент,
Полтавський державний аграрний університет
Тараненко Я.І.[2]
аспірант,
Полтавський державний аграрний університет

Leha Olha
Poltava State Agrarian University
Taranenko Yaroslav
Poltava State Agrarian University

Постановка проблеми. Розвиток цифрових технологій, розширення міжнародних ланцюгів постачання та активне використання електронних платформ у сфері перевезень сприяють не лише підвищенню ефективності логістичних процесів, а й появі нових загроз, пов'язаних із шахрайськими діями та кіберризиками. Логістична діяльність передбачає взаємодію великої кількості учасників, використання значних матеріальних і фінансових ресурсів, а також постійний обмін інформацією, що створює додаткові можливості для виникнення різних видів зловживань [1]. Використання фіктивних перевізників, підроблених документів, незаконне заволодіння вантажами, маніпуляції з банківськими реквізитами та злом цифрових платформ здатні призводити до значних фінансових втрат, порушення договірних відносин, зниження довіри з боку партнерів та погіршення ділової репутації підприємств [2].

Зростання масштабів цифровізації логістичних процесів та поширення сучасних інформаційних технологій зумовлюють трансформацію традиційних шахрайських схем і появу нових форм протиправної діяльності, у тому числі пов'язаних із використанням технологій штучного інтелекту [3]. У зв'язку з цим питання протидії шахрайству набувають важливого значення в контексті забезпечення економічної безпеки підприємств, оскільки своєчасне виявлення та мінімізація відповідних ризиків сприяють підвищенню стабільності функціонування суб'єктів господарювання та збереженню їх конкурентних переваг.

Аналіз останніх досліджень і публікацій. Пробатика шахрайства, ризиків та забезпечення

[1] ORCID: https://orcid.org/0000-0002-0989-8000
[2] ORCID: https://orcid.org/0009-0003-9808-108X

економічної безпеки в логістичній діяльності привертає дедалі більшу увагу науковців, що обумовлено ускладненням ланцюгів постачання, поширенням цифрових технологій та зростанням кіберзагроз. Серед досліджень, присвячених ідентифікації шахрайських ризиків у транспортно-логістичному бізнесі, варто відзначити роботу С. Селіщева, у якій розглянуто особливості виявлення ризику шахрайства в управлінні проєктами та обґрунтовано необхідність застосування ризик-орієнтованого підходу до прийняття управлінських рішень [2]. Питання взаємозв'язку логістичних процесів та економічної безпеки підприємств досліджували І. Боса та А. Мельник, які акцентують увагу на важливості ефективного управління логістичними процесами для забезпечення стабільності функціонування суб'єктів господарювання [1]. A. Przybyłowski та ін. аналізують трансформацію логістичних процесів під впливом цифрових технологій [4], а R. Jones і D. Feoktistov досліджують кіберзагрози в ланцюгах постачання та їх вплив на безпеку функціонування систем постачання [5]. Подібної проблематики стосуються праці A Faisal та ін., у яких розглянуто сучасні кіберзагрози в цифрових ланцюгах постачання та стратегічні підходи до їх мінімізації [6]. M. Clavijo Mesa та ін. приділяють увагу наслідкам кібератак та інструментам захисту морських ланцюгів постачання [7], а P. Mora Lozano та J. Montoya-Torres досліджують роль систем управління безпекою в глобальних ланцюгах постачання [8]. Вагомий внесок у дослідження безпеки логістичних систем зробили K.-F Cheung та ін., які окреслили перспективні напрями розвитку кібербезпеки в логістиці та управлінні ланцюгами постачання [9]. Окрему увагу сучасні науковці приділяють ризикам втрати вантажів і незаконного заволодіння ними. Зокрема, M. Klopott досліджує крадіжки вантажів як системний ризик глобальних ланцюгів постачання [10], а P. Panjee та ін. аналізують причини, наслідки та напрями мінімізації ризиків втрати вантажів під час автомобільних перевезень [11].

Водночас більшість наявних досліджень зосереджена переважно на питаннях кібербезпеки, управління логістичними ризиками або окремих загрозах функціонування ланцюгів постачання. Недостатньо уваги приділено комплексному дослідженню шахрайства в логістичній діяльності як чинника загроз економічній безпеці підприємств, а також систематизації сучасних шахрайських схем і практичних інструментів їх запобігання, що обумовлює необхідність подальших наукових досліджень у цьому напрямі.

Мета статті. Метою статті є розвиток теоретико-прикладних засад забезпечення економічної безпеки підприємств шляхом дослідження шахрайських ризиків у логістичній діяльності та обґрунтування підходів до їх попередження.

Виклад основного матеріалу дослідження. Однією із суттєвих загроз економічній безпеці підприємств є шахрайство, яке проявляється у навмисних протиправних діях, спрямованих на незаконне отримання матеріальної вигоди, привласнення активів, спотворення інформації або введення в оману контрагентів. В умовах цифровізації бізнес-процесів та ускладнення ланцюгів постачання масштаби та способи здійснення шахрайських дій постійно змінюються, що потребує посилення системи економічної безпеки підприємств [3]. Економічна безпека підприємства характеризує стан захищеності його ресурсів, бізнес-процесів та економічних інтересів від внутрішніх і зовнішніх загроз, що можуть негативно впливати на фінансову стійкість, конкурентоспроможність та безперервність діяльності. У цьому контексті шахрайство виступає одним із дестабілізуючих чинників, здатних спричиняти прямі фінансові втрати, порушення операційної діяльності, зниження рівня довіри з боку партнерів та погіршення ділової репутації [12].

Особливу актуальність проблема шахрайства набуває у сфері логістики, яка характеризується значною кількістю учасників, складністю інформаційних та матеріальних потоків, використанням цифрових технологій, а також високим рівнем взаємодії із зовнішніми контрагентами. Багаторівнева структура логістичних процесів створює додаткові можливості для виникнення різних шахрайських схем, пов'язаних із перевезенням вантажів, оформленням документів, взаєморозрахунками, використанням інформаційних систем та управлінням запасами [13]. Тому доцільним є узагальнення найбільш поширених проявів шахрайства, характерних для логістичної діяльності підприємств, що представлено в табл. 1.

Аналіз наведених шахрайських схем свідчить, що найбільш поширеними загрозами для логістичних підприємств є використання підставних перевізників, фіктивних експедиторських компаній та підроблення супровідних документів. Такі схеми здебільшого пов'язані з незаконним заволодінням вантажем або грошовими коштами та характеризуються високим рівнем латентності [14; 15]. Значного поширення також набули маніпуляції з банківськими реквізитами та оформленням фіктивних перевезень, що призводять до фінансових втрат і ускладнюють процеси встановлення відповідальних осіб. Окрему групу становлять кіберзагрози, зокрема злом акаунтів на біржах перевезень та AI-шахрайство. Розвиток цифрових технологій і застосування штучного інтелекту створюють нові можливості для підроблення документів, голосових повідомлень та ділового листування, що суттєво підвищує ризики введення в оману працівників і контрагентів [16]. Залежно від характеру та масштабів шахрайських дій негативні наслідки

Таблиця 1

Основні шахрайські схеми в логістичній діяльності

Вид шахрайської схеми	Сутність схеми	Типова ситуація в логістиці
Підставний перевізник	Шахраї видають себе за реального або надійного перевізника	На завантаження прибуває транспорт із підробленими документами, після чого вантаж зникає
Фіктивна експедиторська компанія	Створюється компанія або профіль на біржі перевезень для отримання замовлень	Після отримання передоплати або вантажу представники компанії припиняють зв'язок
Підробка документів	Використання фальшивих договорів, печаток, CMR, рахунків або довіреностей	Договір підписується нібито від імені реальної компанії, але фактично без її згоди
Підміна банківських реквізитів	Шахраї надсилають нові реквізити для оплати	Кошти перераховуються не реальному перевізнику, а на рахунок шахраїв
Фіктивне перевезення	Документальне оформлення перевезення, яке фактично не виконувалося	Виставляються рахунки та накладні без реального руху вантажу
Фіктивна втрата вантажу	Імітація втрати або пошкодження вантажу для отримання компенсації	Сторона заявляє про втрату товару, хоча фактичні обставини не підтверджені
Злом акаунтів на біржах перевезень	Використання сторінок компаній із позитивною репутацією	Замовник довіряє профілю з рейтингом, але фактично спілкується із шахраями
AI-шахрайство	Використання штучного інтелекту для підробки голосу, документів або ділового листування	Працівник отримує фальшивий дзвінок або лист нібито від керівника чи партнера

Джерело: побудовано за [14–16]

можуть поширюватися на фінансову, операційну, інформаційну, кадрову та репутаційну складові економічної безпеки – табл. 2.

Наведені дані свідчать, що шахрайство в логістичній діяльності має комплексний характер і негативно впливає практично на всі складові економічної безпеки підприємства. Найбільш відчутними є фінансові наслідки, які проявляються у прямих збитках, необхідності повторної оплати транспортних послуг, відшкодуванні вартості втраченого вантажу та додаткових витратах на юридичний супровід. Водночас втрати матеріальних цінностей і порушення договірних зобов'язань можуть спричиняти конфлікти між учасниками ланцюга постачання та ускладнювати взаємодію з контрагентами. Не менш важливими є операційні та інформаційні ризики. Зриви поставок, простої транспорту, затримки на митниці або необхідність проведення додаткових перевірок призводять до порушення безперервності логістичних процесів та зростання витрат. Поширення цифрових технологій одночасно підвищує вразливість підприємств до кіберзагроз,

Таблиця 2

Вплив шахрайства на економічну безпеку логістичних підприємств

Напрям впливу	Можливі наслідки для підприємства	Приклад прояву
Фінансова безпека	Втрата коштів, неоплачені перевезення, додаткові витрати	Компенсація простою транспорту або повторна оплата послуг
Майнова безпека	Втрата, пошкодження або незаконне привласнення вантажу	Зникнення товару після завантаження
Договірна безпека	Спори між замовником, експедитором і перевізником	Сторони не можуть встановити, хто є реальним виконавцем угоди
Репутаційна безпека	Втрата довіри клієнтів і партнерів	Компанію помилково звинувачують у шахрайських діях
Операційна безпека	Зрив строків доставки, простої транспорту, порушення маршруту	Завантажені автомобілі зупиняються біля кордону до з'ясування обставин
Інформаційна безпека	Злом пошти, акаунтів, підміна даних у документах	Шахраї використовують електронну пошту партнера
Правова безпека	Судові спори, претензії, необхідність юридичного супроводу	Компанія змушена доводити добросовісність своїх дій
Кадрова безпека	Помилки персоналу через поспіх або недостатню перевірку	Менеджер погоджує перевезення без глибокої перевірки контрагента

Джерело: побудовано авторами

пов'язаних зі зломом електронної пошти, акаунтів на біржах перевезень і підміною інформації в документах. Крім того, шахрайські інциденти можуть завдавати суттєвої шкоди діловій репутації, знижувати рівень довіри з боку клієнтів і партнерів та спричиняти виникнення судових спорів. Таким чином, наслідки шахрайства виходять за межі окремих фінансових втрат і створюють загрози для стабільності функціонування підприємства в цілому.

Практика правоохоронних органів та судів свідчить, що значна частина спорів у сфері логістики пов'язана з використанням фіктивних перевізників, підробленням документів, незаконним заволодінням вантажами та іншими формами шахрайства – табл. 3.

Аналіз наведених прикладів свідчить, що переважна більшість шахрайських схем у логістичній діяльності пов'язана з використанням підроблених документів, фіктивних перевізників та неналежною перевіркою контрагентів. Зокрема, у справі Новобаварського районного суду м. Харкова встановлено факт заволодіння вантажем вартістю понад 2,2 млн грн шляхом використання документів стороннього ФОП та неправдивих відомостей про транспортний засіб і водія. Подібні випадки підтверджують, що навіть наявність формально оформлених документів не гарантує захисту від шахрайства за відсутності належної процедури верифікації учасників перевезення.

Окрему групу ризиків становлять порушення договірних зобов'язань і недотримання вимог транспортного законодавства, що підтверджується рішеннями Господарського суду Закарпатської області та Дніпропетровського окружного адміністративного суду. Хоча такі випадки не завжди мають ознаки класичного шахрайства, вони негативно впливають на економічну безпеку підприємств, спричиняючи фінансові втрати, затримки поставок та додаткові витрати на правовий супровід.

Водночас практика Німеччини та США демонструє зростання масштабів цифрового

Таблиця 3

Судова та правоохоронна практика щодо шахрайства і ризиків у сфері логістики

№	Судова справа (країна)	Суть шахрайської схеми або порушення	Наслідки та висновки для логістичних підприємств
1	Справа № 639/6216/18, Новобаварський районний суд м. Харкова, 20.10.2025 (Україна)	Обвинувачений, використовуючи документи стороннього ФОП, підроблені документи на транспортний засіб і водія, уклав договір транспортно-експедиційного обслуговування без наміру виконання зобов'язань та заволодів вантажем ТОВ «УКРІНВЕСТ 3000» вартістю 2 244 123,91 грн.	Суд визнав особу винною за ч. 4 ст. 190 КК України. Справа підтверджує необхідність перевірки перевізників, документів та контрагентів перед передачею вантажу.
2	Справа № 907/1006/24, Господарський суд Закарпатської області, 05.03.2025 (Україна)	Невиконання перевізником умов транспортної заявки та договору перевезення.	Суд стягнув штраф за порушення договірних зобов'язань. Справа підкреслює значення належного договірного оформлення логістичних операцій.
3	Справа № 160/25589/25, Дніпропетровський окружний адміністративний суд, 24.11.2025 (Україна)	Оскарження постанов Укртрансбезпеки про накладення адміністративно-господарських штрафів.	Суд підтримав позицію Укртрансбезпеки, підтвердивши важливість дотримання вимог законодавства у сфері автомобільних перевезень.
4	Земельний суд м. Дюссельдорф, 2026 (Німеччина)	Організована група використовувала реквізити реальної транспортно-експедиційної компанії та підроблені електронні адреси, отримувала замовлення через біржі перевезень і привласнювала вантажі.	Учасники схеми отримали покарання від 3 до понад 5 років позбавлення волі. Встановлено важливість перевірки електронних адрес, страхування та контрагентів.
5	United States District Court, Southern District of Georgia, 2026 (США)	Працівник логістичної компанії та власник транспортної компанії створювали фіктивні транспортні замовлення та виставляли підроблені рахунки.	Збитки склали понад 821 тис. дол. США. Винні засуджені за шахрайство. Справа демонструє значення внутрішнього контролю та моніторингу операцій.
6	Supreme Court of the State of New York, 2026 (США)	Злочинна група, використовуючи дані реальних перевізників і брокерів, викрадала вантажі через онлайн-платформи та перепродавала їх на чорному ринку.	Загальна вартість викрадених товарів перевищила 5 млн дол. США. Справа свідчить про зростання кіберризиків та необхідність захисту цифрових логістичних платформ.

Джерело: побудовано за [17–20]

шахрайства у сфері логістики. Використання реквізитів реальних транспортно-експедиційних компаній, фальшивих електронних адрес, онлайн-бірж перевезень і фіктивних транспортних замовлень призводить до значних збитків, які можуть обчислюватися мільйонами доларів. Це свідчить про те, що поряд із традиційними ризиками зростає роль кіберзагроз та необхідність посилення контролю за інформаційною безпекою логістичних процесів.

Отже, судова та правоохоронна практика підтверджує, що ефективна протидія шахрайству потребує комплексного підходу, який поєднує перевірку контрагентів, удосконалення внутрішнього контролю, використання цифрових засобів моніторингу та підвищення рівня захисту інформаційних ресурсів. Наведені інструменти запобігання шахрайству – табл. 4 – свідчать, що ефективна протидія шахрайству в логістичній діяльності повинна мати комплексний характер і охоплювати організаційні, правові, інформаційні та технологічні заходи. Особливе значення має перевірка контрагентів, оскільки значна частина шахрайських схем пов'язана саме з діяльністю фіктивних перевізників, підробленими документами та використанням недостовірних відомостей про учасників логістичних операцій.

Офіційне листування та застосування електронного документообігу сприяють підвищенню прозорості взаємовідносин між сторонами та забезпечують належну доказову базу у разі виникнення спорів.

Зростання кількості кіберінцидентів обумовлює необхідність посилення захисту електронних комунікацій, перевірки банківських реквізитів та використання двофакторної автентифікації. Не менш важливими є внутрішні регламенти перевірки та навчання персоналу, оскільки людський фактор залишається однією з основних причин успішної реалізації шахрайських схем. Своєчасне виявлення підозрілих операцій та додатковий контроль ризикових угод дають змогу мінімізувати потенційні збитки ще до настання негативних наслідків. Узагальнюючи результати дослідження, можна зазначити, що шахрайство в логістичній діяльності є одним із вагомих чинників загроз економічній безпеці підприємств, а його прояви набувають дедалі більшої різноманітності під впливом цифровізації та розвитку інформаційних технологій.

При цьому аналіз судової практики та найбільш поширених шахрайських схем свідчить, що значна частина збитків виникає ще на етапі вибору та перевірки учасників логістичної операції. У зв'язку з цим доцільним є застосування методики комплексної верифікації учасників логістичної операції, яка передбачає послідовну перевірку юридичних, фінансових, документальних, транспортних, інформаційних та репутаційних аспектів співпраці – табл. 5.

Запропонований підхід може застосовуватися як до нових контрагентів, так і під час виконання окремих перевезень, що дає змогу своєчасно виявляти потенційні ризики та мінімізувати ймовірність реалізації шахрайських схем. Використання методики комплексної верифікації учасників логістичної операції сприятиме підвищенню рівня економічної безпеки підприємств, зниженню фінансових

Таблиця 4

Інструменти запобігання шахрайству в логістичній діяльності

Інструмент протидії	Зміст заходу	Результат
Перевірка контрагентів	Аналіз реєстраційних даних, бенефіціарів, судової історії, відгуків і репутації	Зменшення ризику співпраці з фіктивними компаніями
Офіційне листування	Фіксація всіх домовленостей через корпоративну пошту	Можливість підтвердити умови співпраці у разі спору
Електронний документообіг	Використання КЕП та захищених цифрових сервісів	Зниження ризику підробки печаток і договорів
Перевірка банківських реквізитів	Підтвердження реквізитів через офіційні канали зв’язку	Запобігання переказу коштів шахраям
Страхування вантажів	Оформлення страхового захисту на час перевезення	Компенсація можливих збитків у разі втрати або пошкодження
Двофакторна автентифікація	Захист пошти, акаунтів на біржах і внутрішніх систем	Зменшення ризику злому облікових записів
Внутрішній регламент перевірки	Запровадження обов’язкового чек-листа перед укладенням угоди	Уніфікація дій працівників і зниження впливу людського фактора
Навчання персоналу	Ознайомлення працівників із типовими шахрайськими схемами	Підвищення уважності до red flags у щоденній роботі
Контроль підозрілих операцій	Зупинка або додаткова перевірка операцій із високим ризиком	Своєчасне виявлення шахрайства до виникнення збитків

Джерело: побудовано авторами

Таблиця 5

Методика комплексної верифікації учасників логістичної операції

Напрям перевірки	Об'єкт перевірки	Інструменти перевірки	Контрольні критерії	Результат
Юридична верифікація	Перевізник, експедитор, замовник	ЄДР, YouControl, судовий реєстр	Термін діяльності, види діяльності, наявність судових спорів	Підтвердження правосуб'єктності та зниження ризику співпраці з фіктивними компаніями
Контактна верифікація	Телефони, електронна пошта, вебсайт	Корпоративні канали зв'язку, перевірка домену	Відповідність контактних даних офіційній інформації	Підтвердження автентичності комунікацій
Фінансова верифікація	Банківські реквізити	Офіційні листи, телефонне підтвердження	Відсутність неузгоджених змін реквізитів	Зниження ризику помилкових платежів
Документальна верифікація	Договір, CMR, довіреність, ліцензії	Зіставлення реквізитів, КЕП	Узгодженість даних у документах	Мінімізація ризику використання підроблених документів
Транспортна верифікація	Автомобіль, водій, номерні знаки	Фотофіксація, перевірка документів водія	Відповідність фактичних даних попередньо наданій інформації	Підтвердження законності перевезення
Репутаційна верифікація	Ділова репутація контрагента	Біржі перевезень, відгуки, попередній досвід співпраці	Наявність позитивної історії взаємодії	Зменшення ймовірності неналежного виконання зобов'язань
Операційна верифікація	Умови перевезення та оплати	Внутрішній регламент підприємства	Відповідність ціни, строків та маршруту ринковим умовам	Виявлення нетипових та потенційно ризикових операцій

Джерело: побудовано авторами

втрат та посиленню довіри між учасниками ланцюгів постачання.

Висновки. Шахрайство в логістичній діяльності є суттєвим джерелом загроз економічній безпеці підприємств, оскільки його наслідки поширюються на фінансову, майнову, операційну, інформаційну, правову та репутаційну складові. Найбільш поширеними проявами залишаються використання фіктивних перевізників, підроблення документів, маніпуляції з банківськими реквізитами, незаконне заволодіння вантажами та кіберзлочинність. Аналіз судової та правоохоронної практики засвідчив актуальність проблеми як для України, так і для зарубіжних країн, а також зростання ролі цифрових ризиків у логістичних процесах. Підвищення рівня економічної безпеки підприємств потребує комплексного застосування інструментів перевірки контрагентів, внутрішнього контролю, захисту інформаційних ресурсів та підвищення обізнаності персоналу щодо сучасних шахрайських схем. З метою посилення превентивного характеру системи економічної безпеки запропоновано методику комплексної верифікації учасників логістичної операції, яка передбачає послідовну юридичну, фінансову, документальну, транспортну, репутаційну та операційну перевірку контрагентів і може бути адаптована до діяльності підприємств різних масштабів. Перспективи подальших досліджень пов'язані з оцінюванням впливу штучного інтелекту та цифрових технологій на трансформацію шахрайських ризиків у логістичній діяльності.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Боса І., Мельник А. Управління логістичними процесами у забезпеченні економічної безпеки підприємства. *Modeling the Development of the Economic Systems.* 2024. № 3. С. 202–208. DOI: https://doi.org/10.31891/mdes/2024-13-28

2. Селіщев С.В. Ідентифікація ризику шахрайства в управлінні проєктами у транспортно-логістичному бізнесі. *Економіка. Фінанси. Право.* 2021. № 5. С. 13–15. DOI: https://doi.org/10.37634/efp.2021.5.3

3. Канцедал Н. А., Лега О. В., Морозов Є. О. Цифровізація логістики: нові технології для покращення управління та оптимізації. *Економічний простір*. 2025. № 199. С. 45–51. DOI: https://doi.org/10.30838/EP.199.45-51

4. Przybyłowski A., Suchanek M., Miszewski P. COVID-19 Pandemic Impact on a Global Liner Shipping Company Employee Work Digitalization. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*. 2022. Vol. 16, № 4. P. 759–765. DOI: https://doi.org/10.12716/1001.16.04.18

5. Jones R., Feoktistov D. Cybersecurity vulnerabilities in the food supply chain and their impact on food security: a systematic literature review. *Global Smart Food Systems.* 2025. Vol. 1, № 1. P. 1–27. DOI: https://doi.org/10.1108/GSFS-10-2024-0001

6. Faisal A., Cupiadi H., Sopannadi. Cybersecurity in Digital Supply Chains: A Narrative Review of Threats

and Strategic Frameworks for Sustainable Logistics. *Sinergi International Journal of Logistics*. 2024. Vol. 2, № 3. P. 174–186. DOI: https://doi.org/10.61194/sijl.v2i3.728

7. Clavijo Mesa M.V., Patino-Rodriguez C.E., Guevara Carazas F.J. Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information.* 2024. Vol. 15, № 11. Art. 710. DOI: https://doi.org/10.3390/info15110710

8. Mora Lozano P.E., Montoya-Torres J.R. Global Supply Chains Made Visible through Logistics Security Management. *Logistics*. 2024. Vol. 8, № 1. Art. 6. DOI: https://doi.org/10.3390/logistics8010006

9. Cheung K.-F., Bell M.G.H., Bhattacharjya J. Cybersecurity in Logistics and Supply Chain Management: An Overview and Future Research Directions. *Transportation Research Part E: Logistics and Transportation Review*. 2021. Vol. 146. Art. 102217. DOI: https://doi.org/10.1016/j.tre.2020.102217

10. Klopott M. Cargo Theft as a Systemic Risk in Global Supply Chains: Data, Modus Operandi and Emerging Trends (2019–2025). *European Research Studies Journal.* 2025. Vol. XXVIII, № 4. P. 1298–1313. URL: https://ersj.eu/journal/4219 (дата звернення: 22.06.2026).

11. Panjee P., Kaewchueaknang V., Amornsawadwatana S. A Systematic Literature Review of Cargo Loss Risks in Road Transportation: Impacts and Future Directions. *Safety.* 2025. Vol. 11, № 1. Art. 20. DOI: https://doi.org/10.3390/safety11010020

12. Лега О. В., Тараненко Я. І. Інтеграція логістики і виробництва в системі управління собівартістю та стійким розвитком підприємства. *Сталий розвиток економіки.* 2025. № 3 (54). С. 154–161. DOI: https://doi.org/10.32782/2308-1988/2025-54-23

13. Лега О. В., Канцедал Н. А., Богаєнко О. С. Система управління паливно-мастильними матеріалами як інструмент зменшення ризиків у діяльності підприємств агробізнесу. *Підприємництво та інновації*. 2025. № 34. С. 28–36. URL: http://ei-journal.in.ua/index.php/journal/article/download/734/712 (дата звернення: 22.06.2026).

14. Шахрайство: нова схема у сфері логістики. *ITL Group* : вебсайт. URL: https://itl-ltd.com/blog/view/shahrayistvo-nova-shema-u-sferi-logistiki/ (дата звернення: 22.06.2026).

15. Шахрайство в логістиці: як не стати жертвою. *TradeMasterGroup* : вебсайт. URL: https://trademaster.ua/rukov_ved/313188 (дата звернення: 22.06.2026).

16. Malinski D. AI-Driven Fraud in Logistics. *LinkedIn*. 29 July 2025. URL: https://www.linkedin.com/pulse/ai-driven-fraud-logistics-demitri-malinski-sflye/ (дата звернення: 22.06.2026).

17. Каталог судових рішень України. *YouControl* : вебсайт. URL: https://youcontrol.com.ua/catalog/court/ (дата звернення: 22.06.2026).

18. Kulikowska-Wielgus A. Bogus carriers jailed after posing as well-known forwarder and stealing €800,000 of cargo. *Trans.INFO*. 20 May 2026. URL: https://trans.info/en/bogus-carriers-jailed-476869 (дата звернення: 22.06.2026).

19. Two men sentenced to prison for scheme to defraud Savannah Port logistics service. *United States Attorney's Office Southern District of Georgia*. 03 April 2026. URL: https://www.justice.gov/usao-sdga/pr/two-men-sentenced-prison-scheme-defraud-savannah-port-logistics-service (дата звернення: 22.06.2026).

20. Eight alleged US thieves indicted for stealing $5m worth of cheese, beef and cigarettes. *The Guardian*. 04 June 2026. URL: https://www.theguardian.com/us-news/2026/jun/04/eight-thieves-indicted-5m-cheese-beef-cigarettes (дата звернення: 22.06.2026).

REFERENCES:

1. Bosa I., Melnyk A. (2024) Upravlinnia lohistychnymy protsesamy u zabezpechenni ekonomichnoi bezpeky pidpryiemstva [Management of Logistics Processes in Ensuring the Economic Security of an Enterprise]. *Modeling the Development of the Economic Systems*, no. 3, pp. 202–208. DOI: https://doi.org/10.31891/mdes/2024-13-28

2. Selishchev S.V. (2021) Identyfikatsiia ryzyku shakhraistva v upravlinni proiektamy u transportno-lohistychnomu biznesi [Fraud Risk Identification in Project Management in Transport and Logistics Business]. *Ekonomika. Finansy. Pravo – Economy. Finances. Law*, no. 5, pp. 13–15. DOI: https://doi.org/10.37634/efp.2021.5.3

3. Kantsedal N.A., Leha O.V., Morozov Ye.O. (2025) Tsyfrovizatsiia lohistyky: novi tekhnolohii dlia pokrashchennia upravlinnia ta optymizatsii [Digitalization of Logistics: New Technologies for Improving Management and Optimization]. *Ekonomichnyi prostir – Economic Scope*, no. 199, pp. 45–51. DOI: https://doi.org/10.30838/EP.199.45-51

4. Przybyłowski A., Suchanek M., Miszewski P. (2022) COVID-19 Pandemic Impact on a Global Liner Shipping Company Employee Work Digitalization. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 16, no. 4, pp. 759–765. DOI: https://doi.org/10.12716/1001.16.04.18

5. Jones R., Feoktistov D. (2025) Cybersecurity vulnerabilities in the food supply chain and their impact on food security: a systematic literature review. *Global Smart Food Systems*, vol. 1, no. 1, pp. 1–27. DOI: https://doi.org/10.1108/GSFS-10-2024-0001

6. Faisal A., Cupiadi H., Sopannadi (2024) Cybersecurity in Digital Supply Chains: A Narrative Review of Threats and Strategic Frameworks for Sustainable Logistics. *Sinergi International Journal of Logistics*, vol. 2, no. 3, pp. 174–186. DOI: https://doi.org/10.61194/sijl.v2i3.728

7. Clavijo Mesa M.V., Patino-Rodriguez C.E., Guevara Carazas F.J. (2024) Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information*, vol. 15, no. 11, art. 710. DOI: https://doi.org/10.3390/info15110710

8. Mora Lozano P.E., Montoya-Torres J.R. (2024) Global Supply Chains Made Visible through Logistics Security Management. *Logistics,* vol. 8, no. 1, art. 6. DOI: https://doi.org/10.3390/logistics8010006

9. Cheung K.-F., Bell M.G.H., Bhattacharjya J. (2021) Cybersecurity in Logistics and Supply Chain Management: An Overview and Future Research Directions. *Transportation Research Part E: Logistics and Transportation Review*, vol. 146, art. 102217. DOI: https://doi.org/10.1016/j.tre.2020.102217

10. Klopott M. (2025) Cargo Theft as a Systemic Risk in Global Supply Chains: Data, Modus Operandi and Emerging Trends (2019–2025). *European Research Studies Journal*, vol. XXVIII, issue 4, pp. 1298–1313. Available at: https://ersj.eu/journal/4219 (accessed June 22, 2026).

11. Panjee P., Kaewchueaknang V., Amornsawadwatana S. (2025) A Systematic Literature Review of Cargo Loss Risks in Road Transportation: Impacts and Future Directions. *Safety*, vol. 11, no. 1, art. 20. DOI: https://doi.org/10.3390/safety11010020

12. Leha O.V., Taranenko Ya.I. (2025) Intehratsiia lohistyky i vyrobnytstva v systemi upravlinnia sobivartistiu ta stiikym rozvytkom pidpryiemstva [Integration of Logistics and Production in the Cost Management and Sustainable Development System of Enterprises]. *Stalyi rozvytok ekonomiky – Sustainable Economic Development*, no. 3 (54), pp. 154–161. DOI: https://doi.org/10.32782/2308-1988/2025-54-23

13. Leha O.V., Kantsedal N.A., Bohaienko O.S. (2025) Systema upravlinnia palyvno-mastylnymy materialamy yak instrument zmenshennia ryzykiv u diialnosti pidpryiemstv ahrobiznesu [Fuel and Lubricant Management System as a Tool for Risk Reduction in Agribusiness Enterprises]. *Pidpryiemnytstvo ta innovatsii – Entrepreneurship and Innovation*, no. 34, pp. 28–36. Available at: http://ei-journal.in.ua/index.php/journal/article/download/734/712 (accessed June 22, 2026).

14. Shakhraistvo: nova skhema u sferi lohistyky [Fraud: A New Scheme in the Field of Logistics]. *ITL Group*. Available at: https://itl-ltd.com/blog/view/shahrayistvo-nova-shema-u-sferi-logistiki/ (accessed June 22, 2026).

15. Shakhraistvo v lohistytsi: yak ne staty zhertvoiu [Fraud in Logistics: How Not to Become a Victim]. *TradeMasterGroup.* Available at: https://trademaster.ua/rukov_ved/313188 (accessed June 22, 2026).

16. Malinski D. (2025) AI-Driven Fraud in Logistics. *LinkedIn*. Available at: https://www.linkedin.com/pulse/ai-driven-fraud-logistics-demitri-malinski-sflye/ (accessed June 22, 2026).

17. Kataloh sudovykh rishen Ukrainy [Catalogue of Court Decisions of Ukraine]. *YouControl.* Available at: https://youcontrol.com.ua/catalog/court/ (accessed June 22, 2026).

18. Kulikowska-Wielgus A. (2026) Bogus carriers jailed after posing as well-known forwarder and stealing €800,000 of cargo. *Trans.INFO*. Available at: https://trans.info/en/bogus-carriers-jailed-476869 (accessed June 22, 2026).

19. Two men sentenced to prison for scheme to defraud Savannah Port logistics service (2026). *United States Attorney's Office Southern District of Georgia.* Available at: https://www.justice.gov/usao-sdga/pr/two-men-sentenced-prison-scheme-defraud-savannah-port-logistics-service (accessed June 22, 2026).

20. Eight alleged US thieves indicted for stealing $5m worth of cheese, beef and cigarettes (2026). *The Guardian*. Available at: https://www.theguardian.com/us-news/2026/jun/04/eight-thieves-indicted-5m-cheese-beef-cigarettes (accessed June 22, 2026).

Дата надходження статті: 24.06.2026
Дата прийняття статті до публікації: 21.07.2026
Дата публікації статті: 23.07.2026