Міністерство освіти і науки України
Державний біотехнологічний університет
Національний авіаційний університет
Національний технічний університет «Харківський політехнічний інститут»
Національний університет «Полтавська політехніка» ім. Юрія Кондратюка
Національний університет «Чернігівська політехніка»
Національна академія статистики, обліку та аудиту
Харківський національний університет ім. В.Н. Каразіна
Харківський національний економічний університет ім. Семена Кузнеця
Львівський торговельно-економічний університет
Академія Сілезії (Республіка Польща)
Варшавський університет природничих наук (Республіка Польща)
Клайпедський університет прикладних наук (Литовська Республіка)
Естонський університет прикладних наук для підприємництва (Естонська Республіка)
Національний контактний пункт «Європейський інститут технологій
та інновацій» програми Horizon Europe
ГО «Міжнародна фундація науковців та освітян»
Міжнародна асоціація з економіки (Відень, Австрія)

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ СТАЛОГО РОЗВИТКУ ЕКОНОМІКИ: ПРОБЛЕМИ, ПЕРСПЕКТИВИ, МІЖНАРОДНИЙ ДОСВІД

Матеріали
VI Міжнародної науково-практичної конференції

10 жовтня 2025 року

Харків
ДБТУ
2025

automation. On the one hand, this may lead to job losses in certain areas, but on the other hand, it creates new opportunities for highly skilled professionals.

Thus, innovation and information technology have become key factors in the transformation of business and international economic relations. They open up unlimited opportunities for businesses, allowing them to enter global markets, improve management efficiency and ensure transparency of financial transactions. However, along with the opportunities come growing risks associated with cybersecurity, the digital divide and the transformation of the labour market. In today's world, success depends on the ability of businesses and countries to adapt to new realities. Those who actively innovate become leaders in the global economy, while those who ignore technological changes risk being left on the side-lines of global development.

Thus, the future of the global economy depends on how harmoniously humanity will be able to integrate innovations into all spheres of life, maintaining a balance between technological progress and social responsibility. Those who are able to adapt to the new realities will not only secure competitive advantages, but will also shape the future of the digital economy at the international level.

Reference:

1. Baula O., Liutak O., Fedyshyn V. (2024). Rozvytok elektronnoi komertsii ta yii vplyv na vitchyzniane ta mizhnarodne biznes-seredovyshche. *Ekonomichnyi prostir*, 2024. No 191. P. 285-289. DOI: https://doi.org/10.32782/2224-6282/191-47 (accessed October 1, 2025) (in Ukrainian).

КІБЕРЗАГРОЗИ В УМОВАХ ЦИФРОВІЗАЦІЇ ЛОГІСТИКИ: МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ

Биба В.В., канд. техн. наук, доц.
НУ «Полтавська політехніка ім. Юрія Кондратюка
Пінчук Н.М., канд. техн. наук, доц.
Політехнічний університет ді Барі
Андрєєв Д.С., здоб. ВО
Москальов О.В., здоб. ВО
НУ «Полтавська політехніка ім. Юрія Кондратюка

У сучасних умовах глобалізації та інтенсивного розвитку цифрових технологій логістика поступово перетворюється з традиційної системи перевезення і зберігання товарів на високотехнологічний комплекс, який базується на інтеграції інформаційних рішень. Сьогодні важко уявити логістичну компанію без застосування систем управління складом, транспортними процесами, без використання GPS-навігації, Інтернету речей, хмарних сервісів чи блокчейн-рішень. Усе це дозволяє підвищувати ефективність роботи, робити ланцюги постачання більш прозорими та гнучкими, забезпечувати клієнтів актуальною інформацією про стан їхніх замовлень.

Цифровізація логістики має чимало позитивних сторін, але водночас вона суттєво збільшує рівень ризику. Кіберзагрози у цій сфері відрізняються своєю різноманітністю та масштабністю, адже вони можуть впливати як на окрему компанію, так і на глобальні ланцюги постачання [1, 2 ,3].

Сучасна логістика активно інтегрує системи управління великими даними, які допомагають аналізувати транспортні потоки, прогнозувати попит і оптимізувати маршрути. Але саме великі дані часто стають цінною мішенню для зловмисників. Якщо інформація про переміщення вантажів або особисті дані клієнтів потрапляють до рук хакерів, це може стати основою для шахрайських схем або навіть промислового шпигунства.

Окрему увагу слід звернути на проблему взаємозалежності в логістичних ланцюгах. Логістика функціонує як єдина мережа: якщо один учасник стає жертвою кібератаки, це може вплинути й на інших партнерів. Наприклад, якщо система митного оформлення або великий транспортний хаб зазнає кібератаки, це призведе до затримки чи навіть зриву постачань у цілій країні або регіоні. Тобто мова йде не лише про локальні проблеми компанії, а про серйозні системні ризики [1, 2].

Ще одним напрямом є ризики, пов’язані з автоматизацією та використанням робототехніки у складах. Багато сучасних логістичних центрів уже застосовують автоматизовані конвеєри, роботизовані візки та безпілотні транспортні засоби. У разі злому чи втручання в роботу таких систем можливе не тільки порушення процесу обробки замовлень, а й створення фізичної загрози безпеці працівників. Це підкреслює, що кібербезпека в логістиці тісно пов’язана з технікою безпеки на виробництві.

Не менш важливим фактором є розвиток електронної комерції. Зростання онлайн-замовлень створює значне навантаження на логістичні компанії, які мають працювати швидко та безперебійно. У такому середовищі навіть короткочасний збій у роботі інформаційної системи через кібератаку може призвести до втрати клієнтів і підриву довіри. Тому захист інформації стає елементом не лише технічної, але й маркетингової стратегії компаній.

Варто відзначити, що цифрова логістика активно використовує хмарні сервіси для зберігання та обробки інформації. Хоча хмарні технології забезпечують зручність і масштабованість, вони одночасно створюють нові вразливості. Компанії змушені покладатися на постачальників хмарних рішень, а це означає, що відповідальність за безпеку розподіляється між кількома сторонами. Таким чином, виникає необхідність у чітких договорах, що регламентують питання кіберзахисту і відповідальності за інциденти [3].

У цілому можна зробити висновок, що основні кіберзагрози в логістиці стосуються як технічної інфраструктури (GPS, IoT, автоматизація), так і людського фактора (недостатня обізнаність персоналу, помилки користувачів). Подолати їх можна лише за умови комплексного підходу, який враховує всі аспекти роботи логістичної системи.

Ще одним вразливим елементом є пристрої Інтернету речей. У логістиці вони використовуються для контролю температури, місцезнаходження чи технічного стану вантажів, однак через недостатній рівень захисту можуть

стати «вхідними воротами» для зловмисників. Після злому таких пристроїв відкривається можливість не лише викрадення інформації, але й створення перешкод у роботі всієї логістичної мережі.

Не менш небезпечною є проблема витоку та підробки даних. Логістика оперує великими масивами інформації – від особистих даних клієнтів до контрактів і фінансових документів. Якщо ці дані потрапляють у чужі руки, це може спричинити серйозні збитки та підірвати довіру партнерів.

Варто згадати і про загрозу з боку шкідливого програмного забезпечення, зокрема програм-вимагачів. Відомий приклад – атака вірусу NotPetya у 2017 році, яка вразила міжнародну компанію Maersk. Унаслідок цього логістичні процеси були повністю зупинені, а фінансові втрати сягнули сотень мільйонів доларів.

Не варто забувати і про так званий людський фактор. Фішингові листи та прийоми соціальної інженерії залишаються одним із найпоширеніших способів доступу до внутрішніх систем компаній. Часто саме співробітники, не маючи достатнього рівня обізнаності, стають мимовільними «помічниками» у здійсненні кібератак.

Для зменшення ймовірності таких загроз логістичні компанії змушені впроваджувати комплексні системи захисту. Це не лише технічні рішення, але й організаційні заходи, які охоплюють усі рівні діяльності підприємства.

Одним із ключових напрямів є регулярний моніторинг і аудит інформаційних систем. Завдяки цьому вдається своєчасно виявляти підозрілу активність та усувати вразливості. Особлива увага приділяється захисту пристроїв Інтернету речей і систем GPS-навігації. Тут важливими є шифрування каналів зв’язку, постійне оновлення програмного забезпечення та використання багаторівневої автентифікації.

Не менш важливим є навчання персоналу. Працівники мають розуміти основні правила кібергігієни: вміти розпізнавати фішингові повідомлення, користуватися надійними паролями, дотримуватися політики безпечного використання корпоративних ресурсів.

Важливим елементом кіберзахисту є розробка планів реагування на інциденти. У випадку атаки компанія має діяти швидко та злагоджено: ізолювати уражені системи, відновити дані з резервних копій, повідомити партнерів і клієнтів. Наявність такого плану дозволяє зменшити негативні наслідки навіть наймасштабніших кібератак [1, 2 ,3].

Все більшого значення набувають інноваційні технології. Наприклад, блокчейн використовується для створення прозорої та захищеної системи обліку логістичних операцій, що унеможливлює підробку даних. Штучний інтелект допомагає виявляти загрози в режимі реального часу та прогнозувати можливі ризики. А хмарні технології забезпечують збереження резервних копій і швидке відновлення роботи після атак.

У Європейському Союзі вже розроблені спеціальні стандарти кіберзахисту для критичної інфраструктури, включно з логістичною сферою. Зокрема, важливу роль відіграє Директива NIS2, яка регулює питання мережевої та інформаційної безпеки. У США активно працює Агентство з

кібербезпеки та безпеки інфраструктури (CISA), що надає рекомендації для транспортної та логістичної галузей.

В Україні тема кібербезпеки у логістиці особливо актуальна через воєнні виклики. Логістичні системи сьогодні є не лише економічними, але й стратегічними об'єктами, від стабільної роботи яких залежить забезпечення армії, промисловості та цивільного населення. Тому питання кіберстійкості набуває національного значення.

Логістика в умовах цифрової трансформації відкриває нові можливості для розвитку бізнесу та економіки, проте водночас стає мішенню для кібератак. Сучасні загрози охоплюють як технічні системи, так і людський фактор. Для того щоб мінімізувати ризики, необхідно впроваджувати комплексний підхід, який поєднує технічний захист, навчання персоналу, використання інноваційних рішень та міжнародний досвід.

Для України це питання особливо важливе, адже від надійності логістики залежить не лише економічна стабільність, а й безпека держави. Саме тому кібербезпека має стати невід'ємною частиною стратегічного розвитку логістичної галузі.

Інформаційні джерела:

1. Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2019). Digital transformation in logistics and maritime transport. *Business Systems Research Journal, 10*(1), 118–128.

2. Штангрет А.М., Семенов В.Ф. (2021). *Інформаційна безпека та кіберзахист: підручник*. Київ: КНЕУ.

3. Гриценко О.А. (2020). Цифровізація логістичних процесів в умовах глобалізації. *Економіка і регіон, №3 (77)*, с. 35–42.

ТРАНСФОРМАЦІЙНІ ВИКЛИКИ ЦИФРОВІЗАЦІЇ У СФЕРІ СТРАХУВАННЯ

Ватаманіца К.В., здоб. ступ. PhD
Державний біотехнологічний університет

Страхова сфера перебуває на етапі активної цифрової трансформації, що зумовлено потребами підвищення конкурентоспроможності та адаптації до змін у поведінці споживачів. Клієнт очікує швидких рішень, прозорих умов, цифрових каналів комунікації та мінімізації бюрократичних процедур. Саме тому цифровізація стає ефективним інструментом розвитку страхових компаній та основою нової моделі функціонування ринку страхових послуг.

Одним із найважливіших напрямів цифрової трансформації є впровадження технологій InsurTech, що поєднують інновації у сфері даних, фінансових інструментів та автоматизованих сервісів. Цифрові платформи дають змогу здійснювати повний цикл обслуговування клієнта в режимі онлайн: від вибору страхового продукту до оформлення договору та