Нагребельна Д.О.,
здобувач освітнього рівня бакалавр
292 «Міжнародні економічні відносини»
Науковий керівник: **Грабчук І.Л.,** д.е.н., доцент,
завідувач кафедри міжнародних відносин і політичного менеджменту
Державний університет «Житомирська політехніка»

ЗАПОБІГАННЯ КІБЕРАТАКАМ В СФЕРІ ЛОГІСТИЦІ

Логістика є однією з найбільш динамічних сфер цифровізації, що переживає трансформацію під впливом новітніх технологій. Сучасні транспортно-логістичні компанії активно впроваджують передові цифрові рішення для оптимізації своїх операцій, підвищення ефективності та забезпечення прозорості. Ці інновації, хоча й відкривають безпрецедентні можливості для зростання та конкурентоспроможності, одночасно породжують значні виклики. Кожен новий елемент цифрової інфраструктури створює додатковий вектор потенційної кібератаки. Усе більша взаємопов'язаність систем та обсяги критичних даних, що знаходяться в цифровому просторі, роблять логістичний сектор привабливою мішенню для кіберзлочинців. Успішна атака може призвести до зриву постачання, фінансових втрат, витоку конфіденційної інформації та значної шкоди репутації.

За даними Державної служби спеціального зв'язку та захисту інформації України, за 2022 рік логістичний сектор входить до п'ятірки найбільш атакованих галузей економіки [1]. Це пов'язано з тим, що логістичний сектор є критично важливими для функціонування держави, зокрема для енергетики, оборони, транспорту та торгівлі . Порушення їхньої роботи може спричинити не лише фінансові збитки, а й зупинку постачання стратегічних ресурсів.

Забезпечення кібербезпеки в логістичних системах передбачає комплекс технічних і організаційних заходів. Одним із базових напрямів є контроль доступу та багатофакторна автентифікація. Сучасні системи управління перевезеннями (TMS) і складами (WMS) потребують надійного розмежування прав користувачів. У великих компаніях, таких як «Нова Пошта», запроваджено інтегровані системи управління доступом, які дозволяють відстежувати дії персоналу в корпоративних мережах. Вимоги до таких систем закріплені в

Методичних рекомендаціях Держспецзв'язку [2].

Також окрему загрозу становлять пристрої Інтернету речей (IoT), що дедалі частіше використовуються у логістиці для контролю температури, місцезнаходження чи стану вантажів. Кожен трекер або RFID-мітка може стати точкою кібервразливості. Тому сучасні українські логістичні компанії впроваджують шифрування каналів передачі даних (TLS/SSL), цифрову авторизацію пристроїв та централізований моніторинг IoT-інфраструктури. TLS/SSL – це саме протоколи шифрування, які забезпечують захист даних під час їх передачи саме через мережу. Вони створюють окремі канали зв'язку між пристроями, шифруючи все що передається [2].

Однак навіть найсучасніші технології не забезпечують ефективного захисту без підготовленого персоналу. Людський фактор залишається найуразливішим елементом кібербезпеки. Тому в Україні впроваджуються обов'язкові програми підвищення кібергігієни відповідно до наказу Держспецзв'язку № 661 від 21 жовтня 2025 р. [3], які передбачають регулярні навчання, тестування працівників і проведення імітаційних фішингових кампаній.

Кібербезпека стала критично важливою для сучасних логістичних компаній, оскільки перехід на цифрові технології робить їх вразливими до різноманітних загроз. Українські оператори постійно стикаються з фішинговими атаками, спробами злому облікових записів працівників та атаками на їхні інформаційні системи. Ці загрози можуть не лише завдати фінансових збитків, а й зупинити роботу всього підприємства, що особливо небезпечно для логістики, де важлива безперервність операцій.

Для захисту компанії впроваджують сучасні методи безпеки. Хоча детальна інформація про внутрішні системи захисту обмежена, очевидно, що посилення кібербезпеки стало обов'язковим стандартом. Водночас ці методи потребують подальшого вивчення як саме впроваджувати системи управління доступом та і які методи захисту найкраще працюють в логістичній сфері.

Список використаних джерел

1. Державна служба спеціального зв'язку та захисту інформації України. Готовність України до нових викликів. Кібербезпека

і зв’язок. URL:https://cip.gov.ua/ua/news/gotovnist-ukrayini-do-novikh-viklikiv-kiberbe zpeka-i-zv-yazok

2. Державна служба спеціального зв’язку та захисту інформації України. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами. URL:https://zakon.rada.gov.ua/rada/show/v0463519-23?utm_source=chatgpt.c om#n10

3. Наказ Адміністрації Держспецзв’язку від 21.10.2025 № 661 «Про затвердження Методичних рекомендацій щодо проведення інструктажів і тренінгів щодо кібергігієни на період призначення на посади державних службовців, працівників органів державної влади та інших державних органів, військовослужбовців, керівників та працівників державних підприємств, установ та організацій». URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-21-10-2025-661-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-provedennya-instruktazhiv-i-treningiv-shodo-kibergigiyeni-na-period-priznachennya-na-posadi-derzhavnikh-sluzhbovciv-pracivnikiv-organiv-derzhavnoyi-vladi-ta-inshikh-derzhavnikh-organiv-viiskovosluzhbovciv-kerivnikiv-ta-pracivnikiv-derzhavnikh-pidpriyemstv-ustanov-ta-organizacii