

ДО ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМОБІЛЬНИХ ВАНТАЖНИХ ПЕРЕВЕЗЕНЬ ПІД ЧАС ДІЇ ВІЙСЬКОВОГО СТАНУ

Забезпечення інформаційної безпеки у сфері автомобільних вантажних перевезень під час воєнного стану є критичним аспектом національної безпеки та стійкості економіки. В умовах гібридної агресії інформаційні системи логістики стають пріоритетними цілями для кібератак, спрямованих на дезорганізацію постачання та витік стратегічних даних.

В умовах повномасштабної збройної агресії логістична система України трансформувалася в критичну артерію, що забезпечує як гуманітарні, так і військові потреби. Інформаційна безпека у цій сфері перестала бути суто технічним питанням і перейшла у площину національної безпеки. Згідно з дослідженнями, основними загрозами є кібершпигунство за маршрутами та деструктивні атаки на цифрові платформи управління [1, 2]. На рисунку 1 наведені основні специфічні загрози.



Рисунок 1 – Основні специфічні загрози для інформаційної безпеки вантажних автомобільних перевезень

На основі системних загроз можна виділити основні об'єкти, які потребують захисту, та основні вразливості сучасного транспортного підприємства, яке інтегровано в глобальну мережу передачі даних (див. рис. 2)



Рисунок 2 – Основні об'єкти, які потребують захисту

Для забезпечення стійкості перевезень необхідно впроваджувати багаторівневу модель захисту, що базується на принципах Zero Trust (нульової довіри) й частково представлена в таблиці 1.

Таблиця 1 – Основні елементи багаторівневої моделі захисту для забезпеченні інформаційної безпеки вантажних автомобільних перевезень

Компонент захисту	Заходи та інструменти
Технічний захист	Використання VPN з шифруванням за стандартом AES-256, впровадження двофакторної автентифікації (2FA) для доступу до баз даних
Криптографія	Хешування логістичних даних та використання ЕЦП для верифікації товарно-транспортних накладних (е-ТТН)
Моніторинг	Впровадження SIEM-систем для аналізу аномальної активності в мережі компанії в режимі реального часу
Резервування	Створення «холодних» та «гарячих» бекапів критичних даних на серверах, географічно віддалених від зони бойових дій

Аналіз ринку міжнародних перевезень показує, що попри війну, цифровізація галузі лише прискорилося, що вимагає негайного посилення протоколів захисту даних на державному рівні [3].

Інформаційна безпека автомобільних перевезень у воєнний час трансформується з обслуговуючої функції на стратегічну. Пріоритетом стає не лише захист від крадіжки даних, а забезпечення безперервності бізнес-процесів в умовах постійного кібертиску. Інтеграція сучасних засобів

кіберзахисту, навчання персоналу правилам цифрової гігієни та перехід на захищені системи е-ТТН є необхідними кроками для збереження логістичного потенціалу країни.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Galuzinska O., Slobodianiuk A. Development of military logistics in the conditions of martial law. *VNTU Conference (2025)*. [Електронний ресурс]. URL: <https://conferences.vntu.edu.ua/index.php/mn/mn2025/paper/view/24920/20605> (дата звернення: 11.03.2026).

Moroz V. Features of Information Security in Martial Law / V. Moroz . // Legal Bulletin «Air and Space Law» / National Aviation University.- К., 2021. - №2 (59). - С.94-101. [Електронний ресурс]. URL: <https://er.kai.edu.ua/items/d0d60093-06fa-4bc3-9435-750a86905d79> (дата звернення: 11.03.2026).

Dmytriv D., Dmytriv O., Repak O. Analysis of the international road freight transport market in Ukraine under martial law. *Socio-Economic Problems and the State* 29(2), 48-60 p. (2023). DOI:10.33108/sepd2023.02.048.