

СИСТЕМНИЙ ПІДХІД ДО ЗАХИСТУ ЗАЛІЗНИЧНИХ ОБ'ЄКТІВ ВІД ЗАГРОЗ В УМОВАХ ВІЙСЬКОВИХ ДІЙ

Залізничні вузли в умовах військових дій є не лише логістичними об'єктами, а й джерелами розвідувальної інформації про переміщення вантажів стратегічного призначення. Досвід АТ «Укрзалізниця» у 2022-2025 рр. свідчить, що противник систематично використовує щонайменше чотири незалежні канали збору даних для ідентифікації та ураження залізничних об'єктів і рухомого складу. Відсутність системного підходу до нейтралізації цих каналів формує критичну вразливість транспортної системи.

Системність підходу полягає у формуванні чотирикомпонентної матриці загроз «тип розвідки — канал — об'єкт вразливості — спосіб нейтралізації» для залізничної інфраструктури в умовах активного військових дій. Подібна систематизація у вітчизняній транспортній науці раніше не проводилась.

Аналіз роботи залізничних вузлів та дозволив виявити чотири типи загроз з різними каналами та об'єктами вразливості.

Технічна розвідка (SIGINT/Cyber) реалізується через злам централізованих інформаційних систем (АСК ВП УЗ-С, SAP) та перехоплення незашифрованих радіопереговорів. Об'єктом вразливості є цифровий слід вагону: його номер, тип вантажу, маршрут, графіки руху. Запропонована контрзахід — це «цифрове маскування», тобто заміна реальних даних на фіктивні у загальних мережах із паралельним переведенням критичного трафіку на автономні IoT-канали.

Космічна та авіаційна розвідка (IMINT) використовує супутники оптичного та радіолокаційного спостереження (SAR) і розвідувальні безпілотні літальні апарати. Вразливістю для залізниці є тривале перебування складів на відкритих коліях. Нейтралізація подібних загроз передбачає модернізацію інфраструктури: будівництво критич «шлюзів» та ангарів-екранів, мінімізацію часу простою.

Агентурна розвідка (HUMINT) здійснюється через візуальне спостереження інформаторами поблизу станції. Накопичення техніки на виставочних коліях та перевантаження на відкритих рампях є місцем потенційного ураження, тому запропоновано технологію «динамічного вікна», яка полягає у використанні тупиків з обмеженим кутом огляду.

Аналітична розвідка (OSINT) базується на аналізі таких непрямих ознак, як зміни інтенсивності руху й перекриття доріг біля переїздів.

Вразливим місцем є регулярність і циклічність технологічних операцій на станціях. Контрзаходом може стати рандомізація графіків руху та обробки рухомого складу за спеціальним алгоритмом зміни часу та черговості подавань, що унеможливує виявлення шаблонів.

У якості комплексного вимірника можливих загроз може стати інтегральний індекс розвідувальної вразливості залізничних об'єктів, який би динамічно відображав індекси цифрової вразливості, просторової відкритості, агентурного ризику та шаблонності операцій будь-якого залізничного об'єкта з визначеним часовим горизонтом розрахунку.

Таким чином, запропонована матриця є основою для розробки комплексної системи захисту залізничних вузлів від можливих атак. Практичне впровадження чотирьох запропонованих заходів дозволяє суттєво знизити ризик ідентифікації та ураження стратегічних вантажів на всіх етапах їх транспортування. Перспективою подальших досліджень є розробка алгоритму рандомізації графіків та оцінка економічних витрат на модернізацію інфраструктури укриття.