

УСТОЙЧИВОСТЬ ТРАНСПОРТНОЙ ОТРАСЛИ К КИБЕРАТАКАМ: УГРОЗЫ И ПРИЕМЫ ПО ИХ ПРЕДОТВРАЩЕНИЮ

А.А. Двойных, Мустафа Абдулкадим Аль-Амиди Дхаир, Шамсулдин Хайдар
Абдулваххаб Х.

ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация: В статье рассматриваются угрозы и способы предотвращения кибератак на транспортную отрасль в условиях ее стремительной цифровизации. Описываются основные киберриски, с которыми сталкиваются транспортные системы, а также экономические, репутационные и правовые последствия киберинцидентов. В статье предложены практические меры по повышению киберустойчивости транспортных предприятий, такие как развитие киберкомпетенций у сотрудников, резервное копирование данных, сегментация сетей, использование антивирусного ПО, регулярное обновление программного обеспечения и разработка планов реагирования на инциденты.

Ключевые слова: кибератака, транспортная отрасль, кибербезопасность, цифровизация, информационная безопасность, сегментация сетей, резервное копирование данных, фишинг, киберинциденты.

RESILIENCE OF THE TRANSPORT INDUSTRY TO CYBER ATTACKS: THREATS AND TECHNIQUES TO PREVENT THEM

A.A. Dvoynikh, Mustafa Abdulkadhim Al-Ameedee Dhahir, Shamsuldaeen Haidar
Abdulwahhab H.

Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract: The article examines threats and ways to prevent cyberattacks on the transport industry in the context of its rapid digitalization. It describes the main cyber risks faced by transport systems, as well as the economic, reputational and legal consequences of cyber incidents. The article proposes practical measures to improve the cyber resilience of transport enterprises, such as developing cyber competencies among employees, data backup, network segmentation, using antivirus software, regularly updating software and developing incident response plans. The importance of a comprehensive approach to protecting transport infrastructure from cyberattacks is emphasized.

Keywords: cyber attack, transport industry, cyber security, digitalization, information security, network segmentation, data backup, phishing, cyber incidents

Транспорт — одна из ключевых отраслей экономики. К ней может относиться множество различных компаний: логистические организации,

операторы городского транспорта, перевозчики, обслуживающие пассажиров и перевозящие грузы на наземном и воздушном транспорте и другие

Долгое время транспортная отрасль, особенно традиционные виды транспорта, не привлекала особого внимания киберпреступников, поскольку системы управления и операционные процессы не были интегрированы в цифровую среду. Однако с развитием технологий, таких как интернет вещей, автоматизация логистических и операционных процессов, внедрение интеллектуальных транспортных систем (ITS), отрасль стала активно цифровизироваться. Это значительно повысило эффективность управления транспортом, но одновременно открыло новые уязвимости для кибератак. Сегодня транспортная отрасль, особенно с учетом ее стратегической значимости для экономики и общества, становится мишенью для хакеров. Инфраструктура транспорта играет ключевую роль в бесперебойной доставке товаров и услуг, поддержании мобильности населения и логистических цепочек. Любое нарушение в работе транспортных систем может

Рассмотрим более детально типы угроз, которые направлены на транспортную отрасль.

Экономические потери. Прямые финансовые убытки от атак могут быть значительными. Например, остановка транспортных сетей или нарушение работы систем управления движением могут привести к огромным потерям в логистике, задержкам поставок и снижению прибыли.

Ущерб репутации – это потеря доверия со стороны клиентов и партнеров может иметь долгосрочные последствия. Нарушения в безопасности транспортных систем могут затруднить привлечение новых клиентов, а также партнеров для работы в сфере логистики.

Правовые последствия. Нарушение законодательства о защите данных, таких как персональные данные пассажиров или информация о грузах, может привести к штрафам и юридическим издержкам.

Для того, чтобы минимизировать ущерб от кибератак рассмотрим несколько приемов, которые могут быть актуальны в борьбе со злоумышленниками в транспортной отрасли.

Развитие нужных компетенций у работников – это одно из наиболее эффективных мер является обучение сотрудников основам кибербезопасности. Большинство кибератак в транспортной отрасли начинается с социальной инженерии, например, через фишинговые атаки. Сотрудники, знающие, как распознавать угрозы и подозрительные сообщения, могут стать первой линией защиты.

Резервное копирование данных. В транспортной отрасли важны данные о пассажиропотоке, грузоперевозках, логистических маршрутах и системах управления движением. Внедрение программ-вымогателей может заблокировать доступ к этим критически важным данным. Регулярное создание резервных копий поможет восстановить информацию и продолжить работу в случае атаки.

Сегментация сети. Технологические сети управления транспортом и логистикой могут быть отделены от бизнес-сетей для повышения безопасности. При подозрении на кибератаку сегментированная сеть позволяет изолировать уязвимые системы, предотвращая распространение угрозы.

Использование антивирусного ПО на всех устройствах. Транспортные системы, включая управление транспортом, мониторинг движения, системы навигации и другие, также уязвимы перед вредоносным ПО, таким как трояны и программы-вымогатели. Установка и регулярное обновление антивирусного ПО на всех устройствах – от серверов до мобильных устройств сотрудников – поможет предотвратить атаки.

Регулярное исправление и обновление ПО. Обновление программного обеспечения критически важно для транспортной отрасли, где используются сложные системы автоматизации и управления. Уязвимости в ПО могут быть использованы хакерами для проникновения в системы управления транспортом или логистикой.

Разработка плана реагирования на инциденты. Четкий план действий на случай кибератаки, включая этапы восстановления работы транспортных систем и минимизации ущерба, позволит быстро и эффективно реагировать на инциденты.

Экспертиза с привлечением сторонних компаний. Специализированные компании в области кибербезопасности могут предоставить передовые технологии и знания, что значительно повысит уровень защиты транспортных систем и минимизирует риски кибератак.

Также для улучшения контроля и управления киберрисками можно создать центр обработки киберинформации, который бы координировал деятельность по защите ИТ и ОТ систем. Это позволит более эффективно отслеживать, анализировать и реагировать на угрозы, укрепляя связи между ключевыми звеньями в процессе управления кибербезопасностью. Центр также поможет интегрировать управление и контрольные системы ИТ и ОТ, обеспечивая более высокий уровень защиты путем обмена данными и координации действий между различными подразделениями.

Выводы

Устойчивость транспортной отрасли к кибератакам становится важной задачей в условиях стремительной цифровизации сектора. Защита информации и систем управления требует комплексного подхода, включающего обучение сотрудников, инвестиции в технологии и разработку стратегий реагирования на инциденты. Это позволит минимизировать риски и обеспечить стабильную работу транспортных систем в условиях современных вызовов.

Список литературы

1. Кибербезопасность в транспорте и логистике: угрозы и стратегии защиты в эпоху цифровизации. – URL: <https://roscongress.org/materials/kiberbezopasnost-v-transporte-i-logistike-ugrozy-i-strategii-zashchity-v-epokhu-tsifrovizatsii/> (Дата обращения: 07.10.2024).

2. Киберугрозы в транспортной отрасли. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cyber-threats-in-the-transport-sector-2023/> (Дата обращения: 07.10.2024).

3. Информационная безопасность в логистике и на транспорте. – URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_логистике_и_на_транспорте - (Дата обращения: 07.10.2024).

References

1. Cybersecurity in transport and logistics: threats and protection strategies in era of digitalization. – URL: <https://roscongress.org/materials/kiberbezopasnost-v-transporte-i-logistike-ugrozy-i-strategii-zashchity-v-epokhu-tsifrovizatsii/> - (Date of access: 07.10.2024).

2. Cyber threats in the transport industry. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cyber-threats-in-the-transport-sector-2023/> - (Date of access: 07.10.2024).

3. Information security in logistics and transport. – URL: https://www.tadviser.ru/index.php/Article:Information_security_in_logistics_and_transport - (Date of access: 07.10.2024).