УДК 65.011.56

УСТОЙЧИВОСТЬ ЛОГИСТИЧЕСКИХ СИСТЕМ К КИБЕРУГРОЗАМ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

RESILIENCE OF LOGISTICS SYSTEMS TO CYBER THREATS IN THE CONTEXT OF DIGITALIZATION

Стельмашек М.А.
Научный Руководитель – Хартовский В.Е., д.ф.-м.н., доцент
Гродненский государственный университет им. Янки Купалы,
г. Гродно, Беларусь
markstelmasek@gmail.com
M. Stelmashek,
Scientific Supervisor – V.E. Hartovsky, Doctor of Physical and Mathematical Sciences, Associate Professor
Yanka Kupala Grodno State University, Grodno, Belarus.

Аннотация. Цифровая трансформация кардинально улучшает качество услуг в логистической системе. Однако внедрение передовых технологий также открывает новые горизонты уязвимости для информации в логистических системах. Кибератаки могут нанести серьезный финансовый урон бизнесу. В данной статье мы исследуем основные причины угроз кибербезопасности в логистике. Также разработаны рекомендации, направленные на обеспечение надежной защиты информации в логистике.

Abstract. Digital transformation dramatically improves the quality of services in the logistics system. However, the introduction of advanced technologies also opens up new horizons of vulnerability for information in logistics systems. Cyber attacks can cause serious financial damage to a business. In this article, we explore the main causes of cybersecurity threats in logistics. Recommendations have also been developed to ensure reliable protection of information in logistics.

Ключевые слова: логистика, цифровизация, кибербезопасность.
Keywords: logistics, digitalization, cybersecurity.

Введение.

Логистика, происходящая от греческого термина logistics (искусство планирования и расчета), представляет собой ключевую науку, посвященную управлению потоками товаров, информации и

услуг. В эпоху цифровизации, которая кардинально меняет облик транспортно-логистической системы (ТЛС), важность защиты данных и процессов становится более актуальной, чем когда-либо. Эта статья исследует преимущества, и угрозы, связанные с цифровизацией в ТЛС, а также предлагает стратегии для повышения уровня кибербезопасности в отрасли.

Основная часть.

Цифровая логистика, которая основана на применении современных информационных технологий и интеллектуальных систем управления транспортом, является ключевым направлением совершенствования процесса доставки груза от отправителя получателю с соблюдением всех принципов логистики, позволяющих автоматизировать задачи транспортных компаний [1]. Цифровизация стала основным трендом в транспортно-логистическом системе, кардинально трансформируя все его аспекты. Многие логистические процессы могут быть автоматизированы с помощью различных программ и сервисов, таких как:

Создание и изменение задач позволяет быстро адаптироваться к изменяющимся условиям. Документооборот упрощает взаимодействие между торговыми партнерами и минимизирует ошибки. Оптимизация маршрутов помогает находить наиболее эффективные пути доставки. Анализ рентабельности позволяет точно оценивать экономическую целесообразность перевозок. Отслеживание грузов обеспечивает прозрачность на всех этапах доставки.

Эти достижения ведут к значительному увеличению эффективности и расширению доходных каналов. Например, интеграция автоматизированных торговых платформ делает возможным отслеживание поставок в режиме реального времени, что обеспечивает быструю доставку товаров клиентам.

Тем не менее, цифровизация несет с собой и ряд серьезных угроз. Переход на новые технологии открывает двери для кибератак, делая компании (ТЛС) уязвимыми. Угроза кибератак затрагивает все области, включая судоходство, железнодорожные перевозки и логистику, и может привести к дорогостоящим последствиям. Утечка личных данных клиентов в результате хакерских атак может не только причинить финансовый ущерб, но и подорвать доверие к компании.

Кроме того, хакеры активно нацеливаются на информацию, хранящуюся в сетях, что критически важно для дальнейшего развития и модернизации транспортно-логистической индустрии. Эти данные

необходимы для обеспечения более эффективного и качественного обслуживания клиентов. Цифровые системы предлагают множество возможностей: от автоматизированного заказа до отслеживания грузов и управления учетными записями. Однако такие преимущества сопровождаются необходимостью хранения большого объема личных данных на онлайн-платформах и мобильных устройствах, которые могут стать уязвимыми из-за отсутствия строгих мер кибербезопасности. Пользователи растущего количества мобильных устройств производят все больше контента, который удобно хранить в облаках [2]. Однако транспорт и логистика имеют свои слабые места. Во-первых, современные операционные технологии и новые коммуникационные каналы, которые составляют цифровую экосистему компаний, делают их легкой мишенью для злоумышленников. Во-вторых, устаревшие правила и стандарты в области ИТ, а также низкий уровень осведомленности о киберугрозах создают дополнительные риски. И, наконец, наибольшей проблемой остается нехватка квалифицированных кадров, способных обеспечивать защиту.

Киберугрозы постоянно эволюционируют, и главной причиной этого зачастую становятся человеческие ошибки. Например, недобросовестные сотрудники, не распознающие фишинговые письма, могут стать инструментами для старта атак. Более половины утечек данных происходит из-за уязвимостей в организационных процессах и недостаточной квалификации персонала, что делает их первыми жертвами в цепочке атак.

Для защиты от этих атак важно применять строгие меры безопасности, проявлять бдительность в отношении электронной почты и других форм общения, а также обучать сотрудников методам безопасного использования компьютеров [3]. К сожалению, на глобальном уровне наблюдается растущая нехватка специалистов по кибербезопасности. Вместо того чтобы делать эту область более привлекательной, повышая зарплаты и предлагая льготы, многие компании рассматривают кибербезопасность как дополнительную статью расходов, которые нужно сократить.

Корпоративная культура должна перейти от игнорирования к активному признанию важности кибербезопасности. Организации должны инвестировать в обучение персонала о кибербезопасности и методах защиты [4]. Регулярные тренинги по кибербезопасности могут помочь сотрудникам развить навыки, позволяющие

минимизировать риски. Важно акцентировать внимание на том, какие шаги каждый работник может предпринять для защиты, включая использование надежных паролей и отслеживание подозрительной активности в корпоративной сети.

Также стоит акцентировать внимание на управлении киберрисками, что может помочь привлечь квалифицированных специалистов из образовательных учреждений и частного сектора. Компании могут продвигать свои достижения в области кибербезопасности, показывая, что они используют передовые технологии и обновляют свои системы. Кроме того, стоит рассмотреть возможность сотрудничества с независимыми консультантами, которые смогут предложить объективные решения без привязки к конкретным продуктам.

Искусственный интеллект способствует предвидению и предотвращению киберпреступлений, обеспечивает защиту слабо защищённых устройств, требует регулярного обновления паролей [5]. ИИ может мгновенно выявлять угрозы, например подозрительные IP-адреса или запрещенные действия пользователей, тем самым минимизируя человеческое участие в процессе.

Наконец, важно находить сотрудников, активно участвующих в инициативах по кибербезопасности и обладающих необходимыми компетенциями. Обучение, поощрение и создание стимулов для повышения квалификации помогут компаниям в ТЛС сократить существующие пробелы в области кибербезопасности.

Заключение.

Кибербезопасность в транспортно-логистической системе — это не просто необходимость, а стратегическая задача, требующая комплексного подхода. Цифровизация открывает множество возможностей, но также приносит и новые риски. Для успешного преодоления этих угроз компаниям необходимо инвестировать в обучение сотрудников, обновление технологий и привлечение квалифицированных специалистов. Только так можно обеспечить надежную защиту данных и устойчивость бизнеса в условиях быстро меняющегося мира киберугроз.

Литература

1. Дыбская В.В., Сергеев В.И. Цифровая логистика и управление цепями поставок: перспективы развития // Логистика: современные тенденции развития: материалы XVII Меж-дунар. науч.-практ. конф. 12, 13 апреля 2018 г.: Ч. 1: мат. докл. / ред. кол.: В.С. Лукинский (отв.

ред.) и др. - СПб.: Изд-во ГУМРФ им. адм. С.О. Макарова, 2018. - С. 5-11.

2. Прохоров.А.В. Цифровая трансформация анализ, тренды, мировой опыт издание второе, исправленное и дополненное / А.В Прохоров —Москва 2019 — С. 24-27. — URL: https://ацим.рф/wp-content/uploads/2021/09/digital_transformation_book.pdf/ (дата обращения: 04.11.2024).

3. Струнин, Д. А. Кибератаки и их влияние на цифровую экономику / Д. А. Струнин. — Текст : непосредственный // Молодой ученый. — 2023. — № 5 (452). — С. 15-16. — URL: https://moluch.ru/archive/452/99590/ (дата обращения: 04.11.2024).

4. Абдуллаев, Э. А. Кибербезопасность: вызовы и стратегии защиты в цифровую эпоху / Э. А. Абдуллаев. — Текст : непосредственный // Молодой ученый. — 2023. — № 33 (480). — С. 8-9. — URL: https://moluch.ru/archive/480/105493/ (дата обращения: 04.11.2024).

5. Корнев, Л. В. Обеспечение информационной безопасности в условиях цифровизации / Л. В. Корнев. — Текст : непосредственный // Молодой ученый. — 2022. — № 12 (407). — С. 7-11. — URL: https://moluch.ru/archive/407/89650/ (дата обращения: 04.11.2024).

Представлено 05.11.2024