УДК 164.07

КИБЕРБЕЗОПАСНОСТЬ В ЛОГИСТИЧЕСКИХ СИСТЕМАХ
CYBERSECURITY IN LOGISTICS SYSTEMS

Сковорода Д.А., Денисевич М.В.
Научный руководитель – Якубовская Т.Л., старший преподаватель
Белорусский национальный технический университет, г. Минск, Беларусь
daraskovoroda@gmail.com, dzenisevich.m@gmail.com
D.A. Skovoroda, M.V. Denisevich
Supervisor – YakubovskayaT.L., Senior lecturer
Belarusian national technical university, Minsk, Belarus

Аннотация. В условиях стремительного развития технологий и глобализации логистические системы становятся все более зависимыми от цифровых решений. Однако с ростом использования информационных технологий возникает и повышенная угроза кибератак, что делает кибербезопасность критически важным аспектом в управлении логистическими процессами.
Abstract. With the rapid development of technology and globalization, logistics systems are becoming increasinglydependent on digital solutions. However, with the increasing use of information technology, there is also an increased threat of cyber attacks, which makescybersecurity a critically important aspect in managing logistics processes.
Ключевыеслова: кибербезопасность, киберугрозы, кибератака
Keywords: cybersecurity, cyberthreat, cyberattack

Введение.

Кибербезопасность в логистических системах становится всё более важной темой в условиях глобализации и растущей зависимости от технологий. Согласно данным PositiveTechnologies, в 2023 году количество успешных атак на транспортную отрасль увеличилось во всем мире на 36% по сравнению с 2022 годом [1].

Логистика включает множество участников, от поставщиков до конечных потребителей, что делает необходимым обеспечение надежной защиты на всех уровнях. Непредсказуемость киберугроз требует от организаций постоянного мониторинга и адаптации, что

подчеркивает важность кибербезопасности в логистических системах для их эффективной работы и устойчивости в современных условиях.

Основная часть.

Кибербезопасностьвлогистических системах обусловлена ростом цифровизации, которая привела к активному использованию технологий, таких как автоматизация и интернет вещей (IoT), что увеличивает уязвимость киберугроз. С увеличением зависимости от технологий наблюдается рост числа кибератак, включая вредоносное ПО и фишинг, что может привести к серьезным сбоям в работе компаний. Утечка данных или перебои в логистике могут вызвать значительные финансовые потери, а также негативно сказаться на репутации и доверии со стороны клиентов и партнеров. Кроме того, существуют строгие законодательные требования в области защиты данных, и несоблюдение этих норм может привести к штрафам.

Сегодня большинство процессов в логистике автоматизированы, и практически вся информации обрабатывается и хранится в электронном виде. Поэтому любое нарушение безопасности может вызвать сбои в работе всей системы, что в свою очередь приведет к значительным финансовым потерям и ущербу репутации компании. Например, утечка персональных данных клиентов вызовет юридические последствия, штрафы и потерю доверия со стороны клиентов, что негативно скажется на продажах и репутации. Кроме того, если система безопасности будет нарушена и данные о грузах потеряются или исказятся, это может вызвать задержки в доставке и недоставленные отправления, что приведет к дополнительным расходам и возможным компенсациям клиентам. Ошибки в учете запасов, вызванные сбоями в автоматизированных системах, могут способствовать созданию избыточных запасов или нехватке товара, что также повлечет за собой финансовые потери.

В США транспортный сектор оказался под особым давлением: в 2021 году более 20% всех кибератак были направлены на транспортные компании. Средняя стоимость утечки данных для компаний в этой стране в 2024 году достигла рекордного уровня в 4,88 млн. долларов США, что на 10% больше, чем в 2023 году, как сообщает отчет IBM [2].

В Европе ситуация с обеспечением кибербезопасности также достаточно сложная. По данным Европейского агентства по кибербезопасности (ENISA), в 2022 году 60% европейских компаний в сфере логистики сообщили о попытках кибератак. Агентство

Европейского Союза по вопросам сетевой и информационной безопасностипрогнозирует, что цепочки поставок ПО занимают первое место среди 10 главных киберугроз до 2030 года, что свидетельствует о растущей обеспокоенности по поводу безопасности данных [3].

В Азии, особенно в таких странах, как Индия и Китай, наблюдается резкий рост кибератак. В 2022 году Индия сообщила о 30% увеличении инцидентов по сравнению с предыдущим годом. В Китае ожидается, что расходы на кибербезопасность достигнут $30 млрд к 2025 году, что отражает необходимость защиты информации в условиях растущих угроз.

Ситуация в России также вызывает беспокойство: в 2021 году более 40% российских компаний в сфере логистики столкнулись с кибератаками [4]. В ответ на это российские компании увеличили свои инвестиции в кибербезопасность на 25% в 2022 году.

Киберугрозы становятся все более сложными, ключевой уязвимостью остаются люди. Например, на серверы порта Сан-Франциско-ду-Сул (Бразилия) 6 мая 2024 г. была осуществлена кибератака, в результате которой некоторые данные были зашифрованы и системупришлось временно отключить. Несмотря на то, что ИТ-команда порта благодаря поддержке сервис-провайдеров восстановила часть функциональности системы, позволив порту возобновить полноценную работу менее чем за 24 часа, были зафиксирована значительная утечка данных (по данным группы RansomHub, которая взяла на себя ответственность за атаку на портал Сан-Франциско-ду-Сул было украдено 548,72 ГБ данных, включая данные бухгалтерского учета, финансовые отчеты и данные сотрудников) [5].

В некоторых случаях компании – жертвы кибератак не могут восстановить свои системы, что приводит к закрытию бизнеса.

Строгие меры кибербезопасности и создание механизмов их реализации позволяютлогистическим компаниям не только защитить свои активы, но и улучшить свою репутацию в глазах клиентов и партнеров, подчеркивая их приверженность безопасности и надежности.

Для многих компаний в сфере транспорта и логистики такой подход к управлению кибербезопасностью может показаться сложным и ресурсоемким, однако вложения в эти меры являются инвестицией в долгосрочную стабильность и процветание бизнеса. Создание

надежных систем киберзащиты не только снижает риски потерь от кибератак, но и служит залогом уверенности в способности компании справляться с будущими вызовами в области информационной безопасности.

В последние годы Республика Беларусь активно развивает свою инфраструктуру и технологии, что делает её потенциально привлекательной для кибератак. В 2019 году Беларусь заняла 69-е место в мировом рейтинге по кибербезопасности, составленном Международным союзом электросвязи (ITU) [6]. При этом в Беларуси существует ряд законов и нормативных актов, регулирующих вопросы кибербезопасности. Например, Закон «О защите информации» и Закон «О кибербезопасности» обязывают организации принимать меры по защите информации и обеспечению безопасности своих систем.

Заключение.

Таким образом, кибербезопасность в логистических системах становится критически важной задачей для стран по всему миру. Увеличение числа атак и рост затрат на защиту данных подчеркивают необходимость внедрения комплексных мер безопасности и повышения осведомленности среди сотрудников. Страны должны сотрудничать и обмениваться информацией о лучших практиках для защиты своих логистических систем от киберугроз.

Литература

1. Киберугрозы в транспортной отрасли [Электронный ресурс]. Электронные данные. – Режим доступа: **https://www.ptsecurity.com/ru-ru/research/analytics/cyber-threats-in-the-transport-sector-2023/**. Дата доступа: 11.11.2024.

2. IBM: средняя стоимость взлома достигла рекордных $4,88 миллионов в 2024 году [Электронный ресурс]. Электронные данные. – Режим доступа: **https://10guards.com/ru/blog/2024/07/31/ibm-average-breach-costs-hit-record-4-88m-in-2024-up-10-from-last-year/**. Дата доступа: 11.11.2024.

3. Атаки на цепочки поставок являются главной киберугрозой до 2030 года – ENISA[Электронный ресурс]. Электронные данные. – Режим доступа:**https://10guards.com/ru/blog/2024/05/28/supply-chain-attacks-top-cyber-threat-for-2030-enisa/**. Дата доступа: 11.11.2024.

4. Около 40% российских компаний получили ущерб от кибератак – исследование [Электронный ресурс]. Электронные

данные. – Режим доступа: **https://pln-pskov.ru/business/451674.html**. Дата доступа: 11.11.2024.

5. Краткий обзор основных инцидентов промышленной кибербезопасности за второй квартал 2024 года [Электронный ресурс]. Электронные данные. – Режим доступа: **https://ics-cert.kaspersky.ru/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/**. Дата доступа: 12.11.2024.

6. Беларусь – 69 в рейтинге кибербезопасности [Электронный ресурс]. Электронные данные. – Режим доступа: https://news.21.by/other-news/2019/04/03/1762763.html?ysclid.Дата доступа: 12.11.2024.

Представлено 13.11.2024