УДК: 164.07

ЗАЩИТА ИНФОРМАЦИИ В ЛОГИСТИЧЕСКИХ СИСТЕМАХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Л. С. Петросян

студентка факультета инновационных технологий, Гродненский государственный университет имени Янки Купалы, г. Гродно, Беларусь, e-mail: lilia201924@gmail.com.

Научный руководитель: **Ю. В. Крупенко**

кандидат экономических наук, доцент, доцент кафедры логистики и методов управления, Гродненский государственный университет имени Янки Купалы, г. Гродно, Беларусь, e-mail: Julia_kul@list.ru

Цифровая трансформация существенно улучшает качество услуг в логистической отрасли. Однако внедрение инновационных технологий увеличивает и уязвимость информации в логистических системах. Кибератаки могут негативно повлиять как на логистику, так и на общую производительность цепочки поставок. В статье рассмотрен международный опыт, повышающий кибербезопасность в логистике и управлении цепочками поставок. Представлены мероприятия, обеспечивающие защиту информации в секторе логистики.

Ключевые слова: цифровизация; логистика; кибербезопасность; защита информации.

INFORMATION PROTECTION IN LOGISTICS SYSTEMS IN CONDITIONS OF DIGITIZATION

L. S. Petrosian

Student of the Faculty of Innovative Technologies of Mechanical Engineering at Yanka Kupala State University of Grodno, Grodno, Belarus, e-mail: lilia201924@gmail.com

Supervisor: **Yu. V. Krupenko**

PhD in Economics, Associate Professor of the Department of Logistics and Management Methods, Yanka Kupala State University of Grodno, Grodno, Belarus, e-mail: Julia_kul@list.ru

Digital transformation significantly improves the quality of services in the logistics industry. However, the introduction of innovative technologies also increases the vulnerability of information in logistics systems. Cyber attacks can negatively impact both logistics and overall supply chain performance. The article discusses international

experience that improves cybersecurity in logistics and supply chain management. Measures are presented to ensure information security in the logistics sector.

Keywords: digitalization; logistics; cybersecurity; information protection.

По мнению Совета профессионалов по управлению цепочками поставок (CSCMP), логистику можно определить как процесс эффективного планирования, выполнения и мониторинга потоков сырья, незавершенного производства, готовой продукции, услуг и сопутствующей информации из мест происхождения в места потребления (включая внешние и внутренние перемещения, а также входящие и исходящие движения) с целью удовлетворения потребностей клиента. В последние годы логистика стремительно развивается в технологическом направлении и роботизации [1]. Отчеты международных организаций свидетельствуют о том, что логистические компании диверсифицируют свои цепи поставок за счет автоматизации логистических действий [5]. Наиболее распространенным явлением использования роботизации на складах и производственных цехах являются мобильные роботы и дроны. Они позволят более точно отслеживать продукты, проверять и учитывать особенности складов. По данным статистики, склады, оборудованные роботами, могут содержать на 50 % больше товаров, за счет небольших размеров и большей грузоподъемностью по сравнению с человеком [2].

Все больше логистических компаний внедряют ИТ-решения, такие как ERP, WMS или TMS для управления бизнес-процессами во всех сферах. За счет средств цифровизации может быть улучшен процесс управления цепочками поставок за счет обеспечения их прозрачности. Таким образом, цифровизация и автоматизация приводят к более эффективным процессам по всей цепочке поставок.

Несмотря на все достоинства цифровизии, следует отметить, что при ее расширении повышается уязвимость логистических информационных систем. Связано это с появлением и развитием инновационных цифровых платформ, которые аккумулируют огромные информационные базы данных [3]. Это делает компании легкой целью для хакеров. Именно поэтому в логистической системе должны быть предусмотрены доступные средства защиты информации от искажения и несанкционированного доступа.

Информация в цифровой экономике приобретает особый статус и при правильном использовании может предоставить значительные конкурентные преимущества логистическим компаниям за счет технологий, позволяющих лучше управлять внутренними и внешними данными и использовать их. К таким цифровым технологиям можно отнести боль-

шие данные (BigData), порталы сравнения (маркетплейсы), облачные вычисления, Интернет вещей и искусственный интеллект, которые используются во всех видах логистики.

Для защиты данных и информационных систем в логистике необходимо принимать меры по кибербезопасности. Одной из таких мер является использование шифрования данных. Шифрование позволяет защитить данные от несанкционированного доступа и хакерских вторжений. Программа или служба, в которой используется шифрование, принимает сообщения или файлы и преобразует их в код, который не позволит прочитать действительное содержимое. Это значит, что даже если в обмен данными вмешается злоумышленник, он ничего не увидит. Обеспечение безопасности информационных систем может включать в себя: установку антивирусных программ и брандмауэров, регулярное обновление программного обеспечения и мониторинга системы на наличие угроз.

Одним из наиболее серьезных рисков является кибератака на системы управления цепями поставок. Одна кибератака может привести к перерыву в работе системы и существенных проблем с логистикой. Например, базирующаяся в Сиэтле логистическая и экспедиторская компания Expeditors International, известная как один из мировых логистических гигантов, в феврале 2022 года столкнулась с крайне серьезной кибератакой. Компания официально признала факт атаки, но не подтвердила, была ли это атака с использованием программы-вымогателя. Компания с годовым доходом в 10,1 млрд долл США и 35 офисами заявила, что вынуждена была отключить большинство операционных систем по всему миру после того, как заметила кибератаку.

Для защиты от кибератак необходимо принимать меры по обеспечению безопасности сети, включая такой действенный механизм как киберстрахование, а также обучать сотрудников компании основам кибербезопасности [4]. Целесообразна разработки политики безопасности, в которой будет приведен список правил, которые должен соблюдать работник.

Сложностью в обеспечении безопасности логистических систем считается повышенный риск перебоев в работе. Распознавание уязвимостей безопасности и концентрация на автоматизации привилегированных задач необходимы для непрерывности работы и предотвращения потенциальных опасностей несанкционированного доступа к цепочке поставок. Мировые эксперты утверждают, что большинство уязвимостей безопасности вызвано компьютерами общего назначения, используемыми в организации и подключающимися к внутренним сетям извне. Одной из ведущих мер, которые существуют в мире в борьбе с данной уязвимостью, является решение Privileged Access Management (PAM). С его по-

мощью происходит идентификация людей, процессов и технологий, которым требуется привилегированный доступ.

Таким образом, для того чтобы обеспечить защиту информации в секторе логистики, сначала необходимо признать существование киберугроз. Проблемы могут возникнуть из-за взаимодействия с внешними партнерами через неконтролируемые сети в процессе доставки. Такие приложения, как безопасный удаленный доступ и сегментация сети, помогают решить эти проблемы. Некоторые из мер, которые могут быть приняты для обеспечения безопасности данных и защиты компании от кибератак, включают обучение сотрудников компании осведомленности о киберугрозах, использование многофакторной аутентификации и надежных паролей, поддержание актуальности программного обеспечения для предотвращения уязвимостей безопасности и пр.

Библиографические ссылки

1. *Быкова О. Н., Пустохина И. В.* Вызовы и перспективы развития рынка транспортнологистических услуг // Экономика, предпринимательство и право. 2020. Т. 10, № 1.

2. *Дыбская В. В.* Логистика складирования : учебник. М. : ИНФРА-М, 2021. 559 с.

3. *Крупенко Ю. В.* Влияние цифровизации на бизнес-процессы страховой организации // IV Международная научно-практическая конференция «Бизнес. Образование. Экономика» : сборник научных статей / Учреждение образования «ИНСТИТУТ БИЗНЕСА БГУ» ; 6–7 апреля 2023 / редкол.: В. В. Манкевич [и др.]. Минск : Институт бизнеса, 2023. С. 77–80.

4. *Крупенко Ю. В.* Киберриски и теоретические основы киберстрахования // Проблемы современной экономики: глобальный, национальный и региональный контекст : сборник научных статей / Гродненский государственный университет имени Янки Купалы ; гл. ред. М. Е. Карпицкая ; зам. гл. ред. С. Е. Витун ; редкол.: Ли Чон Ку [и др.] ; рецензенты: Н. В. Киреенко, А. И. Тарасенок. Гродно : ГрГУ им. Янки Купалы, 2022. С. 249–258.

5. Sustainable Urban Mobility: What Can Be Done to Achieve It? [Электронный ресурс]. URL: https://www.researchgate.net/publication/336280478 (дата обращения: 10.09.2023.