DOI 10.54220/v.rsue.1991-0533.2024.1.85.004

В. В. Журбина

ЭВОЛЮЦИЯ РОЛИ БЕЗОПАСНОСТИ ЛОГИСТИЧЕСКИХ ЦЕПЕЙ ПОСТАВОК

Аннотация

Ускоренная цифровая трансформация цепей поставок начинает затрагивать уже и национальные интересы. Угрозы безопасности цепей поставок обретают новые формы, а к инструментам конкуренции подключаются кибератаки и цифровые ограничения. Цифровое будущее цепей поставок выдвигает на первый план поиск новых путей предотвращения рисков и угроз безопасности транспортно-логистических цепей поставок.

Ключевые слова

Логистика, безопасность цепей поставок, критическая инфраструктура, предотвращение рисков и угроз.

V. V. Zhurbina

EVOLUTION OF THE ROLE OF SUPPLY CHAIN SECURITY

Abstract

Accelerated digital transformation of supply chains is already beginning to affect national interests. Threats to supply chain security are taking on new forms, and cyberattacks and digital restrictions are joining the tools of competition. Digital future of supply chains highlights the search for new ways to prevent risks and threats to the security of transport and logistics supply chains.

Keywords

Logistics, supply chain security, critical infrastructure, risk and threat prevention.

Введение

Сложившаяся в мире геополитическая ситуация усугубила проблемы бесперебойного, своевременного функционирования системы товародвижения. Российским компаниям удалось переформатировать логистические маршруты и адаптироваться к новым условиям развития мирохозяйственных связей. Однако обеспечить безопасность товародвижения не всегда представляется возможным. Это негативно отражается не только на устойчивости и сбалансированности цепей поставок, но подвергает угрозе стабильность работы всей инфраструктуры страны.

Цифровые технологии делают элементы логистической инфраструктуры еще более уязвимыми [1]. Обобщение рисков применения сквозных цифровых технологий в логистике свидетельствует об их ежегодном возрастании в десятки раз [1]. Только за 2023 г. число атак на российские сервисы в транспортно-логистическом секторе увеличилось в 15 раз; на информационные ресурсы в государственном секторе страны отражено 25 тыс. кибератак. На критическую инфраструктуру страны (энергетика, водоснабжение, транспорт, экологические системы) за 2023 г. было совершено боле 1,2 тыс. атак [1]. Поэтому вопросы предотвращения рисков и угроз безопасности логистическим цепям поставок обретают особую актуальность. Это предполагает формирование комплексной си-

стемы риск-менеджмента и безопасности в логистике.

Существует множество методов и инструментов для оценки вероятности наступления риска и анализа предпосылок угроз безопасности в логистической деятельности. Эти методы позволяют определить наиболее вероятные риски и оценить их последствия, а также разработать план превентивных мероприятий по преодолению этих угроз. Практическое значение этих методов обусловлено тем, что они являются одним из инструментов поддержки бесперебойного, сбалансированного функционирования цепей поставок, а также могут быть использованы для стимулирования разработки и внедрения национальных программных продуктов и сервисов, нивелирующих угрозы и риски в системах поставок. Теоретическая и практическая значимость отмеченной выше проблематики, стала основанием для проведения данного исследования. Результаты исследования используется в учебном процессе РГЭУ (РИНХ) при проведении занятий по дисциплине «Безопасность логистических процессов».

Теоретические аспекты проблемы повышения безопасности логистических цепей поставок

В научной литературе вопросы безопасности логистических цепей поставок рассматриваются под разным углом зрения. Ряд авторов акцентируют внимание на угрозах безопасности логистическим системам со стороны внешней среды [4, 5, 6]. Акцент на угрозы со стороны «вредоносных» программных продуктов делают специалисты, занятые в сфере информационной поддержки цепей поставок [4, 5, 6]. Финансовые риски и угрозы обобщены в работе «О кибератаках и обеспечении безопасности транспортно-логистических экосистем», а также найдем информацию в работах И. Д. Афанасенко, В. В. Борисовой, Т. Е. Евтодиевой, А. В. Дмитриева, В. Н. Клочкова, Е. С. Курбатова. Однако никто из них не раскрывает в полной мере методы и инструменты диагностики и предотвращения угроз безопасности логистических цепей поставок в условиях цифровой экономики.

В России развитие и обеспечение надежности транспортно-логистической инфраструктуры в условиях цифровой среды является одной из приоритетных задач. Решение этих задач направлено на улучшение безопасности транспортных маршрутов, контроль за движением грузов и пассажиров, а также совершенствование систем мониторинга и обеспечения бесперебойной работы транспорта.

Учитывая рост числа кибератак, правительство РФ последовательно внедряет современные технологии защиты информационных систем и разрабатывает стратегии повышения безопасности. Проводятся обучающие мероприятия для специалистов, а также осуществляется мониторинг и анализ уязвимых мест в системах и сетях транспортной инфраструктуры.

Россия делает акцент на развитие логистической инфраструктуры и расширение доступа к информационным сетям по всей территории страны. Новые условия развития высокотехнологичной логистической инфраструктуры сопровождаются не только высокими скоростями соединения ее участников в цепях поставок, но и высокими рисками цифровизации. Без гарантии безопасности проектирование логистических объектов утрачивает свою надежность. В первую очередь это касается критической инфраструктуры – совокупности особо важных для работы государства и общества ключевых объектов инфраструктуры. Контроль над информационной инфраструктурой фактически означает контроль над контентом интернет-платформ. Одним из опасных способов воздействия на стабильность работы логистических цепей поставок становится «вредоносное» программное обеспечение. «В 2,5 раза увеличилось количество инцидентов с применением «вредоносного» программного обеспечения, которые не обнаруживают

антивирусы. Наличие таких программ в фишинговых рассылках повышает успешность атак». Требуется импортозамещение средств защиты программного обеспечения. До 2025 г. Правительство РФ обязало субъекты хозяйствования перейти на отечественное программное обеспечение. Это стратегическое решение, позволит стимулировать развитие отечественной IT-индустрии и обеспечит безопасность и независимость информационных систем. Такой шаг способствует укреплению национальной кибербезопасности и снижает риск, связанный с использованием иностранного программного обеспечения. Одним из примеров отечественного программного обеспечения, которое можно использовать вместо иностранных аналогов, является операционная система «Альт Линукс» (ALT Linux) [14]. Это российский дистрибутив Linux, который предлагает широкие возможности для работы на компьютерах и серверах. Он основан на открытом программном обеспечении, что позволяет пользователям иметь доступ к исходному коду и вносить свои изменения.

«Альт Линукс» поддерживает различные архитектуры процессоров, включая x86, ARM и SPARC, что делает его универсальным и гибким в использовании на различных устройствах. Кроме того, в состав дистрибутива входит большой выбор прикладного программного обеспечения, такого как офисные пакеты, графические редакторы, браузеры и многое другое. Однако качеством российского программного обеспечения в этой сфере остались недовольны более половины перешедших на него компаний. Дополнительные трудности в системе безопасности логистических процессов связаны с дефицитом сотрудников в области кибербезопасности. Сегодня этот дефицит составляет более 50 тыс. человек. Если ситуация с профильным образованием не начнет меняться, этот показатель продолжит расти. Поиск компетентных специалистов в сфере безопасности информационных технологий усложняется. Со сложившимся на рынке кадровым дефицитом в 2023 г. столкнулось 77 % российских компаний (рис. 1).

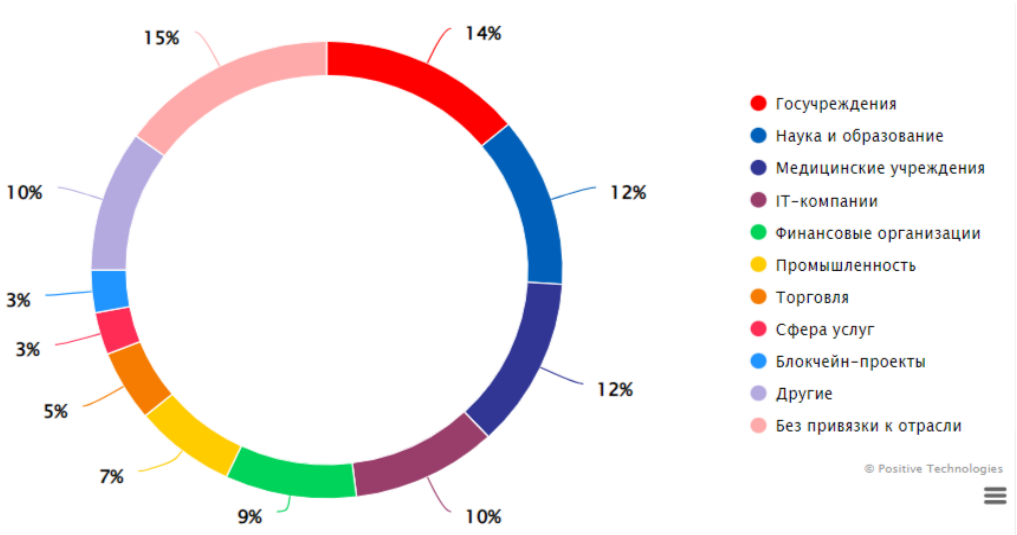

Рисунок 1 – **Статистика по кибератакам во втором квартале 2023 г.***

** Анализ Positive Technologies. 78 % атак имели целенаправленный характер.*

Для противодействия такого рода угрозам необходимо разработать эффективные стратегии кибербезопасности, обучать сотрудников предприятий правилам безопасного поведения в сети, использовать современные технологии защиты информации и регулярно проверять системы на уязвимости. Только та-

ким образом стратегические предприятия могут быть защищены от кибер-угроз и сохранить свою надежность и стабильность в долгосрочной перспективе. Остро назрел вопрос о создании новых поколений систем безопасности. По мере того как цепи поставок виртуализируются и обретают цифровой формат, возрастает роль защитных мер, обеспечивающих их бесперебойное функционирование.

Материалы и методы

Эксперты выделяют целый спектр опасных ситуаций, связанных с цифровыми трансформациями социально-экономической жизни общества, которые могут привести к потере конфиденциальной информации, нарушению работы критической инфраструктуры и финансовым потерям.

Неисправности в безопасности данных, вирусные атаки, программы-шпионы, электронные мошенничества, фальшивые онлайн-ресурсы, случаи кражи личной информации, вредоносный контент, ошибочные настройки приватности – все эти проблемы представляют серьезные угрозы в цифровой среде.

Утечки данных зачастую возникают в следствии хакерских атак, ошибок в защите информации, несанкционированного доступа к базам данных и других уязвимостей.

Собирание и хранение большого объема данных о гражданах приводит к нарушению их приватности, а также к угрозе воровства личной информации и ее злоупотреблению.

Вредоносные программы и вирусы могут нанести ущерб устройствам и системам, вызвать потерю данных, перехват информации, шпионаж или даже блокировку доступа к компьютеру или сети.

«Основные риски функционирования цепей поставок связаны с тем, что существуют фундаментальные причины, в силу которых программное обеспечение нельзя сделать настолько надежным, чтобы не сомневаться в том, что не возникнут нештатные ситуации. Поэтому при сбое информационной подсистемы наступает полный коллапс логистической системы, поскольку даже аналоговые процессы перестают работать в условиях их цифровой трансформации» [1]. Такие ситуации могут привести к серьезным последствиям для бизнеса и экономики в целом. Проблемы с поставками товаров и услуг могут привести к перерывам в работе предприятий, потере доверия со стороны клиентов и потере прибыли. Поэтому важно разработать стратегии предотвращения и управления подобными ситуациями.

Для снижения рисков цифровой трансформации цепей поставок необходимо инвестировать в обновление и защиту информационных систем, обучение персонала, разработку регламентов и процедур управления рисками. Также важно уделить внимание резервированию данных, созданию резервных каналов связи, а также тестированию систем на прочность и готовность к кризисным ситуациям.

Только учитывая все вышеуказанные аспекты и предпринимая соответствующие меры, бизнес сможет обеспечить стабильное и надежное функционирование цепей поставок в условиях цифровой трансформации.

«Внедрение цифровых технологий сопряжено со следующими потенциальными угрозами: интернет вещей (IoT), искусственный интеллект (ИИ) и блокчейн, все эти инструменты открывают перед нами огромные возможности, но при этом возникают и определенные риски, которые также стоит учитывать.

Один из основных рисков, связанных с интернетом вещей, это уязвимость устройств и сетей, которые могут быть подвержены кибер- и хакерским атакам. Недостаточная защита данных и устройств провоцирует утечку информации, перехвату конфиденциальных данных и даже контролю над устройствами со стороны злоумышленников.

Искусственный интеллект также не лишен рисков, включая ошибки в алгоритмах, проблемы с защитой данных, а также этические и нормативные пробле-

мы, связанные с использованием ИИ в различных сферах жизни.

Блокчейн, хотя и считается достаточно безопасным технологическим решением, также имеет свои риски. Атаки на блокчейн-сети представляют серьезную угрозу безопасности, так как блокчейн является основой для функционирования криптовалют и других децентрализованных приложений.

Представим некоторые из наиболее распространенных угроз.

1. 51 %-я атака (атака большинства) [10]: это атака, при которой злоумышленник захватывает более 50 % вычислительной мощности сети блокчейна, что позволяет контролировать создание новых блоков, отклонять транзакции, проводить двойные траты и вмешиваться в работу сети.

2. DDoS (Distributed Denial of Service) [11] – это тип кибератаки, при которой злоумышленники пытаются перегрузить компьютерные ресурсы целевой системы, сети или сервера путем отправки огромного количества фальшивых запросов. Целью DDoS-атаки является нарушение доступности ресурса для легитимных пользователей, делая его недоступным или сильно замедляя работу.

DDoS-атаки могут привести к серьезным последствиям для организаций, таких как потеря доходов, ущерб репутации, время простоя и разрушение бизнес-процессов.

3. Смарт-контрактные уязвимости [12] – представляют собой программные коды, запускаемые на блокчейне для автоматизации и контроле сделок между участниками без необходимости доверять централизованной стороне. Плохо спроектированные смарт-контракты могут привести к утечке средств или другим видам мошенничества.

4. Фишинг и социальная инженерия. Данный метод используется для получения доступа к приватным ключам пользователей и краже их криптовалюты.

5. Майнинг-атаки [13]: работает при помощи использования вычислительных ресурсов устройств пользователей для добычи криптовалюты без согласия владельца (как в случае с майнингом посредством вредоносного программного обеспечения).

Обобщим методы поддержки кибербезопасности и выделим набор стандартных процедур и технологий, соблюдение которых позволяет минимизировать уязвимости и риски, возникающие в логистической деятельности. Согласимся с экспертами, которые обращают внимание на необходимость использования уникальных, длинных и сложных паролей для работающих аккаунтов и задействовать возможности парольного менеджмента для безопасного хранения всех паролей [4, 5, 6].

Полезно также включение дополнительных методов аутентификации, таких как двухфакторная аутентификация (2FA), позволяющих усилить защиту аккаунтов от несанкционированного доступа.

Установка всех доступных обновлений и патчей для операционной системы и программного обеспечения поможет нивелировать существующие угрозы сбалансированности цепи поставок, а создание резервных копий важных данных и хранение их в безопасном месте позволит восстановить информацию в случае кибератаки или сбоя.

В условиях дефицита кадров по поддержке безопасности информационных технологий, обучение логистических операторов и сотрудников, занятых в работе с информационными потоками, повысит их компетентность, даст возможность узнавать фишинговые атаки, управлять конфиденциальной информацией и предотвращать утечки данных. Важны компетенции сотрудников в области использования современных алгоритмов шифрования для защиты конфиденциальных данных.

Востребованным, с точки зрения предотвращения угроз безопасности, становится регулярный мониторинг сетевой активности и использование систем уведомлений.

Результаты и обсуждение

Анализ литературы в области предотвращения рисков и повышения устойчивости работы цепей поставок показал, что «степень риска может быть уменьшена, а его последствия смягчены или устранены в результате:

– прогнозирования вероятности его наступления и уменьшения факторов неопределенности;

– создания страховых, резервных фондов, позволяющих покрывать (полностью или частично) ущерб, возникающий в результате риска;

– страхования, в результате которого риск переносится на третье лицо;

– перераспределения ущерба между участниками сделки (в случае неудачи потери каждого из участников будут не столь велики)» [1].

Методологической основой данного исследования послужили теоретические и прикладные труды российских и зарубежных ученых в области коммерции и логистики, риск-менеджмента, целевые программы Правительства РФ по вопросам укрепления безопасности транспортно-логистической инфраструктуры и кибербезопасности. В ходе решения поставленных задач применялись общенаучные методы и приемы, системный и функциональный анализ; метод экспертных оценок и комплексный подход.

Выводы

В ходе исследования эволюции роли безопасности логистических цепей поставок установлена необходимость как в формировании предпосылок для ускорения процесса предотвращения рисков и угроз, так и в разработке новых правил цифровой безопасности для систем поставок. Для предотвращения нештатных ситуаций и цифрового коллапса в системе поставок целесообразно обновление программного обеспечения, повышение его надежности и создание эффективных средств защиты на базе новых технологий обеспечения как от физических, так и от хакерских взломов и возможных технических сбоев системы. С развитием цифровых технологий и переходом к цифровой трансформации в бизнесе, включая логистику, становится необходимым обеспечить безопасность цифровых систем и данных. Новое поколение систем безопасности в логистике должно эффективно защищать цифровые процессы от киберугроз, включая контроль и защиту грузов на всех этапах их движения, адаптацию к различным международным стандартам и требованиям. Таким образом можно сделать вывод, что новые системы безопасности в логистике должны не только обеспечивать надежность, но и быть устойчивыми к непредвиденным ситуациям и эффективно функционировать в условиях быстро меняющейся среды логистических процессов.

Библиографический список

1. *Афанасенко, И. Д., Борисова, В. В.* Цифровая логистика : учебник для вузов. – СПб. : Питер, 2019. – 272 с.

2. *Журбина, В. В.* Совместное создание ценности в цепи поставок: партнерство и взаимодействие // Вестник Ростовского государственного экономического университета (РИНХ). – 2021. – № 4 (76). – С. 57-63.

3. *Шапкин, А. С., Шапкин, В. А.* Экономические и финансовые риски. Оценка, управление, портфель инвестиций. – 10-е изд., стер. – М. : Дашков и К°, 2020. – 544 с.

4. *Афанасенко, И. Д., Борисова, В. В.* Логистика снабжения : учебник для вузов. – 3-е изд. – СПб. : Питер, 2021. – 384 с.

5. *Дмитриев, А. В.* Безопасность цифровых экосистем транспортно-логистического обслуживания. – СПб. : Изд-во СПбГЭУ, 2023. – 187 с.

6. *Шапкин, А. С., Шапкин, В. А.* Экономические и финансовые риски. Оценка, управление, портфель инвестиций. – 10-е изд., стер. – М. : Дашков и К°, 2020. – 544 с.

7. 15 правил для безопасной работы в интернете [Электронный ресурс]. – URL: https://www.kaspersky.ru/resource-

center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online (дата обращения: 25.01.2024).

8. Цифровизация экономики и риски [Электронный ресурс]. – URL: https://www.comnews.ru/digital-economy/content/111353/2018-01-22/cifrovizaciya-ekonomiki-i-riski-ib (дата обращения: 28.01.2024).

9. *Сюнтюренко, О. В.* Цифровая среда: аналитическая постобработка информации с использованием методов наукометрии и анализа данных // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2019. – № 4. – С. 8-16.

10. Что такое атака 51 % [Электронный ресурс]. – URL: https://academy.binance.com/ru/articles/what-is-a-51-percent-attack (дата обращения: 28.01.2024).

11. Энциклопедия Касперского [Электронный ресурс]. – URL: https://encyclopedia.kaspersky.ru/glossary/ddos-distributed-denial-of-service-attack (дата обращения: 28.01.2024).

12. *Алиев, И. А.* Уязвимости смарт-контрактов блокчейн-платформы Ethereum.

13. Что такое незаконный майнинг? [Электронный ресурс]. – URL: https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/nezakonnyy-mayning (дата обращения: 28.01.2024).

14. Alt-linux : официальный сайт [Электронный ресурс]. – URL: https://alt-linux.ru (дата обращения 28.01.2024).

Bibliographic list

1. *Afanasenko, I. D., Borisova, V. V.* Digital logistics : textbook for universities. – SPb. : Peter, 2019. – 272 p.

2. *Zhurbina, V. V.* Co-creation of value in supply chain: partnership and interaction // Vestnik of Rostov State University of Economics (RINH). – 2021. – № 4 (76). – P. 57-63.

3. *Shapkin, A. S., Shapkin, V. A.* Economic and financial risks. Evaluation, management, investment portfolio. – 10th ed. – M. : Dashkov and K°, 2020. – 544 p.

4. *Afanasenko, I. D., Borisova, V. V.* Supply logistics : textbook for universities. – 3rd ed. – SPb. : Peter, 2021. – 384 p.

5. *Dmitriev, A. V.* Security of digital ecosystems of transportation and logistics service. – SPb. : Publishing house of SPbSUE, 2023. – 187 p.

6. *Shapkin, A. S., Shapkin, V. A.* Economic and financial risks. Evaluation, management, investment portfolio. – 10th ed. – M. : Dashkov and K°, 2020. – 544 p.

7. 15 rules for safe work in the Internet [Electronic resource]. – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online (date of access: 25.01.2024).

8. Digitalization of economy and IS risks [Electronic resource]. – URL: https://www.comnews.ru/digital-economy/content/111353/2018-01-22/cifrovizaciya-ekonomiki-i-riski-ib (date of access: 28.01.2024).

9. *Syunturenko, O. V.* Digital environment: analytical post-processing of information using the methods of scientometrics and data analysis // Scientific and Technical Information. Series 1: Organization and methodology of information work. – 2019. – № 4. – P. 8-16.

10. What is the 51 % attack [Electronic resource]. – URL: https://academy.binance.com/ru/articles/what-is-a-51-percent-attack (date of access: 28.01.2024).

11. Kaspersky Encyclopedia [Electronic resource]. – URL: https://encyclopedia.kaspersky.ru/glossary/ddos-distributed-denial-of-service-attack (date of access: 28.01.2024).

12. *Aliev, I. A.* Vulnerabilities of smart contracts of Ethereum blockchain platform Financial University under Government of Russian Federation.

13. What is illegal mining? [Electronic resource]. – URL: https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/nezakonnyy-mayning (date of access: 28.01.2024).

14. Alt-linux : official site [Electronic resource]. – URL: https://alt-linux.ru (date of access: 28.01.2024).