ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ ЛОГИСТИКИ И УПРАВЛЕНИЯ ЦЕПЯМИ ПОСТАВОК

THEORETICAL AND PRACTICAL PROBLEMS OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

Научная статья
УДК 658.7.01
https://doi.org/10.24143/2073-5537-2024-2-96-103
EDN IFTAVO

Нейтрализация угроз внедрения цифровых инструментов в транспортно-логистических системах

Александр Викторович Дмитриев

Северо-Западный институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Санкт-Петербург, Россия, poliskasko@bk.ru

Аннотация. Обсуждаются вопросы обеспечения экономической безопасности как одной из важнейших качественных характеристик логистических систем, определяющих способность устанавливать в процессе товародвижения параметры материальных потоков при внедрении цифровых систем и технологий. Проводится анализ современных рисков и угроз, характерных для развития цифровых экосистем транспортно-логистического обслуживания. Исследуются ключевые факторы обеспечения экономической безопасности и их значение в логистике с точки зрения оперативного контроля за соблюдением установленных ключевых показателей товародвижения. Дается трактовка понятия «экономическая безопасность» с позиции защищенности субъекта хозяйствования от внешних и внутренних угроз для повышения уровня конкурентоспособности и устойчивости предприятия на рынке. Затрагиваются вопросы обеспечения параметров товародвижения в рамках установленных пороговых значений с целью достижения оптимальности функционирования товаропроводящей системы и обеспеченности хозяйственной деятельности предприятия всеми необходимыми ресурсами. Исследуются логистические системы на предмет эффективной организации и управления материальными потоками, направленными на обеспечение надежности функционирования и реализации стратегии хозяйственных субъектов. Обосновывается необходимость использования современных цифровых технологий для повышения уровня экономической безопасности в логистических системах и прозрачности, контролируемости и прослеживаемости материальных потоков в сфере товародвижения. Факт цифровизации процессов доставки грузов рассматривается с позиции экосистемной парадигмы и платформенной концепции. Обосновываются закономерности трансформации традиционных логистических операторов в провайдеров цифровых логистических услуг. Разработана модель киберфизической экосистемы в логистике, обеспечивающей сквозное управление бизнес-процессами и обмена данными в процессе товародвижения.

Ключевые слова: экономическая безопасность, логистика, цифровые экосистемы, транспорт, цифровые технологии, цифровые платформы

Для цитирования: *Дмитриев А. В.* Нейтрализация угроз внедрения цифровых инструментов в транспортно-логистических системах // Вестник Астраханского государственного технического университета. Серия: Экономика. 2024. № 2. С. 96–103. https://doi.org/10.24143/2073-5537-2024-2-96-103. EDN IFTAVO.

Original article

Neutralizing threats of implementing digital tools in transport and logistics systems

Aleksandr V. Dmitriev

Northwestern Institute of Management − branch FSBTI HE "The Russian Presidential Academy of National Economy and Public Administration", Saint Petersburg, Russia, poliskasko@bk.ru

Abstract. The issues of ensuring economic security are discussed as one of the most important qualitative characteristics of logistics systems, which determine the ability to establish parameters of material flows in the process of commodity movement during the introduction of digital systems and technologies. The analysis of modern risks and threats characteristic of the development of digital ecosystems of transport and logistics services is carried out. The key factors of ensuring economic security and their importance in logistics from the point of view of operational control over compliance with established key indicators of commodity movement are investigated. The definition of the concept of "economic security" is given from the point of view of the protection of the business entity from external and internal threats to increase the level of competitiveness and stability of the enterprise in the market. The issues of ensuring the parameters of commodity movement within the established thresholds are addressed in order to achieve optimal functioning of the commodity distribution system and ensure the economic activity of the enterprise with all necessary resources. Logistics systems are being investigated for the effective organization and management of material flows aimed at ensuring the reliability of the functioning and implementation of the strategy of economic entities. The necessity of using modern digital technologies to increase the level of economic security in logistics systems and transparency, controllability and traceability of material flows in the field of commodity circulation is substantiated. The fact of digitalization of cargo delivery processes is considered from the perspective of the ecosystem paradigm and platform concept. The patterns of transformation of traditional logistics operators into providers of digital logistics services are substantiated. A model of a cyberphysical ecosystem in logistics has been developed that provides end-to-end management of business processes and data exchange in the process of product distribution.

Keywords: economic security, logistics, digital ecosystems, transport, digital technologies, digital platforms

For citation: Dmitriev A. V. Neutralizing threats of implementing digital tools in transport and logistics systems. *Vestnik of Astrakhan State Technical University. Series: Economics*. 2024;2:96-103. (In Russ.). https://doi.org/10.24143/2073-5537-2024-2-96-103. EDN IFTAVO.

Введение

В современных условиях экономическая безопасность выступает одной из важнейших качественных характеристик логистических систем, определяющих способность обеспечивать в процессе товародвижения установленные параметры материальных потоков и достаточную обеспеченность предприятия ресурсами для выполнения его хозяйственной деятельности. По сути, экономическая безопасность – это, с одной стороны, защита субъекта от внешних и внутренних угроз, а с другой – способность субъекта к стабильному функционированию в условиях противодействия негативному влиянию окружающей среды.

В свою очередь, логистика как наука и сфера практической деятельности, связанная с оптимальной организацией и управлением материальными потоками, направлена на обеспечение эффективности функционирования и реализации стратегии хозяйственных субъектов, что позволяет утверждать, что при отсутствии налаженной системы экономической безопасности предприятие не только не сможет реализовать свою стратегию, но рискует потерять конкурентные преимущества на рынке.

Материалы исследования

Одним из важнейших факторов повышения уровня экономической безопасности в области логистики (рис. 1) следует считать применение современных цифровых информационных технологий в сфере товародвижения для обеспечения прозрачности и контролируемости материальных потоков в режиме онлайн.

В последние годы платформенная концепция управления цифровыми экосистемами в транспортной логистике является уже широко применяемой формой организации бизнеса, которая обеспечивает существенно более высокий уровень конкурентоспособности на рынке по отношению к традиционной работе логистических операторов и трансформирует способ предоставления клиентам цифровых логистических услуг.

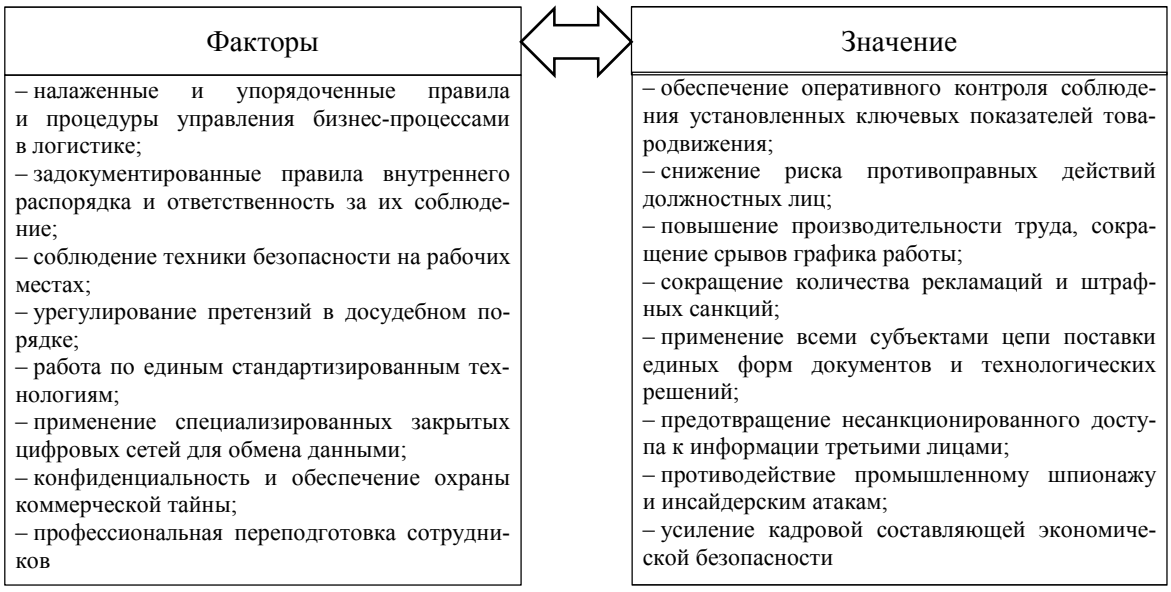

Рис. 1. Ключевые факторы обеспечения экономической безопасности и их значение в логистике [1]

Fig. 1. Key factors of economic security and their importance in logistics [1]

Поскольку предоставление логистических услуг в цифровом виде и развитие киберфизических систем непосредственно зависит от уровня защищенности цифровой инфраструктуры товародвижения, в данном контексте целесообразно остановиться на анализе и оценке рынка кибербезопасности по итогам 2023 г. с прогнозом на 2026 г., опубликованным Фондом «Центр стратегических разработок» (ЦСР) [2].

Прежде всего рассмотрим структурные показатели по объемам долей рынка на 2023 г. и по категориям средств защиты информации (таблица).

Объемные структурно-рыночные показатели в разрезе видов и категорий средств защиты цифровых данных

Volume structural and market indicators by types and categories of digital data protection products

Средства защиты цифровых данных	Доля рынка, %	Доля рынка, млрд руб.	Темп роста, %
Безопасность компьютерных сетей	45	61	20
Защита пользовательских данных	15	20	13
Средства защиты автоматизированных рабочих мест	13	18	17
Инфраструктурная безопасность	12	17	32
Защита пакетов прикладных программ и приложений	8	11	34
Защита учетных записей пользователей	7	9	10

Среднегодовые показатели темпа роста рынка кибербезопасности в России в 2023 г. оцениваются на уровне 56,7 %. Данное значение превышает прирост мировых показателей рынка кибербезопасности, который хотя и имел исторически довольно высокие характеристики благодаря промышленно развитым странам в Западной Европе и Северной Америке, однако в настоящее время в силу сформировавшейся за последние годы зрелости и насыщения растет в меньшей степени (в среднем около 11 % ежегодно). При этом, согласно прогнозам ЦСР, российский рынок кибербезопасности к 2026 г. может достичь показателя в 446 млрд руб. (рис. 2).

Приведенные результаты исследования ЦСР «Прогноз развития рынка решений для информационной безопасности в Российской Федерации в 2022–2026 годах» интересны еще и тем, что в последнее время на конъюнктуру российского рынка кибербезопасности оказывает существенное влияние изменение геополитической обстановки, повлекшее в первом квартале 2022 г. массовое бегство из России западных разработчиков и вендоров комплексных решений и средств информационной защиты, что предопределило существенную реструктуризацию рыночных долей в перспективе ближайших 5 лет.

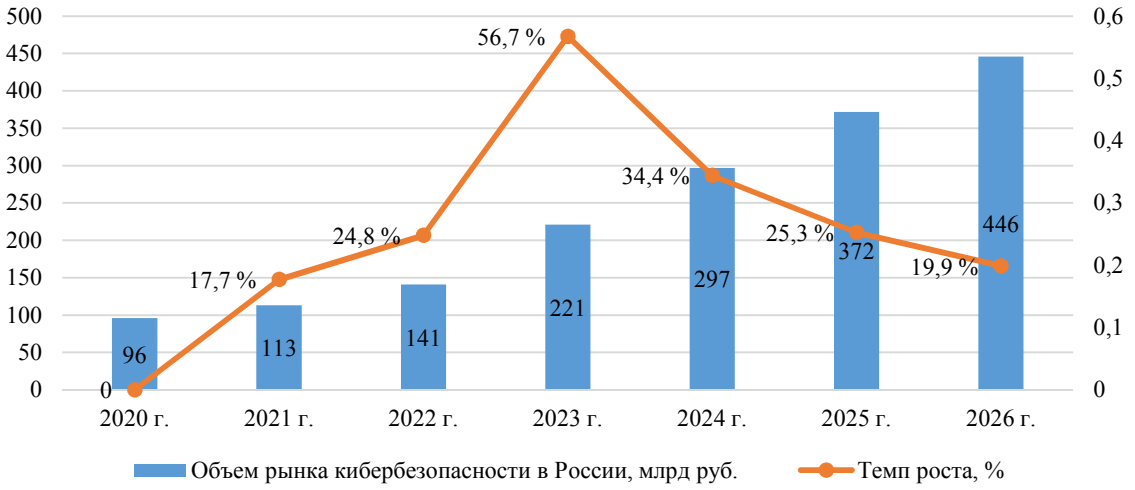

Рис. 2. Динамика и прогноз объема рынка кибербезопасности в России

Fig. 2. Dynamics and forecast of the cybersecurity market in Russia

По оценкам аналитического агентства ЦСР, с 2023 по 2027 г. объемные показатели российского рынка кибербезопасности должны вырасти не менее чем в 2,5 раза. При этом начиная с 2023 г. практически весь бюджет заказчиков на средства защиты информации в секторах B2G и B2B будет потрачен на продукцию российских вендоров, что даст возможность роста этой части рынка с 113 млрд руб. в 2021 г. до 446 млрд руб. в 2026 г.

Также на рынок кибербезопасности значительное влияние оказывает активная позиция регуляторов и органов власти в части необходимости импортозамещения (обеспечения технологической независимости) технических решений, связанных с обеспечением безопасного функционирования объектов критической информационной инфраструктуры [2].

Учитывая вышесказанное, а также то, что общепринятая методика, применяемая ранее в логистике в течение долгого времени, предполагала достижение экономических результатов исключительно за счет деятельности только самого предприятия непосредственно и его ближайшего окружения в цепи поставки, в настоящее время и в перспективе ближайших лет будет доминировать цифровая парадигма транспортно-логистического обслуживания. Данная парадигма основана на использовании цифровой платформенной концепции и создает необходимые предпосылки для формирования развитых экосистем, в которых множество вовлеченных субъектов создают высокую добавленную стоимость совместно, а также существуют условия для выстраивания высокозащищенной и устойчивой цифровой информационной инфраструктуры логистики.

Указанным тенденциям следует и авторский взгляд в публикации [3], направленный на анализ структурно-трансформационных процессов, обеспечивающих развитие сетевой телекоммуникационной конвергенции и расширение информационно-аналитического пространственного взаимодействия на различных уровнях, в том числе на уровне региона, государства и мировом уровне. Отмечаются достоинства внедрения и интеграции цифровых платформенных решений в транспортной логистике отдельной страны, а также цифровых интегрированных платформ глобального охвата, что обеспечивается за счет преодоления временных и пространственных разрывов и барьеров при взаимодействии субъектов транспортно-логистических процессов. В данном контексте целый ряд научных работ, например «Государство как платформа» Центра стратегических исследований, рассматривают физических и юридических лиц в качестве приоритетных потребителей цифровых государственных услуг, когда все подключенные субъекты имеют возможность работать с универсальными базами данных, но с разграниченным уровнем доступа. При этом добавочный синергетический эффект для пользователей цифровых сервисов может быть достигнут благодаря использованию инновационных способов сетевой координации и контроля сетевого взаимодействия [4].

В настоящее время неизбежность, объективность и долговременность цифровых трансформационных процессов практически во всех сферах деятельности предприятий и организаций не вызывает сомнений. Современная эра всеобщих реформ связана с изменением и приобретением инновационных феноменов, содержательно и по форме значительно отличающихся от прежних социально-политических и экономических отношений, техно-

логических и энергетических решений, научно-педагогических и образовательных процессов, природоохранных и экологических мероприятий, а также в сфере обеспечения экономической безопасности транспортно-логистических операций.

Следует признать, что целеполагание будущего миропорядка и его отличительные черты будут иметь прямое отношение к дальнейшему всеобщему и повсеместному внедрению цифровых решений, обусловливаемых нарастающей модернизацией микроэлектроники, телекоммуникационных средств и информационных технологий [5].

Цифровые трансформационные процессы в приоритетных отраслях российской экономики должны осуществляться исключительно с использованием отечественных разработок, платформенных решений и сервисов, создаваемых на основе сквозных универсальных цифровых инструментов, к числу которых относятся:

– Big Data;
– 3D-printing;
– Internet of Things;
– Artificial Intelligence;
– Wireless connection;
– Robotics & Sensors;
– Quantum technologies;
– Blockchain;
– Augmented & Virtual Reality.

В своей общности перечисленные инструменты формируют модель киберфизической экосистемы в логистике (рис. 3), позволяющей формировать совокупность интегрированных взаимодействий в системах «потребитель – поставщик» в функциональном логистическом контуре координации сквозных бизнес-процессов товародвижения и обмена данными о поставках на базе аналитики больших данных о характеристиках товаров и сведений о грузовладельцах для принятия обоснованных и оперативных решений в онлайн-режиме [6].

Рис. 3. Модель киберфизической экосистемы в логистике [4]

Fig. 3. A model of the cyberphysical ecosystem in logistics [4]

Следует признать, что процессам всеобщей цифровой трансформации присущи серьезные риски и угрозы, в частности большое количество автоматизированных транспортно-складских операций в логистике приведут к замене рабочих мест роботами, что может вызвать массовую безработицу в рядах низко- и среднеквалифицированных сотрудников. А это, в свою очередь, может существенно снизить уровень жизни достаточно большой части работоспособного населения. Тем не менее эра цифровых преобразований, формирование которой происходит очень быстро, предопределит в ближайшем будущем востребованность на кадровый потенциал высокой квалификации, а сотрудники будут привлекаться к выполнению функционала по контролю за функционированием роботов и поддержанию их устойчивой работы и долговечности.

Транспортная логистика, в свою очередь, подвержена негативному влиянию целого спектра рисков и угроз внедрения современных цифровых инструментов (рис. 4).

Риски больших данных	Риски промышленного интернета	Риски искусственного интеллекта и роботизации	Риски системы распределенного реестра
– нарушение конфиденциальности данных; – неоптимальная система сбора и хранения больших данных; – частичная или полная утрата данных вследствие ошибок обработки; – обработка больших данных не дает результата для аналитиков; – неготовность к переменам со стороны персонала и руководства	– внедрение вредоносного программного обеспечения, перехват управления устройствами, разрушение и воровство устройств; – уязвимости программного обеспечения; – DDoS-атаки на вычислительную систему; – сбой системы, сети, устройств в результате потери электропитания и других техногенных и природных факторов	– недостаток машинных мощностей для решения задач; – вытеснения рабочей силы искусственным интеллектом; – ошибки в обучении искусственного интеллекта и внедрении робототехники; – уязвимость робототехники (программа, калибровка, контроллеры); – большинство людей предпочитают человеческий контакт	– блокировка и потеря средств из-за уязвимости кода или зацикливания смарт-контракта; – утечка персональных данных; – атаки на узлы отправки и получения транзакций; – захват контроля благодаря доминирующим вычислительным мощностям; – отсутствие нормативного регулирования

Рис. 4. Угрозы при внедрении цифровых инструментов в транспортной логистике [4]

Fig. 4. Threats in the implementation of digital tools in transport logistics [4]

Согласно статистическим данным, на начало 2023 г. общее количество кибератак на Россию возросло на 65 %. Фиксируется 15-кратное повышение количества вредоносных воздействий на российские сервисы. Нейтрализовано около 25 тыс. попыток несанкционированного доступа на государственные цифровые ресурсы. Приблизительно 1 200 покушений на информационную безопасность были направлены на объекты критической инфраструктуры (энергоснабжения, водоснабжения, экологического мониторинга, транспорта и прочих ключевых систем, обеспечивающих жизнедеятельность населения) [7].

На морском транспорте на смену используемым ранее обычным системам, отвечающим за безопасность и оповещение об авариях и бедствиях, пришли локальные полноценные цифровые сети, основанные на использовании облачных технологий, в частности программное обеспечение, управляющее электронной навигацией. Указанные сети стали довольно заманчивой целью для хакерских атак, т. к. их работа направлена на постоянный сбор, интегрирование и анализ бортовой информации для отслеживания местоположения судна, данных о грузовых местах, технических вопросов, а также целого ряда проблем, связанных с судовождением в различных местах Мирового океана и прибрежных акваториях.

С похожими ситуациями сталкивается и железнодорожный транспорт. На смену обычным проводным системам управления движением поездов, которые были довольно сильно ограничены в возможностях информационного обмена с внешней средой, приходят беспроводные стандарты, обеспечивающие работоспособность широких сетей, объединяющих грузовые и пассажирские поезда с пультами управления железнодорожным движением дежурного по станции, что тоже может быть привлекательной мишенью для кибератак.

С целью нейтрализации перечисленных выше рисков и угроз необходимо в большей степени внедрять цифровые экосистемы в транспортной логистике, которые будут предусматривать в своей инфраструктуре комплекс современных информационных систем и технологий, имеющих потенциальную полезность для бизнеса и общества, а также позволяющих существенно повысить эффективность бизнес-процессов в транспортной логистике (рис. 5).

Цифровые информационные технологии, используемые в экосистемах транспортной логистики, обеспечивают доступность по целому ряду показателей контроля и мониторинга:

– сообщения о нештатных событиях;

– контроль температуры скоропортящихся грузов;

– обеспечение работы сенсоров и датчиков;

– определение времени в пути, возможных задержек, длительности стоянок и даты прибытия к месту назначения;

– определение местоположения транспорта, навигация и маршрутизация;

– расчет времени погрузочно-разгрузочных работ.

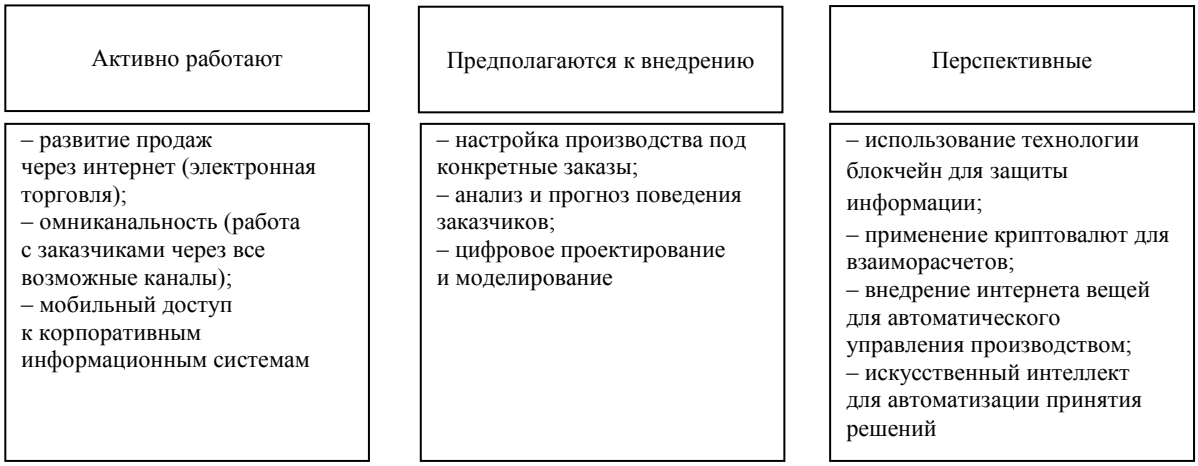

Рис. 5. Современные цифровые информационные технологии в экосистемах транспортно-логистического обслуживания [4]

Fig. 5. Modern digital information technologies in the eco-systems of transport and logistics services [4]

Для устранения проблемных вопросов, связанных с безопасностью экосистемных решений, в транспортной логистике требуется использовать цифровые информационные сервисы, имеющие следующие достоинства:

– усиление результативности логистических бизнес-процессов в части перемещения и доставки грузовых партий;

– выполнение требований по срочности текущих перевозок и интегрированное планирование последующих транспортировок;

– уменьшение доли поврежденных или похищенных грузов в процессе перемещения;

– быстрая реакция на нештатные события и ситуации;

– контроль состояния товаров в процессе транспортировки и мониторинг отгрузок.

Заключение

Таким образом, развитие рынка информационной безопасности России в контексте нейтрализации угроз внедрения цифровых инструментов в транспортно-логистических системах является ключевым для сохранения технологического суверенитета страны. В условиях продолжающейся цифровизации всех отраслей экономики, в частности промышленности и транспортно-логистического комплекса, именно усиление информационной безопасности позволить обеспечить контроль над суверенными цифровыми активами и системами управления товародвижением. В то же время поскольку до 2022 г. в России доля иностранных цифровых решений была достаточно большой, это позволило установить высокий уровень требований к продуктам и российских производителей. Начавшийся до 2022 г. процесс импортозамещения решений в сфере информационной безопасности теперь идет довольно быстро [8].

Необходимо отметить, что процесс перехода на полностью отечественное ПО для компаний транспортно-логистического комплекса все еще непростой и противоречивый, прежде всего, в силу высокой стоимости, т. к. цены на российское программное обеспечение увеличились в среднем на 50 % за последнее время. Поэтому далеко не каждое предприятие готово выделять дополнительные финансовые и материально-технические ресурсы для поддержания надежности своих систем кибербезопасности, хотя в среднем стоимостные показатели российских цифровых решений в области транспортной логистики ниже зарубежных аналогов, ранее представленных на рынке. Основные сложности заключаются в недостаточном уровне соответствия отечественного программного обеспечения требованиям и задачам компаний-заказчиков, поэтому организации и предприятия, связанные с выполнением транспортно-логистических услуг, вынуждены перестраивать свою цифровую информационную инфраструктуру, используя больше отечественных IT-решений, что также способствует увеличению нагрузки на сопровождение и поддержание данной инфраструктуры.

Список источников

1. Щербаков В. В., Букринская Э. М., Гвилия Н. А. и др. Логистика и управление цепями поставок: учеб. М.: Юрайт, 2019. 582 с.

2. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 гг. URL: https://www.csr.ru/ru/research/ (дата обращения: 20.10.2023).

3. Bag S., Dmitriev A. V., Sahu A. K. Barriers to adoption of blockchain technology in green supply chain man-

agement // Journal of Global Operations and Strategic Sourcing. 2020. N. 1. P. 0027. DOI: 10.1108/JGOSS-06-2020-0027.

4. Дмитриев А. В. Диджитализация транспортной логистики. СПб.: Изд-во СПбГЭУ, 2018. 161 с.

5. Гвилия Н. А., Дмитриев А. В., Рудковский И. Ф. и др. Управление цепями поставок: учеб. М.: Юрайт, 2017. 209 с.

6. Дмитриев А. В. Методологические основы управления логистикой транспортно-складских центров // Изв. Санкт-Петербург. ун-та экономики и финансов. 2012. № 6 (78). С. 76–81.

7. Число кибератак на информационные системы России выросло на 65 %. URL: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (дата обращения: 20.10.2023).

8. Информационная безопасность. URL: https://www.tadviser.ru/index.php/ (дата обращения: 20.10.2023).

References

1. Shcherbakov V. V., Bukrinskaia E. M., Gviliia N. A. i dr. *Logistika i upravlenie tsepiami postavok: uchebnik* [Logistics and Supply Chain Management: Textbook]. Moscow, Iurait Publ., 2019. 582 p.

2. *Prognoz razvitiia rynka kiberbezopasnosti v Rossiiskoi Federatsii na 2022–2026 gg.* [Forecast of the development of the cybersecurity market in the Russian Federation for 2022-2026.]. Available at: https://www.csr.ru/ru/research/ (accessed: 20.10.2023).

3. Bag S., Dmitriev A. V., Sahu A. K. Barriers to adoption of blockchain technology in green supply chain management. *Journal of Global Operations and Strategic Sourcing,* 2020, no. 1, p. 0027. DOI: 10.1108/JGOSS-06-2020-0027.

4. Dmitriev A. V. *Didzhitalizatsiia transportnoi logistiki* [Digitalization of transport logistics]. Saint Petersburg, Izd-vo SPbGEU, 2018. 161 p.

5. Gviliia N. A., Dmitriev A. V., Rudkovskii I. F. i dr. *Upravlenie tsepiami postavok: uchebnik* [Supply Chain Management: Tutorial]. Moscow, Iurait Publ., 2017. 209 p.

6. Dmitriev A. V. Metodologicheskie osnovy upravleniia logistikoi transportno-skladskikh tsentrov [Methodological foundations of logistics management of transport and warehouse centers]. *Izvestiia Sankt-Peterburgskogo universiteta ekonomiki i finansov,* 2012, no. 6 (78), pp. 76-81.

7. *Chislo kiberatak na informatsionnye sistemy Rossii vyroslo na 65 %* [The number of cyber attacks on Russian information systems has increased by 65%]. Available at: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (accessed: 20.10.2023).

8. *Informatsionnaia bezopasnost'* [Information security]. Available at: https://www.tadviser.ru/index.php/ (accessed: 20.10.2023).

Статья поступила в редакцию 29.10.2023; одобрена после рецензирования 11.02.2024; принята к публикации 05.06.2024
The article was submitted 29.10.2023; approved after reviewing 11.02.2024; accepted for publication 05.06.2024

Информация об авторе / Information about the author

Александр Викторович Дмитриев – доктор экономических наук, доцент; заведующий кафедрой экономической безопасности; Северо-Западный институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»; poliskasko@bk.ru

Aleksandr V. Dmitriev – Doctor of Economic Sciences, Assistant Professor; Head of the Department of Economic Security; Northwestern Institute of Management – branch FSBTI HE "The Russian Presidential Academy of National Economy and Public Administration"; poliskasko@bk.ru