

5. *Afanasyev, M. V.* Logistics of public procurement of investment goods. – SPb. : Publishing house of SPbSUEF, 2004. – 274 p.

6. *Myasnikova, L. A., Tyurina, K. A.* Modern tools for increasing the efficiency of public procurement system // *Vestnik of Perm University. Series: Economics.* – 2016. – № 3 (30). – P. 132-142.

7. *Scherbakov, V. V., Shulzhenko, T. G.* Strategic priorities of direction and intensity regulation of freight traffic under the new macroeconomic situation // *Railroad transport.* – 2022. – № 9. – P. 51-55.

8. *Borisova, V. V.* International procurement. – SPb. : Publishing house of SPbGEU, 2017. – 104 p.

9. *Oborin, M. S., Ponomarev, A. A.* Comparative analysis of public procurement systems in the world practice // *Innovations and investments.* – 2023. – № 3. – P. 53-59.

10. *Protsenko, I. O.* Strategic and innovative logistics // *Russian entrepreneurship.* – 2005. – Vol. 6, № 4. – P. 67-72.

11. *Kushnaryov, V. V., Albekov, A. U.* Logistic transformation of procurement

management system for public needs // *Commerce and logistics : collection of scient. articles.* – SPb. : Publishing house of SPbGUEF, 2013. – Vol. 11. – P. 14-21.

12. China increased government procurement by almost 12 % [Electronic resource]. – URL: <https://regnum.ru/news/3362137?ysclid=lt4ds6orob877728782> (date of acces: 20.02.2024).

13. *Liu, Nan.* Digital platforms to support innovation in system of public procurement in China // *Logistics and supply chain management : collection of scient. articles / ed. by V. V. Scherbakov, E. A. Smirnova.* – SPb. : Publishing house of SPbGEU, 2024. – Issue 8 (21). – P. 22-26.

14. *Liu, Nan.* Directions for development of digital platforms in public sector of Chinese economy // *Izvestiya of SPbSUE.* – 2021. – № 4 (130). – P. 168-172.

15. *Liu, Nan.* Information technologies in logistics of public procurement. China // *Logistics: foresight-research, profession, practice: materials of I National scient.-educat. conf.* – SPb., 2020. – P. 272-275.

DOI 10.54220/v.rsue.1991-0533.2024.1.85.003

А. В. Дмитриев, В. А. Нос

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ТРАНСПОРТНОЙ ЛОГИСТИКЕ

Аннотация

В статье обсуждаются вопросы обеспечения экономической безопасности как одной из важнейших качественных характеристик логистических систем, определяющих способность обеспечивать в процессе товародвижения установленные 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 обеспечения 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, направленных на обеспечение надежности функционирования и реализации стратегии хозяйственных субъектов. Обосновывается необходимость использования современных цифровых технологий для повышения уровня экономической безопасности в логистических системах и обеспечения прозрачности, контролируемости и прослеживаемости материальных потоков в сфере товародвижения. При этом сам 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

A. V. Dmitriev, V. A. Nos

ENSURING ECONOMIC SECURITY WHEN IMPLEMENTING DIGITAL TECHNOLOGIES IN TRANSPORT LOGISTICS

Abstract

Article discusses issues of ensuring economic security as one of the most important qualitative characteristics of logistics systems that determine the ability to ensure the established parameters of material flows in process of goods distribution when introducing digital systems and technologies. Analysis of modern risks and threats characteristic of development of digital ecosystems of transport and logistics services is carried out. The key factors for ensuring economic security and their importance in logistics are examined from the point of view of ensuring operational control over compliance with established key indicators of product distribution. Interpretation of concept of «economic security» is given from the position of protecting a business entity from external and internal threats to increase the level of competitiveness and sustainability of enterprise in market. Issues of ensuring the parameters of commodity distribution within established threshold values are touched upon in order to achieve optimal functioning of commodity distribution system and ensure the economic activity of enterprise with all the necessary resources. Logistics systems are studied for effective organization and management of material flows, aimed at ensuring the reliability of operation and implementation of strategy of economic entities. Necessity of using modern digital technologies to increase the level of economic security in logistics systems and ensure transparency, controllability and traceability of material flows in the field of commodity distribution is substantiated. At the same time, fact of digitalization of cargo delivery processes is considered from perspective of ecosystem paradigm and platform concept. Patterns of transformation of traditional logistics operators into providers of digital logistics services are substantiated. Model of cyber-physical ecosystem in logistics has been developed, providing end-to-end management of business processes and data exchange in process of goods distribution.

Keywords

Economic security, logistics, digital ecosystems, transport, digital technologies, digital platforms.

Введение

В настоящее время в качестве одной из ключевых качественных характеристик современных транспортно-логистических систем выступает экономическая безопасность, предусматривающая в процессе товародвижения контроль соблюдения установленных параметров материальных и связанных потоков, а также достаточного уровня обеспеченности предприятий всеми видами ресурсов для осуществления ими хозяйственной деятельности.

Экономическая безопасность в данном случае обеспечивает не только защиту хозяйствующих субъектов от внутренних и внешних угроз, но и стимулирует устойчивое и стабильное функционирование субъектов в условиях

эффективного противодействия негативному воздействию условий окружающей среды. В данном контексте роль логистики как науки и сферы практической деятельности направлена на реализацию стратегий хозяйствующих субъектов, поддержание результативности их работы и связана с оптимизацией организационно-управленческих усилий по продвижению материальных потоков. Очевидно, что отсутствие в этом случае налаженной и действенной системы экономической безопасности на предприятии приведет к срыву реализации его стратегии и риску потери конкурентных преимуществ на рынке.

Факторы экономической безопасности в логистике представлены на рисунке 1.

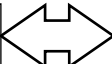
Факторы		Значение
– налаженные и упорядоченные правила и процедуры управления бизнес-процессами в логистике; – задокументированные правила внутреннего распорядка и ответственность за их соблюдение; – соблюдение техники безопасности на рабочих местах; – урегулирование претензий в досудебном порядке; – работа по единым стандартизированным технологиям; – применение специализированных закрытых цифровых сетей для обмена данными; – конфиденциальность и обеспечение и охрана коммерческой тайны; – профессиональная переподготовка сотрудников		– обеспечение оперативного контроля за соблюдением установленных ключевых показателей товародвижения; – снижение риска противоправных действий должностных лиц; – повышение производительности труда, сокращение срывов графика работы; – сокращение количества рекламаций и штрафных санкций; – применение всеми субъектами цепи поставки единых форм документов и технологических решений; – предотвращение несанкционированного доступа к информации третьими лицами; – противодействие промышленному шпионажу и инсайдерским атакам; – усиление кадровой составляющей экономической безопасности

Рисунок 1 – Факторы экономической безопасности в логистике [1]

В современных условиях повышению уровня экономической безопасности в сфере транспортно-логистического обслуживания способствует использование цифровых инноваций и современных информационных технологий в области товародвижения, обеспечивающих прозрачность и контролируемость в режиме онлайн всех видов потоков, в том числе,

материальных, информационных и финансовых.

Целью исследования является обоснование использования методологии обеспечения экономической и информационной безопасности при внедрении современных цифровых технологий в транспортной логистике в условиях нарастающих угроз кибербезопасности.

Материалы и методы

Общепринятые методики, применяемые прежде в логистике в течение длительного периода времени, предполагали получение экономического эффекта только за счет функционирования предприятия как такового, а также его цепи поставки и ближайшего делового окружения. Сейчас и в обозримой перспективе мы будем наблюдать доминирование цифровой парадигмы оказания транспортно-логистических услуг, основанной на применении платформенной концепции и создании необходимых предпосылок для образования зрелых экосистем, интегрирующих большое число участвующих субъектов, создающих совместно высокие показатели добавленной стоимости. При этом ключевым условием реализации новой методики должна стать высокозащищенная и устойчивая цифровая информационная инфраструктура логистики.

Указанным тенденциям следует и авторский взгляд в публикации [4], 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 от 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, таких как, например, «Государство как платформа»,

которое выполнено Центром 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 [5].

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 [3].

В своей общности цифровые инструменты формируют модель киберфизической экосистемы в логистике (рис. 2), 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 [2].

Однако следует признать, что процессам всеобщей цифровой трансформации присущи ряд серьезных рисков и угроз, в частности, риски нарушения конфиденциальности данных, использование вредоносного программного обеспечения, несовершенство регуляторной базы и др. (рис 3).



Рисунок 2 – Модель киберфизической экосистемы в логистике [5]

Результаты и их обсуждение

Одной из достаточно широко применяемых в логистике форм осуществления бизнес-процессов в последнее время становится цифровая экосистемная организация, основанная на платформенной концепции управления товародвижением. Данная концепция является драйвером трансформации способов предоставления потребителям цифрового логистического сервиса и позволяет существенно повысить уровень конкурентоспособности предприятий на рынке относительно традиционного подхода к деятельности логистических операторов.

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 2021 г. и опубликованного в 2022 г. Фондом «Центр стратегических разработок» (ЦСР) [7].

Прежде всего, рассмотрим структурные показатели по объемам долей рынка на 2021 г. по категориям средств защиты информации (табл. 1).

Таблица 1 – Объемные структурно-рыночные показатели в разрезе видов и категорий средств защиты цифровых данных

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

Среднегодовые показатели темпа роста рынка кибербезопасности в России по итогам 2021 г. оцениваются более, чем в 17 %. Данное значение превышает прирост мировых показателей рынка ки-

бербезопасности, 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. 3).

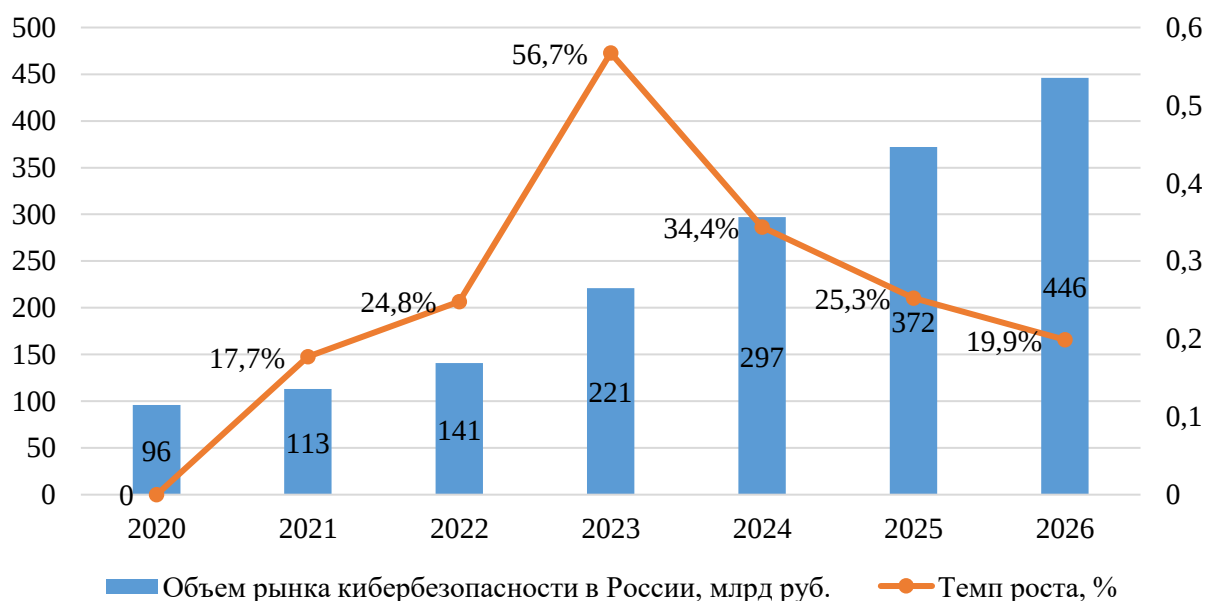


Рисунок 3 – Динамика и прогноз объема рынка кибербезопасности в России, млрд руб.

Приведенные результаты исследования Центра стратегических разработок «Прогноз развития рынка решений для информационной безопасности в Российской Федерации в 2022-2026 гг.» 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 [8].

По оценкам аналитического агентства ЦСР, с 2023 по 2027 гг. 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 [8].

Транспортная логистика, в свою очередь, подвержена негативному влиянию целого спектра рисков и угроз внедрения современных цифровых инструментов (рис. 4). Согласно статистическим данным, на начало 2023 г. на 65 % возросло общее количество кибератак на Россию. Фиксируется 15-кратное повышение количества кибератак на российские сервисы. Нейтрализовано около

25 тыс. кибератак на государственные цифровые ресурсы. Приблизительно 1200 кибератак были направлены на объекты критической инфраструктуры

(энергоснабжения, водоснабжения, экологического мониторинга, транспорта и прочих ключевых систем, обеспечивающих жизнедеятельность населения) [6].

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; • вытеснение 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 заикливания смарт-контракта; • утечка персональных данных • атаки на узлы отправки и получения транзакций • захват контроля благодаря доминирующим вычислительным мощностям • отсутствие нормативного регулирования

Рисунок 4 – Угрозы при внедрении цифровых инструментов в транспортной логистике [5]

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, так как 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. А это тоже может быть привлекательной мишенью для кибератак.

С целью нейтрализации перечисленных выше рисков и угроз необходимо во все 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).

Активно работают	Предполагаются к внедрению	Перспективные
• развитие продаж через интернет (электронная торговля); • омниканальность (работа с заказчиками через все возможные каналы); • мобильный доступ к корпоративным информационным системам	• настройка производства под конкретные заказы; • анализ и прогноз поведения заказчиков; • цифровое проектирование и моделирование	• использование технологии Блокчейн для защиты информации; • применение криптовалют для взаиморасчетов; • внедрение интернета вещей для автоматического управления производством; • искусственный интеллект для автоматизации принятия решений

Рисунок 5 – Современные цифровые информационные технологии в экосистемах транспортно-логистического обслуживания [5]

Изображенные на рисунке 5 цифровые информационные технологии, используемые в экосистемах транспортной логистики, обеспечивают доступность по целому ряду показателей контроля и мониторинга [6]:

- 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.

Выводы

Для устранения проблемных вопросов, связанных с безопасностью экосистемных решений в транспортной логистике, требуется использовать цифровые информационные сервисы, имеющие следующие достоинства [6]:

- 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.

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 позволит обеспечить контроль над суверенными цифровыми активами и системами управления товародвижением. В то же время, поскольку до 2022 г. в России доля ино-

странных 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 [9].

Библиографический список

1. Логистика и управление цепями поставок : учебник / В. В. Щербаков, Э. М. Букринская, Н. А. Гвилия [и др.]. – 1-е изд. – М. : Юрайт, 2019. – 582 с.
2. *Дмитриев, А. В.* Методологические основы управления логистикой транспортно-складских центров // Известия Санкт-Петербургского университета экономики и финансов. – 2012. – № 6 (78). – С. 76-81.
3. Управление цепями поставок : учебник / Н. А. Гвилия, А. В. Дмитриев, И. Ф. Рудковский [и др.]. – М. : Юрайт, 2017. – 209 с.
4. Barriers to adoption of blockchain technology in green supply chain management / S. Bag, A. V. Dmitriev, A. K. Sahu, A. K. Sahu // Journal of Global Operations and Strategic Sourcing. – 2020. – P. 0027.
5. *Дмитриев, А. В.* Диджитализация транспортной логистики. – СПб. : Изд-во СПбГЭУ, 2018. – 161 с.
6. *Дмитриев, А. В., Щербаков, В. В.* Обеспечение экономической безопасности и устойчивости цепей поставок в условиях цифровизации // Вестник факультета управления СПбГЭУ. – 2023. – Вып. 15. – С. 11-18.
7. Число кибератак на информационные системы России выросло на 65 % [Электронный ресурс]. – URL: <https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak> (дата обращения: 29.10.2023).
8. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022-2026 гг. [Электронный ресурс]. –

URL: <https://www.csr.ru/ru/research> (дата обращения: 29.10.2023).

9. Информационная безопасность [Электронный ресурс]. – URL: <https://www.tadviser.ru/index.php> (дата обращения: 29.10.2023).

Bibliographic list

1. Logistics and supply chain management : textbook / V. V. Shcherbakov, E. M. Bukrinskaya, N. A. Gvilia [et al.]. – 1st ed. – M. : Yurait, 2019. – 582 p.
2. *Dmitriev, A. V.* Methodological foundations of logistics management of transport and warehouse centers // Proceedings of SPbUEF. – 2012. – № 6 (78). – P. 76-81.
3. Supply chain management : textbook / N. A. Gvilia, A. V. Dmitriev, I. F. Rudkovsky [et al.]. – M. : Yurait, 2017. – 209 p.
4. Barriers to adoption of blockchain technology in green supply chain management / S. Bag, A. V. Dmitriev, A. K. Sahu, A. K. Sahu // Journal of Global Operations and Strategic Sourcing. – 2020. – P. 0027.
5. *Dmitriev, A. V.* Digitalization of transport logistics. – SPb. : Publishing house of SPbSU, 2018. – 161 p.
6. *Dmitriev, A. V., Shcherbakov, V. V.* Ensuring economic security and sustainability of supply chains in context of digitalization // Bulletin of Faculty of Management of SPbGEU. – 2023. – Issue 15. – P. 11-18.
7. Number of cyber attacks on Russian information systems has increased by 65 % [Electronic resource]. – URL: <https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak> (date of access: 29.10.2023).
8. Forecast of development of cyber security market in Russian Federation for 2022-2026 [Electronic resource]. – URL: <https://www.csr.ru/ru/research> (date of access: 29.10.2023).
9. Information security [Electronic resource]. – URL: <https://www.tadviser.ru/index.php> (date of access: 29.10.2023).