

Организационно-экономические аспекты обеспечения информационной безопасности в логистических системах

Дмитриев А. В.

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация; dmitriev-av@ranepa.ru

РЕФЕРАТ

В статье обсуждаются вопросы обеспечения информационной и экономической безопасности, являющиеся одними из важнейших качественных характеристик логистических систем, определяющих способность соблюдать в процессе товародвижения установленные параметры материальных потоков при внедрении современных информационных 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. 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: информационная безопасность, экономическая безопасность, логистика, цифровые экосистемы, транспорт, цифровые технологии, цифровые платформы

Для цитирования: *Дмитриев А. В.* Организационно-экономические аспекты обеспечения информационной безопасности в логистических системах // Управленческое консультирование. 2025. № 1. С. 34–44.

Organizational and Economic Aspects of Ensuring Information Security in Logistics Systems

Alexander V. Dmitriev

Russian Academy of National Economy and Public Administration under the President of the Russian Federation (North-West Institute of Management RANEPa), St. Petersburg, Russian Federation; dmitriev-av@ranepa.ru

ABSTRACT

The article discusses issues of ensuring information and 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 the process of goods distribution when introducing digital systems and technologies. An analysis of modern risks and threats characteristic of the 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. The issues of ensuring the parameters of commodity distribution within the established threshold values are touched upon in order to achieve optimal functioning of the commodity distribution system and ensure the economic activity of the enterprise with all the necessary resources. Logistics systems are studied for the effective organization and management of material flows, aimed at ensuring the reliability of operation 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 ensure transparency, controllability and traceability of material flows in the field of commodity distribution is substantiated. At the same time, the very 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 cyber-physical ecosystem in logistics has been developed, providing end-to-end management of business processes and data exchange in the process of goods distribution.

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

For citing: Dmitriev A. V. Organizational and Economic Aspects of Ensuring Information Security in Logistics Systems // Administrative consulting. 2025. N 1. P. 34–44.

Введение

В современных экономических и технологических условиях информационная безопасность представляет собой важнейшую качественную характеристику в логистических системах, поскольку в последнее время все больше транспортно-логистических операций выполняется при посредстве информационных технологий. Как экономическая, так и информационная безопасность не только определяют функциональные возможности логистических систем по обеспечению установленных параметров материальных потоков в процессе товародвижения, но и формируют достаточный уровень обеспеченности предприятий и организаций ресурсами для осуществления ими своей хозяйственной деятельности.

Согласно общепринятому определению, безопасность — это, с одной стороны, защита субъекта от внешних и внутренних угроз, а с другой стороны, способность субъекта к стабильному функционированию в условиях противодействия негативному влиянию окружающей среды. Соответственно, экономическая и информационная составляющие представляют собой функциональные направления обеспечения безопасности хозяйствующих субъектов [1].

Поскольку в современном понимании логистику рассматривают как научную дисциплину и сферу практической деятельности, связанную с оптимизацией организационно-технологических и экономико-управленческих механизмов контроля материальных потоков, поэтому инструментарий логистики направлен на поддержание эффективного функционирования хозяйственной деятельности и реализации стратегических целей предприятия в области доведения продукции до конечного потребителя с наименьшими затратами.

Отсутствие налаженной и устойчивой системы экономической и информационной безопасности не позволит хозяйствующим субъектам обеспечить реализацию своей логистической стратегии, а также приведет к высокой степени вероятности потери конкурентных преимуществ на рынке.

При этом можно выделить целый ряд ключевых факторов обеспечения экономической и информационной безопасности, имеющих существенное значение в рамках проектирования и развития логистических систем (табл. 1).

Таблица 1

Ключевые факторы обеспечения экономической и информационной безопасности в логистических системах [1]
Table 1. Key factors for ensuring economic and information security in logistics systems [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, 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

Материалы и методы

Одним из важнейших факторов повышения уровня экономической безопасности в области логистики следует считать применение современных цифровых информационных технологий в сфере товародвижения для обеспечения прозрачности и контролируемости материальных потоков в режиме онлайн [2; 10].

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.

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, основанная на использовании цифровой платформенной концепции и создающей необходимые предпосылки для формирования развитых экосистем, в которых множество вовлеченных субъектов создают высокий процент добавленной стоимости совмест-

но при условии создания высокозащищенной и устойчивой цифровой информационной инфраструктуры 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 транспортную логистику 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 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].

Результаты

Поскольку предоставление логистических услуг в цифровом виде и развитие киберфизических систем непосредственно зависят от уровня защищенности цифровой инфраструктуры товародвижения, в данном контексте целесообразно остановиться на анализе и оценке рынка услуг кибербезопасности по итогам 2023 г., опубликованного Фондом «Центр стратегических разработок» (ЦСР) [7].

Прежде всего, рассмотрим структурные показатели по объемам долей рынка на 2023 г. по категориям средств защиты информации (табл. 2).

Среднегодовые показатели темпа роста рынка кибербезопасности в России по итогам 2021 г. оцениваются более чем в 17%. Данное значение превышает прирост мировых показателей, которые хотя и были исторически довольно высоки, благодаря промышленно развитым странам в Западной Европе и Северной

Таблица 2

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

Table 2. Volumetric structural and market indicators by types and categories of digital data protection tools

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



Рис. 1. Динамика и прогноз объема рынка кибербезопасности в России, млрд руб.

Fig. 1. Dynamics and forecast of the cybersecurity market size in Russia, billion rubles

Америке, однако в настоящее время в силу сформировавшейся за последние годы зрелости и насыщения, растут 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. 1) [9].

Обсуждение

Приведенные выше результаты исследования Центра стратегических разработок «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. массовый уход из России западных разработчиков и вендоров комплексных решений и средств информационной защиты, что предопределило существенную реструктуризацию рыночных долей в перспективе ближайших 5 лет.

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 со 113 млрд руб. в 2021 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 [7].

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, технологических 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 [3].

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. 2), позволяющей формировать совокупность

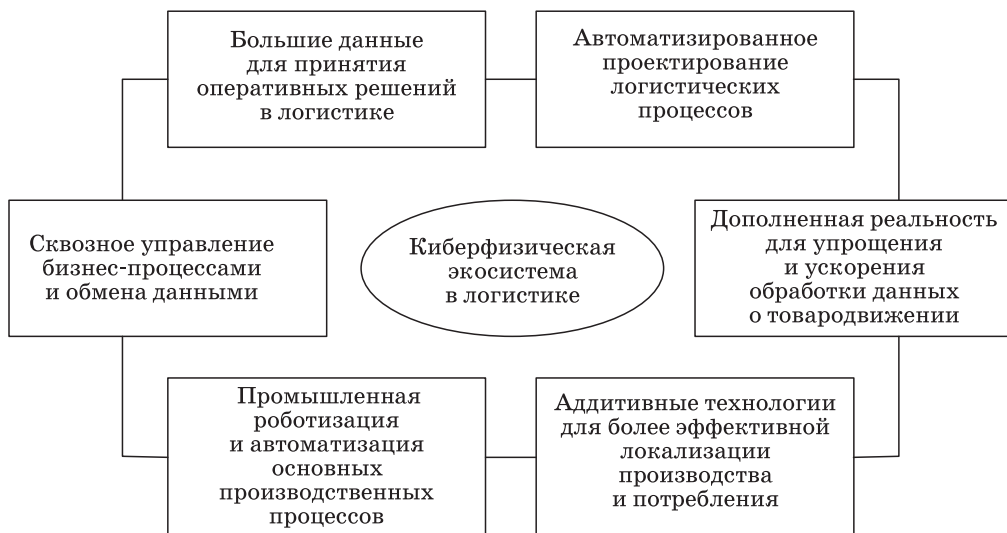


Рис. 2. Модель киберфизической экосистемы в логистике [5]
Fig. 2. Model of the cyber-physical ecosystem in logistics [5]

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 присущ ряд серьезных рисков и угроз, в частности, большое количество автоматизированных транспортно-складских операций в логистике приведет 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 жизнеспособности.

Транспортная логистика, в свою очередь, подвержена негативному влиянию целого спектра рисков и угроз внедрения современных цифровых инструментов (табл. 3).

Таблица 3

**Угрозы при внедрении цифровых инструментов
в транспортной логистике [5; 11]**

Table 3. Threats in the implementation of digital tools in transport logistics [5; 11]

Риски	Угрозы
Риски больших данных	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
Риски промышленного интернета	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
Риски искусственного интеллекта и роботизации	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
Риски системы распределенного реестра	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

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 25 000 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].

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.

Изображенные в табл. 4 цифровые информационные технологии, используемые в экосистемах транспортной логистики, обеспечивают доступность по цело-

Таблица 4

**Современные цифровые информационные технологии
в экосистемах транспортно-логистического обслуживания [5]**
Table 4. Modern digital information technologies in transport
and logistics service ecosystems [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

му 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.

Заключение

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.

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 иностранных цифровых решений была достаточно большой, это позволило установить высокий уровень требований к продуктам и российским производителям. Начавшийся до 2022 г. процесс импортозамещения решений в сфере информационной безопасности теперь идет довольно быстро [8]. Однако надо отметить, что переход на полностью отечественное ПО для компаний транспортно-логистического комплекса процесс все еще непростой и противоречивый. Прежде всего, в силу высокой стоимости, так как цены на российское программное обеспечение возросли 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 надо признать, что в среднем стоимостные показатели российских цифровых решений в области транспортной логистики ниже зарубежных аналогов, ранее представленных на рынке. А 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.

Литература

1. *Дмитриев А. В.* Диджитализация транспортной логистики. СПб. : СПбГЭУ, 2018. 161 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. Информационная безопасность [Электронный ресурс]. URL: <https://www.tadviser.ru/index.php/> (дата обращения: 30.11.2023).
4. 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.
5. Плотников В. А., Погодина В. В., Смирнов А. А. Национальная экономическая безопасность и государственная политика развития промышленности // Управленческое консультирование. 2023. № 9. С. 35–44. <https://doi.org/10.22394/1726-1139-2023-9-35-44>
6. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы [Электронный ресурс]. URL: <https://www.csr.ru/ru/research/> (дата обращения: 30.11.2023).
7. Управление цепями поставок : учебник / Н. А. Гвилия, А. В. Дмитриев, И. Ф. Рудковский [и др.]. М. : Юрайт, 2017. 209 с.
8. Халин В. Г., Чернова Г. В. Цифровизация и киберриски // Управленческое консультирование. 2023. № 7. С. 28–41. <https://doi.org/10.22394/1726-1139-2023-7-28-41>
9. 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: 30.11.2023).
10. Шаббаева С. В., Шаббаев А. И. Инструменты реализации стратегий в условиях цифровой трансформации промышленных предприятий // Управленческое консультирование. 2023. № 10. С. 69–79. <https://doi.org/10.22394/1726-1139-2023-10-69-79>
11. Barriers to adoption of blockchain technology in green supply chain management / S. Bag, A. V. Dmitriev, A. K. Sahu // Journal of Global Operations and Strategic Sourcing. 2020. P. 0027. DOI 10.1108/JGOSS-06-2020-0027

Об авторе:

Дмитриев Александр Викторович, заведующий кафедрой безопасности Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), доктор экономических наук, доцент; dmitriev-av@ranepa.ru

References

1. Dmitriev A. V. Digitalization of transport logistics. Saint Petersburg : Saint Petersburg State Economic University, 2018. 161 p. (In Russ.)
2. Dmitriev A. V. Methodological foundations of logistics management of transport and warehouse centers // News of the Saint Petersburg University of Economics and Finance [Izvestiya Sankt-Peterburgskogo universiteta e'konomiki i finansov]. 2012. N 6 (78). P. 76–81. (In Russ.)
3. Information security [Electronic resource]. URL: <https://www.tadviser.ru/index.php/> (accessed: 30.11.2023). (In Russ.)
4. Logistics and supply chain management : textbook / V. V. Shcherbakov, E. M. Bukrinskaya, N. A. Gviliya [etc.]. 1st ed. Moscow : Yurayt Publishing House, 2019. 582 p. (In Russ.)
5. Plotnikov V. A., Pogodina V. V., Smirnov A. A. National economic security and state policy for industrial development // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2023. N 9. P. 35–44. (In Russ.) <https://doi.org/10.22394/1726-1139-2023-9-35-44>
6. Forecast for the development of the cybersecurity market in the Russian Federation for 2022–2026 [Electronic resource]. URL: <https://www.csr.ru/ru/research/> (accessed: 30.11.2023). (In Russ.)
7. Supply chain management : textbook / N. A. Gviliya, A. V. Dmitriev, I. F. Rudkovsky [etc.]. Moscow : Yurayt Publishing House, 2017. 209 p. (In Russ.)
8. Khalin V. G., Chernova G. V. Digitalization and cyber risks // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2023. N 7. P. 28–41. (In Russ.) <https://doi.org/10.22394/1726-1139-2023-7-28-41>
9. The 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> (accessed: 30.11.2023). (In Russ.)
10. Shabaeva S. V., Shabaev A. I. Tools for implementing strategies in the context of digital transformation of industrial enterprises // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2023. N 10. P. 69–79. (In Russ.) <https://doi.org/10.22394/1726-1139-2023-10-69-79>

11. Barriers to adoption of blockchain technology in green supply chain management / S. Bag, A.V. Dmitriev, A.K. Sahu // Journal of Global Operations and Strategic Sourcing. 2020. P. 0027. DOI: 10.1108/JGOSS-06-2020-0027

About the author:

Alexander V. Dmitriev, Head of the Department of Security, North-West Institute of Management RANEPА (Saint Petersburg, Russian Federation), Doctor of Economics, Associate Professor; dmitriev-av@ranepa.ru