



Экономическая безопасность цифровых экосистемных решений в логистике

А.В. Дмитриев¹¹ Северо-Западный институт управления – филиал РАНХиГС (Санкт-Петербург, Россия)

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 оптимального функционирования товаропроводящей системы и обеспеченности хозяйственной деятельности предприятия всеми необходимыми ресурсами. Исследуются логистические системы на предмет эффективной организации и управления материальными потоками, направленные 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.

Для цитирования:

Дмитриев А.В. (2024). Экономическая безопасность цифровых экосистемных решений в логистике. *Стратегические решения и риск-менеджмент*, 15(1): 23–29. DOI: 10.17747/2618-947X-2024-1-23-29.

Economic security of digital ecosystem solutions in logistics

A.V. Dmitriev¹¹ North-Western Institute of Management – Branch of RANEPA (Saint Petersburg, Russia)

Abstract

The article discusses issues of ensuring economic security as one of the most important qualitative characteristics of logistics systems, which determines the ability to ensure the established parameters of material flows in the process of goods distribution when implementing digital systems and technologies. Contemporary risks and threats characteristic of the development of digital transport and logistics ecosystems are analysed. 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. An interpretation of the concept of 'economic security' is given from the point of view of protecting a business entity from external and internal threats in order to increase the level of competitiveness and sustainability of business in the market. The issues of ensuring the parameters of goods distribution within the established thresholds are addressed in order to achieve the optimal functioning of the goods distribution system and to ensure the economic activity of the enterprise with all the necessary resources. Logistics systems are studied for the effective organisation and management of material flows, aimed at ensuring the reliability of operations and the implementation of the strategy of economic entities. The need to use modern digital technologies to increase the level of economic security in logistics systems and to ensure the transparency, controllability and traceability of material flows in the field of goods distribution has been demonstrated. At the same time, the very fact of digitising cargo delivery processes is considered from the perspective of the ecosystem paradigm and the 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, enabling end-to-end management of business processes and data exchange in the distribution of goods.

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

For citation:

Dmitriev A.V. (2024). Economic security of digital ecosystem solutions in logistics. *Strategic Decisions and Risk Management*, 15(1): 23–29. DOI: 10.17747/2618-947X-2024-1-23-29. (In Russ.)

物流领域数字生态系统解决方案的经济安全

A.V. Dmitriev¹¹ 北西管理学院-俄罗斯联邦总统国民经济和行政学院分校 (俄罗斯, 圣彼得堡)

简介

文章讨论了经济安全性作为物流系统中最重要的质量特征之一的问题, 这些特征决定了在数字化系统和技术的应用过程中, 物流系统在货物流动过程中实现设定的物流参数的能力。对运输物流服务数字生态系统发展中的现代风险和威胁进行分析。研究了在物流中确保经济安全的关键因素以及它们在确保货物流动的关键指标得到遵守方面的重要性。给出了对“经济安全性”概念的解释, 从经济主体受到内部和外部威胁的程度角度来看, 以提高企业在市场上的竞争力和稳定性。讨论了在设定的门槛值范围内确保货物流动参数以实现货物传送系统的最佳运作和企业经营活动所需的所有必要资源的问题。研究了物流系统的有效组织和管理物流流程, 以确保经济主体的可靠运作和战略实施。论证了在物流系统中提高经济安全水平和确保货物流动领域的透明度、可控性和追溯性的必要性, 这需要使用现代数字技术。同时, 将货物交付过程数字化的事实从生态系统范式和平台概念的角度进行了考察。论证了传统物流运营商转变为数字物流服务提供商的规律性。提出了一种在物流中实现端到端业务流程管理和数据交换的模型, 即物理-数字生态系统模型。

关键词: 经济安全, 物流, 数字生态系统, 运输, 数字技术, 数字平台。

引用文本:

Dmitriev A.V. (2024). 物流领域数字生态系统解决方案的经济安全性. 战略决策和风险管理, 15(1): 23–29. DOI: 10.17747/2618-947X-2024-1-23-29. (俄文)

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 этом 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 этом контексте логистика как наука и сфера 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.

Кроме того, высокая устойчивость и функциональность современных механизмов товародвижения, в том числе и в международном сообщении, позволяет повысить эффективность функционирования всех вовлеченных в интегрированную логистическую систему субъектов и наладить бизнес-процессы по доведению товаров до конечных потребителей оптимальным образом.

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

1. Теоретический обзор

Использование цифровых технологий в логистических системах сейчас является объективной и сложившейся реальностью. Однако при всех достоинствах цифровизации, позволяющих ускорять выполнение логистических операций

и отслеживать их в режиме онлайн, цифровые экосистемы могут быть подвержены достаточно высокому уровню внешних и внутренних угроз, связанных прежде всего с уязвимостью информационной инфраструктуры хозяйствующих субъектов. Поскольку логистика как сфера практической деятельности тесно связана со сферой материального производства и доведением продукции до конечных потребителей, ее устойчивое функционирование, в том числе с применением современных информационных технологий, является одним из ключевых факторов экономической безопасности государства и залогом поддержания высокого уровня благосостояния населения.

Проблемам внедрения цифровых технологий и обеспечению экономической безопасности в области логистики и управления цепями поставок посвящено достаточно много научных исследований. Авторы работы [Плотников и др., 2023] делают акцент на формировании широкого спектра новых угроз, порождающих возможность ослабления национальной и экономической безопасности, вызванных турбулентностью и неустойчивостью мировой экономики, что приводит к необходимости усиления промышленного потенциала и опережающего технологического развития нашей страны.

В статье [Малюков и др., 2023] авторы характеризуют устойчивость экономических систем в ракурсе стратегического наполнения с использованием системы сбалансированных показателей, что позволяет обеспечить синхронность управления комплексной эффективностью предприятия, возникающими в процессе работы рисками и реализовать повестку экономической безопасности хозяйственных систем при их функционировании в условиях широкого спектра современных угроз и вызовов.

Исследование [Трачук, Линдер, 2023] посвящено влиянию цифровых платформ на показатели деятельности промышленных предприятий в контексте формирования и развития уникальных конкурентных преимуществ и повышения эффективности основных и вспомогательных процессов в сфере реального производства для поиска источников интернационализации и выхода на новые рынки в условиях отрицательных сетевых эффектов.

В работе [Носов, 2019] обосновывается стратегическая роль логистики в обеспечении экономической безопасности страны, а результативность логистической деятельности

Дмитриев А.В.
Dmitriev A.V.

Экономическая безопасность цифровых экосистемных решений в логистике
Economic security of digital ecosystem solutions in logistics
物流领域数字生态系统解决方案的经济安全

определяется как основа экономики любого государства. При этом методология логистики должна тесно коррелировать с принципиальными задачами, обеспечивающими комплексную модернизацию отраслевой производственно-технологической базы для нейтрализации внешних и внутренних угроз в экономике, в том числе в транспортно-логистическом секторе.

2. Материал и методы исследования

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.

Рис. 1. Факторы экономической безопасности в логистике
Fig. 1. Economic security factors in logistics

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

Источник: [Дмитриев, 2012].

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 [Bag et al., 2020], 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.

Рис. 2. Модель киберфизической экосистемы в логистике
Fig. 2. Model of a cyber-physical ecosystem in logistics



Источник: [Дмитриев, 2018].

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 этом 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 [Богачев, Трифонов, 2022].

Следует признать, что целеполагание будущего миропорядка и его отличительные черты будут иметь прямое отношение к дальнейшему всеобщему и повсеместному внедрению цифровых решений, обуславливаемых нарастающей модернизацией микроэлектроники, телекоммуникационных средств и информационных технологий [Халин, Чернова, 2023].

В своей общности цифровые инструменты формируют модель киберфизической экосистемы в логистике (рис. 2), позволяющей создавать 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-режиме¹.

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

¹ Логистика и управление цепями поставок: учебник для вузов (2019). Под ред. В.В. Щербакова. М., Юрайт.

3. Результаты исследования и их обсуждение

Как было отмечено выше, 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.

Таблица 1
Объемные структурно-рыночные показатели в разрезе видов и категорий средств защиты цифровых данных
Table 1
Volumetric structural and market indicators by type and category of digital privacy tools

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

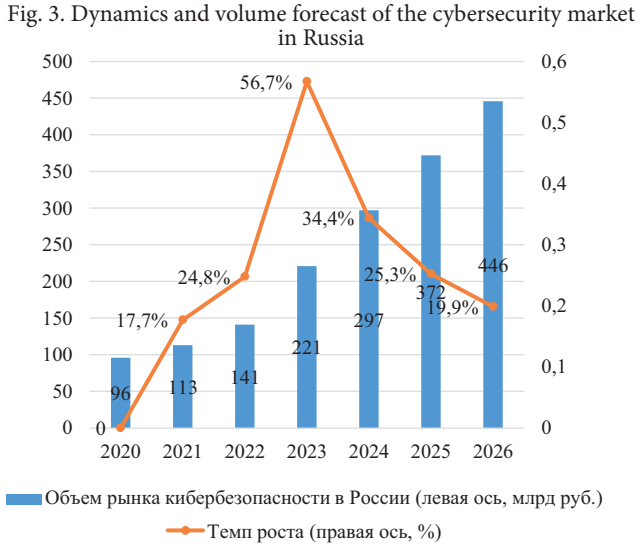
Источник: Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы (2022). <https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022-2026-godakh/>.

Поскольку предоставление логистических услуг в цифровом виде и развитие киберфизических систем непосредственно зависят от уровня защищенности цифровой инфраструктуры товародвижения, в этом контексте целесообразно остановиться на анализе и оценке рынка кибербезопасности по итогам 2021 года, опубликованной в 2022 году фондом «Центр стратегических разработок» (ЦСР)².

Прежде всего рассмотрим структурные показатели по объемам долей рынка на 2021 год по категориям средств защиты информации (табл. 1). Среднегодовые показатели темпа роста рынка кибербезопасности в России по итогам 2021 года оцениваются более чем в 17%.

Это 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% ежегод-

Рис. 3. Динамика и прогноз объема рынка кибербезопасности в России
Fig. 3. Dynamics and volume forecast of the cybersecurity market in Russia



Источник: Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы (2022). <https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022-2026-godakh/>.

но). При этом, согласно прогнозам ЦСР, российский рынок кибербезопасности к 2026 году может достичь показателя в 446 млрд руб. (рис. 3).

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 года массовый уход из России западных разработчиков и вендоров комплексных решений и средств информационной защиты, что предопределило существенную реструктуризацию рыночных долей в перспективе ближайших пяти лет [Баширзаде, 2022].

По оценкам аналитического агентства ЦСР, с 2023 по 2027 год объемные показатели российского рынка кибербезопасности должны вырасти не менее чем в 2,5 раза. При этом начиная с 2023 года 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 году до 446 млрд руб. в 2026-м.

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 инфраструктуры³.

Транспортная логистика, в свою очередь, подвержена негативному влиянию целого спектра рисков и угроз внедрения современных цифровых инструментов (табл. 2).

² Число кибератак на информационные системы России выросло на 65% (2023). <https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak>.

³ Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы (2022). <https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022-2026-godakh/>.

Таблица 2
Угрозы при внедрении цифровых инструментов в транспортной логистике
Table 2
Threats to the introduction of digital tools in transport logistics

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 даст результата для аналитиков - Неготовность к переменам со стороны персонала и руководства	- Внедрение вредоносного программного обеспечения, перехват управления устройствами, разрушение и воровство устройств - Уязвимость 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 заикливания смарт-контракта - Утечка персональных данных - Атаки на узлы отправки и получения транзакций - Захват контроля благодаря доминирующим вычислительным мощностям - Отсутствие нормативного регулирования

Источник: [Дмитриев, 2018].

Согласно статистическим данным, на начало 2023 года 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) [Дмитриев, Щербаков, 2023].

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 совме-

менных информационных систем и технологий, имеющих потенциальную полезность для бизнеса и общества, а также позволяющих существенно повысить эффективность бизнес-процессов в транспортной логистике (табл. 3).

Цифровые информационные технологии из табл. 3, 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 [Шаббаева, Шаббаев, 2023].

Заключение

Таким образом, для устранения проблемных вопросов, связанных с безопасностью экосистемных решений в логистике и управлении цепями поставок, требуется использовать цифровые информационные сервисы, имеющие следующие достоинства [Дмитриев, Щербаков, 2023]:

- 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 отгрузок⁴.

⁴ Информационная безопасность в логистике и на транспорте (2024). https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BB%D0%BE%D0%B3%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B5_%D0%B8_%D0%BD%D0%B0_%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%B5.

Таблица 3
Современные цифровые информационные технологии в экосистемах транспортно-логистического обслуживания
Table 3
Advanced digital information technologies in transport and logistics service ecosystems

Активно работают	Предполагаются к внедрению	Перспективные
- Развитие продаж через интернет (электронная торговля) - Оmnikanальность (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

Источник: [Чернышева и др., 2021].

Развитие рынка информационной и экосистемной 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 [Плотников, 2023]. В то же время, поскольку

до 2022 года в России доля иностранных цифровых решений была достаточно большой, это позволило установить высокий уровень требований к продуктам и российских производителей.

Начавшийся до 2022 года процесс импортозамещения решений в сфере информационной безопасности хотя и идет довольно высокими темпами, тем не менее требует ускорения в части не только перехода на российское программное обеспечение, но и развития информационной инфраструктуры, построенной на отечественной материально-технической и технологической базе.

Литература

Баширзаде Р.Р. (2022). Теоретико-методологические положения обеспечения экономической безопасности логистических систем в условиях цифровизации экономики. *Вестник ОрелГИЭТ*, 1(59): 20–25. DOI: 10.36683/2076-5347-2022-1-59-20-25.

Богачев Ю.С., Трифонов П.В. (2022). Единое цифровое пространство для эффективного функционирования промышленности. *Стратегические решения и риск-менеджмент*, 13(4): 376–383. <https://doi.org/10.17747/2618-947X-2022-4-376-383>.

Дмитриев А.В. (2012). Методологические основы управления логистикой транспортно-складских центров. *Известия Санкт-Петербургского университета экономики и финансов*, 6(78): 76–81.

Дмитриев А.В. (2018). *Диджитализация транспортной логистики*. СПб., СПбГЭУ.

Дмитриев А.В., Щербаков В.В. (2023). Обеспечение экономической безопасности и устойчивости цепей поставок в условиях цифровизации. *Вестник факультета управления СПбГЭУ*, 15: 11–18.

Малюков Ю.А., Недосекин А.О., Абдулаева З.И. (2023). Стратегическое управление экономической устойчивостью предприятия в нечетко-логической парадигме. *Стратегические решения и риск-менеджмент*, 14(2): 136–149. <https://doi.org/10.17747/2618-947X-2023-2-136-149>.

Носов А.Л. (2019). Логистика в системе экономической безопасности России. *Инновационное развитие экономики*, 5–2(53): 228–232.

Плотников В.А., Погодина В.В., Смирнов А.А. (2023). Национальная экономическая безопасность и государственная политика развития промышленности. *Управленческое консультирование*, 9: 35–44. <https://doi.org/10.22394/1726-1139-2023-9-35-44>.

Трачук А.В., Линдер Н.В. (2023). Эффекты цифровых платформ для промышленных компаний: эмпирический анализ в условиях внешнего санкционного давления. *Стратегические решения и риск-менеджмент*, 14(2): 150–163. <https://doi.org/10.17747/2618-947X-2023-2-150-163>.

Халин В.Г., Чернова Г.В. (2023). Цифровизация и киберриски. *Управленческое консультирование*, 7: 28–41. <https://doi.org/10.22394/1726-1139-2023-7-28-41>.

Чернышева Г.Н., Лавренова Г.А., Савич Ю.А., Лубянская Э.Б. (2021). Обеспечение экономической безопасности в логистике гособоронзаказа. *Организатор производства*, 29(3): 171–184. DOI: 10.36622/VSTU.2021.47.14.015.

Шабаета С.В., Шабаета А.И. (2023). Инструменты реализации стратегий в условиях цифровой трансформации промышленных предприятий. *Управленческое консультирование*, (10): 69–79. <https://doi.org/10.22394/1726-1139-2023-10-69-79>.

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

References

- Bashirzade R.R. (2022). Theoretical and methodological provisions for ensuring the economic security of logistics systems in the context of digitalization of the economy. *Bulletin of OrelGIET*, 1(59): 20-25. DOI: 10.36683/2076-5347-2022-1-59-20-25. (In Russ.)
- Bogachev Yu.S., Trifonov P.V. (2022). A single digital space for the efficient functioning of industry. *Strategic Decisions and Risk Management*, 13(4): 376-383. <https://doi.org/10.17747/2618-947X-2022-4-376-383>. (In Russ.)
- Dmitriev A.V. (2012). Methodological foundations of logistics management of transport and warehouse centers. *News of the St. Petersburg University of Economics and Finance*, 6(78): 76-81. (In Russ.)
- Dmitriev A.V. (2018). *Digitalization of transport logistics*. St. Petersburg, St. Petersburg State Economic University. (In Russ.)
- Dmitriev A.V., Shcherbakov V.V. (2023). Ensuring economic security and sustainability of supply chains in the context of digitalization. *Bulletin of the Faculty of Management of St. Petersburg State Economic University*, 15: 11-18. (In Russ.)
- Malyukov Yu.A., Nedosekin A.O., Abdulaeva Z.I. (2023). Strategic management of the economic sustainability of an enterprise in the fuzzy logic paradigm. *Strategic Decisions and Risk Management*, 14(2): 136-149. <https://doi.org/10.17747/2618-947X-2023-2-136-149>. (In Russ.)
- Nosov A.L. (2019). Logistics in the economic security system of Russia. *Innovative Economic Development*, 5-2(53): 228-232. (In Russ.)
- Plotnikov V.A., Pogodina V.V., Smirnov A.A. (2023). National economic security and state policy for industrial development. *Management Consulting*, 9: 35-44. <https://doi.org/10.22394/1726-1139-2023-9-35-44>. (In Russ.)
- Trachuk A.V., Linder N.V. (2023). The effects of digital platforms for industrial companies: An empirical analysis under conditions of external sanctions pressure. *Strategic Decisions and Risk Management*, 14(2): 150-163. <https://doi.org/10.17747/2618-947X-2023-2-150-163>. (In Russ.)
- Khalin V.G., Chernova G.V. (2023). Digitalization and cyber risks. *Management Consulting*, 7: 28-41. <https://doi.org/10.22394/1726-1139-2023-7-28-41>. (In Russ.)
- Chernysheva G.N., Lavrenova G.A., Savich Yu.A., Lubyanskaya E.B. (2021). Ensuring economic security in the logistics of state defense orders. *Production Organizer*, 29(3): 171-184. DOI: 10.36622/VSTU.2021.47.14.015. (In Russ.)
- Shabaeva S.V., Shabaev A.I. (2023). Tools for implementing strategies in the context of digital transformation of industrial enterprises. *Management Consulting*, (10): 69-79. <https://doi.org/10.22394/1726-1139-2023-10-69-79>. (In Russ.)
- Bag S., Dmitriev A.V., Sahu A.K., Sahu A.K. (2020). Barriers to adoption of blockchain technology in green supply chain management. *Journal of Global Operations and Strategic Sourcing*, 0027. DOI: 10.1108/JGOSS-06-2020-0027.

Информация об авторе

Александр Викторович Дмитриев

Доктор экономических наук, доцент, заведующий кафедрой безопасности, Северо-Западный институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Санкт-Петербург, Россия). SPIN: 6893-9410; ORCID: 0000-0002-3083-663X; Scopus Author ID: 57208211545; Researcher ID: ABG-4878-2021. Область научных интересов: экономическая безопасность, логистика, методология управления цепями поставок. dmitriev-av@ranepa.ru

About the author

Alexander V. Dmitriev

Doctor of economic sciences, associate professor, head of the Department of Security, North-Western Institute of Management – Branch of Russian Academy of National Economy and Public Administration under the President of the Russian Federation (Saint Petersburg, Russia). SPIN: 6893-9410; ORCID: 0000-0002-3083-663X; Scopus Author ID: 57208211545; Researcher ID: ABG-4878-2021. Research interests: economic security, logistics, supply chain management methodology. dmitriev-av@ranepa.ru

作者信息

Alexander V. Dmitriev

经济学博士，副教授，安全系主任，北西管理学院-俄罗斯联邦总统国民经济和行政学院分校（俄罗斯，圣彼得堡）。SPIN: 6893-9410; ORCID: 0000-0002-3083-663X; Scopus Author ID: 57208211545; Researcher ID: ABG-4878-2021. 科研兴趣领域：经济安全，物流，供应链管理方法论。dmitriev-av@ranepa.ru

Статья поступила в редакцию 16.01.24; после рецензирования 08.02.24 принята к публикации 20.02.24. Автор прочитал и одобрил окончательный вариант рукописи.

The article was submitted on 16.01.24; revised on 08.02.24 and accepted for publication on 20.02.24. The author read and approved the final version of the manuscript.

文章于 16.01.24 提交给编辑。文章于 08.02.24 已审稿。之后于 20.02.24 接受发表。作者已经阅读并批准了手稿的最终版本。