DOI 10.37882/2223-2974.2024.09.13

РИСКИ И УГРОЗЫ ЦИФРОВОЙ ЭКОНОМИКИ В ЛОГИСТИЧЕСКИХ СИСТЕМАХ

RISKS AND THREATS OF THE DIGITAL ECONOMY IN LOGISTICS SYSTEMS

A. Dmitriev
N. Orekhova

Summary. The article is devoted to the analysis of modern risks and threats of the digital economy characteristic of logistics systems. 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 position of protecting a business entity from negative exogenous and endogenous factors to increase the level of competitiveness and sustainability of the enterprise in the market. At the same time, the very fact of digitalization of cargo delivery processes is considered from the position of the ecosystem paradigm and platform concept. Approaches to the implementation of network coordination and control of network interaction have been developed, ensuring end-to-end management of business processes and data exchange in the process of product distribution.

The purpose of this study is to substantiate the use of a methodology for ensuring economic and information security when implementing modern digital ecosystem solutions in logistics in the context of growing cybersecurity threats.

Keywords: economic security, logistics, digital economy, transport, digital technologies, cyber threats, data protection.

Дмитриев Александр Викторович
доктор экономических наук, доцент, Северо-Западный институт управления — филиал РАНХиГС при Президенте РФ (г. Санкт-Петербург)
dmitriev-av@ranepa.ru
Орехова Наталья Леонидовна
кандидат юридических наук, доцент, Северо-Западный институт управления — филиал РАНХиГС при Президенте РФ (г. Санкт-Петербург)
nataliaorekhova@bk.ru

Аннотация. Статья посвящена вопросам анализа современных рисков и угроз цифровой экономики, характерных для логистических систем. 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 негативных экзогенных и эндогенных факторов для повышения уровня конкурентоспособности и устойчивости предприятия на рынке. При этом сам факт цифровизации процессов доставки грузов рассматривается с позиции экосистемной парадигмы и платформенной концепции. Разработаны подходы к реализации сетевой координации и контролю сетевого взаимодействия, обеспечивающие сквозное управление бизнес-процессами и обмена данными в процессе товародвижения.

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.

Ключевые слова: экономическая безопасность, логистика, цифровая экономика, транспорт, цифровые технологии, киберугрозы, защита данных.

В настоящее время 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.

Отсутствие налаженной и действенной системы экономической безопасности на логистическом предприятии приведет к срыву реализации его стратегии и риску потери конкурентных преимуществ на рынке [5].

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.

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, её устойчивое функционирование с применением

современных информационных технологий рассматривается, как одно из важнейших условий экономической безопасности государства и залогом поддержания высокого уровня благосостояния населения.

Проблемам внедрения цифровых технологий и обеспечению экономической безопасности в области логистики посвящено достаточно много научных исследований. Авторы Плотников В.А., Погодина В.В., Смирнов А.А. в работе [8] 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 [9] авторы характеризуют устойчивость экономических систем в ракурсе стратегического наполнения с использование 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 [4] посвящено влиянию цифровых платформ на показатели деятельность промышленных предприятий в контексте формирования и развития уникальных конкурентных преимуществ и повышении 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 [6] обосновывается стратегическая роль логистики в обеспечении экономической безопасности страны, а результативность логистической деятельности 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].

Современные логистические системы интегрируют большое число участвующих субъектов, создающих совместно высокие показатели добавленной стоимости. При этом ключевым условием реализации новой методики управления товарными потоками в условиях цифровой экономики должна стать высокозащищенная и устойчивая информационная инфраструктура логистических предприятий [3].

Указанным тенденциям следует и авторский взгляд в публикации [1], направленный на анализ структурно-трансформационных процессов, обеспечивающих развитие сетевой телекоммуникационной конвергенции и расширение информационно-аналитического пространственного взаимодействия на различных уровнях (региональном, национальном и мировом).

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 между участниками цепей поставок. 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.

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 [6].

Однако, 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. 1).

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.

Поскольку предоставление логистических услуг в цифровом виде и развитие киберфизических систем

Рис. 1. Риски и угрозы при внедрении цифровых инструментов в транспортной логистике [5]

непосредственно зависит от уровня защищенности цифровой инфраструктуры товародвижения, в данном контексте целесообразно остановиться на анализе и оценка рынка кибербезопасности по итогам 2023 года, опубликованного Фондом «Центр стратегических разработок» (ЦСР) [10].

Прежде всего, рассмотрим структурные показатели по объемам долей рынка на 2023 год по категориям средств защиты информации (табл. 1).

Таблица 1.

Объемные структурно-рыночные показатели в разрезе видов и категорий средств защиты цифровых данных [7]

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 2023 года оцениваются более, чем в 17 %.

Указанное значение превышает прирост мировых показателей рынка кибербезопасности, которые хотя и имели исторически довольно высокие характеристики, благодаря промышленно развитым, западным странам, 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 году может достичь показателя в 446 млрд руб. (рис. 2) [7].

Приведенные выше результаты исследования Центра стратегических разработок, связанные с прогнозированием развития рынка информационной безопасности в России на ближайшие годы, 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 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.

По оценкам аналитического агентства ЦСР, с 2023 по 2027 годы объемные показатели российского рын-

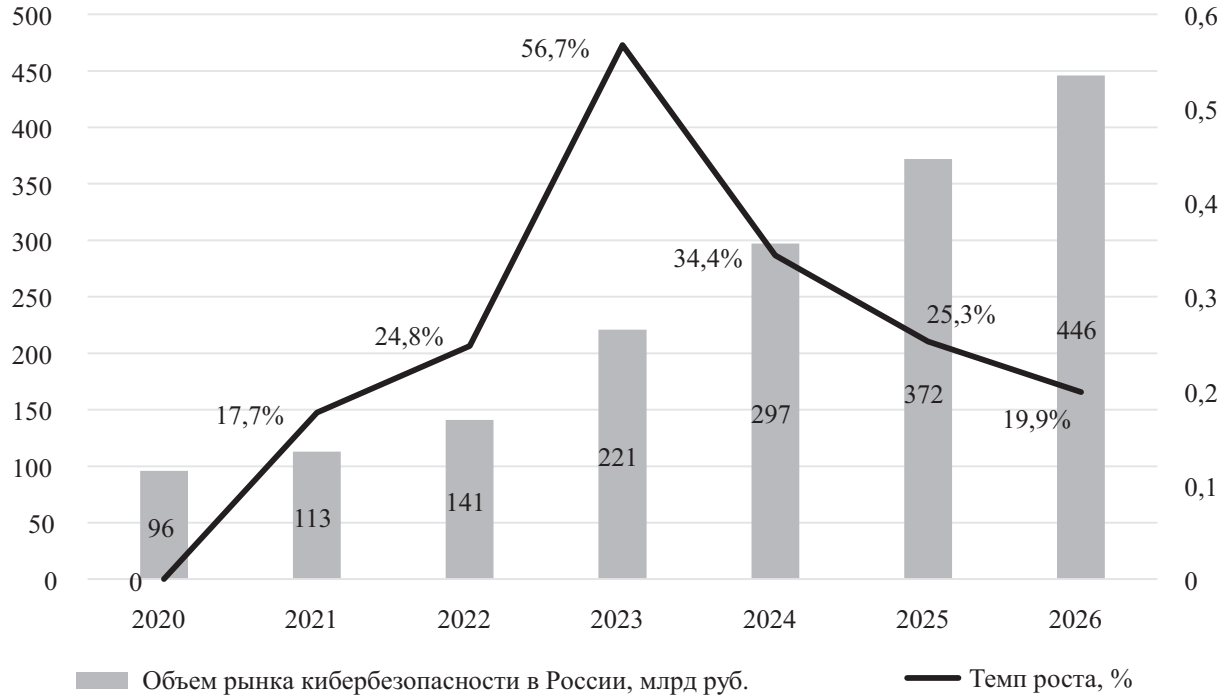

Рис. 2. Динамика и прогноз объема рынка кибербезопасности в России, млрд руб. [7]

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 технологи Блокчейн для защиты информации; •Применение Криптовалют для взаиморасчетов; •Внедрение Интернета вещей для автоматического управления производством; •Искусственный интеллект для автоматизации принятия решений

Рис. 3. Инструменты цифровой экономики в логистических системах [7]

ка кибербезопасности должны вырасти не менее, чем в 2,5 раза.

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

В частности, на железной дороге на смену обычным, аналоговым системам управления транспортными потоками, 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 инструменты цифровой экономики в транспортной логистике, которые будут предусматривать в своей инфраструктуре комплекс современных информационных технологий, имеющих потенциальную полезность для бизнеса и общества, а также позволяющих существенно повысить эффективность функционирования логистических систем по целому ряду показателей:

— 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.

Таким образом, развитие рынка информационной и экосистемной безопасности в России в контексте нейтрализация угроз внедрения инструментов цифровой экономики в логистических системах позволит устранить основные проблемные вопросы, связанные с безопасностью товародвижения и управления материальными потоками.

ЛИТЕРАТУРА

1. Баширзаде, Р.Р. Теоретико-методологические положения обеспечения экономической безопасности логистических систем в условиях цифровизации экономики / Р.Р. Баширзаде // Вестник ОрелГИЭТ. — 2022. — № 1(59). — С. 20–25. — DOI 10.36683/2076-5347-2022-1-59-20-25.
2. Богачев Ю.С., Трифонов П.В. Единое цифровое пространство для эффективного функционирования промышленности // Стратегические решения и риск-менеджмент. — 2022. № 13(4). — с. 376–383. https://doi.org/10.17747/2618-947X-2022-4-376-383
3. Информационная безопасность [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/index.php/ (дата обращения 29.10.2023 г.)
4. Малюков Ю.А., Недосекин А.О., Абдулаева З.И. Стратегическое управление экономической устойчивостью предприятия в нечетко-логической парадигме // Стратегические решения и риск-менеджмент. — 2023; № 14(2). — с. 136–149. https://doi.org/10.17747/2618-947X-2023-2-136-149
5. Носов, А.Л. Логистика в системе экономической безопасности России / А.Л. Носов // Инновационное развитие экономики. — 2019. — № 5-2(53). — С. 228–232.
6. Обеспечение экономической безопасности в логистике гособоронзаказа / Г.Н. Чернышева, Г.А. Лавренова, Ю.А. Савич, Э.Б. Лубянская // Организатор производства. — 2021. — Т. 29, № 3. — С. 171–184. — DOI 10.36622/VSTU.2021.47.14.015.
7. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы [Электронный ресурс]. Режим доступа: https://www.csr.ru/ru/research/ (дата обращения 29.10.2023 г.)
8. 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
9. Трачук А.В., Линдер Н.В. Эффекты цифровых платформ для промышленных компаний: эмпирический анализ в условиях внешнего санкционного давления // Стратегические решения и риск-менеджмент. — 2023. № 14(2). — с. 150–163. https://doi.org/10.17747/2618-947X-2023-2-150-163
10. Число кибератак на информационные системы России выросло на 65 %. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (дата обращения 29.10.2023 г.)

Журнал «Современная наука: актуальные проблемы теории и практики»