



УДК 658.7

## Нейтрализация угроз экономической безопасности в цифровых экосистемах логистики

*Дмитриев А. В., доктор экон. наук, доцент  
Северо-Западный институт управления РАНХиГС  
199178, Россия, г. Санкт-Петербург, Средний пр-т В. О., 57/43*

**Аннотация.** В статье обсуждаются вопросы экономической безопасности, как одной из важнейших качественных характеристик логистических систем, определяющих способность обеспечивать в процессе товародвижения установленные параметры материальных потоков. Исследуются логистические системы на предмет оптимальной организации и управления материальными потоками, направленных на обеспечение эффективности функционирования и реализации стратегии хозяйственных субъектов. Обосновывается необходимость использования современных цифровых технологий для повышения уровня экономической безопасности в логистических системах.

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

### **Neutralizing economic security threats in digital logistics ecosystems**

*Dmitriev A. V.  
North-West Institute of Management of the Presidential Academy  
of National Economy and Public Administration*

**Annotation.** The article discusses issues of 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. Logistics systems are examined for optimal organization and management of material flows aimed at ensuring the efficiency of functioning and implementation of the strategy of economic entities. The necessity of using modern digital technologies to increase the level of economic security in logistics systems is substantiated.

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

**Введение.** В современных условиях экономическая безопасность выступает одной из важнейших качественных характеристик логистических систем, определяющих способность обеспечивать в процессе товародвижения установленные параметры материальных потоков и достаточную обеспеченность предприятия ресурсами для выполнения его хозяйственной деятельности.

По сути, экономическая безопасность – это, с одной стороны, защита субъекта от внешних и внутренних угроз, а с другой стороны, способность субъекта к стабильному функционированию в условиях противодействия негативному влиянию окружающей среды [5].



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

**Основная часть.** 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 [6].

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. Общепринятая методика, применяемая в логистике в течение долгого времени, предполагала достижение экономических результатов исключительно за счет деятельности самого предприятия непосредственно и его ближайшего окружения в цепи поставки, в то время как использование цифровой платформенной концепции создает необходимые предпосылки для формирования развитых экосистем, в которых множество вовлеченных субъектов создают высокую добавленную стоимость совместно [1] (рис. 1).

Факторы	Значение
Налаженные и упорядоченные правила и процедуры управления бизнес-процессами в логистике. Задокumentированные 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 сети 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.

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



Авторский взгляд в публикации [4] направлен 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», которая выполнена 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 ограниченным уровнем доступа. При этом добавочный синергетический эффект для пользователей цифровых сервисов может быть достигнут благодаря использованию инновационных способов сетевой координации и контроля сетевого взаимодействия [7].

В настоящее время неизбежность, объективность и долговременность цифровых трансформационных процессов практически во всех сферах деятельности предприятий и организаций не вызывают 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 [8].



В своей общности перечисленные 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].



Рис. 2. Модель киберфизической экосистемы в логистике

Однако, следует признать, что процессам всеобщей цифровой трансформации присущи ряд серьезных рисков и угроз, в частности, большое количество автоматизированных транспортно-складских операций в логистике приведут к замене рабочих мест роботами, что может вызвать массовую безработицу в рядах низко- и среднеквалифицированных сотрудников. А это, в свою очередь, может существенно снизить уровень жизни достаточной большой части работоспособного населения. Тем не менее, эра цифровых преобразований, формирование которой происходит очень быстро, предопределяет 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 [9].

Транспортная логистика, в свою очередь, подвержена негативному влиянию целого спектра рисков и угроз внедрения современных цифровых инструментов (рис. 3) [12].



Риски больших данных	Риски промышленного интернета	Риски искусственного интеллекта и роботизации	Риски системы распределенного реестра
<ul style="list-style-type: none"><li>• нарушение конфиденциальности данных ;</li><li>• неоптимальная система сбора и хранения больших данных;</li><li>• частичная или полная утрата данных вследствие ошибок обработки</li><li>• обработка больших данных не дает результата для аналитиков</li><li>• Неготовность к переменам со стороны персонала и руководства</li></ul>	<ul style="list-style-type: none"><li>• внедрение вредоносного программного обеспечения, перехват управления устройствами, разрушение и воровство устройств;</li><li>• уязвимости программного обеспечения</li><li>• DDoS-атаки на вычислительную систему;</li><li>• сбой системы, сети, устройств в результате потери электропитания и других техногенных и природных факторов</li></ul>	<ul style="list-style-type: none"><li>• недостаток машинных мощностей для решения задач;</li><li>• вытеснения рабочей силы искусственным интеллектом</li><li>• Ошибки в обучении искусственного интеллекта и внедрении робототехники;</li><li>• Уязвимость робототехники (программа, калибровка, контроллеры);</li><li>• большинство людей предпочитают человеческий контакт</li></ul>	<ul style="list-style-type: none"><li>• блокировка и потеря средств из-за уязвимости кода или заикливания смарт-контракта;</li><li>• утечка персональных данных</li><li>• атаки на узлы отправки и получения транзакций</li><li>• захват контроля благодаря доминирующим вычислительным мощностям</li><li>• отсутствие нормативного регулирования</li></ul>

Рис. 3. Угрозы при внедрении цифровых инструментов в транспортной логистике

Согласно статистическим данным, начиная с 2020 года, на 80 % 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) [10].

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 [11].

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. 4).

Активно работают	Предполагаются к внедрению	Перспективные
<ul style="list-style-type: none"><li>• Развитие продаж через Интернет (электронная торговля);</li><li>• Омниканальность (работа с заказчиками через все возможные каналы);</li><li>• Мобильный доступ к корпоративным информационным системам</li></ul>	<ul style="list-style-type: none"><li>• Настройка производства под конкретные заказы;</li><li>• Анализ и прогноз поведения заказчиков;</li><li>• Цифровое проектирование и моделирование</li></ul>	<ul style="list-style-type: none"><li>• Использование технологии Блокчейн для защиты информации;</li><li>• Применение Криптовалют для взаиморасчетов;</li><li>• Внедрение Интернета вещей для автоматического управления производством;</li><li>• Искусственный интеллект для автоматизации принятия решений</li></ul>

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

Изображенные на рис. 4 цифровые информационные технологии, используемые в экосистемах транспортной логистики, обеспечивают доступность по целому ряду показателей контроля и мониторинга:

- сообщения о нештатных событиях;
- контроль температуры скоропортящихся грузов;
- обеспечение работы сенсоров и датчиков;
- определение времени в пути, возможных задержек, длительности стоянок и даты прибытия к месту назначения;
- определение местоположения транспорта, навигация и маршрутизация;
- расчет времени погрузочно-разгрузочных работ.

**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.



## Литература

1. Логистика и управление цепями поставок / В. В. Щербаков [и др.]. – М. : Юрайт, 2019. – 582 с.
2. Дмитриев, А. В. Методологические основы управления логистикой транспортно-складских центров / А. В. Дмитриев // Известия Санкт-Петербургского университета экономики и финансов. – 2012. – № 6 (78). – С. 76–81.
3. Управление цепями поставок / Н. А. Гвилия [и др.]. – М. : ООО «Издательство ЮРАЙТ», 2017. – 209 с.
4. Дмитриев, А. В. Формирование цифровой среды транспортной логистики / А. В. Дмитриев // Логистика – евразийский мост : материалы XIII Международной научно-практической конференции, 25–29 апреля 2018 года. – Красноярск : Красноярский государственный аграрный университет, 2018. – Т. 1. – С. 88–92.
5. Barriers to adoption of blockchain technology in green supply chain management / S. Bag [and other] // Journal of Global Operations and Strategic Sourcing. – 2020. – P. 27.
6. Дмитриев, А. В. Диджитализация транспортной логистики / А. В. Дмитриев. – СПб. : Санкт-Петербургский государственный экономический университет, 2018. – 161 с.
7. Стратегии развития инструментов коммерции / И. А. Аренков [и др.]. – СПб. : Санкт-Петербургский государственный университет экономики и финансов, 2010. – 347 с.
8. Дмитриев, А. В. Цифровые информационные технологии в экосистемах транспортно-логистического обслуживания / А. В. Дмитриев. – СПб. : Санкт-Петербургский государственный экономический университет, 2021. – 160 с.
9. Moldagulova, A. Application of Big Data in Logistics / A. Moldagulova, R. Satybaldiyeva, A. Kuandykov // ICEMIS'20: Proceedings of the 6th International Conference on Engineering & MIS. – 2020. – Article № 50. – P. 1–6.
10. Рейтинг «ИТ-тренды CNews 2020»: самые востребованные технологии [Электронный ресурс]. Режим доступа : [https://www.cnews.ru/reviews/ittrendy2020/review\\_table/a0f78dcb53d27d6f4ed201cb53f89342a02ccb89](https://www.cnews.ru/reviews/ittrendy2020/review_table/a0f78dcb53d27d6f4ed201cb53f89342a02ccb89) (дата обращения: 27.09.2023).
11. Fritz, M. M. C. Sustainability Management in Supply Chains: Developing a Supply Chain View to operationalize sustainability among multiple supply chain stakeholders / M. M. C. Fritz. – University of Graz, Austria. – 2017.
12. Salminen, V. From supply chain to digital circular value chain / V. Salminen, H. Ruohomaa, T. Pöykkö // 2016 International conference on production research. – Africa, Europe and the Middle East and 4th International conference on quality and innovation in engineering and management. – 2020.