Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2024, 3: 134–140

https://doi.org/10.26163/GIEF.2024.72.83.019
EDN HVMZHW
УДК 338.2

А.В. Дмитриев

РАЗВИТИЕ ЦИФРОВЫХ ЭКОСИСТЕМ ТРАНСПОРТНО-ЛОГИСТИЧЕСКОГО ОБСЛУЖИВАНИЯ В УСЛОВИЯХ ВНЕШНИХ РИСКОВ И УГРОЗ

Александр Викторович Дмитриев – зав. кафедрой безопасности, Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при президенте Российской Федерации (СЗИУ РАНХиГС), доктор экономических наук, доцент, г. Санкт-Петербург.
✉ **dmitriev-av@ranepa.ru**

Аннотация. *Статья посвящена обсуждению вопросов 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. Автор обосновывает возможность нейтрализации внешних вызовов и угроз в сфере транспортно-логистического обслуживания с позиции усиления цифровой экосистемной безопасности.*

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

A.V. Dmitriev

DEVELOPMENT OF DIGITAL ECOSYSTEMS OF TRANSPORT AND LOGISTICS SERVICES UNDER EXTERNAL RISKS AND THREATS

Alexander Dmitriev – head of the Department of Security, North-West Institute of Management, Presidential Academy, Doctor of Economics, associate professor, St. Petersburg. ✉ **dmitriev-av@ranepa.ru**

Annotation. *The research is devoted to ensuring economic security as one of the key qualitative characteristics of logistics systems that determine the ability to guarantee set parameters of material flow when implementing digital systems and technologies. We substantiate the possibility to neutralize external challenges and threats in transport and logistics services from the point of view of increasing digital ecosystem security.*

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

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

Экономическая безопасность в данном случае обеспечивает не только защиту хозяйствующих субъектов от внутренних и внешних угроз, но и стимулирует устойчивое и стабильное функционирование субъектов в условиях эффективного противодействия негативному воздействию усло-

вий окружающей среды [5].

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.

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 [11].

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 [12].

Проблемам внедрения цифровых технологий и обеспечению экономической безопасности в области логистики и управления цепями поставок посвящено достаточно много научных исследований. Например, В.А. Плотников, В.В. Погодина, А.А. Смирнов 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 [8].

В статье [6] авторы характеризуют устойчивость экономических систем в ракурсе стратегического наполнения с использование системы сбалансированных показателей, что позволяет обеспечить синхронность управления комплексной эффективностью предприятия, минимизировать возникающие в процессе работы риски и реализовать повестку экономической безопасности хозяйственных систем при их функционировании в условиях широкого спектра современных угроз и вызовов.

Исследование [9] 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 [7] 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.

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 [3].

Указанным тенденциям следует и авторский взгляд в публикации [13], направленный на анализ структурно-трансформационных процессов, обеспечивающих развитие сетевой телекоммуникационной конвергенции и расширение информационно-аналитического пространственного взаимодействия на различных уровнях, в том числе на уровне региона, государства и мировом уровне.

Отмечаются достоинства от внедрения и интеграции цифровых платформенных решений в транспортной логистике отдельной страны, а также цифровых интегрированных платформ глобального охвата, что обеспечивается за счет преодоления временных и пространственных разрывов и барьеров при взаимодействии субъектов транспортно-логистических процессов. При этом добавочный синергетический эффект для пользователей цифровых сервисов может быть достигнут благодаря использованию инновационных способов сетевой координации и контроля сетевого взаимодействия [2].

В ближайшем будущем целеполагание в экономических системах и отличительные черты хозяйствования будут иметь прямое отношение к дальнейшему всеобщему и повсеместному внедрению цифровых решений, обусловливаемых нарастающей модернизацией микроэлектроники, телекоммуникационных средств и информационных технологий [10].

В своей общности цифровые инструменты формируют модель киберфизической экосистемы в логистике (рис. 1), позволяющей формировать совокупность интегрированных взаимодействий в рамках замкнутого цикла реализации процедуры доставки грузов и управления товародвижением, а также контроля и мониторинга выполнения основных логистических операций с использованием широко спектра сквозных информационных технологий[1].

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. (рис. 2).

Поскольку предоставление логистических услуг в цифровом виде и развитие киберфизических систем непосредственно зависит от уровня защищенности цифровой инфраструктуры товародвижения, в данном контексте целесообразно остановиться на анализе и оценке рынка кибербезопасности по итогам 2022 года, опубликованного в 2023 году Фондом «Центр стратегических разработок» (ЦСР)[2].

Рис. 1. Модель киберфизической экосистемы в логистике

Источник: [4].

[1] Логистика и управление цепями поставок / В.В. Щербаков, Э.М. Букринская, Н.А. Гвилия [и др.]. М.: Юрайт, 2019. 582 с.

[2] Число кибератак на информационные системы России выросло на 65% // Ведомости: ведущее деловое издание России. URL: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (дата обращения: 29.10.2023).

Риски больших данных	Риски промышленного интернета	Риски искусственного интеллекта и роботизации	Риски системы распределенного реестра
•нарушение конфиденциальности данных ; •неоптимальная система сбора и хранения больших данных; •частичная или полная утрата данных вследствие ошибок обработки; •обработка больших данных не дает результата для аналитиков; •неготовность к переменам со стороны персона и руководства.	•внедрение вредоносного программного обеспечения, перехват управления устройствами, разрушение и воровство устройств; •уязвимости программного обеспечения; •DDoS-атаки на вычислительную систему; •сбой системы, сети, устройств в результате потери электропитания и других техногенных и природных факторов.	•недостаток машинных мощностей для решения задач; •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 зацикливания смарт-контракта; •утечка персональных данных; •атаки на узлы отправки и получения транзакций •захват контроля благодаря доминирующим вычислительным мощностям; •отсутствие нормативного регулирования.

Рис. 2. Риски и угрозы при внедрении цифровых инструментов в транспортной логистике

Источник: [5].

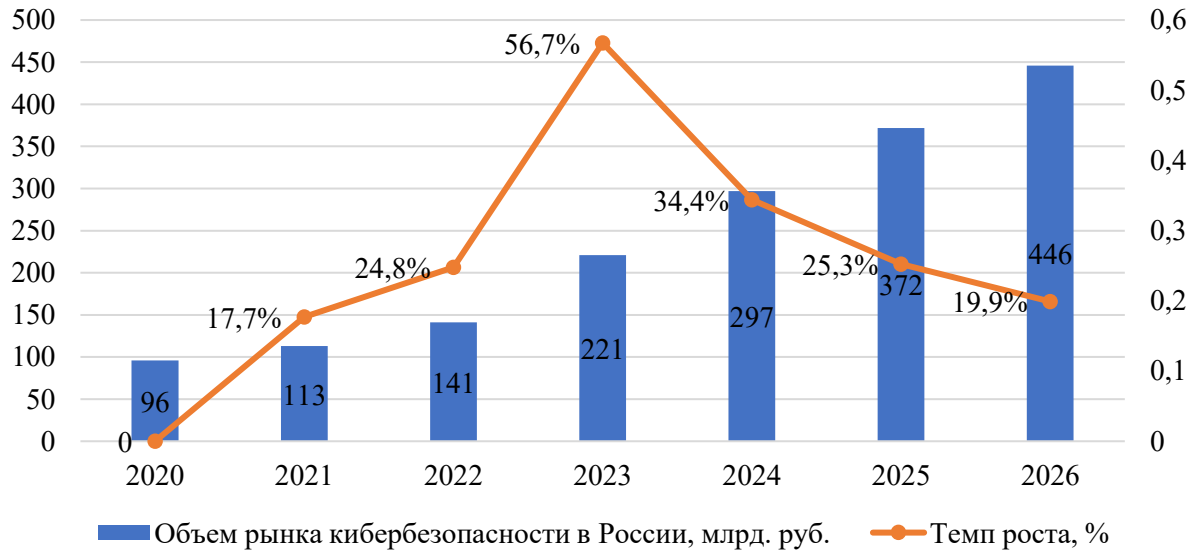

Рис. 3. Динамика и прогноз объема рынка кибербезопасности в России, млрд руб.

Источник: Число кибератак на информационные системы России выросло на 65% // Ведомости: ведущее деловое издание России. URL: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (дата обращения 29.10.2023).

Среднегодовые показатели темпа роста рынка кибербезопасности в России по итогам 2021 года оцениваются более чем в 17%.

Данное 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% ежегодно). 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 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 [1].

Согласно статистическим данным, на начало 2023 года на 65% возросло общее количество кибератак на Россию. Нейтрализовано около 25000 попыток внешнего воздействия на государственные цифровые ресурсы, приблизительно 1200 из которых были направлены на объекты критической инфраструктуры (энергоснабжения, водоснабжения, экологического мониторинга, транспорта и прочих ключевых систем, обеспечивающих жизнедеятельность населения)[3].

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. 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.

Таким образом, для устранения проблемных вопросов, связанных с безопасностью экосистемных решений в логистике и управлением цепями поставок, 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;

[3] Прогноз развития рынка решений для информационной безопасности в Российской Федерации в 2022–2026 годах // Центр стратегических разработок. URL: https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022-2026-godakh/ (дата обращения: 29.10.2023).

- быстрая реакция на нештатные события и ситуации;

- контроль состояния товаров в процессе транспортировки и мониторинг отгрузок[4].

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. В то же время, поскольку до 2022 года в России доля иностранных цифровых решений была достаточно большой, это позволит установить высокий уровень требований к продуктам российских производителей.

ЛИТЕРАТУРА

1. *Баширзаде Р.Р.* Теоретико-методологические положения обеспечения экономической безопасности логистических систем в условиях цифровизации экономики // 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. URL: https://doi.org/10.17747/2618-947X-2022-4-376-383 (дата обращения: 29.10.2023).

3. *Дмитриев А.В.* Методологические основы управления логистикой транспортно-складских центров // Известия Санкт-Петербургского университета экономики и финансов. 2012. № 6 (78). С. 76–81.

4. *Дмитриев А.В.* Диджитализация транспортной логистики. СПб.: Санкт-Петербургский государственный экономический университет, 2018. 161 с.

5. *Дмитриев А.В., Щербаков В.В.* Обеспечение экономической безопасности и устойчивости цепей поставок в условиях цифровизации // Вестник факультета управления СПбГЭУ. 2023. Вып. 15. С. 11–18.

6. *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. URL: https://doi.org/10.17747/2618-947X-2023-2-136-149 (дата обращения: 29.10.2023).

7. *Носов А.Л.* Логистика в системе экономической безопасности России // Инновационное развитие экономики. 2019. № 5-2(53). С. 228–232.

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. URL: https://doi.org/10.22394/1726-1139-2023-9-35-44 (дата обращения: 29.10.2023).

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. URL: https://doi.org/10.17747/2618-947X-2023-2-150-163 (дата обращения: 29.10.2023).

10. *Халин В.Г., Чернова Г.В.* Цифровизация и киберриски // Управленческое консультирование. 2023. № (7). С. 28–41. URL: https://doi.org/10.22394/1726-1139-2023-7-28-41 (дата обращения: 29.10.2023).

11. *Чернышева Г.Н., Лавренова Г.А., Савич Ю.А., Лубянская Э.Б.* Обеспечение

[4] Информационная безопасность.
URL: https://www.tadviser.ru/index.php/Информационная_безопасность (дата обращения: 29.10.2023).

экономической безопасности в логистике гособоронзаказа // Организатор производства. 2021. Т. 29. № 3. С. 171–184. DOI 10.36622/VSTU.2021.47.14.015.

12. *Шабаева С.В., Шабаев А.И.* Инструменты реализации стратегий в условиях цифровой трансформации промышленных предприятий // Управленческое консультирование. 2023. № (10). С. 69–79. URL: https://doi.org/10.22394/1726-1139-2023-10-69-79 (дата обращения: 29.10.2023).

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