DOI 10.37882/2223-2974.2026.03.15

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ЛОГИСТИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ РАСТУЩЕЙ ЦИФРОВИЗАЦИИ

ENSURING CYBERSECURITY OF LOGISTICS SYSTEMS IN THE CONTEXT OF GROWING DIGITALIZATION

T. Logutova
Yu. Lazarevskaya

Summary. The article examines cybersecurity of logistics systems under conditions of digital transformation of transport and logistics infrastructure in the Russian Federation. It is substantiated that cyber threats targeting automated logistics management systems generate economic risks affecting supply chain stability. The legal framework for countering cyber impacts in logistics is analyzed in the context of economic security.

Keywords: cybersecurity, logistics systems, economic security, transport security, critical information infrastructure, logistics digitalization, cyber threats, information systems, automated control systems, supply chains, information protection.

Логутова Тамара Григорьевна
доктор экономических наук, профессор, Мариупольский государственный университет им. А.И. Куинджи
t.logutova7@mail.ru
Лазаревская Юлианна Артуровна
старший преподаватель, Мариупольский государственный университет им. А.И. Куинджи
y.lazarevskaya@mgumariupol.ru

Аннотация. В статье исследована кибербезопасность логистических систем в условиях цифровизации транспортно-логистической инфраструктуры Российской Федерации. Обосновано, что киберугрозы, направленные на автоматизированные системы управления логистикой, формируют риски экономического характера, влияющие на устойчивость цепей поставок и транспортных процессов. Проанализированы правовые основы противодействия кибервоздействиям в логистике с позиции федерального законодательства и показана их роль в обеспечении экономической безопасности логистических систем. Исследована экономическая специфика киберугроз как неотъемлемого элемента обеспечения экономической безопасности логистических систем.

Ключевые слова: кибербезопасность, логистические системы, экономическая безопасность, транспортная безопасность, критическая информационная инфраструктура, цифровизация логистики, киберугрозы, информационные системы, автоматизированные системы управления, цепи поставок, защита информации.

Функционирование современных логистических систем осуществляется в условиях устойчивого роста киберугроз, затрагивающих транспортно-логистическую инфраструктуру на глобальном уровне. По данным отраслевых аналитических исследований, в 2023 году транспортная отрасль вошла в число десяти наиболее атакуемых секторов мировой экономики. Количество успешных кибератак на транспортные компании увеличилось на 36 % по сравнению с 2022 годом, что свидетельствует о системном характере цифровых угроз в сфере перевозок и логистики. Наиболее часто применяемыми методами кибервоздействия в 2023 году стали использование вредоносного программного обеспечения (35 % от общего числа зафиксированных инцидентов), эксплуатация уязвимостей информационных систем (18 %) и атаки на цепочки поставок (8 %).

Рост кибератакивности в транспортно-логистическом секторе сопровождается значительными экономическими потерями. По оценкам экспертов, ущерб от одной масштабной кибератаки на транспортно-логистическую компанию может достигать 50 млн долларов США и более. Киберинциденты приводят к блокированию грузоперевозок, сбоям в системах диспетчеризации и бронирования, нарушению работы навигационных и складских систем, а также к повреждению или утрате перевозимых грузов. В авиационном и морском сегментах кибервоздействия способны вызывать простой критически важных систем управления, а в сфере городской транспортной инфраструктуры — нарушать функционирование светофоров, информационных табло и автоматизированных систем управления движением.

Усиление киберугроз в логистике напрямую связано с углублением цифровизации транспортных процессов и расширением использования автоматизированных систем управления, операционных технологий и сетевых коммуникаций. Если ранее кибератаки в секторе транспорта и логистики носили эпизодический характер и фиксировались раз в несколько лет, то в последние годы наблюдается переход к регулярным инцидентам, происходящим с периодичностью один–два раза в месяц. Одновременно с этим существенно снизились барьеры входа для злоумышленников: вредоносное

программное обеспечение, включая вирусы-вымогатели, доступно для аренды, что повышает интенсивность и масштабность кибератак и усиливает уязвимость логистических систем как элемента экономической безопасности.

Функционирование современных логистических систем в Российской Федерации осуществляется в условиях высокой степени цифровизации, охватывающей управление цепями поставок, транспортную инфраструктуру, складские комплексы, таможенно-логистические процедуры и финансово-расчетные операции. Информационные технологии перестали выполнять вспомогательную роль и превратились в системообразующий элемент логистики, обеспечивающий синхронизацию потоков материальных ресурсов, данных и денежных средств. В результате устойчивость логистических систем напрямую зависит от состояния их цифровой среды, что предопределяет необходимость рассмотрения кибербезопасности как самостоятельного и критически значимого аспекта экономической безопасности.

Экономическая безопасность логистических систем традиционно анализировалась через призму рисков, связанных с транспортными сбоями, инфраструктурными ограничениями, колебаниями спроса, финансовой нестабильностью и внешнеэкономическими факторами. Однако расширение цифровых контуров управления привело к формированию нового класса угроз, не укладывающихся в классические модели хозяйственных рисков. Кибервоздействия на логистические информационные системы способны нарушать непрерывность поставок, искажать данные о движении грузов, блокировать транспортные процессы и провоцировать значительные экономические потери, выходящие за рамки отдельных хозяйствующих субъектов и затрагивающие интересы государства [4].

Специфика логистики как объекта киберугроз обусловлена ее сетевой природой. Логистические системы объединяют множество участников — перевозчиков, операторов терминалов, экспедиторов, складских комплексов, информационных посредников и государственных органов. Цифровая взаимосвязанность этих элементов формирует сложную распределенную инфраструктуру, в которой уязвимость одного сегмента способна вызвать каскадные нарушения в смежных звеньях цепи поставок. В условиях высокой концентрации цифровых сервисов и зависимости от автоматизированных систем управления транспортом киберугрозы приобретают системный характер и трансформируются в фактор макроэкономической нестабильности.

Для Российской Федерации данная проблематика приобретает особую значимость с учетом масштабов транспортно-логистического комплекса, его пространственной протяженности и роли в обеспечении внутреннего рынка, экспортных потоков и транзитных функций. Железнодорожный, автомобильный, морской и авиационный транспорт активно используют автоматизированные системы диспетчеризации, навигации, мониторинга грузов и электронного документооборота. Нарушение их работы вследствие кибервоздействий способно приводить не только к прямым финансовым потерям, но и к подрыву доверия к национальной логистической инфраструктуре, снижению инвестиционной привлекательности и ослаблению конкурентных позиций страны на международных рынках перевозок.

Кибербезопасность в данном контексте не может рассматриваться исключительно как техническая задача защиты информационных ресурсов. Она выступает элементом комплексной системы обеспечения экономической безопасности логистики, включающей правовое регулирование, институциональные механизмы координации, стандартизацию процессов управления рисками и ответственность участников цифровых цепей поставок. Отсутствие должного правового и организационного обеспечения киберустойчивости логистических систем формирует предпосылки для реализации угроз, последствия которых выходят за пределы сферы информационных технологий и затрагивают транспортную, промышленную и финансовую безопасность.

Актуальность исследования усиливается ростом количества и усложнением характера киберинцидентов в логистике, наблюдаемым в последние годы. Цифровые атаки все чаще ориентированы не на хищение информации как таковой, а на дестабилизацию операционной деятельности, блокирование критических сервисов и создание управляемых сбоев в транспортных и складских процессах. В условиях, когда логистические системы интегрированы в национальные и международные цепи создания стоимости, подобные воздействия приобретают признаки экономического давления и могут использоваться как инструмент гибридного воздействия.

В научной и правоприменительной плоскости проблема кибербезопасности логистических систем остается фрагментарно разработанной. Существенная часть исследований сосредоточена на технических аспектах защиты информационных систем либо на общей проблематике кибербезопасности критической информационной инфраструктуры. Вместе с тем логистика как особый объект экономических и правовых рисков требует самостоятельного анализа, учитывающего отраслевую специфику, множественность участников и высокую степень межотраслевой взаимосвязанности.

В этой связи целью настоящего исследования является формирование целостного представления о кибербезопасности логистических систем как элементе

обеспечения их экономической безопасности. В рамках статьи была исследована экономическая специфика киберугроз, как неотъемлемого элемента обеспечения экономической безопасности логистических систем и характера влияния киберугроз на функционирование логистики. Также были выявлены ключевые направления и формы кибервоздействий на транспортно-логистическую инфраструктуру, и определены правовые и организационные механизмы противодействия таким угрозам с учетом их экономических последствий. Исследование указанных аспектов позволяет обосновать необходимость интеграции кибербезопасности в систему стратегического управления логистическими рисками и развития правового регулирования в сфере цифровой устойчивости логистических систем. [10]

Кибербезопасность логистических систем в условиях цифровой трансформации экономики Российской Федерации приобретает значение одного из ключевых факторов обеспечения их экономической устойчивости. Логистика в современных условиях представляет собой сложный межотраслевой комплекс, объединяющий транспортную инфраструктуру, складские и распределительные центры, информационные платформы управления цепями поставок, а также финансово-расчётные и контрольные механизмы. Функционирование данного комплекса невозможно без использования информационных технологий, что предопределяет зависимость логистических процессов от состояния цифровой среды и уровня её защищённости.

Правовые предпосылки формирования цифровых логистических систем закреплены в нормах Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [7], который определяет информацию как объект правовой охраны и возлагает на обладателей информационных ресурсов обязанность по обеспечению их защиты. Для логистических систем это означает необходимость предотвращения неправомерного доступа к данным о маршрутах перевозок, параметрах грузов, графиках движения, складских операциях и иных сведениях, утрата либо искажение которых способно привести к значительным экономическим потерям.

Включение логистических информационных систем в сферу правового регулирования кибербезопасности усиливается положениями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [6]. В соответствии с данным законом значимыми объектами критической информационной инфраструктуры признаются информационные системы и автоматизированные системы управления, функционирующие в сфере транспорта. Таким образом, цифровые решения, применяемые в управлении перевозками, навигации, диспетчеризации и мониторинге грузопотоков, приобретают особый правовой статус, предполагающий усиленные требования к их защите от компьютерных атак.

Экономическая безопасность логистических систем напрямую связана с устойчивостью транспортной инфраструктуры, что находит отражение в Федеральном законе от 09.02.2007 № 16-ФЗ «О транспортной безопасности» [5]. Указанный закон ориентирован на защиту транспортных объектов и транспортных средств от актов незаконного вмешательства, к которым в условиях цифровизации относятся и кибервоздействия на автоматизированные системы управления транспортом. Нарушение работы таких систем способно повлечь дестабилизацию перевозочного процесса, увеличение сроков доставки и рост логистических издержек, что формирует прямую угрозу экономическим интересам участников логистических цепей.

Цифровизация логистики в Российской Федерации сопровождалась ростом количества киберинцидентов, затрагивающих транспортно-логистическую сферу. Компьютерные атаки все чаще направлены на нарушение доступности и целостности информационных систем, обеспечивающих управление логистическими процессами. Вмешательство в работу систем диспетчеризации, электронного документооборота и мониторинга грузов приводит к формированию сбоев, которые трансформируются в экономические потери не только для конкретных организаций, но и для связанных с ними хозяйствующих субъектов [2].

Особое значение имеют киберугрозы, реализуемые в отношении автоматизированных систем управления технологическими процессами на транспорте. В условиях высокой степени автоматизации вмешательство в функционирование таких систем может приводить к несоответствию между планируемыми и фактическими параметрами перевозок, нарушению согласованности логистических операций и формированию «узких мест» в цепях поставок. Экономические последствия данных воздействий выражаются в росте транзакционных издержек, штрафных санкциях за нарушение договорных обязательств и снижении общей эффективности логистических систем.

Правовое регулирование защиты информации в логистике дополняется нормами Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [9]. Сведения, используемые логистическими компаниями в процессе организации перевозок и управления складской инфраструктурой, обладают высокой экономической ценностью. Несанкционированный доступ к таким данным в результате кибератак способен создавать условия для недобросовестной конкуренции, подрывать рыночные позиции хозяйствующих субъектов и нару-

шать баланс экономических интересов в логистической сфере.

Наряду с этим Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [8] распространяется на обработку сведений о работниках транспортно-логистических организаций, водителях, экспедиторах и иных участниках логистических процессов. Киберинциденты, влекущие утечку или неправомерное использование персональных данных, формируют дополнительные экономические риски, связанные с привлечением к ответственности, приостановкой деятельности и утратой деловой репутации.

Экономическая специфика киберугроз в логистических системах проявляется в их способности вызывать каскадные эффекты. Нарушение функционирования одного элемента цифровой логистической инфраструктуры способно дестабилизировать смежные звенья цепи поставок, включая производство, торговлю и внешнеэкономическую деятельность. В условиях высокой интеграции логистики в национальную экономику такие воздействия приобретают системный характер и трансформируются в угрозы экономической безопасности государства.

Федеральный закон № 187-ФЗ устанавливает обязанность субъектов критической информационной инфраструктуры выявлять компьютерные инциденты, принимать меры по их локализации и взаимодействовать с уполномоченными государственными органами. Реализация данных требований в логистической сфере направлена на снижение вероятности реализации киберугроз и минимизацию экономического ущерба. Вместе с тем многообразие участников логистических цепей и преобладание частных операторов усложняют практическую реализацию данных норм и требуют согласования публичных и частных интересов [10].

Экономические последствия кибератак на логистические системы выходят за рамки прямых убытков, связанных с восстановлением работоспособности информационных ресурсов. Существенное значение имеют косвенные эффекты, включая снижение доверия контрагентов, рост страховых издержек и ухудшение условий договорного взаимодействия. В условиях конкурентного рынка транспортно-логистических услуг киберинциденты становятся фактором, влияющим на долгосрочную устойчивость бизнеса.

Таким образом, кибербезопасность логистических систем представляет собой самостоятельное направление обеспечения их экономической безопасности, имеющее нормативное закрепление в системе федерального законодательства. Воздействие киберугроз на цифровую логистическую инфраструктуру способно нарушать устойчивость хозяйственных связей, увеличивать издержки и снижать эффективность логистических процессов. В условиях цифровой экономики правовое обеспечение киберустойчивости логистики становится ключевым элементом защиты экономических интересов хозяйствующих субъектов и государства.

Проведённый анализ позволяет констатировать, что кибербезопасность логистических систем в условиях цифровизации приобретает самостоятельное значение в структуре их экономической безопасности. Логистика, функционирующая на основе автоматизированных систем управления, цифровых платформ и электронного документооборота, становится уязвимой к кибервоздействиям, последствия которых выходят за рамки информационных рисков и трансформируются в экономические потери, нарушение устойчивости хозяйственных связей и снижение эффективности транспортно-логистической деятельности.

Нормы федерального законодательства Российской Федерации формируют правовую основу защиты цифровой логистической инфраструктуры, включая положения Федеральных законов № 149-ФЗ «Об информации, информационных технологиях и о защите информации», № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и № 16-ФЗ «О транспортной безопасности». Совокупное применение данных актов позволяет рассматривать киберугрозы в логистике как разновидность угроз экономической безопасности, направленных на устойчивость транспортных процессов и стабильность цепей поставок. Вместе с тем действующее регулирование носит фрагментарный характер и не всегда учитывает межотраслевую природу логистических систем и множественность вовлечённых субъектов [3].

В условиях дальнейшей цифровой трансформации логистики обеспечение кибербезопасности требует комплексного правового подхода, основанного на согласовании норм информационного, транспортного и хозяйственного законодательства, а также на интеграции требований киберустойчивости в систему управления экономическими рисками. Рассмотрение кибербезопасности исключительно как технической задачи не отражает её реального значения для экономики логистических систем и не позволяет эффективно противодействовать угрозам, имеющим системный характер.

Таким образом, кибербезопасность логистических систем должна рассматриваться как неотъемлемый элемент обеспечения их экономической безопасности, направленный на поддержание устойчивости логистических процессов, защиту экономических интересов участников цепей поставок и сохранение стабильности транспортно-логистической инфраструктуры Российской Федерации.

ЛИТЕРАТУРА

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Дмитриев А.В. Организационно-экономические аспекты обеспечения информационной безопасности в логистических системах //Управленческое консультирование. — 2025. — №. 1 (187). — С. 34–44.
3. Карпов М.А. Кибербезопасность в инфокоммуникационных системах //Парадигма. — 2025. — №. 4-2. — С. 172–177.
4. Семашко Е.А. Кибербезопасность в логистических системах. — 2024.
5. Федеральный закон от 09.02.2007 N 16-ФЗ (ред. от 21.04.2025) «О транспортной безопасности».
6. Федеральный закон от 26.07.2017 N 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации».
7. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.09.2025).
8. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) «О персональных данных».
9. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 08.08.2024) «О коммерческой тайне».
10. Ягудина Г.Р., Фатихова Л.Э. Кибербезопасность в логистике: риски взлома автономных систем и защита данных //Социально-экономические и технические системы: исследование, проектирование, оптимизация. — 2025. — №. 2. — С. 123–127.

© Логутова Тамара Григорьевна (t.logutova7@mail.ru); Лазаревская Юлианна Артуровна (y.lazarevskaya@mgumariupol.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»