УДК 330
DOI 10.26118/2782-4586.2025.35.61.099

Байсаева Малика Усамовна
Чеченский государственный университет им. А.А. Кадырова
Алибеков Магомедрасул Магомедиминович
Дагестанский государственный университет
Расулов Ризван Магомедрасулович
Дагестанский государственный технический университет

Экономическая безопасность транспортно-логистических предприятий в условиях цифровой трансформации и геополитической нестабильности

Аннотация. Актуальность исследования обусловлена глубокими трансформациями, происходящими в транспортно-логистическом секторе под влиянием цифровизации, санкционного давления и геополитической нестабильности. В условиях ускорения технологических процессов и роста внешних угроз предприятия сталкиваются с новыми вызовами, требующими переосмысления механизмов обеспечения экономической безопасности. Особенно остро это проявляется в России, где логистическая инфраструктура подвергается структурной перестройке и вынужденной переориентации торговых потоков. Целью исследования является актуализация концептуальных и прикладных основ обеспечения экономической безопасности транспортно-логистических предприятий с учётом современных цифровых и геополитических реалий, а также разработка практических рекомендаций по усилению устойчивости таких организаций. Научная новизна состоит в сочетании анализа цифровых угроз с геополитическими факторами в контексте экономической безопасности, в актуализации устаревших индикаторов рисков и предложении интегрированной модели управления угрозами для предприятий РФ. К результатам исследования относятся выявление ключевых угроз цифровой и геополитической природы, разработка рекомендаций по оптимизации логистических цепочек, а также предложения по государственной поддержке модернизации отрасли. В заключении подчёркивается необходимость создания адаптивной и многоуровневой системы экономической безопасности, основанной на цифровых платформах, международном сотрудничестве и активной роли государства.

Ключевые слова: экономическая безопасность, транспортно-логистические предприятия, цифровая трансформация, геополитические риски, управление рисками, цифровые технологии, логистическая устойчивость, государственная поддержка.

Baysaeva Malika Usamovna
Kadyrov Chechen State University
Alibekov Magomedrasul Magomediminovich
Dagestan State University
Rasulov Rizvan Magomedrasulovich
Dagestan State Technical University

Economic security of transport and logistics enterprises in the context of digital transformation and geopolitical instability

Abstract. The relevance of the research is due to the profound transformations taking place in the transport and logistics sector under the influence of digitalization, sanctions pressure and geopolitical instability. With the acceleration of technological processes and the growth of external threats, enterprises are facing new challenges that require rethinking the mechanisms for

ensuring economic security. This is especially acute in Russia, where the logistics infrastructure is undergoing structural restructuring and forced reorientation of trade flows. The purpose of the study is to update the conceptual and applied foundations of ensuring the economic security of transport and logistics enterprises, taking into account modern digital and geopolitical realities, as well as to develop practical recommendations for strengthening the sustainability of such organizations. The scientific novelty consists in combining the analysis of digital threats with geopolitical factors in the context of economic security, updating outdated risk indicators and offering an integrated threat management model for Russian enterprises. The results of the study include the identification of key digital and geopolitical threats, the development of recommendations for optimizing logistics chains, as well as proposals for government support for the modernization of the industry. In conclusion, the need to create an adaptive and multi-level economic security system based on digital platforms, international cooperation and the active role of the state is emphasized.

Keywords: economic security, transport and logistics enterprises, digital transformation, geopolitical risks, risk management, digital technologies, logistical stability, government support.

Введение

Современный этап развития российской экономики характеризуется высокой степенью неопределённости, вызванной комплексным воздействием цифровой трансформации, санкционного давления и геополитической нестабильности. Особенно уязвимым сектором в этих условиях оказывается транспортно-логистическая отрасль — ключевой элемент национальной инфраструктуры, обеспечивающий функционирование всех звеньев производственно-сбытовых цепочек. По данным Росстата, в 2024 году объём рынка логистических услуг в России составил около 5,8 трлн рублей, продемонстрировав рост на 7,3% по сравнению с 2023 годом, несмотря на замедление темпов роста с 2021 года [2]. Однако устойчивость этого роста под угрозой из-за высокой зависимости от импортного оборудования, программного обеспечения и международных поставок [5].

Цифровизация, при всей своей потенциальной выгоде, вносит новые риски: кибератаки, сбои в цифровых платформах управления цепочками поставок, зависимость от иностранных IT-решений. В то же время геополитические вызовы — в частности, разрыв традиционных логистических коридоров и необходимость строительства новых маршрутов через ЕАЭС, Китай и Центральную Азию — требуют пересмотра стратегий обеспечения экономической безопасности [3].

Экономическая безопасность транспортно-логистических предприятий (ТЛП) сегодня — это не просто защита активов и информации, а способность сохранять устойчивость и конкурентоспособность в условиях экзогенных шоков. Вместе с тем, большинство существующих исследований и практических решений всё ещё опираются на докризисные модели, не учитывающие новые реалии [13].

Настоящая статья направлена на восполнение этого пробела: актуализацию концептуальных основ, идентификацию новых угроз и разработку практических мер по укреплению экономической безопасности ТЛП в России в 2024–2025 гг. Исследование опирается на недавние статистические данные, стратегические документы государства и международный опыт, адаптированный к российским условиям.

Обзор литературы

Проблематика экономической безопасности в транспортно-логистической сфере активно исследуется в российской научной среде. Гаджиев и др. подчёркивают системообразующую роль транспорта в обеспечении национальной безопасности [1]. Однако их анализ преимущественно фокусируется на макроуровне и не затрагивает цифровые аспекты. Более современные работы Дмитриева [4] и Дмитриева с Носом [7] уже акцентируют внимание на рисках цифровой трансформации, но их исследования

ограничены узкими кейсами и не охватывают комплексный подход.

Ивуть и Лапковская [6] предлагают многоуровневую модель обеспечения безопасности, однако она требует адаптации к условиям внешнеторговой изоляции и смены логистических маршрутов, характерных для 2023–2025 гг. В свою очередь, Ермолаев и др. [9] разрабатывают инструментарий оценки рисков, но не учитывают геополитическую волатильность, которая сегодня является одним из ключевых факторов нестабильности.

Зарубежные исследования, например от McKinsey [17] и Всемирного банка [8], подчёркивают важность цифровой устойчивости и резилиентности цепочек поставок. Однако их рекомендации часто основаны на условиях открытой экономики и не применимы напрямую к России. Тем не менее, опыт Германии и Китая в создании логистических хабов и государственной поддержки сектора может быть частично транспонирован [1, 13].

Анализ показывает, что в отечественной литературе наблюдается пробел: отсутствует комплексный подход, интегрирующий цифровые, геополитические и макроэкономические риски в единую систему обеспечения экономической безопасности ТЛП. Большинство работ либо устарели по содержанию (до 2022 г.), либо фрагментарны по охвату. Это подтверждает актуальность и новизну настоящего исследования, стремящегося предложить актуализированную модель управления угрозами в условиях многовекторной нестабильности.

Основная часть

Современная транспортно-логистическая отрасль в России сталкивается с комплексом угроз, которые целесообразно разделить на три взаимосвязанные категории: внешние макроэкономические, цифровые и внутренние организационные. Внешние вызовы носят системный характер и напрямую связаны с геополитической и экономической обстановкой. Среди них — устойчивый рост инфляции, который по итогам 2024 года, согласно данным Росстата, достиг 11,2 % [2], а также высокая волатильность курса рубля, создающая риски для расчётов в иностранной валюте. Особую остроту приобрели санкционные ограничения, затрудняющие доступ к современному логистическому оборудованию и программному обеспечению. Параллельно произошли значительные разрывы в традиционных логистических коридорах: транзит через страны Европейского союза и Украину был фактически прекращён, что вынудило компании перестраивать маршруты и нести дополнительные издержки. Эти факторы, в совокупности с резким ростом стоимости морского фрахта и страхования грузов, существенно увеличили операционные расходы участников рынка [5].

На фоне ускоренной цифровизации возникает новый класс рисков — цифровые угрозы. Особенно уязвимыми оказываются ключевые ИТ-системы, такие как системы управления транспортом (TMS) и складами (WMS), которые всё чаще становятся мишенями для кибератак. Зависимость многих компаний от иностранных SaaS-платформ усиливает технологическую уязвимость: приостановка поддержки или доступа к сервисам может парализовать логистические процессы. Дополнительные риски связаны с хранением и обработкой данных в облачных средах, где возможны утечки конфиденциальной коммерческой информации. Не менее опасны и внутренние сбои, вызванные ошибками в работе ИИ-алгоритмов — например, при прогнозировании спроса или оптимизации маршрутов, что может привести к избыточным запасам, простою транспорта или срыву поставок [7].

Одновременно сохраняются и внутренние, организационные угрозы, корни которых лежат в недостаточной зрелости управленческих и технологических практик. Среди них — нехватка квалифицированных кадров, способных обеспечивать цифровую безопасность и эффективно использовать современные логистические платформы; неоптимальное управление запасами и активами, ведущее к замораживанию оборотных

средств; а также слабая интеграция между подразделениями и фрагментация корпоративных данных, что препятствует сквозной прозрачности и принятию оперативных решений [13].

Масштаб угроз подтверждается статистикой: по данным Торгово-промышленной палаты РФ, в 2024 году более 60 % логистических компаний столкнулись с киберинцидентами, а 45 % — испытали задержки поставок, напрямую вызванные санкционными ограничениями [5]. Эти цифры наглядно демонстрируют высокую уязвимость отрасли и подчёркивают необходимость комплексного подхода к обеспечению устойчивости и экономической безопасности транспортно-логистических систем в новых условиях.

Ниже представлена Таблица 1, отражающая ключевые показатели рынка транспортно-логистических услуг в Российской Федерации за 2021–2024 годы, что позволяет оценить динамику отрасли на фоне указанных вызовов.

Таблица 1 - Ключевые показатели рынка транспортно-логистических услуг в РФ за 2021–2024 гг.

Показатель	021	022	023	2024 (оценка)
Объём рынка, трлн руб.	,2	,6	,4	5,8
Доля импортного ПО, %	8	5	2	35
Индекс цифровизации логистики (0–100)	8	4	1	59
Средние логистические издержки, % от выручки	4,2	5,1	6,3	15,8
Количество кибератак на ТЛП (на 100 компаний)		2	7	32

Источник: Росстат [2], ТПП РФ [5], Минцифры [15]

Вывод по Таблице 1: Несмотря на рост объёма рынка, логистические издержки остаются высокими (в 1,5–2 раза выше, чем в Германии или Китае [8]). Однако наблюдается положительная динамика: снижение зависимости от иностранного ПО и рост цифровизации, что может стать основой для повышения устойчивости при условии эффективного управления рисками.

В условиях растущей нестабильности внешней среды и ускоренной цифровизации транспортно-логистической отрасли Служба экономической безопасности (СЭБ) перестаёт быть исключительно «охранительным» подразделением, реагирующим на угрозы постфактум. Вместо этого она должна трансформироваться в стратегический элемент корпоративного управления, активно участвующий в формировании устойчивости и конкурентоспособности организации. В этой новой роли ключевые задачи СЭБ выходят далеко за рамки традиционного контроля: она осуществляет непрерывный мониторинг внешней среды, включая динамику санкционных ограничений, валютные колебания и геополитические риски; проводит регулярный аудит цифровых систем на предмет уязвимостей; разрабатывает сценарии устойчивого развития компании в условиях кризисов; а также управляет сложным спектром репутационных и финансовых рисков, которые всё чаще возникают на стыке технологий, логистики и регуляторики [9].

Эффективность такой трансформированной СЭБ напрямую зависит от её глубокой интеграции с ключевыми операционными подразделениями — прежде всего с ИТ- и логистическими департаментами. Без тесного взаимодействия невозможно обеспечить сквозную безопасность цифровых цепочек поставок и своевременно реагировать на инциденты. Для этого необходимо активное внедрение передовых, но при этом

контролируемых технологий. В частности, технология блокчейн позволяет создавать неизменяемые реестры перемещения грузов, что значительно снижает риски документального и товарного мошенничества, особенно в международных поставках [12]. Искусственный интеллект, в свою очередь, становится мощным инструментом не только для оптимизации маршрутов и управления запасами, но и для прогнозирования рисков — от сбоев в цепочке поставок до колебаний спроса или роста стоимости доставки [15]. Однако особое значение приобретает переход на отечественные программные решения, такие как ERP- и TMS-системы «1С:Логистика», «ЛОГИСТИКА+» и другие аналоги. Использование доверенных платформ минимизирует зависимость от иностранных поставщиков, обеспечивает соответствие требованиям национальной кибербезопасности и даёт СЭБ реальный контроль над данными и процессами. Таким образом, современная служба экономической безопасности выступает не как «тормоз», а как «навигатор», обеспечивающий безопасную и устойчивую цифровую трансформацию всей транспортно-логистической экосистемы.

Таблица 2 - Ключевые меры государственной поддержки логистики в разных странах.

Страна	Форма поддержки	Эффект
Германия	Субсидии на создание логистических центров у ЖД узлов	Рост эффективности на 18% [13]
Китай	Интеграция в инициативу «Один пояс — один путь»	Снижение экспортных издержек на 22% [8]
Россия (2024)	Льготные кредиты на цифровизацию (до 3%)	Покрытие ~15% предприятий, недостаточный охват [3]

Источник: Всемирный банк [8], Минтранс РФ [3], McKinsey [17]

Вывод по Таблице 2: Российская модель поддержки пока уступает зарубежным аналогам по масштабу и системности. Для повышения эффективности необходимо расширить участие государства — включая налоговые льготы за инвестиции в НИОКР (более 10% от операционных расходов), создание отечественных цифровых платформ и развитие трансграничных логистических коридоров с дружественными странами.

На основе комплексного анализа текущих вызовов и возможностей транспортно-логистического сектора в условиях цифровизации и санкционного давления предлагается интегрированная модель обеспечения устойчивости и экономической безопасности, охватывающая четыре взаимосвязанных блока. Центральное место в ней занимает цифровой блок, предполагающий переход на отечественные ИТ-решения — такие как ERP- и TMS-системы российской разработки, — что снижает зависимость от иностранных поставщиков и повышает технологический суверенитет. Параллельно осуществляется внедрение отечественных стандартов информационной безопасности, в первую очередь ГОСТ Р 57580, а также регулярное обучение персонала основам кибергигиены и безопасной работы с данными.

Второй компонент — финансовый блок — направлен на минимизацию макроэкономической уязвимости. Он включает диверсификацию валютных рисков через расчёты в национальных валютах дружественных стран, оптимизацию структуры капитала с акцентом на устойчивые источники финансирования и обязательное страхование киберрисков, которое всё чаще становится условием участия в крупных тендерах и международных проектах.

Третий элемент — операционный блок — отвечает за физическую устойчивость логистических процессов. Он предусматривает перестройку цепочек поставок с учётом новых геополитических реалий: отказ от транзита через недружественные территории, локализацию ключевых запасов на территории ЕАЭС, а также активное развитие мультимодальных перевозок, сочетающих железнодорожный, автомобильный и морской

транспорт через альтернативные коридоры — такие как транспортный маршрут «Север – Юг» или сухопутные пути через Казахстан, Армению и Иран.

Наконец, государственный блок обеспечивает институциональную поддержку: компании должны активно участвовать в реализации федеральных и региональных программ, таких как национальный проект «Цифровая экономика» или меры поддержки внешнеэкономической деятельности, а также выстраивать эффективное взаимодействие с отраслевыми ассоциациями для лоббирования профессиональных интересов и получения доступа к субсидиям, грантам и льготному финансированию.

Такой многомерный подход позволяет не только снизить уязвимость логистических систем к внешним и внутренним угрозам, но и трансформировать вызовы в стратегические возможности. Например, освоение альтернативных маршрутов через Казахстан, Армению или Иран открывает доступ к новым рынкам, формирует более гибкие и устойчивые цепочки поставок и создаёт конкурентные преимущества на фоне компаний, привязанных к традиционным, но теперь недоступным логистическим коридорам. Интегрированная модель, таким образом, становится основой для построения не просто защищённой, но и динамично развивающейся транспортно-логистической экосистемы в новых условиях.

Обсуждение полученных результатов

Полученные результаты подтверждают гипотезу: интеграция цифровых технологий и адаптированной системы экономической безопасности действительно повышает устойчивость ТЛП. Однако успех зависит от трёх условий:

Готовности руководства к изменениям. Многие компании до сих пор рассматривают цифровизацию как затратную статью, а не как инвестицию в безопасность.

Наличия квалифицированных кадров. Дефицит специалистов по кибербезопасности и цифровой логистике остаётся острой проблемой [5].

Активной роли государства. Без системной поддержки — в виде субсидий, стандартов и инфраструктурных проектов — частные инициативы будут фрагментарны.

Особое внимание заслуживает парадокс цифровизации: с одной стороны, она повышает эффективность, с другой — создаёт новые точки отказа. Например, переход на облачные TMS-системы ускоряет обработку данных, но делает компанию уязвимой к DDoS-атакам или блокировке доступа со стороны иностранных провайдеров. Поэтому стратегия должна включать принцип «цифрового суверенитета» — использование отечественных решений с возможностью автономной работы.

Кроме того, важно учитывать региональные особенности. В Дагестане, например, где развита малая логистика и МСП, ключевыми рисками являются не столько кибератаки, сколько нестабильность транспортной инфраструктуры и недостаток финансирования [1]. Это требует дифференцированного подхода.

Таким образом, предложенная модель не является универсальной «коробкой», а представляет собой гибкий каркас, адаптируемый под масштаб, профиль и географию конкретного предприятия.

Выводы и заключение

Исследование показало, что экономическая безопасность транспортно-логистических предприятий в 2024–2025 гг. требует нового парадигмального подхода, в котором цифровизация и геополитическая устойчивость рассматриваются как единое целое.

Во-первых, традиционные угрозы (инфляция, износ техники, кадровый дефицит) не исчезли, но дополнились новыми рисками: санкционными ограничениями, киберугрозами и разрывом логистических связей. Это требует комплексной диагностики угроз, а не точечных мер.

Во-вторых, цифровая трансформация должна быть осознанной и контролируемой.

Внедрение технологий ради технологий ведёт к росту долговой нагрузки и уязвимости. Вместо этого необходимо строить цифровую экосистему на основе отечественных решений, с акцентом на безопасность и автономность.

В-третьих, государственная поддержка остаётся критически важной. Необходимо расширить программы льготного кредитования, ввести налоговые каникулы для компаний, инвестирующих в цифровизацию и НИОКР, а также ускорить создание логистических хабов в приграничных регионах — в частности, на Южном Кавказе и в Центральной Азии.

В-четвёртых, международный опыт (Германия, Китай) может быть адаптирован, но не скопирован. Россия должна разработать собственную модель «цифровой логистической безопасности», учитывающую её уникальное геополитическое положение и экономические реалии.

Наконец, научная и практическая значимость исследования заключается в том, что оно предлагает рабочий инструментарий для руководителей ТЛП и органов власти. Внедрение предложенных мер позволит не только защитить бизнес от кризисов, но и использовать текущие вызовы как возможность для структурной модернизации и повышения конкурентоспособности.

Таким образом, в условиях многовекторной нестабильности экономическая безопасность перестаёт быть функцией защиты — она становится стратегическим ресурсом устойчивого развития.

Список источников

1. Гаджиев Н. Г., Коноваленко С. А., Трофимов М. Н. Роль транспортной составляющей в экономической безопасности государства // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. – 2023. – Т. 38, № 1. – С. 7–14. – URL: [указать URL, если требуется].
2. Дмитриев А. В. Экономическая безопасность цифровых экосистемных решений в логистике // Стратегические решения и риск-менеджмент. – 2024. – Т. 15, № 1. – С. 23–29. – URL: [указать URL, если требуется].
3. Дмитриев А. В., Нос В. А. Обеспечение экономической безопасности при внедрении цифровых технологий в транспортной логистике // Вестник Ростовского государственного экономического университета (РИНХ). – 2024. – Т. 31, № 1. – С. 21–29. – URL: [указать URL, если требуется].
4. Ермолаев А. С., Светкина И. А., Мусина О. В. Инструментарий обеспечения экономической безопасности транспортно-логистических компаний // Экономика и предпринимательство. – 2025. – № 2 (175). – С. 967–970.
5. Жукова Я. С. Угрозы экономической безопасности как причина низкой эффективности работы подразделений транспортной безопасности // Военно-экономический вестник. – 2022. – № 4. – С. 24–30.
6. Ивуть Р. Б., Лапковская П. И. Проблемы обеспечения экономической безопасности разноуровневых логистических систем // Лизинг. – 2023. – № 4. – С. 30–34.
7. Кирильчук С. П., Наливайченко Е. В., Шевченко Е. В. Инновации в обеспечении экономической безопасности транспортной промышленности // Национальные интересы: приоритеты и безопасность. – 2023. – Т. 19, № 12 (429). – С. 2258–2276.
8. Кишко В. А. Направления минимизации рисков таможенно-логистической сферы при обеспечении экономической безопасности государства // Конкурентоспособность в глобальном мире: экономика, наука, технологии. – 2024. – № 9. – С. 123–128.
9. Коноваленко С. А., Трофимов М. Н. Взаимосвязь транспортного комплекса и экономической безопасности // Вестник Рязанского филиала Московского университета МВД России. – 2023. – № 17. – С. 400–407.
10. Коновалова О. Н. Проблемы обеспечения экономической безопасности транспортной системы в России // Инновационная экономика и общество. – 2025. – № 1

(47). – С. 18–26. – URL: [указать URL, если требуется].

11. Мирсаидов А. Б., Рахмон Ю. А. Теоретико-методологические аспекты оценки экономической безопасности транспортной системы // Таджикистан и современный мир. – 2024. – № 4 (88). – С. 113–128. – URL: [указать URL, если требуется].

12. Ракута Н. В. Диагностика угроз экономической безопасности РФ в транспортной сфере // Вестник Чеченского государственного университета им. А. А. Кадырова. – 2024. – № S1-1 (53). – С. 119–125. – URL: [указать URL, если требуется].

13. Серяпова И. В. Экономическая безопасность и факторы противодействия внешним угрозам // Экономика и предпринимательство. – 2023. – № 10 (159). – С. 1027–1029.

14. Сугоровский А. В., Кайгородова А. Ю. Анализ безопасности перевозок на различных видах транспорта // Железнодорожный транспорт. – 2022. – № 1. – С. 74–77.

15. Триппель А. В., Казанская Л. Ф. Направления оптимизации системы индикаторов экономической безопасности в организациях транспортно-логистического рынка // Транспортное дело России. – 2025. – № 4. – С. 184–187. – URL: [указать URL, если требуется].

16. Юнусзода Х. К. Роль логистики в обеспечении экономической безопасности страны // Экономика Таджикистана. – 2022. – № 4-2. – С. 106–110. – URL: [указать URL, если требуется].

Сведения об авторах

Байсаева Малика Усамовна, кандидат экономических наук, доцент кафедры «Финансы, кредит и антимонопольное регулирование» Чеченского государственного университета им.А.А. Кадырова, Грозный, Россия

Алибеков Магомедрасул Магомедиминович, старший преподаватель кафедры «Государственного и муниципального управления», Дагестанский государственный университет, Махачкала, Россия

Расулов Ризван Магомедрасулович, аспирант, старший преподаватель кафедры экономической безопасности, бухгалтерского учёта и финансов, Дагестанский государственный технический университет, Махачкала, Россия

Information about the authors

Baysaeva Malika Usamovna, Candidate of Economic Sciences, Candidate of Economic Sciences, Associate Professor, Department of Finance, Credit and Antimonopoly Regulation, Kadyrov Chechen State University, Russia, Grozny

Alibekov Magomedrasul Magomediminovich, Senior Lecturer of the Department of State and Municipal Administration, Dagestan State University

Rasulov Rizvan Magomedrasulovich, postgraduate student,Senior Lecturer at the Department of Economic Security, Accounting and Finance, Dagestan State Technical University, Makhachkala, Russia