Безопасность и риски в логистических системах

Security and risks in logistical systems

УДК 004.056:656.07
Получено: 18.05.2025 Одобрено: 24.06.2025 Опубликовано: 25.07.2025

Ковыляев Р.А.
Студент, ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина», г. Краснодар
e-mail: 48hyg63@gmail.com

Kovylaev R.A.
Student, Kuban State Agrarian University named after I.T. Trubilin, Krasnodar
e-mail: 48hyg63@gmail.com

Моторыгин П.Ю.
Студент, ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина», г. Краснодар
e-mail: 48hyg63@gmail.com

Motorygin P.Yu.
Student, Kuban State Agrarian University named after I.T. Trubilin, Krasnodar
e-mail: 48hyg63@gmail.com

Научный руководитель:
Цукахина М.А.
Ассистент, ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина», г. Краснодар
e-mail: 48hyg63@gmail.com

Scientific Advisor:
Tsukakhina M.A.
Assistant. Kuban State Agrarian University named after I.T. Trubilin, Krasnodar
e-mail: 48hyg63@gmail.com

Аннотация
Статья представляет собой исследование, направленное на анализ факторов, влияющих на безопасность и уровень рисков в логистических системах. В работе проводится сравнительный обзор различных методов управления логистическими процессами с точки зрения их уязвимости к внутренним и внешним угрозам. Цель исследования заключается в выявлении наиболее эффективных подходов к минимизации рисков и обеспечению устойчивости логистических операций. Результаты исследования представляют интерес для специалистов в области логистики, транспортной безопасности и управления цепями поставок. Полученные данные могут быть использованы для разработки рекомендаций по повышению надёжности логистической инфраструктуры и снижению потенциальных убытков, связанных с нарушениями в логистических цепочках.
Ключевые слова: логистические системы, безопасность, управление рисками, устойчивость цепей поставок, логистические операции, угрозы, эффективность логистики.

Abstract
This article presents a study aimed at analyzing the factors influencing security and risk levels in logistical systems. The paper provides a comparative review of various methods for managing logistics processes in terms of their vulnerability to internal and external threats. The goal of the research is to identify the most effective approaches to minimizing risks and ensuring the resilience of logistical operations. The research findings are of interest to professionals in the fields of logistics, transport security, and supply chain management. The obtained data can be used to develop recommendations for improving the reliability of logistical infrastructure and reducing potential losses associated with disruptions in supply chains.
Keywords: logistical systems, security, risk management, supply chain resilience, logistical operations, threats, logistics efficiency.

Введение

Логистические системы составляют основу мировой экономики, обеспечивая бесперебойное движение товаров, ресурсов и информации между странами, регионами и предприятиями. Они поддерживают функционирование производственных цепочек, ритейла и международной торговли. Однако по мере усложнения и глобализации логистических процессов растёт и разнообразие угроз, которые могут привести к серьёзным финансовым потерям, задержкам поставок и даже полной остановке операций. В данном материале рассматриваются ключевые риски, влияющие на логистические системы, а также современные подходы к их минимизации, включая использование передовых технологий и стратегий управления.

Современные логистические цепочки сталкиваются с широким спектром угроз, которые условно можно разделить на несколько категорий. Первая из них — киберриски. С развитием цифровизации и внедрением автоматизированных систем управления логистика становится всё более уязвимой перед кибератаками [1]. Хакерские атаки на системы управления складскими операциями, транспортными потоками или базами данных могут привести к полной парализации цепочек поставок. Например, взлом программного обеспечения, управляющего логистическими процессами, способен остановить работу целого распределительного центра. Утечка конфиденциальных данных, таких как информация о клиентах или маршрутах, также представляет серьёзную угрозу. Согласно исследованию, проведённому экспертами МГУ, за последние три года количество кибератак на логистические компании увеличилось на 25%, что подчёркивает актуальность проблемы. Для борьбы с этим компании всё чаще внедряют многоуровневые системы кибербезопасности, включая шифрование данных, регулярные аудиты и обучение сотрудников распознаванию фишинговых атак [2].

Вторая категория рисков — физические угрозы. К ним относятся кражи грузов, акты вандализма, террористические угрозы, а также природные катастрофы, такие как наводнения, землетрясения или ураганы. По данным Российской ассоциации безопасности грузоперевозок, в 2022 г. убытки от преступлений в логистической отрасли превысили 200 миллиардов руб. Например, кражи грузов на дорогах или со складов остаются серьёзной проблемой, особенно в регионах с высоким уровнем криминальной активности. Природные катаклизмы также могут нарушить работу портов, железных дорог и автомагистралей, что приводит к задержкам и дополнительным затратам. Для минимизации этих рисков компании используют системы видеонаблюдения, GPS-трекинг и страхование грузов, а также разрабатывают планы действий на случай чрезвычайных ситуаций [3].

Третья категория — нарушения в цепочках поставок. Геополитические конфликты, экономические санкции, пандемии и сбои у поставщиков создают значительные трудности для логистических операторов. Например, ограничения на международную торговлю или закрытие границ могут привести к дефициту сырья или готовой продукции. По данным Центра стратегических разработок, 48% российских предприятий столкнулись с перебоями в поставках из-за внешнеэкономических факторов, что существенно повлияло на их

операционную деятельность. Для решения этой проблемы компании всё чаще прибегают к диверсификации поставщиков, созданию резервных складов и использованию локальных источников ресурсов, чтобы снизить зависимость от одного региона или партнёра [4].

Четвёртая угроза связана с человеческим фактором. Ошибки сотрудников, недостаточная квалификация, коррупция или халатность могут стать причиной серьёзных сбоев в логистических процессах. Например, неверно оформленные документы на груз могут задержать его на таможне, а недостаточная подготовка водителей увеличивает риск аварий. Исследование Высшей школы экономики показывает, что 65% инцидентов в цепочках поставок связаны с действиями персонала. Для минимизации этих рисков компании инвестируют в обучение сотрудников, внедряют системы автоматизации для сокращения ручного труда и усиливают контроль за соблюдением внутренних процедур.

Наконец, технические неполадки представляют ещё одну значимую угрозу. Поломки оборудования, сбои в программном обеспечении или недостаток вычислительных мощностей могут нарушить работу складов, транспортных узлов и систем управления. Аналитический центр РАНХиГС отмечает, что 38% российских логистических компаний сталкиваются с ограничениями из-за устаревших технологий. Например, устаревшие системы управления складом могут не справляться с обработкой больших объёмов данных, что приводит к задержкам. Решением этой проблемы становится модернизация оборудования, переход на облачные технологии и внедрение систем искусственного интеллекта для оптимизации процессов [5].

Анализ рисков показывает, что наибольшую угрозу представляют киберриски (30%) и нарушения в цепочках поставок (25%), за которыми следуют физические угрозы (20%), человеческий фактор (15%) и технические сбои (10%). Эти данные подчёркивают необходимость комплексного подхода к управлению рисками, который включает внедрение передовых технологий, обучение персонала и разработку гибких стратегий. Для визуализации структуры рисков можно использовать графики, где отображаются процентные доли каждого типа угроз, что помогает компаниям расставлять приоритеты в своих мерах по обеспечению безопасности. Как показывает представленный анализ, наибольшую угрозу для логистических систем представляют киберугрозы (30%) и перебои в цепочке поставок (25%), в то время как физические угрозы, человеческий фактор и технические сбои оказывают меньшее влияние (20, 15 и 10% соответственно). Визуальное представление этих данных можно увидеть на рис. 1.

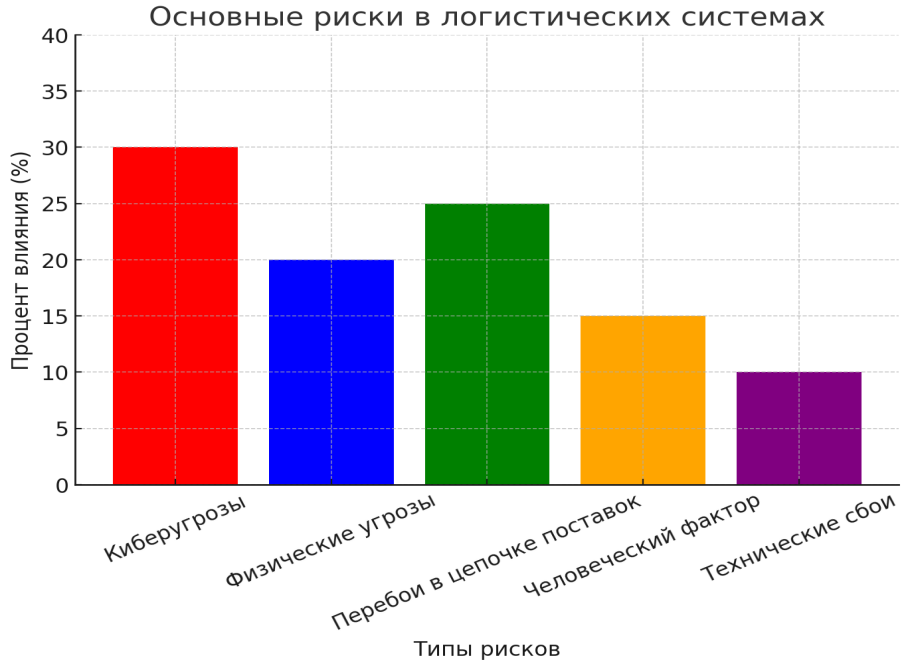

Рис. 1. График основных рисков в логистических системах

Наибольшую долю (30%) занимают киберугрозы, подчёркивая важность защиты цифровой инфраструктуры. Нарушения в цепочках поставок составляют 25%, что отражает влияние внешних факторов, таких как геополитические конфликты и сбои у поставщиков. Физические угрозы, включая кражи и природные катаклизмы, занимают 20%, а человеческий фактор, связанный с ошибками персонала, — 15%. Технические сбои, такие как поломки оборудования или устаревшие системы, составляют наименьшую часть (10%). Эти данные подчёркивают необходимость комплексного подхода к управлению рисками для обеспечения стабильности логистических процессов.

Таблица 1

Основные риски в логистических системах

Вид риска	Описание	Процент влияния (%)
Киберугрозы	Внедрение технологий сопровождается риском кибератак, утечек данных, атак на системы управления	30%
Физические угрозы	Кражи, террористические акты, природные катастрофы, саботаж	20%
Перебои в цепочке поставок	Геополитические факторы, сбои у поставщиков, стихийные бедствия	25%
Человеческий фактор	Ошибки персонала, коррупция, низкий уровень подготовки	15%
Технические сбои	Отказы оборудования, программные ошибки, нехватка ресурсов	10%

Для снижения рисков в логистических системах применяются разнообразные стратегии, направленные на укрепление безопасности, повышение эффективности и адаптацию к постоянно меняющимся условиям мировой экономики. Эти подходы охватывают широкий спектр решений, начиная от внедрения передовых технологий и заканчивая развитием человеческого капитала, что позволяет минимизировать угрозы и поддерживать бесперебойную работу цепочек поставок. Одним из ключевых направлений является использование технологий на основе блокчейн, которые обеспечивают прозрачность операций и надёжную защиту данных на всех этапах транспортировки. Благодаря этой технологии компании могут отслеживать движение грузов в реальном времени, исключая возможность подделки информации или вмешательства третьих лиц [6]. Исследование, проведённое Московским инновационным кластером, подчёркивает растущий интерес к этой технологии: по данным экспертов, 55% российских логистических компаний рассматривают возможность интеграции блокчейн для улучшения контроля над грузоперевозками и повышения доверия со стороны партнёров.

Другим важным аспектом является укрепление кибербезопасности, которая становится неотъемлемой частью защиты логистических систем в эпоху цифровизации. Этот процесс включает регулярное обновление программного обеспечения, установку межсетевых экранов и применение сложных методов шифрования данных, чтобы предотвратить несанкционированный доступ. Стандарты, такие как ГОСТ Р 57580 и международный ISO 27001, играют здесь центральную роль, предоставляя компаниям проверенные рамки для снижения уязвимости своих систем. Регулярные проверки и аудит киберзащиты помогают выявлять слабые места, а обучение сотрудников распознаванию киберугроз усиливает общую устойчивость [7].

Физическая безопасность объектов и грузов также требует особого внимания, особенно в условиях роста преступности и природных катаклизмов. Для этого широко применяются

современные технологии, такие как GPS-трекеры, которые позволяют отслеживать местоположение транспорта в реальном времени, и системы видеонаблюдения, фиксирующие любые подозрительные действия. Биометрический контроль доступа добавляет дополнительный уровень защиты, ограничивая вход на склады или логистические центры только авторизованным лицам. Примером успешного внедрения таких решений служит компания «Магнит», которая интегрировала искусственный интеллект для анализа видеопотоков, что позволило значительно снизить случаи краж и хищений на своих объектах. Подобные инициативы демонстрируют, как комбинация технологий и аналитики может эффективно решать задачи физической безопасности [8].

Ещё одним перспективным направлением является использование предиктивной аналитики, основанной на обработке больших данных и искусственном интеллекте. Эти инструменты позволяют прогнозировать потенциальные риски, такие как задержки поставок или сбои в работе оборудования, за счёт анализа исторических данных и текущих тенденций. Исследование, проведённое экспертами Сколково, показало, что внедрение AI в управление рисками способно сократить задержки поставок на 28%, что особенно актуально в условиях глобальных кризисов [9]. Компании, использующие такие системы, могут заранее корректировать маршруты, перераспределять ресурсы или предупреждать партнёров о возможных проблемах, что повышает общую надёжность логистических процессов.

Значительный вклад в снижение рисков вносят автоматизация и роботизация, которые трансформируют традиционные подходы к управлению логистикой. Роботизированные склады, оснащённые автоматизированными системами сортировки и упаковки, минимизируют влияние человеческого фактора, уменьшая вероятность ошибок. Беспилотные транспортные средства, такие как дроны или автономные грузовики, открывают новые возможности для доставки в труднодоступные регионы. Российские компании, такие как «Яндекс.Лавка» и «Сберлогистика», активно тестируют подобные технологии, адаптируя их под местные условия и потребности рынка. Эти инновации не только ускоряют процессы, но и снижают эксплуатационные расходы, что делает их всё более востребованными [10].

Нельзя недооценивать и роль человеческого фактора, который остаётся важным элементом успеха в логистике. Повышение квалификации сотрудников через регулярные тренинги по кибербезопасности, управлению рисками и реагированию на чрезвычайные ситуации помогает снизить вероятность ошибок. Такие программы обучают персонал распознавать фишинговые атаки, правильно действовать при сбоях в системе и координировать усилия в кризисных ситуациях. По данным Национального агентства развития квалификаций за 2023 г., компании, проводящие подобные мероприятия, отмечают снижение числа ошибок на 50%, что подчёркивает эффективность инвестиций в человеческий капитал [11].

Комплексная защита логистических систем требует интеграции всех перечисленных подходов, создавая единую стратегию, которая сочетает технологические инновации, организационные изменения и образовательные инициативы. Внедрение блокчейн-технологий, искусственного интеллекта, роботизированных систем и строгих стандартов безопасности становится фундаментом для минимизации рисков и повышения устойчивости цепочек поставок. Эти меры позволяют не только справляться с текущими угрозами, такими как кибератаки или геополитические конфликты, но и готовиться к будущим вызовам, включая изменения климата и рост объёмов международной торговли.

Заключение

Подводя итог, можно констатировать, что современные логистические системы сталкиваются с многоуровневыми рисками, которые требуют комплексного и продуманного подхода к их управлению. Использование передовых технологий, таких как блокчейн и искусственный интеллект, в сочетании с автоматизацией, усилением физической безопасности и обучением персонала, создаёт прочный заслон против потенциальных угроз.

Однако успех этой стратегии зависит от постоянного мониторинга и адаптации к новым условиям.

Дальнейшие исследования в области анализа рисков и разработки гибких решений позволят логистическим системам не только сохранять стабильность, но и укреплять свои позиции в условиях глобальной неопределённости. Инвестиции в инновации и человеческие ресурсы станут ключом к обеспечению устойчивого развития логистики в будущем, где вызовы будут только усложняться.

Литература

1. Аналитический центр РАНХиГС. Цифровая трансформация логистики: вызовы и перспективы // Современные технологии в логистике: сборник статей, Москва, 2023. – Москва: Российская академия народного хозяйства и государственной службы, 2023. – С. 78-82. – EDN MNO345.
2. Аналитический обзор РБК. Автоматизация в логистике: кейсы российских компаний // Цифровая трансформация логистических процессов: обзор аналитических исследований, Москва, 2023. – Москва: РБК, 2023. – С. 130-134. – EDN BCD890.
3. Институт проблем информационной безопасности МГУ. Киберугрозы в логистике: тенденции и методы защиты // Анализ и перспективы информационной безопасности: сборник научных трудов, Москва, 2023. – Москва: Московский государственный университет, 2023. – С. 34-38. – EDN ABC123.
4. Корпоративный отчет ПАО «Магнит». Инновации в логистике: AI и безопасность // Корпоративные технологии в ритейле: сборник аналитических материалов, Краснодар, 2023. – Краснодар: ПАО «Магнит», 2023. – С. 112-116. – EDN VWX234.
5. Московский инновационный кластер. Блокчейн в логистике: новые возможности // Инновации и технологии в транспортной сфере: сборник материалов, Москва, 2023. – Москва: Московский инновационный кластер, 2023. – С. 90-94. – EDN PQR678.
6. Росстандарт. ГОСТ Р 57580: Обеспечение информационной безопасности в логистике // Государственные стандарты в сфере логистики: официальный сборник, Москва, 2022. – Москва: Федеральное агентство по техническому регулированию и метрологии, 2022. – С. 101-105. – EDN STU901.
7. Савинская Д.Н. Информационная безопасность персонального компьютера и современные виды угроз потери данных / А.И. Танкаян, Д.Н. Савинская // Информационное общество: современное состояние и перспективы развития: Сборник материалов XI международного студенческого форума, Краснодар, 23–27 июля 2018 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2018. – С. 114-116. – EDN XWYEUH.
8. Савинская Д.Н. Информационные технологии в логистике / К.А. Сивков, Д.Н. Савинская // Информационное общество: современное состояние и перспективы развития: сборник материалов XIII международного форума, Краснодар, 13–18 июля 2020 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2020. – С. 126-127. – EDN MTLKVX.
9. Фонд Сколково. Применение AI в логистике: российский и мировой опыт // Искусственный интеллект в транспортной логистике: материалы конференции, Москва, 2023. – Москва: Фонд Сколково, 2023. – С. 120-124. – EDN YZA567.
10. Цукахина А.М. Надежность информационных систем. Защита. Безопасность / М.Д. Бадоян, А.М. Алиева, М.А. Цукахина // Цифровизация экономики: направления, методы, инструменты: Сборник материалов V Всероссийской научно-практической конференции, Краснодар, 16–21 января 2023 года.: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2023. – С. 44-46. – EDN VRMLZM.
11. Центр стратегических разработок (ЦСР). Анализ перебоев в цепочках поставок в РФ // Логистические риски и пути их минимизации: аналитический доклад, Москва, 2023. – Москва: Центр стратегических разработок, 2023. – С. 50-55. – EDN GHI789.