УДК 656.073 **DOI: 10.34670/AR.2026.96.90.074**

Кибербезопасность систем отслеживания грузов в реальном времени как фактор надёжности международных логистических цепей

Евсеев Дмитрий Владимирович

Студент,
Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет), 105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: Dmitry2004evseev4002@gmail.com

Потапова Дарья Дмитриевна

Студент,
Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет), 105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: ms.dasha.pd@mail.ru

Афанасьев Всеволод Алексеевич

Студент,
Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет), 105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: Afanasyevvsevolod@gmail.com

Ерантаева Анастасия Владимировна

Студент,
Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет), 105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5;
e-mail: anastasiyaerantaeva@mail.ru

Назмиев Тимур Айдарович

Студент,
Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет), 105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5, стр. 1;
e-mail: naztimaid@mail.ru

Аннотация

Цифровая трансформация международного товародвижения сместила периметр уязвимости логистических операторов с физических объектов на потоки телеметрии, поступающей со спутниковых трекеров, RFID-меток и навигационных пломб; одновременно интенсивность таргетированных атак на сегмент транспорта и хранения возросла настолько, что доверие к данным отслеживания уже квалифицируется в качестве самостоятельного экономического актива. Однако в отечественной литературе кибербезопасность чаще трактуется как побочный аспект цифровизации, а не как параметр, детерминирующий надёжность цепи поставок. Цель работы — обосновать прямую функциональную связь между уровнем защищённости систем мониторинга грузов в реальном времени и интегральным показателем надёжности международных логистических цепей. Методология объединяет системный анализ, контент-анализ открытых отчётов индустриальных вендоров за 2022–2024 годы, эконометрическую обработку вторичных данных Росстата и Минтранса, метод цепных подстановок для факторной декомпозиции. Получены три ключевых результата. Во-первых, доля инцидентов с раскрытием конфиденциальной информации в транспортных компаниях достигла 36,8% при доле DDoS-атак 50,7%; средняя оценка прямого ущерба от единичного инцидента варьируется в диапазоне 47,3–62,4 млн рублей в зависимости от категории оператора. Во-вторых, индекс киберустойчивости системы отслеживания вносит вклад в интегральный показатель надёжности цепи поставок на уровне 27,4% — больше, чем фактор технологической сложности оборудования (18,9%). В-третьих, выявлены три архитектурных принципа защиты, обеспечивающих наибольший прирост надёжности при сопоставимых инвестициях. Полученные оценки применимы при формировании корпоративных программ цифровизации, разработке отраслевых регламентов и обосновании затрат на средства защиты информации в транспортно-логистической отрасли.

Для цитирования в научных исследованиях

Евсеев Д.В., Потапова Д.Д., Афанасьев В.А., Ерантаева А.В., Назмиев Т.А. Кибербезопасность систем отслеживания грузов в реальном времени как фактор надёжности международных логистических цепей // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 4А. С. 768-781. DOI: 10.34670/AR.2026.96.90.074

Ключевые слова

Кибербезопасность, системы отслеживания грузов, логистические цепи, информационная безопасность, цифровая трансформация, киберфизические системы, надёжность поставок, навигационные пломбы, телематика, DDoS-атаки, управление рисками.

Введение

Перевод грузовой логистики в режим непрерывного мониторинга – давно не вопрос конкурентного преимущества, а условие участия в международных торговых потоках. Спутниковые трекеры, RFID-метки, электронные пломбы, единая цифровая транспортно-логистическая платформа «ГосЛог» – все эти элементы формируют замкнутый контур обмена данными, в котором каждая операция оставляет цифровой след. Парадокс, однако, заключается в следующем. По мере того как полнота наблюдаемости приближается к идеальной, периметр уязвимости логистического оператора смещается от физического груза к информационному потоку, который этим грузом сопровождает. Точка приложения атаки изменилась – отрасль это осознала позднее, чем хотелось бы.

Реальные инциденты последних лет последовательно подтверждают сместившийся ландшафт рисков. Кибератака на британскую систему точного позиционирования Microlise в октябре 2024 года парализовала отслеживание автопарка курьерской службы DHL и подрядчика Министерства юстиции на несколько суток. Глобальный рынок телематических транспортных и информационных систем управления, по результатам маркетингового анализа [Окольнишникова, Келлер, Конкс, 2022], растёт темпами, опережающими динамику традиционных сегментов автотранспортной индустрии, – то есть масштабирование инфраструктуры мониторинга идёт быстрее, чем формируется архитектура её защиты. Параллельно угрозы информационной безопасности перестали быть локальной технической темой: статистика инцидентов в государственном секторе России демонстрирует устойчивый рост, а доля атак с раскрытием конфиденциальных данных в публичных системах достигла исторических максимумов [Забайкина, 2025]. Цифры некомфортные – особенно в сопоставлении с темпами проникновения цифровых платформ. Спрос отрасли на передовые цифровые технологии прогнозируется на уровне 626,6 млрд рублей к 2030 году против 89,4 млрд в 2020 году. Кратное увеличение инвестиций в технологии создаёт пропорциональное расширение поверхности атаки.

Академическое поле, в котором обсуждается обозначенная проблематика, заметно фрагментировано. Одна группа исследований концентрируется на экономических эффектах цифровизации логистики и формировании конкурентных преимуществ: проекты группы Fesco описаны у Гулого [Гулый, 2023]; трансформация международной логистической системы в Евразийском регионе разобрана у Подольской и Сотникова [Подольская, Сотников, 2024b]; технологический ассортимент в транспортно-логистической отрасли систематизирован теми же авторами в работе по передовым цифровым технологиям [Подольская, Сотников, 2024a]; формирование транспортно-логистической инфраструктуры в направлении стран Азии – у Дробота с соавторами [Дробот, Макаров, Колесников, Жидков, 2023]. Вторая группа – на отдельных технологиях обеспечения прозрачности: блокчейн и смарт-контракты при формировании цепей поставок – у Квятковского [Квятковский, 2024], нейросети в складских процессах – у Беньямина [Беньямин, 2024], цифровые двойники как самостоятельный класс активов – у Абрамова и соавторов [Abramov, Gordeev, Stolyarov, 2024]. Третья – на рынке научных разработок для развития высокотехнологичных решений в транспортной логистике, систематизированном Келлером и соавторами [Келлер, Окольнишникова, Ухова, 2023]. Системного построения, в котором кибербезопасность фигурирует не как сопутствующее ограничение, а как параметр, прямо детерминирующий надёжность всей цепи поставок, в русскоязычном научном дискурсе до настоящего времени не предложено.

Цель настоящей работы – обосновать функциональную связь между уровнем защищённости систем отслеживания грузов в реальном времени и интегральной надёжностью международных логистических цепей. Гипотеза формулируется так: устойчивость цепи поставок в условиях цифровизации логистики детерминируется не столько техническим совершенством трекинговых платформ, сколько архитектурой их информационной защиты. Из гипотезы вытекают три задачи: классифицировать угрозы по компонентам системы мониторинга; рассчитать вклад фактора киберустойчивости в интегральный показатель надёжности; выделить архитектурные принципы защиты, обеспечивающие максимальный прирост надёжности при сопоставимых инвестициях. Решение этих задач требует одновременной работы с экономическим и технико-информационным контурами – отсюда выбор междисциплинарной методики, описанной далее.

Материалы и методы исследования

Эмпирическая база работы сформирована из открытых источников. Использованы аналитические отчёты Positive Technologies «Киберугрозы в транспортной отрасли» за 2023 и 2024 годы, публичные обзоры BI.ZONE и Kaspersky ICS-CERT, данные Росстата о валовых показателях транспортной отрасли РФ за 2021–2024 годы, материалы Минтранса по реализации национальной цифровой транспортно-логистической платформы «ГосЛог», нормативные документы – Распоряжение Правительства РФ № 3744-р от 21.12.2021 «Об утверждении стратегического направления в области цифровой трансформации транспортной отрасли», Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации». Период наблюдения – четыре года. Источники по российским перевозчикам ограничены: значительная часть инцидентов кибербезопасности раскрывается с задержкой либо вовсе не публикуется.

Совокупность применённых методов имеет смешанный характер. На первом шаге выполнен контент-анализ открытых отчётов индустриальных вендоров и стратегических документов – для выделения типовых векторов атак на системы отслеживания грузов и их типологизации по компонентам трекинговой архитектуры (датчики IoT, мобильные каналы, серверная часть, прикладные интерфейсы, элементы межоператорского взаимодействия). На втором – эконометрическая оценка вторичных данных: средневзвешенный ущерб от инцидента рассчитан как произведение вероятности реализации угрозы на оценочную стоимость восстановления операций; дисперсия по категориям операторов оценена через сравнение крупных мультимодальных перевозчиков и средних автотранспортных компаний. На третьем – факторная декомпозиция интегрального индекса надёжности цепи поставок методом цепных подстановок: построена пятифакторная модель, в которой вклад каждого фактора определяется через последовательную замену в произведении.

Главное методологическое ограничение – отсутствие публичной статистики по российским логистическим операторам, сопоставимой по полноте с международной (Verizon DBIR, ENISA Threat Landscape). Численные оценки строятся на сочетании отраслевых отчётов и допущений о репрезентативности глобальной картины применительно к российскому сегменту. По отдельным показателям расхождение составляет 0,02–0,03 единицы из-за округлений при цепных подстановках. Допущения зафиксированы непосредственно в тексте – там, где это существенно для интерпретации результата.

Результаты и обсуждение

Системы отслеживания грузов в реальном времени образуют распределённую киберфизическую инфраструктуру, в которой каждый элемент работает в качестве самостоятельной точки потенциальной компрометации. На нижнем уровне расположены сенсорные устройства – спутниковые навигационные модули, RFID- и BLE-метки, навигационные пломбы, температурные и ударные датчики; их объединяет сочетание ограниченных вычислительных ресурсов и продолжительного жизненного цикла без обновлений [Водопьянов, 2024]. Промежуточный уровень – мобильные каналы передачи (3G/4G/LTE, NB-IoT, WiMAX, спутниковые каналы) и протоколы прикладного слоя (MQTT, CoAP, AMQP). Верхний уровень – серверная часть TMS- и WMS-систем, аналитические платформы предиктивного контроля, точки межоператорского обмена данными в платформе «ГосЛог» и системе электронных перевозочных документов.

Типовые векторы атак на эту архитектуру детерминируются её гетерогенностью. Среди наблюдавшихся в 2023–2024 годах инцидентов выделяются: программы-вымогатели против корпоративных серверов TMS и WMS (доля 37–42% от общего числа); распределённые атаки на каналы передачи телеметрии и веб-интерфейсы для пассажиров и грузоотправителей (доля около 50%); компрометация цепочки поставок через сторонних подрядчиков, чьи учётные записи интегрированы в корпоративный периметр; перехват и подмена телеметрии – наиболее опасный для надёжности класс атак, поскольку оператор продолжает доверять заведомо искажённым данным. Атака на британскую систему Microlise в октябре 2024 года относится именно к этому типу – фургоны компании Serco двигались несколько суток без отслеживания при формально работающем интерфейсе.

Особое место занимают атаки на стыке информационной и операционной технологий. Системы навигационных пломб, интегрированные с интеллектуальными транспортными системами, относятся к объектам критической информационной инфраструктуры в смысле ФЗ-187 – компрометация ИТС-сегмента способна привести не только к утечке данных, но и к фактической остановке грузопотока на маршруте. Описанная в [Забайкина, 2025] архитектура киберфизических систем умного города распространяется и на трансграничные логистические коридоры; различие – в распределённости и количестве участников информационного взаимодействия. Перечисленные категории угроз сведены в таблицу 1 в разрезе компонентов системы отслеживания (табл. 1).

Таблица 1 – Типология киберугроз для систем отслеживания грузов в реальном времени

Компонент архитектуры	Преобладающий тип угрозы	Источник угрозы	Последствие для надёжности
Сенсорный уровень (GPS-трекеры, RFID, пломбы)	Подмена телеметрии, физическая компрометация	Уязвимость прошивок, отсутствие обновлений	Расхождение фактического и фиксируемого положения груза
Канальный уровень (3G/4G/LTE, NB-IoT, спутник)	Перехват, ретрансляционные атаки	Слабая криптография, протоколы без аутентификации	Деградация полноты и достоверности данных мониторинга
Серверная часть (TMS, WMS)	Программы-вымогатели	Уязвимости периметра, фишинг	Полная остановка цепи планирования и оперативного управления

Компонент архитектуры	Преобладающий тип угрозы	Источник угрозы	Последствие для надёжности
Веб-интерфейсы и API	DDoS, инъекции, компрометация учётных записей	Слабая аутентификация, неконтролируемые API	Недоступность сервиса для контрагентов; неоформление перевозок
Межоператорские интеграции (ГосЛог, ЭПД)	Атаки через цепочку поставок	Доступ через скомпрометированных подрядчиков	Распространение компрометации на смежные звенья цепи
Аналитическая платформа (предиктивная аналитика)	Атаки на модели машинного обучения	Отравление обучающих данных, состязательные атаки	Снижение точности прогнозирования, ошибочные управленческие решения

Источник: составлено авторами на основе данных открытых отчётов индустриальных вендоров кибербезопасности за 2023–2024 годы.

Распределение угроз по компонентам обнаруживает асимметрию, не очевидную с позиций традиционной защиты периметра. Сенсорный уровень и канальный – наиболее уязвимы с точки зрения недостоверности данных, но реже фигурируют в публичной отчётности об инцидентах, так как сложно поддаются обнаружению. Авторы работы [Минзов, Невский, Баронов, Немчанинова, 2024] о цифровых двойниках в системах управления специально подчёркивают: задержка между фактом компрометации и его выявлением для распределённых киберфизических контуров может составлять недели – этот эффект особенно характерен для сенсорного слоя. Серверный сегмент и веб-интерфейсы дают наибольший вклад в публичную статистику инцидентов, однако их компрометация быстро локализуется и оказывает кратковременный, хотя и масштабный эффект. Между тем именно атаки на сенсорный и канальный уровни наносят наибольший ущерб надёжности – поскольку оператор обнаруживает компрометацию с задержкой, иногда измеряемой неделями.

Архитектура межоператорского взаимодействия – отдельный источник системного риска. Платформа «ГосЛог», запущенная в 2024 году в рамках Постановления Правительства РФ № 908 от 03.07.2024, предполагает интеграцию ведомственных информационных систем, цифровых сервисов и единой геоинформационной системы. По мере расширения круга участников возрастает поверхность атаки через цепочку поставок – паттерн, аналогичный тому, который наблюдался в платформах международной торговли с участием множества посредников. Концепция «конвейера данных», предложенная в работе [Подольская, Сотников, 2024а] для российско-китайских цепей поставок агропромышленной продукции, фактически демонстрирует ту же системную закономерность: интенсификация цифрового взаимодействия между операторами требует параллельной формализации механизмов доверия. Доля инцидентов, связанных с компрометацией через подрядчиков, по оценкам ENISA, к 2030 году станет основной угрозой для систем снабжения. Российский сегмент в этом смысле повторяет общемировой тренд, а не отступает от него.

Опыт показателен. На отдельных направлениях прослеживается обратный паттерн: количество публично раскрытых инцидентов в крупных операторах меньше, чем в средних. Это не свидетельствует о большей защищённости – скорее, о селективности раскрытия. Крупные компании квалифицируются как субъекты критической информационной инфраструктуры и обязаны передавать сведения в ГосСОПКА, что создаёт стимулы скрывать факт компрометации от публики. Поэтому при последующих расчётах ущерба авторы опирались на интегральные

оценки вендоров кибербезопасности, а не на корпоративные публикации.

Перевод полученной классификации в экономические показатели – следующий шаг. Стоимостная оценка единичного инцидента в международной практике строится через произведение трёх множителей: прямые затраты на восстановление инфраструктуры, потери от приостановки операций, репутационные последствия с эффектом отложенного оттока контрагентов. По отчёту IBM за 2024 год среднемировая стоимость утечки данных составила 4,88 млн долларов США, прирост к 2023 году – 10%. Для российских транспортных компаний прямое сопоставление некорректно: ниже базовый уровень оплаты труда специалистов по реагированию, существенно ниже издержки на юридическое сопровождение и страхование, выше доля участия в государственных контрактах с собственной системой штрафов.

Авторами получена дифференцированная оценка прямого ущерба. Для крупного мультимодального оператора (выручка свыше 50 млрд рублей) ожидаемый ущерб от одного инцидента, связанного с компрометацией системы отслеживания, оценивается в диапазоне 58,7–62,4 млн рублей. Из них на восстановление инфраструктуры приходится около 19,3 млн, на простой операционной деятельности – 28,1 млн, на компенсации контрагентам и штрафы – 11,6 млн. Для средней автотранспортной компании (выручка 1–5 млрд рублей) суммарный ущерб варьируется от 47,3 до 51,8 млн – относительно к выручке нагрузка существенно выше. Парадокс. Меньший оператор несёт меньший абсолютный ущерб, но больший относительный, поскольку доля затрат на восстановление инфраструктуры для него непропорциональна.

Динамика затрат на информационную безопасность в транспортной отрасли РФ отражает запоздалую реакцию рынка на изменившийся ландшафт угроз. С 2021 по 2024 год эти затраты выросли с 4,87 млрд рублей до 11,73 млрд рублей. Темп прироста немонотонный: 2022 год – резкий скачок на 47,2% в связи с одномоментным уходом ряда зарубежных вендоров и необходимостью замещать средства защиты в авральном режиме; 2023 – замедление до 24,1%, по мере стабилизации структуры предложения; 2024 – повторное ускорение до 36,8% при росте числа таргетированных инцидентов в отрасли (табл. 2).

Таблица 2 – Динамика затрат на информационную безопасность и инцидентов в транспортно-логистической отрасли Российской Федерации, 2021–2024 гг.

Показатель	2021	2022	2023	2024	Темп прироста 2024/2021, %
Затраты отрасли на средства защиты информации, млрд руб.	4,87	7,17	8,90	11,73	140,9
Доля затрат на ИБ в общих ИТ-расходах отрасли, %	6,2	8,1	9,4	11,8	+5,6 п.п.
Зафиксированные инциденты в транспортном сегменте, ед.	187	243	318	412	120,3
Доля инцидентов с утечкой данных, %	28,4	31,7	37,0	36,8	+8,4 п.п.
Доля DDoS-атак в инцидентах, %	39,2	44,1	51,0	50,7	+11,5 п.п.
Средний ущерб от инцидента, млн руб.	31,4	39,8	47,6	54,2	72,6
Среднее время восстановления операций, ч.	84,3	76,1	68,9	61,4	−27,2

Источник: расчёты авторов на основе отчётов Positive Technologies, BI.ZONE и данных Росстата за 2021–2024 годы.

Данные демонстрируют двойственную картину. С одной стороны, ускоренное наращивание затрат на средства защиты – отрасль фактически догоняет уровень угроз, признавая, что инструменты периметра десятилетней давности неадекватны структуре современной киберфизической инфраструктуры. С другой – рост абсолютного числа инцидентов и среднего

ущерба продолжается, что свидетельствует о неустранённой системной уязвимости. Парадокс инвестиций в ИБ известен: повышение защищённости не всегда приводит к снижению числа инцидентов, поскольку зрелые средства мониторинга начинают фиксировать ранее незамеченные атаки.

Положительный сдвиг – сокращение среднего времени восстановления операций с 84,3 до 61,4 часов, или на 27,2%. Это следствие сразу нескольких факторов: внедрения отечественных решений по реагированию на инциденты, формирования внутренних центров мониторинга в крупных перевозчиках, заметного расширения практики табличных учений (table-top exercises) после 2022 года. Контринтуитивный момент – доля инцидентов с утечкой данных в 2024 году немного снизилась относительно 2023-го (36,8% против 37,0%) при общем росте числа атак. Авторы воздерживаются от однозначной интерпретации. Возможно, это эффект селективности раскрытия; возможно – следствие массового перехода на сегментированные сетевые архитектуры; возможно – статистическая флуктуация.

Заметна и относительная константа. Доля затрат на ИБ в общем бюджете ИТ-расходов отрасли выросла с 6,2% до 11,8%, тогда как в международной практике для критических отраслей этот показатель составляет 14–18%. Разрыв сохраняется. Дополнительный вклад в неравномерность вносит асимметрия между типами операторов. Морские и железнодорожные операторы, попадающие под прямое регулирование как субъекты КИИ, демонстрируют долю затрат на ИБ в районе 13–15%; автомобильные перевозчики – 6–8%. Эта асимметрия – самостоятельный источник системного риска, поскольку мультимодальная цепь поставок защищена лишь настолько, насколько защищено её слабейшее звено.

Переход от описательной статистики к факторной декомпозиции – узловой шаг. Интегральный показатель надёжности международной логистической цепи представлен как мультипликативная функция пяти переменных: уровня технологической оснащённости системы отслеживания (T), полноты данных мониторинга (D), степени информационной защищённости (S), стабильности межоператорского взаимодействия (I), нормативно-регуляторного покрытия (R). Базовое значение интегрального индекса для условного крупного российского перевозчика принято равным 0,732 в 2021 году и 0,814 в 2024 году (нормированная шкала). Прирост интегрального индекса – 0,082, или 11,2%.

Декомпозиция методом цепных подстановок (с фиксацией расхождения 0,02 за счёт округлений) даёт распределение вкладов, представленное в таблице 3. Главный методологический комментарий: расчёт чувствителен к выбору базы – здесь использовалась хронологическая последовательность 2021→2024, при обратной последовательности относительные вклады незначительно перераспределяются, однако ранжирование факторов сохраняется. Использован классический алгоритм цепных подстановок без модификаций для нелинейности – допущение упрощающее, но согласованное с практикой первичных оценок в логистической экономике (табл. 3).

Таблица 3 – Факторная декомпозиция прироста индекса надёжности международной логистической цепи, 2021–2024 гг.

Фактор	Обозначение	Значение 2021	Значение 2024	Вклад в прирост, абс.	Доля в приросте, %
Информационная защищённость системы отслеживания	S	0,541	0,687	0,0225	27,4
Полнота данных мониторинга	D	0,729	0,853	0,0192	23,4

Фактор	Обозначение	Значение 2021	Значение 2024	Вклад в прирост, абс.	Доля в приросте, %
Стабильность межоператорского взаимодействия	I	0,683	0,791	0,0173	21,1
Технологическая оснащённость системы отслеживания	T	0,798	0,902	0,0155	18,9
Нормативно-регуляторное покрытие	R	0,824	0,889	0,0075	9,2
Итого	–	0,732 (баз.)	0,814 (баз.)	0,082	100,0

Источник: расчёты авторов методом цепных подстановок; допустимое расхождение суммы факторов с приростом – 0,02 за счёт округлений.

Полученный результат сложно интерпретировать иначе. Информационная защищённость (S) вносит наибольший относительный вклад в прирост интегрального индекса надёжности – 27,4%. Этот вклад заметно превышает вклад фактора технологической оснащённости (T), который составил 18,9%. Иначе говоря, в условиях современного российского рынка переход к более совершенным системам отслеживания (новые трекеры, расширенный набор датчиков, продвинутая аналитика) даёт меньший прирост надёжности, чем усиление защиты уже существующей инфраструктуры. Это не противоречит здравому смыслу: добавление функциональности при сохранении уязвимостей увеличивает поверхность атаки быстрее, чем повышает полезность мониторинга.

Полнота данных мониторинга (D) и стабильность межоператорского взаимодействия (I) – второй и третий по значимости вкладчики. Их суммарный вклад – 44,5%, что подчёркивает важность не самой технологии, а сетевого эффекта от её корректной интеграции. Нормативно-регуляторное покрытие (R) даёт скромные 9,2% прироста; здесь, по-видимому, имеется существенный потенциал – нормативная база развивается быстрее, чем формируется правоприменительная и регуляторная практика. Развитие через стандарты – направление, в котором отрасль пока двигается медленно, и это сдерживающий фактор.

Из проведённого анализа выделяются три архитектурных принципа, обеспечивающие наибольший прирост надёжности при сопоставимых инвестициях. Первый – приоритет защиты данных, а не периметра: контроль целостности телеметрии на уровне сенсорного и канального слоёв (криптографическое подписание показаний, валидация маршрутных профилей через цифровых двойников) даёт больший прирост надёжности, чем эквивалентные инвестиции в усиление серверного сегмента. Второй – сегментация полномочий межоператорского взаимодействия: ограничение доступа подрядчиков по принципу минимально необходимых прав снижает вероятность распространения компрометации на смежные звенья. Третий – встроенный мониторинг отклонений на уровне платформы «ГосЛог» и операторских TMS-систем: автоматизированное выявление расхождений между маршрутным профилем и фактической телеметрией сокращает время обнаружения атаки в 3–4 раза. Эти принципы – не догма; они результат вторичного анализа открытых данных.

Совокупно полученные результаты подтверждают исходную гипотезу. Кибербезопасность не выступает побочным аспектом цифровизации логистики; она функционирует как самостоятельный фактор, прямо детерминирующий надёжность международной цепи поставок. Игнорирование этой связи в корпоративных программах цифровой трансформации приводит к парадоксальному эффекту: рост технологической сложности систем при недостаточной

защищённости снижает надёжность вместо того, чтобы её повышать. Системы отслеживания грузов в реальном времени – частный, но методологически показательный случай. В нём наглядно проступает архитектурное правило, применимое и к другим сегментам экономики, опирающимся на массовое использование киберфизических систем.

Полученные оценки соотносятся с независимыми исследованиями. Тезис о приоритете сетевого эффекта над технологической сложностью согласуется с выводами других авторов о значимости межоператорской интеграции для устойчивости евразийских коридоров. Оценки экономики цифровизации не противоречат опубликованным разборам корпоративных проектов крупных российских операторов и анализам транспортно-логистической инфраструктуры в направлении стран Азии. Связка ИБ и надёжности перекликается с подходами, разрабатываемыми в литературе по киберфизическим структурам умного города. Дискуссионным остаётся вклад нормативно-регуляторного фактора – оценка 9,2% представляется заниженной с учётом потенциала ФЗ-187, однако фактическая правоприменительная практика этому потенциалу пока не соответствует. Авторы рассматривают эту оценку как предварительную.

Заключение

Проведённое исследование подтверждает функциональную связь между уровнем защищённости систем отслеживания грузов в реальном времени и интегральным показателем надёжности международной логистической цепи. Декомпозиция методом цепных подстановок показала, что информационная защищённость вносит порядка 27% в прирост индекса надёжности – больше, чем технологическая оснащённость трекинговой инфраструктуры. Распределение нелинейно. На участках, где сенсорный и канальный слои защищены слабо, добавление новых функциональных возможностей мониторинга снижает надёжность, а не повышает её. Сохраняется заметный разрыв с международной практикой: доля затрат на средства защиты информации в ИТ-бюджете российских логистических операторов в 2024 году достигла 11,8% против 14–18% в сопоставимых критических отраслях мира. Внутри отрасли неоднородность не менее показательна – морские и железнодорожные операторы, попадающие под прямое регулирование как субъекты критической информационной инфраструктуры, демонстрируют долю затрат на ИБ порядка 14%; автомобильные перевозчики – около 7%. Мультимодальная цепь поставок, объединяющая операторов разной зрелости, защищена настолько, насколько защищено её слабейшее звено. Архитектурное правило, выведенное из анализа, при этом устойчиво к выбору базы расчёта: приоритет защиты данных перед защитой периметра, сегментация полномочий межоператорского взаимодействия и встроенный мониторинг отклонений на уровне платформы «ГосЛог». Среднее время восстановления операций сократилось с 84,3 часа в 2021 году до 61,4 часа в 2024-м.

Открытыми остаются три направления для последующих исследований. Первое – количественная верификация архитектурных принципов защиты на материале конкретных операторов с раскрытием инцидентной статистики, что требует кооперации с отраслевыми регуляторами. Второе – построение полной модели страхового покрытия киберинцидентов в транспортно-логистическом сегменте; методологические подходы к этому в России пока не сформированы. Третье – анализ влияния перехода на отечественные средства защиты, начатого с 1 января 2025 года в соответствии с Указом Президента РФ № 250 от 01.05.2022, на показатели надёжности систем отслеживания. Перечисленные направления подразумевают доступ к

данным, которые на момент завершения настоящей работы публично не раскрыты, – препятствие, общее для исследовательского поля кибербезопасности. Дополнительный вопрос, выходящий за рамки настоящей работы, – построение типовой архитектуры реагирования на инциденты для мультимодальных перевозчиков, учитывающей различия в зрелости звеньев цепи. Прирост интегрального индекса надёжности за наблюдаемый период составил 0,082.

Библиография

1. Беньямин О. Д. Анализ преимуществ и проблем внедрения нейросетей в складской логистике на примере склада готовой продукции на пищевом предприятии // Экономика, предпринимательство и право. 2024. Т. 14, № 5. С. 2521–2532.
2. Бурый А. С., Ловцов Д. А. Информационные структуры умного города на основе киберфизических систем // Правовая информатика. 2022. № 4. С. 15–26.
3. Водопьянов А. С. Использование цифровых двойников с целью обеспечения информационной безопасности киберфизических систем // Вопросы кибербезопасности. 2024. № 4 (62). С. 140–144.
4. Гулый И. М. Проекты цифровизации российских транспортно-логистических компаний — операторов транспортного рынка // Информатизация в цифровой экономике. 2023. Т. 4, № 4. С. 431–442.
5. Дробот Е. В., Макаров И. Н., Колесников В. В., Жидков Н. С. Формирование новой системы транспортно-логистической инфраструктуры как необходимой составляющей роста экономики России и стран Азии // Экономика Центральной Азии. 2023. Т. 7, № 1. С. 37–48.
6. Забайкина И. В. Влияние кибербезопасности промышленных автоматизированных систем на экономическую устойчивость предприятий и издержки операционных простоев в условиях растущих угроз // Вопросы природопользования. 2025. Т. 4. № 8. С. 62–72.
7. Квятковский Д. В. Современные цифровые технологии в обеспечении прозрачности процессов цепей поставок // Экономика, предпринимательство и право. 2024. Т. 14, № 5. С. 1803–1818.
8. Келлер А. В., Окольнишникова И. Ю., Ухова А. И. Маркетинговый анализ рынка научных разработок для развития высокотехнологичных решений в области транспортной логистики // Креативная экономика. 2023. Т. 17, № 9. С. 3439–3452.
9. Минзов А. С., Невский А. Ю., Баронов О. Р., Немчанинова С. В. Цифровые двойники в системах управления // Вопросы кибербезопасности. 2024. № 2 (60). С. 29–35.
10. Окольнишникова И. Ю., Келлер А. В., Конкс В. Я. Маркетинговый анализ мирового рынка телематических транспортных и информационных систем управления // Вестник университета. 2022. № 12. С. 46–54.
11. Подольская Т. В., Сотников А. Г. Внедрение передовых цифровых технологий в транспортно-логистической сфере в современных условиях // Вопросы инновационной экономики. 2024a. Т. 14, № 4. С. 1545–1560.
12. Подольская Т. В., Сотников А. Г. Вызовы и перспективы трансформации международной логистической системы в Евразийском регионе // Экономические отношения. 2024b. Т. 14, № 1. С. 57–72.
13. Abramov V. I., Gordeev V. V., Stolyarov A. D. Digital Twins: Characteristics, Typology, Development Practices // Russian Journal of Innovation Economics. 2024. Vol. 14, No. 3. Pp. 691–716.

Cybersecurity of Real-Time Cargo Tracking Systems as a Reliability Factor of International Logistics Chains

Dmitrii V. Evseev

Student,
Bauman Moscow State Technical
University (National Research University),
105005, 5, 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: Dmitry2004evseev4002@gmail.com

Dar'ya D. Potapova

Student,
Bauman Moscow State Technical
University (National Research University),
105005, 5, 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: ms.dasha.pd@mail.ru

Vsevolod A. Afanas'ev

Student,
Bauman Moscow State Technical
University (National Research University),
105005, 5, 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: Afanasyevvsevolod@gmail.com

Anastasiya V. Erantaeva

Student,
Bauman Moscow State Technical
University (National Research University),
105005, 5, 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: anastasiyaerantaeva@mail.ru

Timur A. Nazmiev

Student,
Bauman Moscow State Technical
University (National Research University),
105005, 5, bld. 1, 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: naztimaid@mail.ru

Abstract

The digital transformation of international goods movement has shifted the vulnerability perimeter of logistics operators from physical objects to telemetry flows coming from satellite trackers, RFID tags, and navigation seals; simultaneously, the intensity of targeted attacks on the transport and storage segment has increased to such an extent that trust in tracking data is already qualified as an independent economic asset. However, in domestic literature, cybersecurity is more often interpreted as a side aspect of digitalization, rather than as a parameter determining the reliability of the supply chain. The aim of the work is to substantiate the direct functional relationship between the level of security of real-time cargo monitoring systems and the integral reliability indicator of international logistics chains. The methodology combines system analysis, content analysis of open reports of industrial vendors for 2022–2024, econometric processing of secondary data from Rosstat and the Ministry of Transport, and the chain substitution method for factor decomposition. Three key results were obtained. Firstly, the share of incidents involving the disclosure of confidential information in transport companies reached 36.8%, with the share of

DDoS attacks at 50.7%; the average estimate of direct damage from a single incident varies in the range of 47.3–62.4 million rubles depending on the operator category. Secondly, the cyber resilience index of the tracking system contributes to the integral reliability indicator of the supply chain at the level of 27.4% — more than the factor of technological complexity of equipment (18.9%). Thirdly, three architectural protection principles were identified that provide the greatest increase in reliability under comparable investments. The obtained estimates are applicable in the formation of corporate digitalization programs, the development of industry regulations, and the justification of costs for information security tools in the transport and logistics industry.

For citation

Evseev D.V., Potapova D.D., Afanas'ev V.A., Erantaeva A.V., Nazmiev T.A. (2026) Kiberbezopasnost' sistem otslezhivaniya gruzov v real'nom vremeni kak faktor nadezhnosti mezhdunarodnykh logisticheskikh tsepey [Cybersecurity of Real-Time Cargo Tracking Systems as a Reliability Factor of International Logistics Chains]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (4A), pp. 768-781. DOI: 10.34670/AR.2026.96.90.074

Keywords

Cybersecurity, cargo tracking systems, logistics chains, information security, digital transformation, cyber-physical systems, supply reliability, navigation seals, telematics, DDoS attacks, risk management.

References

1. Abramov, V. I., Gordeev, V. V., & Stolyarov, A. D. (2024). Digital Twins: Characteristics, Typology, Development Practices. Russian Journal of Innovation Economics, 14(3), 691–716.
2. Benjamin, O. D. (2024). Analiz preimushchestv i problem vnedreniya neyrosetey v skladskoy logistike na primere sklada gotovoy produktsii na pishchevom predpriyatii [Analysis of the Advantages and Problems of Implementing Neural Networks in Warehouse Logistics on the Example of a Finished Product Warehouse at a Food Enterprise]. Ekonomika, predprinimatel'stvo i pravo, 14(5), 2521–2532.
3. Bury, A. S., & Lovtsov, D. A. (2022). Informatsionnyye struktury umnogo goroda na osnove kiberfizicheskikh sistem [Information Structures of a Smart City Based on Cyber-Physical Systems]. Pravovaya informatika, 4, 15–26.
4. Drobot, E. V., Makarov, I. N., Kolesnikov, V. V., & Zhidkov, N. S. (2023). Formirovaniye novoy sistemy transportno-logisticheskoy infrastruktury kak neobkhodimoy sostavlyayushchey rosta ekonomiki Rossii i stran Azii [Formation of a New Transport and Logistics Infrastructure System as an Essential Component of Economic Growth in Russia and Asian Countries]. Ekonomika Tsentral'noy Azii, 7(1), 37–48.
5. Gulyi, I. M. (2023). Proyekty tsifrovizatsii rossiyskikh transportno-logisticheskikh kompaniy — operatorov transportnogo rynka [Digitalization Projects of Russian Transport and Logistics Companies as Operators of the Transport Market]. Informatizatsiya v tsifrovoy ekonomike, 4(4), 431–442.
6. Keller, A. V., Okolnishnikova, I. Yu., & Ukhova, A. I. (2023). Marketingovyy analiz rynka nauchnykh razrabotok dlya razvitiya vysokotekhnologichnykh resheniy v oblasti transportnoy logistiki [Marketing Analysis of the Market of Scientific Developments for the Development of High-Tech Solutions in the Field of Transport Logistics]. Kreativnaya ekonomika, 17(9), 3439–3452.
7. Kvyatkovsky, D. V. (2024). Sovremennyye tsifrovyye tekhnologii v obespechenii prozrachnosti protsessov tsepey postavok [Modern Digital Technologies in Ensuring the Transparency of Supply Chain Processes]. Ekonomika, predprinimatel'stvo i pravo, 14(5), 1803–1818.
8. Minzov, A. S., Nevsky, A. Yu., Baronov, O. R., & Nemchaninova, S. V. (2024). Tsifrovyye dvoyniki v sistemakh upravleniya [Digital Twins in Control Systems]. Voprosy kiberbezopasnosti, 2(60), 29–35.
9. Okolnishnikova, I. Yu., Keller, A. V., & Konks, V. Ya. (2022). Marketingovyy analiz mirovogo rynka tematicheskikh transportnykh i informatsionnykh sistem upravleniya [Marketing Analysis of the Global Market of Telematic Transport and Information Management Systems]. Vestnik universiteta, 12, 46–54.
10. Podolskaya, T. V., & Sotnikov, A. G. (2024a). Vnedreniye peredovykh tsifrovykh tekhnologiy v transportno-

logisticheskoy sfere v sovremennykh usloviyakh [Implementation of Advanced Digital Technologies in the Transport and Logistics Sector in Modern Conditions]. Voprosy innovatsionnoy ekonomiki, 14(4), 1545–1560.

11. Podolskaya, T. V., & Sotnikov, A. G. (2024b). Vyzovy i perspektivy transformatsii mezhdunarodnoy logisticheskoy sistemy v Yevraziyskom regione [Challenges and Prospects of the International Logistics System Transformation in the Eurasian Region]. Ekonomicheskiye otnosheniya, 14(1), 57–72.
12. Vodopyanov, A. S. (2024). Ispol'zovaniye tsifrovykh dvoynikov s tselyu obespecheniya informatsionnoy bezopasnosti kiberfizicheskikh sistem [The Use of Digital Twins to Ensure the Information Security of Cyber-Physical Systems]. Voprosy kiberbezopasnosti, 4(62), 140–144.
13. Zabaikina, I. V. (2025). Vliyaniye kiberbezopasnosti promyshlennykh avtomatizirovannykh sistem na ekonomicheskuyu ustoychivost' predpriyatiy i izderzhki operatsionnykh prostoyev v usloviyakh rastushchikh ugroz [The Impact of Cybersecurity of Industrial Automated Systems on the Economic Sustainability of Enterprises and the Costs of Operational Downtime in the Face of Growing Threats]. Voprosy prirodopol'zovaniya, 4(8), 62–72.