**УДК 004.056:656:334.722**

***Райлян Денис Анатольевич,***
***Студент,***
***Министерство транспорта Российской Федерации. ФГАОУ ВО «Российский университет транспорта», Москва***

# ВЛИЯНИЕ ЦИФРОВИЗАЦИИ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЙ

*Аннотация. Актуальность исследования продиктована фундаментальным противоречием — с одной стороны, цифровизация транспортной инфраструктуры открывает малым и средним предприятиям доступ к глобальным логистическим цепочкам, а с другой — делает их весьма уязвимым звеном в асимметричной среде киберугроз. Цель в статье — провести анализ этого влияния, систематизировать специфические угрозы, сформулировать практико-ориентированные рекомендации для их смягчения. На основе методов системного и сравнительного анализа, а также классификации, автор приходит к выводу, что традиционные корпоративные модели информационной безопасности нерелевантны для малого и среднего бизнеса. Вместо этого рационален переход к новой парадигме, которая базируется на потреблении защиты как сервиса и формировании поддерживающей отраслевой экосистемы.*

*Ключевые слова: информационная безопасность, кибербезопасность, малые и средние предприятия, транспортная инфраструктура, цифровизация, цепочка поставок*

***Railyan Denis Anatolyevich,***
***Student,***
***Ministry of Transport of the Russian Federation,***
***Federal State Autonomous Educational Institution of Higher Education***
***"Russian University of Transport", Moscow, Russia***

# THE IMPACT OF TRANSPORT INFRASTRUCTURE DIGITALIZATION ON THE INFORMATION SECURITY OF SMALL AND MEDIUM-SIZED ENTERPRISES

*Abstract. The relevance of this study arises from a fundamental contradiction: on the one hand, the digitalization of transport infrastructure provides small and medium-sized enterprises (SMEs) with access to global logistics chains; on the other hand, it renders them a highly vulnerable link in an asymmetric cyberthreat environment. The aim of the article is to analyze this impact, systematize specific threats, and formulate practical recommendations for their mitigation. Using methods of systemic and comparative analysis as well as classification, the author concludes that traditional corporate information security models are largely irrelevant for SMEs. Instead, a shift toward a new paradigm is proposed—one based on the consumption of security as a service and the formation of a supportive sectoral ecosystem.*

*Keywords: information security, cybersecurity, small and medium-sized enterprises, transport infrastructure, digitalization, supply chain*

**Введение.** Современное экономическое развитие сопровождается процессами повсеместной цифровой трансформации, которые фундаментально изменяют операционные модели, а также конкурентную

среду в ключевых отраслях. Транспортный комплекс, будучи системообразующей артерией национальной и мировой экономики, находится в авангарде этих преобразований. Внедрение технологий Интернета вещей (IoT), анализа больших данных (Big Data), искусственного интеллекта (ИИ), digital-платформ в управление транспортной инфраструктурой призвано весомо повысить её эффективность, скорость функционирования. Создание интеллектуальных транспортных систем, переход на электронный документооборот в сочетании с развитием автономных логистических цепочек открывают многообещающие перспективы для оптимизации грузовых и пассажирских перевозок. В описываемом контексте малые и средние предприятия (МСП), которые составляют значительную долю в секторе транспортно-логистических услуг, получают беспрецедентные возможности для роста и интеграции в глобальные цепочки поставок. Между тем, интенсификация цифровизации имплицитно порождает новую, многомерную реальность рисков, сопряжённых с обеспечением информационной безопасности.

**Методы исследования**. В ходе подготовки статьи применены системный и сравнительный анализ, контент-оценка научных публикаций, классификация, обработка статистических сводок, обобщение.

**Результаты и обсуждение**. По сведением Минэкономразвития, количество малых и средних предприятий (МСП) в России по итогам I квартала 2025 года превысило 6,7 миллиона. Показатель стал рекордным с начала ведения специального реестра соответствующих субъектов в 2016 году[1]. По данным Минтранса, в 2023-2024 годах на цифровизацию транспорта в РФ выделено 45 млрд руб.[2].

[1] В России количество малых и средних предприятий превысило рекордные 6,7 млн // URL: https://finance.mail.ru/article/v-rossii-kolichestvo-malyh-i-srednih-predpriyatij-prevysilo-rekordnye-67-mln-65926182/ (дата обращения: 26.10.2025).

[2] Квашенкина О. Уровень цифровизации транспортно-логистической отрасли в РФ отстает от финсектора, ритейла и телекоммуникаций // URL: https://www.rzd-partner.ru/logistics/opinions/uroven-tsifrovizatsii-transportno-logisticheskoy-otrasli-v-rf-otstaet-ot-finsektora-riteyla-i-teleko/ (дата обращения: 26.10.2025).

Цифровые преобразования транспортной отрасли сказываются на формировании сложной многоуровневой экосистемы, в которой МСП становятся зависимым звеном. Она включает в себя государственные и коммерческие digital-платформы, системы управления дорожным движением, электронные торговые площадки для фрахта, высокоавтоматизированные транспортные средства, элементы «умной» инфраструктуры[1]. Малые и средние компании интегрируются в данную среду, применяя облачные сервисы в целях управления автопарком, площадки для поиска заказов, системы электронного документооборота, навигационные решения. Подобная интеграция, с одной стороны, сопряжена со снижением операционных издержек и барьеров для входа на рынок, а с другой — переносит риски, связанные с безопасностью централизованной инфраструктуры, на всех её участников[2] (таблица 1).

Таблица 1 – Классификация угроз информационной безопасности для МСП в цифровой транспортной экосистеме (составлено автором)

| Тип угрозы | Описание и примеры | Потенциальные последствия для МСП |
|---|---|---|
| Инфраструктурные | DDoS-атаки на логистические платформы, взлом систем бронирования, компрометация облачных сервисов управления транспортом | Прямые финансовые убытки из-за простоя, срыв сроков доставки, репутационный ущерб, утрата контроля над операционной деятельностью |
| Целевые атаки на МСП | Фишинговые рассылки с вредоносными вложениями, действия программ-вымогателей (шифровальщиков), социальная инженерия | Блокировка или уничтожение критически важных данных (базы клиентов, финансовая отчетность), хищение денежных средств, шантаж |
| Атаки на цепочку поставок | Компрометация IT-поставщика, взлом систем партнера с целью | Утечка конфиденциальной коммерческой информации |

[1] Щелканова М. А., Романенко Е. В. Развитие субъектов малого и среднего предпринимательства на транспорте в условиях формирования цифровой экономики // Архитектурно-строительный и дорожно-транспортный комплексы: проблемы, перспективы, инновации. Сборник материалов V Международной научно-практической конференции. – Омск: 2021. – С. 398.

[2] Козаченко Н. Е. О понятии информационной безопасности в транспортной сфере // Транспортное право и безопасность. – 2024. – № 2 (50). – С. 77.

| | | |
|---|---|---|
| | получения доступа к целевой компании, задействование зараженной инфраструктуры МСП для последующих атакующих шагов | и персональных данных, разрыв деловых отношений |
| Вызовы «умного» транспорта | Вмешательство в работу бортовых систем автомобиля, перехват управления беспилотными средствами, манипуляции с данными датчиков IoT (например, температуры рефрижератора) | Физическое повреждение либо утрата груза, создание аварийных ситуаций, угон транспортных средств, прямая угроза жизни и здоровью |

Уязвимость МСП в цифровой транспортной среде обусловлена как внешними угрозами, так и комплексом внутренних факторов, которые отличают их от крупных корпораций (таблица 2). Основной лимитирующей детерминантой служат ограниченные ресурсы[1]. Малый бизнес не может позволить себе содержание штата специалистов по информационной безопасности, внедрение дорогостоящих комплексных систем защиты (SIEM или SOC). Инвестиции в кибербезопасность зачастую воспринимаются в качестве второстепенных расходов, а не как необходимое условие устойчивости бизнеса[2].

Таблица 2 – Сравнительный анализ факторов уязвимости МСП и крупных предприятий в транспортной отрасли

| Фактор | Проявление у МСП | Влияние для крупных предприятий |
|---|---|---|
| Финансовые ресурсы | Острый дефицит бюджета на закупку средств защиты информации (СЗИ) и оплату услуг экспертов | Наличие выделенных бюджетов, возможность инвестировать в передовые технологии, страхование киберрисков |
| Кадры | Отсутствие штатных специалистов по ИБ, функции защиты информации выполняются IT-специалистом широкого | Наличие департаментов ИБ, центров мониторинга, специалистов по анализу угроз и реагированию на инциденты |

[1] Малышев М. И., Филиппова Н. А. Уровень цифровизации российского транспорта // Информационные технологии и инновации на транспорте. Материалы VI Международной научно-практической конференции. – Орел: 2020. – С. 66.

[2] Борзенко К. В. Вопросы цифровой трансформации в транспортной отрасли: актуализация развития спроса на цифровые технологии // Вестник Ростовского государственного экономического университета (РИНХ). – 2023. – Т. 28. – № 1. – С. 14.

| | | |
|---|---|---|
| | профиля или не реализуются вовсе | |
| Уровень компетенций | Низкая осведомленность персонала и руководства об актуальных киберугрозах и методах защиты, игнорирование кибергигиены | Регулярное обучение сотрудников, проведение тренировок по отражению атак, наличие формализованных политик безопасности |
| Отношения с поставщиками | Критическая зависимость от безопасности внешних цифровых платформ и облачных сервисов без возможности их аудита | Возможность предъявлять требования к безопасности поставщиков, проводить их аудит, разрабатывать собственные программные решения |
| Гибкость, скорость реакции | Потенциально более быстрая адаптация к новым политикам, но медленное восстановление после инцидента из-за отсутствия планов и резервных копий | Бюрократизированные процессы внедрения, но наличие планов непрерывности бизнеса и аварийного восстановления для смягчения последствий |

В целях разрешения проблемы уязвимости МСП в цифровой транспортной среде требуется системный, многоуровневый подход, с учётом которого фокус смещается с попыток построить автономную защиту в каждой компании на формирование доступной экосистемы безопасности. На уровне самих хозяйствующих субъектов предлагается перейти к модели «безопасность как услуга», что позволит получать профессиональную защиту по подписке, дополнив это обязательным внедрением базовой кибергигиены (двухфакторная аутентификация, регулярное резервное копирование данных). На отраслевом и государственном уровнях эти меры рекомендуется подкреплять разработкой адаптированных для малого бизнеса стандартов безопасности, созданием программ субсидирования для снижения финансовых барьеров, законодательным закреплением ответственности операторов digital-платформ за защищенность их инфраструктуры, что в совокупности создаст эластичную и устойчивую к угрозам среду для всех участников рынка.

**Заключение**. С помощью проведенного анализа показывается, что цифровизация транспортной инфраструктуры, являясь мощным

«драйвером» экономического роста, одновременно формирует асимметричное поле угроз для малых и средних компаний. Интегрируясь в новую digital-реальность, МСП наследуют все её риски, не обладая при этом достаточными ресурсами и компетенциями для их действенного парирования. Их информационная безопасность становится производной от защищенности глобальных платформ, действий поставщиков и т. д., что делает их положение достаточно неустойчивым.

Основной вывод в рамках данного исследования заключается в том, что традиционные подходы к корпоративной кибербезопасности, которые рассчитаны на крупные организации, неприменимы для МСП в транспортной отрасли. Требуется принципиально иная модель, базирующаяся на аутсорсинге функций защиты и создании поддерживающей отраслевой и государственной экосистемы.

Дальнейшие изыскания в данной области предлагается направить на проведение эмпирических оценок экономического ущерба от киберинцидентов для МСП в транспортном секторе России, а также на разработку количественных моделей для оценки эффективности различных мер поддержки и их влияния на конкурентоспособность малого бизнеса.

**Использованные источники:**

1. Борзенко К. В. Вопросы цифровой трансформации в транспортной отрасли: актуализация развития спроса на цифровые технологии // Вестник Ростовского государственного экономического университета (РИНХ). – 2023. – Т. 28. – № 1. – С. 10-16.

2. В России количество малых и средних предприятий превысило рекордные 6,7 млн // URL: https://finance.mail.ru/article/v-rossii-kolichestvo-

malyh-i-srednih-predpriyatij-prevysilo-rekordnye-67-mln-65926182/ (дата обращения: 26.10.2025).

3. Квашенкина О. Уровень цифровизации транспортно-логистической отрасли в РФ отстает от финсектора, ритейла и телекоммуникаций // URL: https://www.rzd-partner.ru/logistics/opinions/uroven-tsifrovizatsii-transportno-logisticheskoy-otrasli-v-rf-otstaet-ot-finsektora-riteyla-i-teleko/ (дата обращения: 26.10.2025).

4. Козаченко Н. Е. О понятии информационной безопасности в транспортной сфере // Транспортное право и безопасность. – 2024. – № 2 (50). – С. 74-89.

5. Малышев М. И., Филиппова Н. А. Уровень цифровизации российского транспорта // Информационные технологии и инновации на транспорте. Материалы VI Международной научно-практической конференции. – Орел: 2020. – С. 62-68.

6. Щелканова М. А., Романенко Е. В. Развитие субъектов малого и среднего предпринимательства на транспорте в условиях формирования цифровой экономики // Архитектурно-строительный и дорожно-транспортный комплексы: проблемы, перспективы, инновации. Сборник материалов V Международной научно-практической конференции. – Омск: 2021. – С. 397-401.