DOI: 10.58168/MTST2026_92-95
УДК 681.3

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ

А.Р. Глушанков[1], С.В. Дорохин[2], Д.Г. Тертерашвили[3], Р.Р.Жидков[2]
[1] ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова», г. Воронеж, Россия, glushankov2000@inbox.ru
[2] ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова», г. Воронеж, Россия, dsvvrn@yandex.ru
[3] ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова», г. Воронеж, Россия, terterashvili26@gmail.com

Аннотация: В статье исследуются актуальные проблемы кибербезопасности интеллектуальных транспортных систем, возникающие при интеграции современных цифровых платформ с устаревшей инфраструктурой. Проанализированы ключевые угрозы, риски каскадных атак и недостатки финансирования защиты. Предложен комплексный подход, объединяющий технические, нормативные и организационные меры обеспечения безопасности операторов.

Ключевые слова: кибербезопасность, интеллектуальные транспортные системы, киберугрозы, киберфизические системы, уязвимости инфраструктуры, комплексные меры защиты.

CHALLENGES IN ENSURING CYBERSECURITY IN INTELLIGENT TRANSPORT SYSTEMS

A.R. Glushankov[1], S.V. Dorokhin[2], D.G. Terterashvili[3], R.R. Zhidkov[2]
[1] Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia, glushankov2000@inbox.ru
[2] Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia, dsvvrn@yandex.ru
[3] Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia, terterashvili26@gmail.com

Abstract: This article examines current cybersecurity challenges within Intelligent Transport Systems that arise from the integration of modern digital platforms with legacy infrastructure. It analyzes key threats, the risks of cascading attacks, and deficiencies in security funding. A comprehensive approach is proposed that combines technical, regulatory, and organizational measures to ensure the security of system operators.

Keywords: cybersecurity, intelligent transport systems, cyber threats, cyber-physical systems, infrastructure vulnerabilities, comprehensive protection measures.

Ускоряющаяся информатизация и цифровая трансформация социальной и производственной среды сопровождаются усилением киберрисков. Для организаций подобная тенденция приобретает критический характер, поскольку совершенствование цифровых решений и информационных платформ происходит быстрее, чем развитие средств противодействия угрозам.

В транспортной сфере активно внедряются технологические решения нового поколения, включая интернет вещей, киберфизические комплексы, аналитику больших массивов данных и механизмы открытых данных. Функционируя в составе

© Глушанков А. Р., Дорохин С. В., Тертерашвили Д. Г., Жидков Р. Р., 2026

интеллектуального общественного транспорта, подобные системы осуществляют сбор, обработку и передачу сведений, повышая качество сервиса и расширяя набор доступных пассажиру функций.

Как правило, формирование интеллектуальной инфраструктуры протекает в условиях переходного этапа, когда современные решения эксплуатируются одновременно с устаревшими. Традиционные системы, проектировавшиеся без учета актуального ландшафта цифровых угроз, в сочетании с новыми платформами формируют дополнительные проблемы в области кибербезопасности и увеличивают спектр потенциальных атак (рис. 1).

На интеллектуальные транспортные комплексы распространяются как типовые киберугрозы, затрагивающие ИТ-компоненты - рабочие станции, почтовые сервисы и серверные узлы, - так и риски, ориентированные на специализированные операционные и критически значимые подсистемы. Вследствие сетевой связанности к ним возможен дистанционный доступ, а часть из них оказывается доступной через интернет-инфраструктуру. Отдельные элементы относятся к киберфизическим системам: программное управление в них непосредственно связано с воздействием на материальные процессы, например при централизованном регулировании сигнализации из диспетчерского пункта.



Рисунок 1 – Основные виды информационных угроз
Figure 1 – Main Types of Information Threats

В программных компонентах транспортной инфраструктуры присутствуют уязвимости, а высокая степень взаимосвязанности подсистем повышает вероятность каскадного распространения инцидента. Получив контроль над одним узлом, нарушитель потенциально способен повлиять и на смежные сегменты системы.

Практика эксплуатации транспортных сетей в разных странах показывает следующее: программные атаки, вредоносное ПО, компрометация проездных носителей и иные формы вмешательства уже приводили к нарушениям их работы.

Угрозы могут принимать как непреднамеренный характер, включая отказы систем, так и умышленную форму, например, атаки типа распределённого отказа в обслуживании. Их объектом выступают не только транспортные операторы, но и связанные с ними субъекты - иные эксплуатанты, контрагенты, прочие стейкхолдеры, а в ряде случаев и население. Спектр последствий широк: от компрометации сведений до остановки предоставляемых сервисов.

Киберугрозы затрагивают и контур безопасности перевозок. Нарушение работы критически значимого компонента вследствие атаки способно непосредственно

подорвать безопасное функционирование транспортной системы. По указанной причине операторы обязаны поддерживать одновременно и защищённость, и безопасность своих комплексов, обеспечивая выполнение эксплуатационных задач, сохранение деловой репутации, устойчивость деятельности и охрану жизни людей.

Определение кибербезопасности применительно к общественному транспорту сопряжено с методологическими трудностями. Архитектура у каждого оператора своеобразна, а уровень понимания взаимосвязей между защищённостью и безопасностью у поставщиков заметно варьирует. Используемые процедуры риск-анализа остаются недостаточно адресными: в них слабо отражена проблематика безопасности критических активов, при этом отсутствует целостная нормативная или методическая рамка, увязывающая безопасность и сохранность.

Отдельную проблему образует ограниченное финансирование кибербезопасности. Ассигнования на интеллектуальные системы защиты нередко оцениваются без должной проверки их ресурсной адекватности. В результате данные статьи расходов выглядят заниженными относительно совокупного бюджета интеллектуального оператора общественного транспорта.

Безопасность программного обеспечения по-прежнему пребывает на раннем этапе зрелости. Производителям приходится учитывать запросы заказчиков за несколько лет до вывода решения на рынок, тогда как сами заказчики лишь начинают осмыслять новые вызовы в данной области. Параллельно с современными контурами подключаются морально устаревшие системы, а их уязвимые места способны поставить под угрозу весь интеллектуальный комплекс общественного транспорта.

Несмотря на многослойный характер угроз, у операторов интеллектуального общественного транспорта уже имеются практические возможности для укрепления защищенности. Комплекс эффективных мер охватывает предупреждение киберинцидентов, действия в период кризисной ситуации и последующее восстановление с корректировкой уязвимых элементов. При этом результативный подход не исчерпывается инженерными средствами: наряду с технологиями существенную роль играют управленческие процедуры и организационные меры. В рамках данного подхода меры безопасности целесообразно объединять в три блока (рис. 1).

К первому блоку относятся технические меры, направленные на защиту систем, инфраструктуры и применяемых цифровых решений. В их составе рассматриваются инструменты киберзащиты и физической охраны, предназначенные для сохранности критически важных ресурсов. По мере роста связности транспортных платформ усиливается воздействие как внутренних, так и внешних источников риска, поэтому первостепенное значение приобретает анализ защищенности активов, включая сложные контуры обмена сведениями с внешними контрагентами. Операторам необходимо согласовывать с поставщиками и партнерами единый приемлемый уровень безопасности. В частности, при значимости межсистемного обмена для операционной деятельности должны применяться специальные механизмы, поддерживающие целостность передаваемой информации.

Во второй блок включаются практики, связанные с нормативной политикой и стандартами, на основании которых формируются требования к защите деятельности оператора. Для транспортной отрасли характерен длительный цикл эксплуатации систем, нередко достигающий 10-20 лет, тогда как закупка подобных решений обычно осуществляется через конкурсные процедуры. При отсутствии требований к защищенности в договорной документации рассчитывать на их полноценную реализацию затруднительно. Ориентируясь на принципы безопасности по замыслу, операторам интеллектуального общественного транспорта необходимо еще на ранних стадиях согласовывать и проверять механизмы защиты на всем протяжении жизненного

цикла продукта: при разработке, в процессе встраивания в уже функционирующую инфраструктуру и на этапе вывода из эксплуатации.

Транспортные операторы несут ответственность за защиту своей деятельности путем обеспечения сохранности своей структуры, материальных ценностей и жизней людей. Если бы стоимость кибербезопасности могла восприниматься как значимая, влияние происшествия на репутацию, действия, доходы и даже на человеческие жизни можно было бы оценить, как очень важную и уделить большее внимание. Такие возможности необходимо учитывать до того, как будут какие-либо жертвы в результате кибератаки.

Таким образом, обеспечение кибербезопасности интеллектуального транспорта требует системного подхода на всех этапах жизненного цикла цифровых решений. Интеграция современных технических средств защиты, строгих нормативных требований и эффективных организационных процедур позволяет существенно минимизировать риски каскадных атак. Своевременное инвестирование в защиту критически важно для сохранения бесперебойной работы инфраструктуры, деловой репутации операторов и безопасности жизни пассажиров.

СПИСОК ЛИТЕРАТУРЫ

1. Арифджанова, Н. З. Инновационные концепции развития логистических услуг по перевозке и складированию грузов / Н. З. Арифджанова // Научный журнал «A Posteriori». — 2015. — № [номер выпуска]. — С. 23.
2. Карпова, Ю. А. Цифровые технологии по оценке персонала в управлении и образовании: настоящее состояние и перспективы / Ю. А. Карпова, Н. Н. Соколов // [Название сборника/конференции] / Редакционная коллегия. — [Город] : [Издательство], 2019. — С. 104.
3. Годунов, А. Е. К вопросу об обеспечении транспортной безопасности объекта транспортной инфраструктуры на стадии проектирования и строительства / А. Е. Годунов, Д. С. Алтынов, М. А. Дергунова // Труды Ростовского государственного университета путей сообщения. — 2021. — № 3 (56). — С. 10–15.

REFERENCES

1. Arifdzhanova, N. Z. Innovative concepts for the development of logistics services for the transportation and storage of goods / N. Z. Arifdzhanova // Scientific Journal "A Posteriori". — 2015. — P. 23.
2. Karpova, Yu. A. Digital technologies for personnel assessment in management and education: current state and prospects / Yu. A. Karpova, N. N. Sokolov // Editorial Board [Proceedings of the Conference]. — 2019. — P. 104.
3. Godunov, A. E. On the issue of ensuring transport security of a transport infrastructure facility at the design and construction stage / A. E. Godunov, D. S. Altynov, M. A. Dergunova // Proceedings of the Rostov State Transport University. — 2021. — No. 3 (56). — P. 10–15.