

## ДОВЕРЕННАЯ СРЕДА РАЗРАБОТКИ И ЭКСПЛУАТАЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ – ТРЕБОВАНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

<sup>1</sup>Михалеви́ч И.Ф., <sup>2</sup>Назаров А.Н.

<sup>1</sup>*Российский университет транспорта (МИИТ), Москва, Россия, mif-orel@mail.ru*

<sup>2</sup>*МИРЭА - Российский технологический университет (РТУ МИРЭА), Москва, Россия a.nazarov06@bk.ru*

---

Статья посвящена проблемным вопросам обеспечения безопасности интеллектуальных транспортных систем (ИТС). Рассмотрены актуальный ландшафт угроз безопасности ИТС, его динамичный характер, причины изменчивости и тенденции расширения. Показано смещение вектора актов незаконного вмешательства в процессы разработки и эксплуатации ИТС из физической в нефизическую сферу. Приведены примеры актов незаконного вмешательства нефизического характера и тенденций в данной области безопасности ИТС. Разработана базовая архитектура ИТС, дана общая характеристика ее элементов. Исследовано влияние ИТС на различные области безопасности, в том числе на безопасность критической информационной инфраструктуры, транспортную безопасность, национальную безопасность в целом. Представлена модель отношений областей безопасности ИТС. Приведен пример состава типовых объектов ИТС, оказывающих влияние на безопасность критической информационной инфраструктуры, транспортную и национальную безопасность в России. Рассмотрены актуальные вызовы безопасности ИТС, обусловленные зависимостью процессов разработки, внедрения и эксплуатации программного обеспечения, аппаратных средств, программно-аппаратных комплексов, компьютерных технологий, аппаратно-программных платформ от поставок из-за рубежа. Показаны предпосылки замедления темпов научно-технологического развития страны, обусловленные зависимостью от импорта и нарушениями в цепочках зарубежных поставок. Определена необходимость создания доверенной среды для разработки и эксплуатации ИТС. Предложено дополнение состава критериев безопасности ИТС критерием «доверие». Приведены принципы создания доверенной среды разработки и эксплуатации ИТС, основанные на опыте создания отечественных автоматизированных систем в защищенном исполнении. Представленные в статье результаты исследований направлены на повышение уровня технологического суверенитета ИТС, системности и качества решения задач обеспечения безопасности разработки и эксплуатации ИТС, снижение риска наступления негативных последствий при совершении актов незаконного вмешательства нефизического характера.

---

Ключевые слова: акты незаконного вмешательства, импортнезависимость, компьютерные технологии, критическая информационная инфраструктура, интеллектуальная транспортная система, принципы доверия, технологический суверенитет, угрозы, уязвимости, цепочки поставок.

## TRUSTED ENVIRONMENT OF INTELLIGENT TRANSPORTATION SYSTEMS DEVELOPMENT AND OPERATION – A REQUIREMENT OF NATIONAL SECURITY

Igor F. Mikhalevich, Alexey N. Nazarov

*Russian University of Transport (MIIT), Moscow, Russia, mif-orel@mail.ru*

*Russian Technological University (RTU MIREA), Moscow, Russia, a.nazarov06@bk.ru*

---

The article is devoted to the problematic issues of ensuring the security of intelligent transport systems (ITS). The current landscape of ITS security threats, its dynamic nature, causes of variability and expansion trends are considered. The shift in the vector of acts of illegal interference in the processes of ITS development and operation from the physical to the non-physical sphere is shown. Examples of acts of illegal interference of a non-physical nature and trends in this area of ITS security are given. The basic architecture of ITS has been developed, a general description of its elements is given. The influence of ITS on various areas of security, including the security of critical information infrastructure, transport security, and national security in general has been studied. A model of relationships between ITS security areas is presented. An example of the composition of typical ITS objects that affect the security of critical information infrastructure, transport and national security in Russia is given. The current challenges to ITS security caused by the dependence of the processes of development, implementation and operation of software, hardware, software and hardware systems, computer technologies, hardware and software

platforms on supplies from abroad are considered. The article shows the prerequisites for the slowdown in the country's scientific and technological development due to dependence on imports and disruptions in foreign supply chains. It defines the need to create a trusted environment for the development and operation of ITS. It is proposed to supplement the composition of ITS security criteria with the "trust" criterion. Presents the principles of creating a trusted environment for the development and operation of ITS based on the experience of creating domestic automated systems in a secure design. The research results presented in the article are aimed at increasing the level of technological sovereignty of ITS, the consistency and quality of solving the problems of ensuring the security of the development and operation of ITS, reducing the risk of negative consequences when committing acts of illegal interference of a non-physical nature.

---

Keywords: acts of illegal interference, computer technologies, critical information infrastructure, import independence, intelligent transport system, principles of trust, supply chains, technological sovereignty, threats, vulnerabilities.

## Введение

Интеллектуализация транспорта сопровождается конвергенцией традиционных [1-3] и новых компьютерных технологий: облачных [4, 5], больших данных [6 - 8], искусственного интеллекта (ИИ) [9 - 11]. На основе конвергентных технологий в составе интеллектуальных транспортных систем (ИТС) создаются и функционируют интегрированные автоматизированные системы корпоративного и технологического управления (ИАСКиТУ) [12, 13]. Такие системы характеризуют высокая сложность и, зачастую, необдуманная открытость. Сложность ИАСКиТУ вызывает непреднамеренные ошибки, связанные с недостатками проектирования архитектуры, разработки, поставки, развертывания и эксплуатации аппаратных средств и программного обеспечения ИТС. В отношении необдуманной открытости ИАСКиТУ отметим следующее. Пандемия COVID вызвала массовый переход к удаленной работе в корпоративном секторе, для чего были использованы ресурсы Интернета. В это же время активно проводилась цифровизация сектора технологического управления, который подвергся соблазну также масштабного использования Интернета. Но не было учтено цифровое неравенство корпоративного и технологического секторов в части обеспечения безопасности информации в корпоративном управлении и данных – в технологическом [12]. Корпоративный сектор оказался более готовым к использованию Интернета, так как был достаточно обеспечен аппаратными и программными средствами защиты информационных ресурсов в сетях ТСП/IP. Технологический сектор развивался на иных принципах и переход к масштабному применению технологий Интернета требовал принятия новых мер, обеспечивающих безопасность информации и данных, формируемых и используемых в данном секторе иначе. Разработка и реализация таких мер началась со значительной задержкой, что послужило причиной цифрового неравенства составных частей ИАСКиТУ.

Сложность и необдуманная открытость ИАСКиТУ создает дополнительные риски безопасности ИТС, существенно расширяя поверхность для совершения актов незаконного вмешательства в их разработку и эксплуатацию. Угрозы безопасности из физической области смещаются в нефизическую, в которой совершение актов незаконного вмешательства не требует обязательного непосредственного доступа к объекту ИТС. О возможности реализации и высокой опасности такого рода угроз свидетельствуют многочисленные зарегистрированные инциденты [14] и результаты исследований безопасности автомобилей, в частности, Mercedes-Benz [15, 16], BMW [17], Lexus [18], Lexus [17], Tesla [19] и других [20, 21]. Известны случаи несанкционированного физического доступа к транспортному средству, удаленного захвата управления автопилотом, нештатной сработки подушек безопасности и наступления иных неблагоприятных событий безопасности, которые вызваны ошибками разработки и эксплуатации программного и аппаратного обеспечения информационных развлекательных систем [15, 18]<sup>1</sup> и других компьютеризированных систем транспортных средств<sup>2, 3, 4</sup>. Связанные с ними нарушения безопасности носят характер актов незаконного вмешательства непреднамеренного характера. Возможности их своевременного обнаружения и устранения предполагаются, но в обычных условиях разработки и эксплуатации ИТС.

Акты незаконного вмешательства преднамеренного характера возникают в связи с внесенными злоумышленниками в аппаратные средства и программное обеспечение ИТС недостатками (недекларированными возможностями и уязвимостями) с целью их последующего использования путем

---

<sup>1</sup> Researchers jailbreak a Tesla to get free in-car feature upgrades.

<https://techcrunch.com/2023/08/03/researchers-jailbreak-a-tesla-to-get-free-in-car-feature-upgrades/>

<sup>2</sup> Игорь Савкин. Хакеры взломали Tesla и выиграли Model 3. 08.06.2025. <https://kod.ru/tesla-vzlomana-za-odin-dien?ysclid=mbngyf3usx203249576> (дата доступа 08.06.2025).

<sup>3</sup> Dexter. Хакеры взломали Tesla и обнаружили в нем скрытый «режим Илона», активирующий полный автопилот. 31.12.2023, Новости iXBT.com. <https://www.ixbt.com/news/2023/12/31/hakery-vzломali-tesla-i-obnaruzhili-v-nem-skrytyj-rezhim-ilona-aktivirujushij-polnyj-avtopilot.html?ysclid=mbngy0hx3278927600> (дата доступа 08.06.2025).

<sup>4</sup> Мария Нефёдова. Исследователи продемонстрировали взлом и угон Tesla с использованием Flipper Zero. 07.03.2024, новости Хакер.ру. <https://haker.ru/2024/03/07/tesla-phone-key/> (дата доступа 08.06.2025).

проведения или активации компьютерных атак. Такие недостатки аппаратных средств и программного обеспечения ИТС надежно маскируются и скрываются, что затрудняет их обнаружение, а высокая сложность затрудняет исправление.

Зависимость ИТС от импорта негативно влияет на темпы их создания и развития и безопасность ИТС [22, 23]. Ситуация обострилась в 2022 году, когда фактически обрушились цепочки поставок программного обеспечения, аппаратных средств и компьютерных технологий ИТС зарубежного происхождения. Иностраные компании массово отказались от оказания услуг технической поддержки. Предполагавшиеся возможности для своевременного обнаружения и устранения недостатков разработки и эксплуатации ИТС стали недоступными. Вместе с этим активизировались нарушители информационной (компьютерной) безопасности ИТС, связанные с правительствами недружественных стран и/или финансируемые ими, что создало новые риски безопасности не только для ИТС, но и национальной безопасности в целом, так как ИТС являются частью критической инфраструктуры страны<sup>5</sup>.

В сложившихся условиях устранение зависимости от импорта и обеспечение технологического суверенитета приобретают приоритетный характер. Для решения этих проблем необходимо развивать средства и методы обеспечения безопасности ИТС, используя ранее реализованные решения [24, 25] и накопленный опыт создания и эксплуатации отечественных защищенных доверенных аппаратно-программных платформ для критической информационной инфраструктуры [26] и иных защищаемых систем [27].

### **Базовая архитектура ИТС**

В соответствии с «Транспортной стратегией Российской Федерации до 2030 года с прогнозом на период до 2035 года»<sup>6</sup>, другими документами стратегического планирования<sup>7, 8</sup> ИТС создаются во всех видах транспорта. Для всех видов ИТС общим является принцип V2X (Vehicle-to-everything), устанавливающий сложную систему отношений и связей объектов ИТС [28, 29], а также следующие признаки общности [30]:

- вхождение всех видов ИТС в состав критической и критической информационной инфраструктур страны и возможность влияния на их безопасность;

- развертывание в составе всех видов ИТС программно-технических комплексов «Единой государственной информационной системы обеспечения транспортной безопасности» и обработка разнородной информации, в том числе, содержащей сведения, составляющие государственную тайну<sup>9</sup>;

- наличие в составе всех видов ИТС компонентов информационных систем общего назначения, систем автоматического и автоматизированного управления, распределенных корпоративных сетей и внутриобъектовых ЛВС;

- опора всех видов ИТС на радиоканалы, что делает ИТС уязвимыми от воздействия средств радиоэлектронной борьбы и подмены радиосигналов злоумышленниками.

С учетом признаков общности, ГОСТ Р 56829-2015 «Интеллектуальные транспортные системы. Термины и определения», который разработан для автомобильных ИТС, и результатов работ [12, 30, 31] дадим общеприменимое для всех видов транспорта определение термина «интеллектуальная транспортная система». Под ИТС (в широком смысле) будем понимать «распределенную систему управления, интегрирующую современные информационные, телекоммуникационные технологии, искусственный интеллект, и предназначенную для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления транспортным комплексом, транспортной компанией, транспортным средством или группой транспортных средств, а также объектами транспортной инфраструктуры с целью обеспечения заданной мобильности населения, максимизации показателей доставки грузов, повышения безопасности и эффективности транспортных процессов, комфортности для лиц, осуществляющих управление транспортными средствами, и пассажиров». Отметим, что искусственный интеллект не является ключевым признаком ИТС.

Основной отличительной чертой разновидностей ИТС является природа путей сообщения транспортных средств: поверхность земли или воды, подземные коммуникации, подводное или воздушное пространство, - определяющая конкретный вид архитектуры ИТС. Пример базовой архитектуры интеллектуальных систем водного транспорта приведен в [30, 31]. На рисунке 1 приведена базовая архитектура городских наземных ИТС.

---

<sup>5</sup> Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

<sup>6</sup> Транспортная стратегия Российской Федерации до 2030 года с прогнозом на период до 2035 года (утверждена распоряжением Правительства Российской Федерации от 27 ноября 2021 года №3363-р).

<sup>7</sup> Приоритетные направления научно-технологического развития Российской Федерации (утв. Указом Президента Российской Федерации от 18.06.2024 № 529).

<sup>8</sup> Перечень важнейших наукоемких технологий Российской Федерации (утв. Указом Президента Российской Федерации от 18.06.2024 № 529).

<sup>9</sup> Положение о Единой государственной информационной системе обеспечения транспортной безопасности (утверждено постановлением Правительства Российской Федерации от 1 августа 2023 года № 1251).

Базовая архитектура городской наземной ИТС включает семь типов групп элементов, которые сформированы на основе общности существенных признаков объектов, входящих в состав соответствующих групп. Ввиду многообразия видов связей между элементами ИТС и их объектами на рисунке 1 показана только часть видов связей. Остальные виды связей приведены далее по тексту.

В группу V (Vehicle) включены беспилотные и иные интеллектуальные транспортные средства, в том числе роботы-доставщики. Это те виды транспортных средств, которые обладают возможностями автоматического обнаружения любых других транспортных средств, пользователей ИТС и опасностей на пути следования, автоматического непрерывного определения собственных пространственных координат, автоматического обмена данными с другими интеллектуальными транспортными средствами, автоматического реагирования на обнаруженные опасности на пути следования и иные события безопасности.

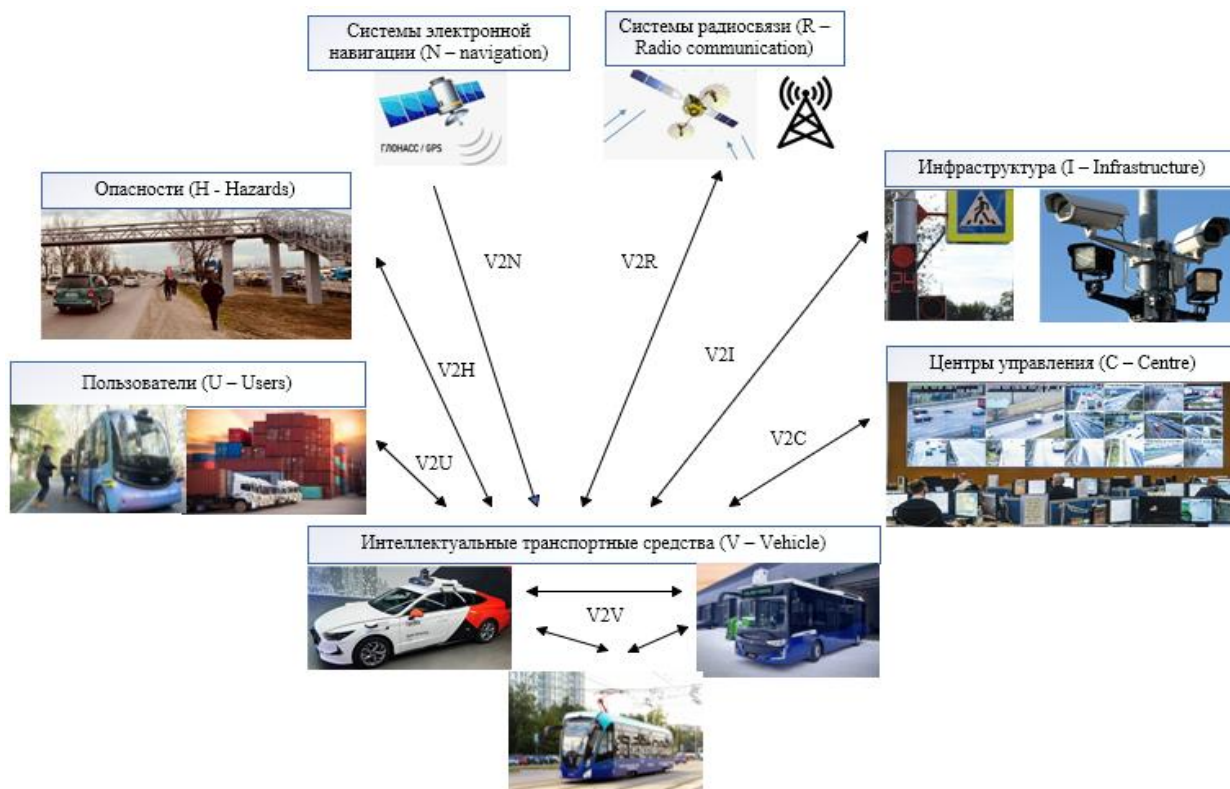


Рис. 1. Базовая архитектура городской наземной ИТС (пример)

Функционирование и безопасность объектов группы V обеспечивает реализация совокупности технологий взаимодействия интеллектуальных транспортных средств с:

- другими интеллектуальными транспортными средствами (V2V – Vehicle-to-Vehicle);
- центрами управления ИТС (V2C, Vehicle-to-Centre);
- инфраструктурой ИТС (V2I, Vehicle-to-Infrastructure);
- пользователями ИТС (V2U, Vehicle-to-Users);
- опасностями на пути следования (V2H - Vehicle-to-Hazards).
- навигационными системами (V2N, Vehicle-to-Navigation systems);
- системами радиосвязи и телекоммуникаций (V2R, Vehicle-to-Radio and Telecommunication Systems).

Уровень зрелости ИТС может быть определен по количеству (процентным отношением) транспортных средств определенных уровней автоматизации. Характеристики уровней автоматизации транспортных средств в составе соответствующих ИТС установлены нормативно<sup>10, 11, 12</sup>.

<sup>10</sup> Характеристики уровней автоматизации транспортных средств. Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования. (утв. Распоряжением Правительства РФ от 25.03.2020 № 724-р. Приложение).

<sup>11</sup> ГОСТ Р 58823-2020. Автомобильные транспортные средства. Системы автоматизации управления движением. Классификация и определения.

Группу С (Centre) формируют центры управления ИТС. Это:

- центры дистанционного управления беспилотными автомобилями и летательными аппаратами, полностью автономными (безэкипажными) и полуавтономными судами и т.п. транспортными средствами;
- центры организации движения;
- центры управления инфраструктурой и т.п.

Функционирование и безопасность объектов группы С обеспечивает реализация совокупности технологий взаимодействия центров управления ИТС с:

- интеллектуальными транспортными средствами (C2V, Centre-to-Vehicle);
- другими центрами управления данной ИТС, а также с центрами управления других ИТС (C2C, Centre-to-Centre);
- инфраструктурой ИТС (C2I, Centre-to-Infrastructure);
- пользователями ИТС (C2U, Centre-to-Users);
- опасностями в зоне своей ответственности (C2H, Centre-to-Hazards);
- навигационными системами (C2N, Centre-to-Navigation systems);
- системами радиосвязи и телекоммуникаций (C2R, Centre-to-Radio and Telecommunication Systems).

Группа I (Infrastructure) включает в себя размещенные на транспортных путях интеллектуальные средства навигационного оборудования, интеллектуальные путевые знаки, интеллектуальные остановки общественного транспорта, иные интеллектуальные средства управления движением, транспортным обслуживанием, безопасностью транспортных средств и путей сообщения.

Функционирование и безопасность объектов группы I обеспечивает реализация совокупности технологий взаимодействия объектов инфраструктуры с:

- интеллектуальными транспортными средствами (I2V, Infrastructure-to-Vehicle);
- центрами управления ИТС (I2C, Infrastructure-to-Centre);
- пользователями ИТС (I2U, Infrastructure-to-Users);
- опасностями в зоне своего обслуживания (I2H, Infrastructure -to-Hazards);
- навигационными системами (I2N, Infrastructure-to-Navigation systems);
- системами радиосвязи и телекоммуникаций (I2R, Infrastructure-to-Radio and Telecommunication Systems).

Группу U (Users) формируют пользователи ИТС. Ими являются пассажиры интеллектуальных транспортных средств, а также отправители и получатели грузов, доставляемых такими средствами. Автоматизированную организацию поездок и перемещения грузов в ИТС обеспечивают технологии взаимодействия пользователей с:

- центрами управления ИТС (U2C, Users-to-Centre);
- инфраструктурой ИТС (U2I, Users-to-Infrastructure);
- навигационными системами (U2N, Users-to-Navigation systems);
- системами радиосвязи и телекоммуникаций (U2R, Users-to-Radio and Telecommunication Systems).

Взаимное автоматическое определение местоположения, обмен данными и реагирование пользователей с интеллектуальными транспортными средствами дополнительно обеспечивают технологии U2V (Users-to-Vehicle).

К группе H (Hazards) отнесены опасности на пути следования интеллектуальных транспортных средств. В эту группу входят традиционные (неинтеллектуальные) транспортные средства, навигационные и иные средства оборудования транспортных путей, пешеходы и лица, перемещающиеся на средствах индивидуальной мобильности, а также провалы, обвалы и иные нарушения дорожного полотна, новообразованные отмели на водных путях, иные путевые опасности случайного (неучтенного) характера. Интеллектуальные транспортные средства должны иметь возможность автоматически обнаруживать опасности на своем пути следования, что реализуется технологиями V2H, V2R, V2N, V2C, V2I;

Группу N (Navigation systems) формируют системы электронной навигации. Это глобальные спутниковые (GPS, ГЛОНАСС, др.) и локальные (национальные, региональные, иные) наземные электронные навигационные системы. Интеллектуальные транспортные средства должны иметь возможность автоматически и непрерывно принимать и обрабатывать сигналы электронных навигационных систем, использовать их в целях обеспечения эффективного и безопасного движения, что реализуется технологиями V2N, C2N.

К группе R (Radio and Telecommunication Systems) отнесены системы, сети и линии спутниковой, сотовой, радиорелейной, Wi-Fi связи, а также базирующиеся на них информационно-телекоммуникационные сети, что реализуется технологиями V2R, C2R, U2R, I2R.

#### **Расширенный ландшафт угроз безопасности ИТС**

Широкое использование компьютеризированных систем существенно расширяет ландшафт угроз безопасности ИТС, наиболее распространенные из которых приведены в таблице 1.

---

<sup>12</sup> НД № 2-020101-174/2023. Правила классификации и постройки морских судов. Часть XV. Автоматизация. СПб.: Российский морской регистр судоходства, 2023.

Реализация компьютерных атак в значительной степени проще совершения актов незаконного вмешательства физического характера (поджога, подрыва, химического или бактериологического заражения и т.п.), так как не требует обязательного непосредственного доступа к транспортным средствам, инфраструктуре путей сообщения и иным объектам ИТС. При этом ущерб от их совершения таких атак может достигать критических размеров, которые существенно превышают сумму затрат на подготовку и реализацию атаки. Это определяет смещение вектора атак на транспортный сектор из области физических в область нефизических воздействий.

Компьютеризированные системы используются в корпоративной и технологической частях ИАСКиТУ, что создает в ИТС уязвимости от различных видов компьютерных атак. Сложные атаки могут вызывать не одно, а несколько негативных для безопасности ИТС последствий. Такие виды атак указаны в таблице 2 как комплексные. Их примером могут служить атаки, приводящие к одновременному нарушению подлинности сведений об источнике информации (отправителе) и изменению содержания информации, передаваемой отправителем. Им, например, подвержены глобальные навигационные спутниковые системы, функционирующие уже длительное время и разработанные без учета данного фактора риска безопасности. Вытекающие из таблицы 2 виды угроз в 2023-2024 годах существенных изменений не претерпели [33, 34]. В 2024 году в общемировом ландшафте наибольшее число компьютерных атак пришлось на секторы государственного управления (19%), транспорта (11%) и финансов (9%) [34]. В транспортном секторе из общего числа зарегистрированных актов незаконного воздействия не физического характера 21% пришлось на DDoS-атаки.

Таблица 1. Основные виды актов незаконного вмешательства нефизического характера в функционирование транспортного комплекса (на примере Европейского Союза [32]<sup>13</sup>)

Типы актов незаконного вмешательства	Частота реализации	
	2021 год	2022 год
Комплексные атаки	35%	25%
Программы-вымогатели	13%	25%
Атаки, связанные с данными	21%	9%
Вредоносное ПО	11%	6%
Атаки «отказ в обслуживании»	2%	13%
Фишинг	7%	3%
Атаки на цепочки поставок	3%	7%
Атаки нарушения функционирования	4%	4%
Подмена источника	3%	2%
Эксплуатация уязвимостей	4%	1%

### Модель отношения областей безопасности ИТС

Компьютерные атаки на ИТС могут вызвать негативные последствия в других областях безопасности, что обусловлено связанностью различных областей. Модель областей безопасности ИТС имеет вид пирамиды [30], вертикальная проекция которой показана на рисунке 2.

Каждый горизонтальный слой использует свой набор средств и технологий безопасности. Расположенные ближе к вершине пирамиды слои могут негативно влиять на состояние слоев, расположенных ближе к ее основанию. Это соответствует модели «дырявого ведра» [35, 36].

С учетом этого на каждом слое должны быть реализованы надежные меры безопасности для достижения всех целей безопасности. Чем ниже к основанию пирамиды, тем больше поверхность для совершения актов незаконного вмешательства преднамеренного и непреднамеренного характера.

Представленная модель отношений областей безопасности ИТС интегрирует российские подходы нормативного регулирования защиты компьютеризированных систем от актов незаконного вмешательства физического (поджог, подрыв, вандализм и др.) и нефизического (компьютерная атака, неустранение программных и иных уязвимостей, др.) характера.

Ее пирамидальная форма представления наглядно отражает комплексный характер угроз, средств и методов обеспечения безопасности, а также влияние ИТС на безопасность критической информационной и критической инфраструктур, национальную безопасность в целом.

<sup>13</sup> Threat Landscape Transport Sector. ENISA, March 21, 2023. URL: <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>. (дата обращения 26.04.2025)



Рис. 2. Модель областей отношений безопасности компьютеризированных систем транспортной отрасли [30]

### Интеллектуальные транспортные системы в составе критической информационной инфраструктуры Российской Федерации

В соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» компьютеризированные системы транспортной отрасли входят в состав критической информационной инфраструктуры (КИИ) страны.

В зависимости от значений показателей критериев значимости, которые установлены нормативно<sup>14, 15</sup>, объекты ИТС могут быть отнесены к одной из трех категорий, что влечет обязанность выполнения комплекса мер по защите объектов от актов незаконного вмешательства нефизического характера<sup>16, 17</sup>.

«Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта» утвержден заместителем министра Минтранса России 26.04.2024 г.

В таблице 2 приведен состав типовых объектов КИИ автомобильного транспорта и перечень выполняемых ими критических процессов.

<sup>14</sup> Правила категорирования объектов критической информационной инфраструктуры Российской Федерации (утверждены постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127).

<sup>15</sup> Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (утвержден постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127).

<sup>16</sup> Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239).

<sup>17</sup> Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утверждены приказом ФСТЭК России от 21 декабря 2017 г. № 235).

Таблица 2. Типовые объекты ИТС автомобильного транспорта в составе КИИ<sup>18</sup>

Типовые объекты КИИ	Критические процессы, осуществляемые типовым объектом
Автоматизированные системы, обеспечивающие управление дорожным движением	Адаптивное централизованное и локальное управление транспортными и пешеходными потоками (светофорами) Сбор, накопление и обработка статистической информации о транспортных потоках (классификации по типам и интенсивности) Обеспечение приоритетного пропуски общественного транспорта Обеспечение участников дорожного движения необходимой информацией
Автоматизированные системы, предназначенные для управления автовокзалами	Хранение информации о тарифах, остановках, маршрутах и расписаний Прием и отправка рейсов, печать посадочных ведомостей, пересадка пассажиров, предоставление справочной информации Обеспечение процесса продажи билетов, предоставление льгот, учет сборов Обеспечение процесса работы с фискальным оборудованием, автоматизация процесса формирования отчетов, выгрузка персональных данных пассажиров в автоматизированную централизованную базу персональных данных пассажиров
Автоматизированные системы управления, предназначенные для взимания платы на платных дорогах	Автоматизированное управление пропускными устройствами. Удаленный мониторинг состояния оборудования. Интеллектуальное распознавание транспортных средств. Автоматизация платежей Выявление должников и нарушителей
Автоматизированные системы, обеспечивающие управление диспетчерских грузоперевозок и контроля транспорта	Обеспечение подбора водителей и автомобиля Определение маршрута и затрат на перевозку грузов Формирование и оформление документов о перевозке Отслеживание грузов Контроль перемещения автомобильного транспорта Контроль грузового транспорта и контроль перевозки грузов Контроль параметров автомобильного транспорта (расход топлива, температура технологических жидкостей и другие)
Автоматизированные системы, обеспечивающие управление разводным мостом	Управление светофорами и шлагбаумами. Управление гидравлическими системами, домкратами и приводами моста Контроль состояния оборудования и механизмов моста
Системы, предназначенные для управления состоянием автомобильных дорог и искусственных сооружений	Управление, контроль за состоянием автомобильных дорог и искусственных сооружений
Системы, предназначенные для автоматизации контроля эксплуатации самоходных машин и иной техники	Исполнение функции органа власти в сферах регистрации и контроля за эксплуатацией самоходных машин, выдачи удостоверений, обеспечивает контроль платежей и остатков, бланков спецпродукции, неоплаченных штрафов при проведении операции, а также отвечает за ведение истории всех проведенных операций по владельцу, по машине

<sup>18</sup> Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утвержден Министерством транспорта Российской Федерации 26.04.2024). URL: <https://mintrans.gov.ru/documents/8/13678?ysclid=m8lif2h22y720469699> (дата обращения 23.03.2025).

Таблица 2. Типовые объекты ИТС автомобильного транспорта в составе КИИ<sup>18</sup>

Типовые объекты КИИ	Критические процессы, осуществляемые типовым объектом
Автоматизированные системы, предназначенные для управления автопарками (колесные любого типа) используемых в интересах или под управлением государственных органов власти	Управление и сбор данных о транспортных средствах, используемых для коммерческих перевозок пассажиров Контроль перемещения транспортных средств Контроль параметров транспортных средств Удаленный мониторинг Обеспечение доступа к данным с технических средств обеспечения транспортной безопасности, а также передача таких данных в соответствии с установленными требованиями
Автоматизированные системы, предназначенные для автоматизации, контроля и сбора данных от транспортных средств	Контроль перемещения транспортных средств. Мониторинг оборудования, установленного на транспортном средстве Обеспечение доступа к данным с технических средств обеспечения транспортной безопасности, а также передача таких данных в соответствии с установленными требованиями
Автоматизированные системы автотранспортной телематики при оказании услуг автомобильным транспортом	Контроль перемещения автомобильного транспорта Контроль параметров автомобильного транспорта (расход топлива, температура технологических жидкостей и другие) Хранение телематической информации

Учитывая возможность негативного влияния ИТС на безопасность КИИ, с ранних стадий жизненного цикла необходимо принимать меры обеспечения безопасности от актов незаконного вмешательства нефизической природы [24, 25, 37 - 39], наряду с традиционными для транспортных систем мерами защиты от воздействий физического характера.

#### Расширение состава критериев безопасности ИТС, принципы доверия

С 2022 года иностранные высокотехнологичные компьютеризированные системы остались без авторского сопровождения и технической поддержки, что создало новые угрозы безопасности ИТС. В соответствии с Указами Президента Российской Федерации от 30.03.2022 № 166, от 18.06.2024 № 529 разработка и эксплуатация ИТС должны осуществляться в доверенной среде с использованием отечественных аппаратных средств и программного обеспечения. В связи с этим известные системы критериев эффективности и безопасности информационных систем [40], автоматизированных систем управления и иных компьютеризованных систем ИТС [41-43] целесообразно дополнить критерием «доверие».

Принципы доверия в динамике их развития рассмотрены в [26, 30]. Под доверенными будем понимать аппаратные средства, программное обеспечение и технологии ИТС, удовлетворяющие следующим основным принципам:

- «безопасность;
- защищенность;
- правовая охрана;
- разграничение ответственности разработчиков, поставщиков и пользователей;
- защита потребителей;
- контролируемость;
- полноценность;
- импортонезависимость;
- технологический суверенитет;
- промышленный уровень;
- универсальность;
- гарантии развития и поддержки;
- аппаратная и программная совместимость;
- гибкость;
- оперативность;
- преемственность;
- целостность инновационного цикла;
- поддержка конкуренции», - характеристика которых приведена в [30].

Предложенное расширение состава критериев учитывает требования ГОСТ 56939-2024 «Разработка безопасного программного обеспечения. Общие требования», отечественный опыт [24-26], результаты международных исследований [45-48] и зарубежные практики [49-51] обеспечения безопасности аппаратных средств, программного обеспечения и технологий, используемых в ИТС.

#### Заключение

Интеллектуальные транспортные системы являются частью критической инфраструктуры страны, а используемые в них информационные системы и автоматизированные системы управления, в случае уязвимого состояния, могут нарушить безопасность критической информационной инфраструктуры и, как следствие, безопасность критической инфраструктуры страны, снизить уровень национальной безопасности.

Нарушения в цепочках поставок, отказ от авторского сопровождения и технической поддержки нарушил доверие к аппаратным средствам, программному обеспечению и компьютерным технологиям иностранного происхождения, используемым в ИТС. В этих условиях создание доверенной среды разработки и эксплуатации ИТС является задачей национального масштаба.

Приведенные принципы создания доверенной среды разработки и эксплуатации ИТС были использованы при создании доверенных отечественных автоматизированных систем в защищенном исполнении, к которым относятся автоматизированные системы корпоративного и технологического управления ИТС.

Представленные результаты исследования повышают уровень технологического суверенитета ИТС, системности и качества решения задач обеспечения безопасности разработки и эксплуатации ИТС, снижают риск наступления негативных последствий при совершении актов незаконного вмешательства нефизического характера.

Рассмотренные решения были использованы при выполнении РУТ (МИИТ):

- работ по Стратегическому технологическому проекту «Интеллектуальные транспортные системы и автономные транспортные средства» по Программе стратегического академического лидерства «Приоритет - 2030»;

- НИР «Централизованные доверенные интеллектуальные системы управления внеуличным городским транспортом на основе отечественных решений» по государственному заданию от 15.01.2026 № 103-00001-26-00.

### Список литературы

1. Nyrkov, A. P. On the issue of categorization of critical information infrastructure objects of seaports / K. V. Natashova, S. S. Sokolov, O. N. Gubernators [et al.] // Information Technology Security. - 2020. - Vol. 27, No. 2. - P. 35-46. - DOI 10.26583/bit.2020.1.03. (In Russian)
2. Новиков, А. Н. Цифровизация управления транспортно-логистическими процессами сетевой доставки груза автомобильным транспортом / А. Н. Новиков, С. А. Жесткова // Мир транспорта и технологических машин. – 2025. – № 1-3(88). – С. 18-23. – DOI 10.33979/2073-7432-2025-1-3(88)-18-23.
3. Построение архитектуры интеллектуальной системы управления городской рельсовой транспортной системой / В. М. Алексеев, Л. А. Баранов, М. А. Кулагин, В. Г. Сидоренко // Мир транспорта. – 2021. – Т. 19, № 1(92). – С. 18-46. – DOI 10.30932/1992-3252-2021-19-1-18-46.
4. Трофименко, Ю. В. Концепция создания эффективных транспортных систем с использованием «облачных» интеллектуальных технологий / Ю. В. Трофименко, Р. С. Рунец, С. В. Ушков // Мир транспорта и технологических машин. – 2024. – № 3-3(86). – С. 111-119. – DOI 10.33979/2073-7432-2024-3-3(86)-111-119.
5. Sheik, A.T.; Maple, C.; Epiphaniou, G.; Dianati, M. A Comprehensive Survey of Threats in Platooning—A Cloud-Assisted Connected and Autonomous Vehicle Application. Information 2024, 15, 14. URL: <https://doi.org/10.3390/info15010014>.
6. Lian, Y., Zhang, G., Lee, J., Huang, H. Review on big data applications in safety research of intelligent transportation systems and connected/automated vehicles. Accident Analysis and Prevention. Volume 146, October 2020. URL: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85090201638&origin=inward&txGid=32e08334c7c961480021c5d73af1f607>.
7. Abdullah M. Algarni, Vijey Thayanathan. Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication. November 2022. Symmetry 14(12):2494. DOI:10.3390/sym14122494.
8. Okur, C.; Dener, M. Symmetrical Resilience: Detection of Cyberattacks for SCADA Systems Used in IIoT in Big Data Environments. Symmetry 2025, 17, 480. URL: <https://doi.org/10.3390/sym17040480>.
9. Kim, D.; Lee, C.; Park, S.; Lim, S. Potential Liability Issues of AI-Based Embedded Software in Maritime Autonomous Surface Ships for Maritime Safety in the Korean Maritime Industry. J. Mar. Sci. Eng. 2022, 10, 498. URL: <https://doi.org/10.3390/jmse10040498>.
10. Sandeep Gupta, Roberto Passerone, Carsten Maple. An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles. 2023, Journals & Magazines IEEE Access, Volume 11. URL: DOI: 10.1109/ACCESS.2023.3307473.
11. Durlík, I.; Miller, T.; Kostecka, E.; Tuński, T. Artificial Intelligence in Maritime Transportation: A Comprehensive Review of Safety and Risk Management Applications. Appl. Sci. 2024, 14, 8420. URL: <https://doi.org/10.3390/app14188420>.

12. Михалевич, И. Ф. Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем / И. Ф. Михалевич // Надежность. – 2024. – Т. 24, № 2. – С. 72-87. – DOI 10.21683/1729-2646-2024-24-2-72-87.
13. Модели и алгоритмы формирования интегрированной телематической автоматизированной системы управления автомобильными перевозками опасных грузов / Р. Н. Сафиуллин, Х. Тянь, Ю. Н. Кацуба, М. В. Богданов // Мир транспорта и технологических машин. – 2025. – № 1-4(88). – С. 10-17. – DOI 10.33979/2073-7432-2025-1-4(88)-10-17.
14. Mikhalevich, I. F. Intelligent Transport Systems Software as a Source of Transport Security Threats / I. F. Mikhalevich // Systems of Signals Generating and Processing in the Field of on Board Communications. – 2023. – Vol. 6, No. 1. – P. 303-308. – DOI 10.1109/IEEECONF56737.2023.10092129.
15. Mercedes-Benz MBUX Security Research Report. Experimental Security Assessment of Mercedes-Benz Cars. Tencent Security Keen Lab. [https://keenlab.tencent.com/en/whitepapers/Mercedes\\_Benz\\_Security\\_Research\\_Report\\_Final.pdf](https://keenlab.tencent.com/en/whitepapers/Mercedes_Benz_Security_Research_Report_Final.pdf) (дата доступа 10.12.2021).
16. Mercedes-Benz Head Unit security research report (2025). By GIXnews / January 17, 2025. <https://gixtools.net/2025/01/mercedes-benz-head-unit-security-research-report/> (дата доступа 13.06.2025).
17. Experimental Security Assessment of BMW Cars: A Summary Report. [https://keenlab.tencent.com/en/whitepapers/Experimental\\_Security\\_Assessment\\_of\\_BMW\\_Cars\\_by\\_KeenLab.pdf](https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf) (дата доступа 13.06.2025).
18. Experimental Security Assessment on Lexus Cars (2020). Tencent Security Keen Lab. <https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars> (дата доступа 13.06.2025).
19. Experimental Security Research of Tesla Autopilot (2019). Tencent Security Keen Lab. [https://keenlab.tencent.com/en/whitepapers/Experimental\\_Security\\_Research\\_of\\_Tesla\\_Autopilot.pdf](https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf) (дата доступа 13.06.2025).
20. Christopher Corbett, Karsten Schmidt, Martin Jakob. Security Testing for Networked Vehicles. September 2018. Conference: FKFS: 7th Autotest Conference. At: Stuttgart
21. Feng Luo, Xuan Zhang, and others. Cybersecurity Testing for Automotive Domain: A Survey Sensors 2022, 22(23), 9211. <https://doi.org/10.3390/s22239211>.
22. Пушкин, П. Ю. Инновационные технологии для беспилотных систем / П. Ю. Пушкин, Ю. Н. Ризаева, А. Б. Сухатерин // Мир транспорта и технологических машин. – 2024. – № 3-3(86). – С. 102-110. – DOI 10.33979/2073-7432-2024-3-3(86)-102-110.
23. Баранов, Л. А. Планирование движения поездов в интеллектуальных транспортных системах / Л. А. Баранов, А. И. Сафронов, В. Г. Сидоренко // Надежность. – 2022. – Т. 22, № 3. – С. 35-43. – DOI 10.21683/1729-2646-2022-22-3-35-43.
24. Ивашко, А.М. К созданию защищенных систем обработки информации / Зегжда Д.П., Ивашко А.М. // Проблемы информационной безопасности. Компьютерные системы. 1999. № 1. С. 99-107.
25. Ивашко, А.М. Технология создания безопасных систем обработки информации на основе отечественной защищенной операционной системы / Зегжда Д.П., Ивашко А.М. // Проблемы информационной безопасности. Компьютерные системы. 1999. № 2. С. 59-64.
26. Михалевич, И. Ф. Методологические основы создания национальных защищенных аппаратно-программных платформ для критических информационных инфраструктур / И. Ф. Михалевич // Т-Comm: Телекоммуникации и транспорт. – 2018. – Т. 12, № 3. – С. 75-81. – DOI 10.24411/2072-8735-2018-10056.
27. Марков, А.С. О систематике информационной безопасности цепей поставки программного обеспечения / Барабанов А.В., Марков А.С. Цирлов В.Л. // Безопасность информационных технологий. 2019. Т. 26, № 3. С. 68-79. DOI: 10.26583/bit.2019.3.06.
28. Ahmad Alalewi; Iyad Dayoub; Soumaya Cherkaoui. On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey. IEEE Transactions on Green Communications and Networking. Vol. 8, Issue: 1, March 2024. P.205-223. <https://doi.org/10.1109/ACCESS.2021.3100472>.
29. Toghi, Behrad; Saifuddin, Md; Nourkhiz Mahjoub, Hossein; Mughal, M. O.; Fallah, Yaser P., and others. Multiple Access in Cellular V2X: Performance Analysis in Highly Congested Vehicular Networks. Eprint arXiv:1809.02678. [https://ui.adsabs.harvard.edu/link\\_gateway/2018arXiv180902678T/doi:10.48550/arXiv.1809.02678](https://ui.adsabs.harvard.edu/link_gateway/2018arXiv180902678T/doi:10.48550/arXiv.1809.02678).
30. Михалевич И. Ф. О доверии к системам автономного судоходства критической информационной инфраструктуры / Л. А. Баранов, И. Ф. Михалевич // Т-Comm: Телекоммуникации и транспорт. 2025. Том 19. №6. С. 52-59. DOI: 10.36724/2072-8735-2025-19-6-52-59.

31. Михалевич, И. Ф. Проблемы обеспечения безопасности автономного судоходства на внутренних водных путях (монография) / И. Ф. Михалевич. – Москва: Научно-техническое издательство «Горячая линия – Телеком», 2024. – 336 с.
32. Threat Landscape Transport Sector. ENISA, March 21, 2023. URL: <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>. (дата обращения 26.10.2024)
33. ENISA Threat Landscape 2024. Published September 19, 2024. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (дата обращения 26.10.2024).
34. Threat landscape for industrial automation systems. Q2 2024. URL: <https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024/>.
35. Таненбаум Эндрю, Фимстер Ник, Уэзеролл Дэвид. Компьютерные сети. Шестое издание. Серия: Классика computer science. - Издательство: Питер. – 2023. – 992 с. - ISBN: 978-5-4461-1766-6.
36. Михалевич, И. Ф. Оценка устойчивости развития критической инфраструктуры Российской Федерации на базе технологии оценки и мониторинга информационной безопасности / И. Ф. Михалевич, А. П. Рыжов // Т-Comm: Телекоммуникации и транспорт. – 2018. – Т. 12, № 5. – С. 70-76. – DOI 10.24411/2072-8735-2018-10089.
37. Dennis Kengo Oka, “Building Secure Cars: Assuring the Automotive Software Development Lifecycle”. Hoboken, NJ: John Wiley & Sons, Inc., 2021. <https://www.oreilly.com/library/view/building-secure-cars/9781119710745/> (дата доступа 16.06.2025).
38. Mikhalevich, I. F. Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems / I. F. Mikhalevich // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications. DOI 10.1109/IEEECONF53456.2022.9744337.
39. Зегжда, П.Д. Теоретико-множественная модель техник атак отравления данных в системах искусственного интеллекта / Н. В. Гололобов, Д. П. Зегжда // Проблемы информационной безопасности. Компьютерные системы. – 2023. – № S2(55). – С. 120-129. – DOI 10.48612/jisp/9agd-ребр-b82a.
40. Зацаринный, А. А. Некоторые методические аспекты выбора показателей эффективности информационных систем / А. А. Зацаринный, Ю. С. Ионенков // Системы высокой доступности. – 2019. – Т. 15, № 4. – С. 19-26. – DOI 10.18127/j20729472-201904-03.
41. Епифанов, В. В. Обоснование показателей качества в системе функционирования беспилотного автомобиля / В. В. Епифанов, С. Е. Визгалин, А. О. Статенин // Мир транспорта и технологических машин. – 2025. – № 1-2(88). – С. 114-118. – DOI 10.33979/2073-7432-2025-1-2(88)-114-118.
42. Митряев, И. С. Аспекты эффективности интеллектуальных транспортных систем / И. С. Митряев // Мир транспорта и технологических машин. – 2024. – № 4-3(87). – С. 89-95. – DOI 10.33979/2073-7432-2024-4-3(87)-89-95.
43. Kalashnikov, A. O. About the single system of protection classes elements of critical information infrastructure by the criteria of importance and information security / A. O. Kalashnikov, I. F. Mikhalevich // International Journal of Engineering and Technology(UAE). – 2018. – Vol. 7, No. 2. – P. 247-250. – DOI 10.14419/ijet.v7i2.23.11952.
44. Михалевич, И. Ф. Проблемы создания доверенной среды разработки и реализации интеллектуальных систем водного транспорта / И. Ф. Михалевич // Надежность. – 2025. – Т. 25, № 2. – С. 39-47. – DOI 10.21683/1729-2646-2025-25-2-39-47.
45. Nkoro E.C., Njoku J.N., Nwakanma C.I., Lee J.-M., Kim D.-S. Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach. Electronics 2024, 13, 276. URL: <https://doi.org/10.3390/electronics13020276>.
46. Nwakanma C.I., Ahakonye L.A.C., Njoku J.N.; Odirichukwu J.C., Okolie S.A. Uzundu C., Ndubuisi Nweke C.C., Kim D.-S. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review. Appl. Sci. 2023, 13, 1252. doi.org/10.3390/app13031252.
47. Bolbot, V.; Sandru, A.; Saarniniemi, T.; Puolakka, O.; Kujala, P.; Valdez Banda, O.A. Small Unmanned Surface Vessels—A Review and Critical Analysis of Relations to Safety and Safety Assurance of Larger Autonomous Ships. J. Mar. Sci. Eng. 2023, 11, 2387. URL: doi.org/10.3390/jmse11122387.
48. Raheman, F. (2024) From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. Journal of Computer and Communications, 12, 252-282. URL: doi: 10.4236/jcc.2024.123016.
49. Fabro, M., Gorski, E., Spiers, N., Diedrich, J., Kuipers, D.: Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies. DHS Industrial Control Systems Cyber Emergency Response Team, (2016). URL: <https://www.hsdl.org/c/view?docid=797585>.
50. Zero Trust Strategy and Roadmap. US Department of Defense Releases Nov. 22, 2022 URL: <https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/>.

51. Zero Trust. Maturity Model. April 2023. Version 2.0. Cybersecurity and Infrastructure Security Agency. Cybersecurity Division. URL: [https://www.cisa.gov/sites/default/files/2023-04/CISA\\_Zero\\_Trust\\_Maturity\\_Model\\_Version\\_2\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf).

## References

1. Nyrkov, A. P. On the issue of categorization of critical information infrastructure objects of seaports / K. V. Natashova, S. S. Sokolov, O. N. Gubernators [et al.] // *Information Technology Security*. - 2020. - Vol. 27, No. 2. - P. 35-46. - DOI 10.26583/bit.2020.1.03.
2. Novikov A.N., Zhestkova S.A. Digitalization of management of transport and logistics processes of network delivery of cargo by road transport. *The world of transport and technological machines*. 2025, № 1-3(88), P. 18-23. – DOI 10.33979/2073-7432-2025-1-3(88)-18-23. (In Russian)
3. Alexeev V.M., Baranov L.A., Kulagin M.A., Sidorenko V.G. Building Architecture of Intelligent Control System for Urban Rail Transit System. *World of Transport and Transportation*. 2021;19(1):18-46. <https://doi.org/10.30932/1992-3252-2021-19-1-18-46>.
4. Trofimenko Yu.V., Runets R.S., Ushkov S.V. The concept of creating efficient transport systems using "cloud" intelligent technologies. *The world of transport and technological machines*. 2024, № 3-3(86), P. 111-119. – DOI 10.33979/2073-7432-2024-3-3(86)-111-119. (In Russian)
5. Sheik, A.T.; Maple, C.; Epiphaniou, G.; Dianati, M. A Comprehensive Survey of Threats in Platooning—A Cloud-Assisted Connected and Autonomous Vehicle Application. *Information* 2024, 15, 14. <https://doi.org/10.3390/info15010014>.
6. Lian, Y., Zhang, G., Lee, J., Huang, H. Review on big data applications in safety research of intelligent transportation systems and connected/automated vehicles. *Accident Analysis and Prevention*. Volume 146, October 2020. <https://www.scopus.com/record/display.uri?eid=2-s2.0-85090201638&origin=inward&txGid=32e08334c7c961480021c5d73af1f607>.
7. Abdullah M. Algarni, Vijey Thayanathan. Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication. November 2022. *Symmetry* 14(12):2494. DOI:10.3390/sym14122494.
8. Okur, C.; Dener, M. Symmetrical Resilience: Detection of Cyberattacks for SCADA Systems Used in IIoT in Big Data Environments. *Symmetry* 2025, 17, 480. <https://doi.org/10.3390/sym17040480>.
9. Kim, D.; Lee, C.; Park, S.; Lim, S. Potential Liability Issues of AI-Based Embedded Software in Maritime Autonomous Surface Ships for Maritime Safety in the Korean Maritime Industry. *J. Mar. Sci. Eng.* 2022, 10, 498. <https://doi.org/10.3390/jmse10040498>.
10. Sandeep Gupta, Roberto Passerone, Carsten Maple. An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles. 2023, *Journals & Magazines IEEE Access*, Volume 11. DOI: 10.1109/ACCESS.2023.3307473.
11. Durluk, I.; Miller, T.; Kostecka, E.; Tuński, T. Artificial Intelligence in Maritime Transportation: A Comprehensive Review of Safety and Risk Management Applications. *Appl. Sci.* 2024, 14, 8420. <https://doi.org/10.3390/app14188420>.
12. Mikhalevich I.F. (2024). Conceptual problems of transportation security of intelligent water transportation systems." *Dependability* 2024;2:72-87. <https://doi.org/10.21683/1729-2646-2024-24-2-72-87>. (In Russian).
13. Safiullin R.N., Tian H., Katsuba Y.N., Bogdanov M.V. Models and algorithms for the formation of an integrated telematic automated control system for road transport of dangerous goods. *World of transport and technological machines*, 2025 88(1-4):10-17. DOI:10.33979/2073-7432-2025-1-4(88)-10-17. (In Russian)
14. Mikhalevich, I. F. Intelligent Transport Systems Software as a Source of Transport Security Threats / I. F. Mikhalevich // *Systems of Signals Generating and Processing in the Field of on Board Communications*. – 2023. – Vol. 6, No. 1. – P. 303-308. – DOI 10.1109/IEEECONF56737.2023.10092129.
15. Mercedes-Benz MBUX Security Research Report. Experimental Security Assessment of Mercedes-Benz Cars. Tencent Security Keen Lab. [https://keenlab.tencent.com/en/whitepapers/Mercedes\\_Benz\\_Security\\_Research\\_Report\\_Final.pdf](https://keenlab.tencent.com/en/whitepapers/Mercedes_Benz_Security_Research_Report_Final.pdf) (access date 10.12.2021).
16. Mercedes-Benz Head Unit security research report (2025). By GIXnews / January 17, 2025. <https://gixtools.net/2025/01/mercedes-benz-head-unit-security-research-report/> (access date 13.06.2025).
17. Experimental Security Assessment of BMW Cars: A Summary Report. [https://keenlab.tencent.com/en/whitepapers/Experimental\\_Security\\_Assessment\\_of\\_BMW\\_Cars\\_by\\_KeenLab.pdf](https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf) (access date 13.06.2025).

18. Experimental Security Assessment on Lexus Cars (2020). Tencent Security Keen Lab. <https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars> (access date 13.06.2025).
19. Experimental Security Research of Tesla Autopilot (2019). Tencent Security Keen Lab. [https://keenlab.tencent.com/en/whitepapers/Experimental\\_Security\\_Research\\_of\\_Tesla\\_Autopilot.pdf](https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf) (access date 13.06.2025).
20. Christopher Corbett, Karsten Schmidt, Martin Jakob. Security Testing for Networked Vehicles. September 2018. Conference: FKFS: 7th Autotest Conference. At: Stuttgart
21. Feng Luo, Xuan Zhang, and others. Cybersecurity Testing for Automotive Domain: A Survey. *Sensors* 2022, 22(23), 9211. <https://doi.org/10.3390/s22239211>.
22. Pushkin P.Yu, Rizaeva Yu.N., Sukhaterin A.B. Innovative technologies for unmanned systems . The world of transport and technological machines. 2024, № 3-3(86), P. 102-110. – DOI 10.33979/2073-7432-2024-3-3(86)-102-110. (In Russian)
23. Baranov, L.A., Safronov A.I., Sidorenko V.G. Train traffic planning in intelligent transportation systems. *Dependability*. 2022;22(3):35-43. (In Russ.) <https://doi.org/10.21683/1729-2646-2022-22-3-35-43>. (In Russian)
24. Ivashko, A.M. On the creation of protected information processing systems / Zegzhda D.P., Ivashko A.M. // *Problems of information security. Computer systems*. 1999. No. 1. P. 99-107. (In Russian)
25. Ivashko, A.M. Technology of creating secure information processing systems based on a domestic protected operating system / Zegzhda D.P., Ivashko A.M. // *Problems of information security. Computer systems*. 1999. No. 2. P. 59-64. (In Russian)
26. Mikhalevich I.F. (2018). Methodological foundations of creation of national protected hardware-software platforms for critical information infrastructures. *T-Comm*, vol. 12, no.3, pp. 75-81. DOI 10.24411/2072-8735-2018-10056.
27. Markov, A.S. On the taxonomy of information security of software supply chains / Barabanov A.V., Markov A.S. Tsirlov V.L. // *Information Technology Security*. 2019. Vol. 26, No. 3. Pp. 68-79. DOI: 10.26583/bit.2019.3.06. (In Russian)
28. Ahmad Alalewi; Iyad Dayoub; Soumaya Cherkaoui. On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey. *IEEE Transactions on Green Communications and Networking*. Vol. 8, Issue: 1, March 2024. P.205-223. <https://doi.org/10.1109/ACCESS.2021.3100472>.
29. Toghi, Behrad; Saifuddin, Md; Nourkhiz Mahjoub, Hossein; Mughal, M. O.; Fallah, Yaser P., and others. Multiple Access in Cellular V2X: Performance Analysis in Highly Congested Vehicular Networks. *Eprint arXiv:1809.02678*. [https://ui.adsabs.harvard.edu/link\\_gateway/2018arXiv180902678T/doi:10.48550/arXiv.1809.02678](https://ui.adsabs.harvard.edu/link_gateway/2018arXiv180902678T/doi:10.48550/arXiv.1809.02678).
30. Mikhalevich I. F. On trust in autonomous shipping systems of critical information infrastructure / L. A. Baranov, I. F. Mikhalevich // *T-Comm*. – 2025. – Vol. 19, No. 6. – P. 52-59. – DOI 10.36724/2072-8735-2025-19-6-52-59.
31. Mikhalevich, I. F. *Problems of Ensuring the Safety of Autonomous Shipping on Inland Waterways* / I. F. Mikhalevich. - Moscow: Scientific and Technical Publishing House "Hot Line - Telecom", 2024. - 336 p. – ISBN 978-5-9912-1106-2. (In Russian)
32. Threat Landscape Transport Sector. ENISA, March 21, 2023. URL: <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape> (дата обращения 26.10.2024)
33. ENISA Threat Landscape 2024. Published September 19, 2024. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (дата обращения 26.10.2024).
34. Threat landscape for industrial automation systems. Q2 2024. URL: <https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024/>.
35. Tanenbaum Andrew, Feamster Nick, Weatherall David. *Computer networks*. Sixth edition. Series: Classics of computer science. - Publisher: Peter., 2023, 992 p. - ISBN: 978-5-4461-1766-6.
36. Mikhalevich I.F., Ryjov A.P. (2018). Assessment of the sustainability of the development of the critical infrastructures on the basis of information security evaluation and monitoring technology. *T-Comm*, vol. 12, no.5, pp. 71-76. DOI 10.24411/2072-8735-2018-10089.
37. Dennis Kengo Oka, “Building Secure Cars: Assuring the Automotive Software Development Lifecycle”. Hoboken, NJ : John Wiley & Sons, Inc., 2021. <https://www.oreilly.com/library/view/building-secure-cars/9781119710745/> (access date 16.06.2025).
38. Mikhalevich, I. F. Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems / I. F. Mikhalevich // *2022 Systems of Signals Generating and Processing in the Field of on Board Communications*. DOI 10.1109/IEEECONF53456.2022.9744337.

39. Zegzhda, P.D. Set-theoretic model of data poisoning attack techniques in artificial intelligence systems / N. V. Gololobov, D. P. Zegzhda // *Problems of information security. Computer systems.* - 2023. - No. S2 (55). - P. 120-129. - DOI 10.48612/jisp/9agd-pe6p-b82a. (In Russian)
40. Zatsarinny A.A., Ionenkov Y.S. Some methodological aspects of the choice of performance indicators of information systems. *High availability systems*, 2019, vol. 15, № 4. – P. 19-26. – DOI 10.18127/j20729472-201904-03. (In Russian)
41. Epifanov V.V., Vizgalin S.E., Statenin A.O. Justification of quality indicators in the operating system of an unmanned vehicle. *The world of transport and technological machines.* 2025, № 1-2(88), P. 114-118. – DOI 10.33979/2073-7432-2025-1-2(88)-114-118. (In Russian)
42. Mitryaev, I. S. Aspects of the efficiency of intelligent transport systems. *The world of transport and technological machines.* 2024, № 4-3(87), P. 89-95. – DOI 10.33979/2073-7432-2024-4-3(87)-89-95. (In Russian)
43. Kalashnikov, A. O. About the single system of protection classes elements of critical information infrastructure by the criteria of importance and information security / A. O. Kalashnikov, I. F. Mikhalevich // *International Journal of Engineering and Technology(UAE).* – 2018. – Vol. 7, No. 2. – P. 247-250. – DOI 10.14419/ijet.v7i2.23.11952.
44. Mikhalevich I.F. Matters of trusted development framework creation and implementation of intelligent water transportation systems. *Dependability* 2025;2:39-47. [https:// doi.org/10.21683/1729-2646-2025-25-2-39-47](https://doi.org/10.21683/1729-2646-2025-25-2-39-47). (In Russian)
45. Nkoro E.C., Njoku J.N., Nwakanma C.I., Lee J.-M., Kim D.-S. Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach. *Electronics* 2024, 13, 276. URL: <https://doi.org/10.3390/electronics13020276>.
46. Nwakanma C.I., Ahakonye L.A.C., Njoku J.N.; Odirichukwu J.C., Okolie S.A. Uzundu C., Ndubuisi Nweke C.C., Kim D.-S. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review. *Appl. Sci.* 2023, 13, 1252. doi.org/10.3390/app13031252.
47. Bolbot, V.; Sandru, A.; Saarniniemi, T.; Puolakka, O.; Kujala, P.; Valdez Banda, O.A. Small Unmanned Surface Vessels—A Review and Critical Analysis of Relations to Safety and Safety Assurance of Larger Autonomous Ships. *J. Mar. Sci. Eng.* 2023, 11, 2387. URL: [doi.org/10.3390/jmse11122387](https://doi.org/10.3390/jmse11122387).
48. Raheman, F. (2024) From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. *Journal of Computer and Communications*, 12, 252-282. URL: doi: 10.4236/jcc.2024.123016.
49. Fabro, M., Gorski, E., Spiers, N., Diedrich, J., Kuipers, D.: Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies. DHS Industrial Control Systems Cyber Emergency Response Team, (2016). URL: <https://www.hsd.org/c/view?docid=797585>.
50. Zero Trust Strategy and Roadmap. US Department of Defense Releases Nov. 22, 2022 URL: <https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/>.
51. Zero Trust. Maturity Model. April 2023. Version 2.0. Cybersecurity and Infrastructure Security Agency. Cybersecurity Division. URL: [https://www.cisa.gov/sites/default/files/2023-04/CISA\\_Zero\\_Trust\\_Maturity\\_Model\\_Version\\_2\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf).