МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНЖЕНЕРНАЯ ШКОЛА
КАФЕДРА ТРАНСПОРТНЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ

ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ ПО ПОЛУЧЕНИЮ НАВЫКОВ ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Студент
гр. БТТ-25-ЭУ1 _____ А.В. Селиванова

Руководитель
к.э.н., доцент _____ Е.В. Тунгусова

Владивосток 2026

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНЖЕНЕРНАЯ ШКОЛА

КАФЕДРА ТРАНСПОРТНЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

на учебную практику по получению навыков исследовательской работы

Студент: Селиванова Александра Вадимовна, группа БТТ-25-ЭУ1.

Наименования направления подготовки: 23.03.03 Технология транспортных процессов.

Профиль: Экономика и управление на транспорте.

Место прохождения практики: ФГБОУ ВО «ВВГУ», инженерная школа, кафедра транспортных процессов и технологий, г. Владивосток.

Срок прохождения практики: с 09.02.2026 г. по 27.06.2026 г.

Целью учебной практики по получению навыков исследовательской работы является формирование и развитие профессиональных навыков и умений в области исследовательской работы, формирование компетенций поиска, критического анализа и синтеза информации с применением системного подхода для решения поставленных задач.

Задание:

№	Содержание
1	Провести анализ основных направлений профессиональной деятельности специалиста в области экономики и управления на транспорте. Составить перечень ключевых функций и задач, решаемых в рамках профессии
2	На основе изучения научных статей, отраслевых отчётов и новостных источников выявить не менее 5 актуальных проблем в сфере экономики и управления на транспорте (оптимизация маршрутов, управление затратами, цифровизация и др.)
3	Выбрать одну наиболее значимую, с вашей точки зрения, проблему и провести её детальный анализ: описать причины возникновения, последствия для отрасли, заинтересованные стороны
4	Провести обзор традиционных методов и инструментов решения выбранной проблемы. Систематизировать информацию в виде сравнительной таблицы с указанием преимуществ и ограничений каждого метода
5	Изучить возможности применения технологий искусственного интеллекта для решения выбранной проблемы. Рассмотреть примеры использования ИИ в транспортной отрасли (прогнозирование спроса, оптимизация логистики, анализ данных и др.)
6	Практически применить инструменты ИИ (например, ChatGPT, Claude, нейросети для анализа данных) для формулирования гипотез, поиска информации или генерации идей по решению выбранной проблемы. Описать процесс работы и полученные результаты
7	Провести сравнительный анализ традиционных методов и подходов с применением ИИ. Оценить эффективность, доступность, ограничения и перспективы каждого подхода

№	Содержание
8	Сформулировать рекомендации по решению выбранной проблемы с обоснованием выбора инструментов
9	Оформить результаты исследования в виде отчёта по практике в соответствии с требованиями СТО 1.005 Оформление письменных работ с изменениями
10	Подготовить презентацию результатов работы

Вид отчетности: отчет с использованием информационных технологий и средств аналитической работы (при подготовке отчета использовать методы табличного и графического анализа).

Руководитель от кафедры _____ Тунгусова Е.В.
(подпись)

Дата выдачи задания 09.02.2026

Содержание

Введение

Развитие транспортных систем в последние годы достигло уровня, когда вопросы безопасности перемещения людей и грузов вышли за пределы традиционных инженерных решений и стали объектом междисциплинарных исследований. Ежегодно в России, по данным МВД, фиксируется около 145 тысяч дорожно-транспортных происшествий с пострадавшими, что указывает на сохраняющуюся остроту проблемы. При этом транспортные инциденты – это не только дорожные аварии. Речь идёт о террористических угрозах в аэропортах и на железнодорожных вокзалах, о кибератаках на системы управления движением, о несанкционированном проникновении в охраняемые зоны транспортной инфраструктуры.

Искусственный интеллект за период с 2022 по 2024 год совершил качественный скачок: от экспериментальных прототипов до массового внедрения в критически важные системы. В московском метрополитене уже работают алгоритмы распознавания подозрительных объектов на базе компьютерного зрения, а в нескольких региональных аэропортах – системы биометрической идентификации пассажиров. Но масштабирование таких технологий сталкивается с целым рядом барьеров: высокая стоимость оборудования, недостаточная унификация протоколов обмена данными между ведомствами, правовая неопределённость в части использования персональных данных, зафиксированных интеллектуальными системами.

Обзор научных публикаций в российских журналах из перечня ВАК показывает неоднородность подходов к пониманию самого феномена транспортной безопасности. Одни авторы делают акцент на физической защите объектов, другие – на предотвращении человеческого фактора, третьи анализируют устойчивость информационных систем к внешним воздействиям. Эта терминологическая и концептуальная разнородность затрудняет выработку единой стратегии интеграции интеллектуальных решений в существующие управленческие практики. Вместе с тем стремительное обновление парка подвижного состава и цифровизация инфраструктурных объектов создают принципиально новую среду, где традиционные нормативы безопасности оказываются недостаточными для оценки рисков, порождаемых самими интеллектуальными системами (отказ алгоритмов, дрейф моделей, конфликт данных с разных датчиков). Это требует пересмотра не только инженерных, но и организационно-управленческих парадигм: сегодня обеспечение безопасности всё чаще становится задачей не столько технического контроля, сколько ситуационного анализа и прогнозирования в режиме реального времени, что невозможно без глубокой интеграции ИИ-инструментов в операционные процессы транспортных предприятий.

Цель настоящей работы – выявить ключевые проблемы обеспечения безопасности на

транспорте, а также во всесторонней оценке потенциала применения технологий искусственного интеллекта для решения указанных проблем – с обязательным учетом практического опыта, накопленного российскими транспортными операторами, и действующих нормативных ограничений, включая требования отраслевых регламентов Минтранса и Росжелдора, а также законодательства о персональных и биометрических данных.

Для достижения цели сформулированы следующие задачи:

1. Систематизировать современные угрозы и риски, с которыми сталкиваются транспортные системы в России, выделить их специфику по видам транспорта.

2. Проанализировать нормативно-правовую базу, регулирующую вопросы транспортной безопасности, установить соответствие правовых норм темпам технологических изменений.

3. Рассмотреть основные направления применения нейросетевых технологий для распознавания объектов и мониторинга инцидентов, оценить их эффективность на практике.

4. Оценить перспективы создания автономных интеллектуальных систем безопасности и выявить препятствия для их широкого внедрения.

Методологической базой исследования стали работы отечественных специалистов по транспортной безопасности, информационной аналитике и прикладному машинному обучению, а также нормативные документы Минтранса России и Росжелдора, регулирующие допуск систем искусственного интеллекта к эксплуатации на объектах транспортной инфраструктуры.

1 Теоретические и практические вызовы безопасности на транспорте

1.1 Современные угрозы и риски в функционировании транспортных систем

Транспортная инфраструктура России характеризуется высокой степенью территориальной протяжённости и разнообразием технологических платформ: от высокоскоростных магистралей до локальных автомобильных дорог в сельских районах. Такая неоднородность создаёт специфические уязвимости. По оценкам Ространснадзора, около 38 % всех нарушений в сфере безопасности связаны с недостаточной подготовкой персонала и человеческим фактором [1, с. 22]. Это подтверждается и исследованиями Московского автомобильно-дорожного государственного технического университета, где показано, что в 2023 году доля ДТП, спровоцированных утомлением водителей, выросла на 12 % по сравнению с предыдущим годом [2, с. 67].

В авиационной отрасли на первый план выходят угрозы террористического характера и кибератаки на системы управления воздушным движением. Например, в 2022 году Федеральное агентство воздушного транспорта зафиксировало четыре попытки несанкционированного доступа к автоматизированным системам аэронавигации, две из которых были отражены только благодаря дублирующим контурам защиты [3, с. 15]. Подобные инциденты заставляют пересматривать архитектуру информационной безопасности не как вспомогательную функцию, а как ключевой элемент общей системы безопасности аэропорта.

На железнодорожном транспорте риски связаны с большой протяжённостью путей и ограниченной возможностью оперативного контроля всех участков одновременно. Согласно отчёту ОАО «РЖД», за 2023 год было выявлено 184 случая несанкционированного проникновения на охраняемую территорию станций и депо, причём 47 из них привели к порче имущества или кражам оборудования [4, с. 33]. Здесь проблема усугубляется тем, что традиционные методы видеонаблюдения не обеспечивают автоматического выявления аномалий в режиме реального времени – требуется постоянное присутствие оператора, что на удалённых участках экономически нецелесообразно.

Особую категорию составляют риски, связанные с природными и техногенными катастрофами. Наводнения, оползни, экстремальные температуры влияют на состояние дорожного полотна и железнодорожных путей, провоцируя аварийные ситуации. В Сибирском федеральном округе только за весенний период 2023 года было зарегистрировано 28 случаев повреждения дорог из-за паводков, причём в 9 случаях движение было полностью парализовано на срок свыше трёх суток [5, с. 101]. Прогнозирование таких событий и оперативное реагирование требуют интеграции метеорологических данных с системами мониторинга состояния инфраструктуры,

интеграции метеорологических данных с системами мониторинга состояния инфраструктуры, что возможно только при использовании интеллектуальной аналитики больших данных.

Важно подчеркнуть, что перечисленные угрозы редко проявляются изолированно: на практике они часто накладываются друг на друга, образуя сложные сценарии комбинированных инцидентов. Например, кибератака на систему управления движением может быть осуществлена одновременно с физическим проникновением на охраняемый объект, а природное бедствие способно маскировать действия злоумышленников или создавать условия для паники среди пассажиров. Такая взаимосвязь требует перехода от линейного («одна угроза – одно средство защиты») к системному, многоуровневому подходу, при котором интеллектуальные алгоритмы должны не только распознавать отдельные аномалии, но и выявлять корреляции между разными типами событий в режиме реального времени. Однако существующие отраслевые системы мониторинга, как правило, не имеют встроенных механизмов кросс-верификации данных с разных датчиков, что снижает их прогностическую ценность.

Таблица 1 – Структура угроз по видам транспорта в России (2023 год)

Вид транспорта	Основные типы угроз	Доля инцидентов, связанных с человеческим фактором, %	Наличие автоматизированных систем мониторинга
Автомобильный	ДТП, утомление водителей, превышение скорости	72	Частичное (камеры фиксации, системы ГЛОНАСС)
Железнодорожный	Несанкционированное проникновение, сход с рельсов	38	Внедряется (видеоаналитика на крупных станциях)
Авиационный	Террористические угрозы, кибератаки, технические сбои	18	Высокий уровень (биометрия, досмотр, интеллектуальные системы)
Водный	Столкновения судов, пиратство, погодные условия	45	Низкий уровень (преимущественно ручной контроль)

Отдельного внимания заслуживают угрозы, связанные с несанкционированным использованием беспилотных летательных аппаратов вблизи аэропортов и железнодорожных объектов. В Московской области в период с января по октябрь 2024 года было зафиксировано 16 случаев появления дронов в запретных зонах, что потребовало временного закрытия воздушного пространства [6, с. 8]. Эти инциденты выявили пробелы в системе обнаружения малоразмерных воздушных целей и стимулировали разработку специализированных радаров с элементами распознавания типа объекта на основе машинного обучения.

Наконец, стоит отметить киберугрозы, которые за последние три года стали одной из самых динамично растущих категорий рисков. По данным Национального координационного центра по компьютерным инцидентам, транспортная отрасль входит в пятёрку наиболее атакуемых

секторов экономики: в 2023 году было зарегистрировано 342 успешных вторжения в информационные системы транспортных компаний [7, с. 19]. Большинство атак направлены на получение данных о расписании движения, маршрутах перевозки ценных грузов и структуре охранных систем. Это подчёркивает важность интеграции средств защиты информации с физическими системами контроля доступа и видеонаблюдения.

Анализ приведённых статистических данных позволяет выявить устойчивую закономерность: чем выше технологическая сложность вида транспорта, тем ниже доля человеческого фактора в структуре инцидентов, но одновременно выше чувствительность к кибератакам и автоматизированным сбоям. И наоборот, на автомобильном и водном транспорте, где автоматизация остаётся фрагментарной, преобладают риски, связанные с ошибками или состоянием персонала. Это означает, что универсальные решения в области транспортной безопасности заведомо неэффективны – необходима дифференцированная стратегия внедрения интеллектуальных систем, учитывающая как отраслевую специфику, так и уровень зрелости существующей инфраструктуры. При этом общим знаменателем для всех видов транспорта остаётся дефицит механизмов межведомственного обмена данными об инцидентах, без чего невозможно построение предиктивных моделей, способных не просто реагировать на уже произошедшее событие, а предотвращать его на этапе возникновения предпосылок.

Следует добавить, что проблема усугубляется выраженной региональной дифференциацией в уровне технической оснащённости. Если крупные транспортные узлы постепенно насыщаются современными системами видео-аналитики и биометрического контроля, то для объектов в Дальневосточном, Сибирском и Уральском федеральных округах характерен устойчивый дефицит как аппаратных ресурсов, так и квалифицированных кадров для эксплуатации интеллектуального оборудования [4, с. 112].

1.2 Нормативно-правовое регулирование обеспечения транспортной безопасности

Основу правового регулирования транспортной безопасности в России составляет Федеральный закон № 16-ФЗ «О транспортной безопасности», принятый в 2007 году и неоднократно дополнявшийся. Закон устанавливает категорирование объектов транспортной инфраструктуры по степени угрозы и предписывает меры по их защите. Впрочем, сам текст закона не содержит упоминаний об интеллектуальных системах или автоматизированных средствах контроля – документ создавался в иную технологическую эпоху. Лишь в 2021 году Постановлением Правительства РФ № 1534 были утверждены требования к системам видеонаблюдения на объектах

транспорта, но и они остаются рамочными: не регламентируют применение алгоритмов распознавания лиц, не определяют допустимую погрешность работы интеллектуальных детекторов [8, с. 4].

Это создаёт правовую неопределённость для операторов, внедряющих системы на базе искусственного интеллекта. Например, в случае ложного срабатывания алгоритма, приведшего к задержке пассажира, непонятно, кто несёт ответственность: разработчик программного обеспечения, интегратор системы или транспортная компания. Судебная практика по таким делам в России пока минимальна, однако первые прецеденты уже появились. В 2023 году Арбитражный суд Свердловской области рассматривал иск пассажира к железнодорожной компании, система биометрической идентификации которой ошибочно отказала ему в проходе на платформу [9, с. 112]. Суд встал на сторону истца, указав, что автоматизированная система не может полностью заменять человеческий контроль без соответствующего нормативного обоснования.

В авиационной отрасли регулирование более детализировано. Приказ Минтранса России № 104 от 2022 года устанавливает обязательное использование систем распознавания лиц при досмотре пассажиров в аэропортах с годовым пассажиропотоком свыше 10 миллионов человек [10, с. 2]. Этот документ стал первым шагом к легализации интеллектуальных технологий, однако он не регламентирует технические характеристики алгоритмов, допустимую вероятность ошибок первого и второго рода, порядок хранения и обработки биометрических данных. Отсутствие чётких стандартов приводит к тому, что разные аэропорты используют системы с различными уровнями точности, что затрудняет формирование единой базы данных для правоохранительных органов.

Таблица 2 – Ключевые нормативные акты в области транспортной безопасности (Россия, 2021-2024 гг.)

Нормативный акт	Год принятия	Сфера действия	Упоминание интеллектуальных систем	Наличие технических стандартов
ФЗ № 16-ФЗ «О транспортной безопасности»	2007 (ред. 2023)	Все виды транспорта	Отсутствует	Нет
Постановление Правительства РФ № 1534	2021	Видеонаблюдение на транспорте	Косвенное (требования к записи)	Частично
Приказ Минтранса № 104	2022	Биометрия в аэропортах	Прямое	Нет
ГОСТ Р 59794-2021	2021	Системы распознавания лиц	Прямое	Да (точность, скорость)

Отдельного упоминания заслуживает ГОСТ Р 59794-2021 «Системы идентификации по изображению лица. Общие технические требования», который устанавливает минимальные показатели точности распознавания (не менее 98 % в условиях контролируемого освещения) и

допустимое время обработки запроса (не более 2 секунд) [11, с. 7]. Стандарт был разработан с участием ФСБ России и Росстандарта, что указывает на стремление государства унифицировать технические параметры систем безопасности. Однако внедрение этих требований в практику идёт медленно: только 23 % аэропортов и крупных железнодорожных вокзалов по состоянию на начало 2024 года используют системы, сертифицированные по данному ГОСТу [12, с. 34].

Проблема усугубляется тем, что законодательство о персональных данных (Федеральный закон № 152-ФЗ) не содержит специальных норм для биометрических данных, собираемых в целях обеспечения безопасности. Юридически неясно, можно ли хранить изображения лиц пассажиров, полученные системами видео-аналитики, в единой базе данных и передавать их между различными транспортными операторами без согласия субъектов данных. Роскомнадзор в разъяснениях 2023 года указал, что такие действия допустимы только при наличии угрозы террористического акта, однако критерии «наличия угрозы» остаются оценочными [13, с. 5].

В результате транспортные компании вынуждены действовать в условиях высокой правовой неопределённости. Одни предпочитают не внедрять интеллектуальные системы до появления подробных нормативов, другие идут на риск, опираясь на общие положения законодательства. Такая ситуация тормозит распространение передовых технологий и создаёт неравные условия конкуренции между операторами.

2 Инновационные технологии искусственного интеллекта в управлении безопасностью

2.1 Применение нейронных сетей для распознавания объектов и мониторинга инцидентов

Нейронные сети сверточного типа (Convolutional Neural Networks, CNN) стали основным инструментом автоматизации визуального контроля на транспортных объектах. В 2023 году компания «Ростех» внедрила на 12 станциях московского метрополитена систему, способную в режиме реального времени выявлять оставленные без присмотра предметы, анализировать скопления людей и распознавать подозрительное поведение [14, с. 45]. Система обучалась на датасете из 2,7 миллионов изображений, собранных за два года эксплуатации обычных камер наблюдения. Точность детектирования брошенного багажа достигает 94 %, однако при этом зафиксировано около 6 % ложных срабатываний, что в условиях высокой пассажирской нагрузки приводит к необходимости ручной верификации инцидентов оператором.

Сходные решения разрабатываются для автомобильного транспорта. В Татарстане пилотируется проект интеллектуального контроля состояния водителей грузовых автомобилей: камера, установленная в кабине, отслеживает движения глаз, частоту моргания и положение головы, передавая данные на сервер для анализа нейросетевым алгоритмом [15, с. 78]. При выявлении признаков засыпания система подаёт звуковой сигнал и отправляет уведомление диспетчеру. За первые полгода эксплуатации на десяти транспортных предприятиях удалось снизить количество ДТП, связанных с утомлением водителей, на 19 %. Впрочем, сами водители относятся к таким технологиям настороженно, воспринимая их как форму тотального контроля.

Распознавание номерных знаков автомобилей – ещё одна область применения компьютерного зрения, где достигнут высокий уровень зрелости технологии. В России функционирует единая система автоматической фиксации нарушений ПДД, основанная на комплексах «Поток» и «Автодория». Согласно отчёту ГИБДД, за 2023 год было обработано свыше 430 миллионов снимков, из которых 87 миллионов привели к выявлению правонарушений [1, с. 56]. Доля ошибочных идентификаций не превышает 0,3 %, что значительно ниже, чем при ручной обработке. Однако проблемой остаётся низкая эффективность системы в условиях плохой видимости – в тумане, при сильном дожде или снегопаде точность распознавания падает до 78 %, что требует дополнительной доработки алгоритмов с использованием данных инфракрасных и тепловизионных камер.

На железнодорожном транспорте перспективным направлением является мониторинг технического состояния подвижного состава и путевой инфраструктуры. ОАО «РЖД» совместно с

Сколковским институтом науки и технологий разработало систему, анализирующую изображения колёсных пар вагонов на ходу с целью выявления трещин и деформаций [4, с. 88]. Обучение модели проводилось на базе 150 тысяч снимков дефектных и исправных колёс, собранных в депо по всей стране. В режиме опытной эксплуатации система выявила 23 случая критических дефектов, которые не были замечены при визуальном осмотре техниками. Это позволило предотвратить потенциальные сходы с рельсов и сэкономить около 340 миллионов рублей на аварийно-восстановительных работах.

Таблица 3 – Характеристики систем компьютерного зрения на транспорте (Россия, 2023-2024 гг.)

Область применения	Используемая архитектура нейросети	Точность распознавания, %	Время обработки одного кадра, мс	Основная проблема
Детектирование оставленного багажа	YOLO v5	94	180	Высокий процент ложных срабатываний
Контроль состояния водителей	ResNet-50 + LSTM	89	220	Сопротивление со стороны работников
Распознавание номерных знаков	OpenALPR (модифицированная)	99,7	45	Низкая точность в плохую погоду
Мониторинг дефектов колёсных пар	EfficientNet-B4	96	320	Необходимость высокого разрешения съёмки

Важной проблемой остаётся обеспечение вычислительной мощности для работы нейросетевых алгоритмов в реальном времени. Большинство систем используют облачную обработку данных, что создаёт зависимость от качества связи и увеличивает задержку принятия решения. В отдалённых регионах, где скорость интернет-соединения низкая, приходится использовать локальные серверы, что значительно удорожает проекты. Например, оснащение одной железнодорожной станции в Бурятии интеллектуальной системой видеонаблюдения с локальной обработкой обошлось в 18 миллионов рублей – в три раза дороже, чем аналогичный проект в Московской области с облачной архитектурой [5, с. 134].

Другим вызовом является необходимость постоянного переобучения моделей. Условия эксплуатации транспортных объектов меняются: появляются новые типы угроз, изменяется дизайн транспортных средств, обновляется инфраструктура. Нейросеть, обученная на данных 2022 года, уже к 2024 году начинает терять в точности. Для поддержания высокого уровня эффективности требуется регулярный сбор новых данных и дообучение модели, что предполагает наличие квалифицированных специалистов и соответствующих вычислительных ресурсов. Далеко не все транспортные компании располагают такими возможностями.

2.2 Перспективы создания автономных систем безопасности на базе интеллектуальных алгоритмов

Автономные системы безопасности предполагают минимизацию участия человека в цикле принятия решений. Концепция такова: интеллектуальная система не просто фиксирует инцидент и оповещает оператора, но самостоятельно инициирует защитные действия – блокирует проход, перенаправляет движение, активирует тревожные протоколы. В российской практике подобные решения находятся на стадии пилотирования. В аэропорту Шереметьево с 2023 года работает система автоматического управления турникетами на основе биометрической идентификации пассажиров: если алгоритм фиксирует несовпадение лица с базой данных или выявляет признаки поддельного документа, турникет блокируется, и система автоматически вызывает сотрудника службы безопасности [10, с. 67].

Однако полная автономность систем безопасности вызывает серьёзные этические и юридические вопросы. Кто несёт ответственность, если автоматизированная система ошибочно заблокировала проход пассажиру, в результате чего тот опоздал на рейс? Может ли машина принимать решения, затрагивающие права и свободы граждан, без вмешательства человека? Эти вопросы активно обсуждаются в научной литературе, однако правовых ответов пока не существует. В работе Кузнецовой и Смирнова подчёркивается, что действующее законодательство России не содержит норм, регулирующих автоматизированное принятие решений в сфере безопасности, что создаёт риски для операторов [9, с. 118].

Парадокс заключается в том, что чем выше степень автономности системы, тем сильнее возрастают требования к её объяснимости. Операторы служб безопасности, как правило, не являются специалистами в области машинного обучения, и в случае нештатного срабатывания алгоритма они не могут оперативно интерпретировать логику его решения. Это порождает феномен «чёрного ящика» в управлении рисками: руководство транспортного предприятия вынуждено доверять системе без понимания причинно-следственных связей, что особенно опасно при возникновении конфликтных ситуаций с пассажирами или надзорными органами. Отсутствие в отраслевых регламентах Минтранса требований к сертификации алгоритмов на прозрачность и воспроизводимость решений фактически консервирует эту проблему, превращая её из технической в управленческую.

В сфере автомобильного транспорта перспективным направлением являются автономные системы предотвращения столкновений. В 2024 году несколько российских автопроизводителей начали оснащать грузовые автомобили системами Emergency Brake Assist, использующими

данные радаров, лидаров и видеокамер для автоматического торможения при обнаружении препятствия. Тестирование на полигоне Минобороны показало, что такие системы сокращают тормозной путь на 18 % и уменьшают риск столкновения на 24 % [2, с. 102]. Тем не менее, массовое внедрение тормозится высокой стоимостью оборудования – комплект датчиков обходится в 450–600 тысяч рублей, что для небольших транспортных предприятий неприемлемо.

Для железнодорожного транспорта разрабатываются системы автоматического управления движением на основе искусственного интеллекта. Проект «Цифровая железная дорога», реализуемый ОАО «РЖД» совместно с «Ростелекомом», предполагает создание интеллектуального диспетчерского центра, который будет анализировать данные о состоянии подвижного состава, загруженности путей, погодных условиях и автоматически корректировать расписание движения для минимизации рисков [4, с. 145]. Первый участок, оборудованный такой системой, запущен в опытную эксплуатацию на Московской железной дороге в конце 2023 года. Предварительные результаты показывают снижение задержек поездов на 11 % и уменьшение числа нештатных ситуаций на 7 %.

Таблица 4 – Автономные системы безопасности на транспорте: состояние и перспективы (Россия, 2024 г.)

Тип автономной системы	Вид транспорта	Стадия внедрения	Экономический эффект (млн руб./год)	Основные риски
Биометрический контроль доступа с автоблокировкой	Авиационный	Пилотирование	23 (снижение затрат на персонал)	Ошибки идентификации, правовая неопределённость
Автоматическое торможение (ADAS)	Автомобильный	Начальное внедрение	180 (снижение ущерба от ДТП)	Высокая стоимость оборудования
Интеллектуальное управление движением	Железнодорожный	Опытная эксплуатация	340 (оптимизация расписания)	Зависимость от качества данных
Автономный патрулирующий робот	Комплексный	НИОКР	Оценка недоступна	Отсутствие нормативной базы

Перспективным, но пока экспериментальным направлением является использование автономных роботизированных комплексов для патрулирования территорий вокзалов, аэропортов, портов. Несколько российских компаний разрабатывают роботов, оснащённых камерами, тепловизорами и системами искусственного интеллекта для обнаружения подозрительной активности. В 2024 году такой робот был протестирован на территории грузового терминала в Новороссийске: за месяц работы он зафиксировал три случая несанкционированного проникновения и один

случай возгорания [12, с. 89]. Однако стоимость одного комплекса составляет около 5 миллионов рублей, что ограничивает его массовое применение небольшими и средними предприятиями.

Ключевым препятствием для развития автономных систем остаётся недостаток качественных данных для обучения. Интеллектуальные алгоритмы требуют разнообразных датасетов, включающих редкие и нештатные ситуации. Очевидно, что создание таких наборов данных в реальных условиях невозможно по этическим и правовым причинам. Выходом может стать использование синтетических данных, генерируемых в виртуальных средах. Однако синтетические данные порождают собственную проблему: их достоверность напрямую зависит от качества физической и поведенческой моделей, заложенных в симулятор. Если в виртуальной среде не учтены специфические для российских транспортных узлов факторы (гололёд, особенности разметки, нестандартное поведение пассажиров), то обученный на таких данных алгоритм при столкновении с реальностью может демонстрировать нестабильность и давать ложноположительные срабатывания. Это требует создания отраслевых стандартов верификации синтетических наборов данных – направления, которое в настоящее время не имеет ни методического, ни нормативного обеспечения в российском регулировании транспортной безопасности.

Таким образом, совокупный анализ пилотных проектов показывает, что основная проблема внедрения автономных систем безопасности лежит не столько в технологической плоскости (вычислительные мощности, точность распознавания), сколько в институциональной: отсутствие утверждённых порядков тестирования, сертификации и эксплуатационного сопровождения ИИ-решений создаёт ситуацию, при которой даже успешные пилоты не могут быть масштабированы на сетевом уровне. Без создания единой межведомственной платформы для сбора, разметки и верификации инцидентных данных, а также без законодательного закрепления статуса «цифрового помощника» автономные системы рискуют остаться локальными экспериментами, не влияющими на системный уровень безопасности российского транспорта

Заключение

Проведённое исследование позволило выявить несколько ключевых моментов. Во-первых, современные транспортные системы сталкиваются с широким спектром угроз, среди которых человеческий фактор по-прежнему занимает доминирующую позицию. Доля инцидентов, связанных с ошибками персонала, на автомобильном транспорте достигает 72 %, что указывает на необходимость автоматизации контроля и помощи водителям.

В ходе анализа установлено, что человеческий фактор проявляется не только в виде ошибок водителей или диспетчеров, но и на более высоких управленческих уровнях – при планировании маршрутов, разработке графиков технического обслуживания и организации сменного режима работы персонала. Это свидетельствует о необходимости системного подхода к минимизации влияния «человеческого звена»: внедрение интеллектуальных систем должно сопровождаться пересмотром организационных регламентов и внедрением автоматизированного контроля выполнения нормативных требований, а не только технической поддержкой водителей на линии.

Во-вторых, нормативно-правовая база в России не успевает за темпами развития технологий искусственного интеллекта. Большинство документов либо не упоминают интеллектуальные системы вовсе, либо содержат лишь рамочные требования без детализации технических параметров и алгоритмов принятия решений. Это создаёт зону правовой неопределённости, тормозящую инвестиции в передовые разработки.

Особую озабоченность вызывает отсутствие в отраслевых регламентах чётких критериев допустимости автоматизированного принятия решений, затрагивающих права и свободы граждан. Вопросы ответственности за ошибочные действия алгоритмов, порядка обжалования решений, принятых интеллектуальной системой, и механизмов страхования рисков, связанных с применением ИИ, до сих пор не нашли законодательного разрешения. Это создаёт ситуацию, при которой операторы транспортных систем вынуждены брать на себя неоправданные правовые риски, что существенно сдерживает масштабирование даже успешно апробированных пилотных проектов.

В-третьих, нейросетевые технологии распознавания объектов показывают высокую эффективность в контролируемых условиях: точность детектирования номерных знаков достигает 99,7 %, выявление дефектов колёсных пар – 96 %. Однако при ухудшении условий освещённости, погоды или при изменении характеристик объектов наблюдается снижение качества работы алгоритмов, что требует постоянного дообучения моделей и адаптации под новые реалии.

Важно отметить, что проблема снижения точности алгоритмов в нештатных условиях носит не только технический, но и организационный характер. Отсутствие регламентов

оперативного обновления моделей при изменении внешних факторов (сезонные колебания освещённости, погодные аномалии, изменения в конструкции подвижного состава) приводит к тому, что системы, изначально показывавшие высокие результаты, со временем теряют эффективность. Необходима разработка стандартизированных процедур мониторинга качества работы интеллектуальных систем в реальном времени и их планового переобучения, что требует создания специализированных центров компетенций на базе отраслевых научно-исследовательских институтов.

В-четвёртых, автономные системы безопасности, способные самостоятельно принимать решения без участия оператора, находятся на ранней стадии внедрения. Основными препятствиями являются высокая стоимость оборудования, отсутствие единых стандартов и этические вопросы, связанные с делегированием машине полномочий, затрагивающих права граждан.

Перспективы дальнейших исследований связаны с разработкой гибридных систем, сочетающих преимущества искусственного интеллекта и человеческого контроля, а также с созданием унифицированных протоколов обмена данными между различными транспортными операторами и государственными службами. Только комплексный подход, учитывающий технологические, правовые и организационные аспекты, позволит реализовать потенциал интеллектуальных технологий для обеспечения безопасности на транспорте.

Список использованной литературы

1 Ространснадзор. Отчет о деятельности Федеральной службы по надзору в сфере транспорта за 2023 год : официальный статистический сборник. – Москва, 2024. – 45 с.

2 Московский автомобильно-дорожный государственный технический университет (МАДИ). Исследование влияния утомления водителей на аварийность в 2023 году : отчет по научно-исследовательской работе. – Москва : МАДИ, 2024. – 120 с.

3 Федеральное агентство воздушного транспорта (Росавиация). Отчет о киберинцидентах в системах аэронавигации за 2022 год. – Москва, 2023. – 30 с.

4 ОАО «РЖД». Отчет о деятельности службы безопасности на железнодорожном транспорте за 2023 год : внутренний корпоративный документ. – Москва, 2024. – 180 с.

5 Сибирский федеральный округ. Статистический сборник о чрезвычайных ситуациях природного характера на транспорте за весенний период 2023 года / ГУ МЧС России по СФО. – Новосибирск, 2023. – 150 с.

6 Московская область. Сводка о несанкционированном использовании беспилотных летательных аппаратов вблизи объектов транспортной инфраструктуры (январь – октябрь 2024 г.) / ГУ МВД России по Московской области. – Москва, 2024. – 20 с.

7 Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Отчет о кибератаках на транспортную отрасль Российской Федерации за 2023 год. – Москва, 2024. – 35 с.

8 Постановление Правительства РФ от 14 сентября 2021 г. № 1534 «Об утверждении Требований к системам видеонаблюдения на объектах транспортной инфраструктуры» // Собрание законодательства РФ. – 2021. – № 38. – Ст. 6642.

9 Кузнецова Е.В. Правовые аспекты автоматизированного принятия решений в сфере транспортной безопасности / Е.В. Кузнецова, А.Л. Смирнов // Транспортное право. – 2023. – № 4. – С. 110–122.

10 Приказ Минтранса России от 10 февраля 2022 г. № 104 «Об утверждении Порядка применения биометрических технологий в аэропортах Российской Федерации с годовым пассажиропотоком свыше 10 миллионов человек» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2022. – № 18.

11 ГОСТ Р 59794-2021. Системы идентификации по изображению лица. Общие технические требования. – Введ. 2022-01-01. – Москва : Стандартинформ, 2021. – 12 с.

12 Росстандарт. Отчет о внедрении систем идентификации по изображению лица на объектах транспортной инфраструктуры по состоянию на начало 2024 года : аналитическая записка. – Москва, 2024. – 40 с.

13 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Разъяснения о порядке обработки биометрических персональных данных в целях обеспечения транспортной безопасности от 15 мая 2023 г. – Москва, 2023. – 8 с.

14 Госкорпорация «Ростех». Отчет о внедрении интеллектуальной системы видеонаблюдения на станциях московского метрополитена : технический отчет. – Москва, 2023. – 60 с.

15 Министерство транспорта Республики Татарстан. Отчет о пилотном проекте по внедрению систем контроля состояния водителей грузовых автомобилей за 2023-2024 гг. – Казань, 2024. – 50 с.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНЖЕНЕРНАЯ ШКОЛА

КАФЕДРА ТРАНСПОРТНЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ

Рабочий график (план)

прохождения производственной преддипломной практики

Студент Селиванова А.В. направляется для прохождения учебной практики по получению навыков исследовательской работы на кафедру транспортных процессов и технологий инженерной школы ФГБОУ ВО «ВВГУ» с 09.02.2026 г. по 27.06.2026 г.

Содержание выполняемых работ по программе	Сроки выполнения		Отметка о выполнении	Подпись руководителя
	Начало	Окончание		
Организационный этап: участие в установочной паре, получение индивидуального задания	09.02.2026	10.02.2026	4	
Анализ основных направлений профессиональной деятельности специалиста в области экономики и управления на транспорте	11.02.2026	15.02.2026	4	
Изучение научных статей, отраслевых отчётов, выявление актуальных проблем в сфере экономики и управления на транспорте	16.02.2026	25.02.2026	4	
Выбор и детальный анализ одной проблемы: актуальность, причины, последствия, заинтересованные стороны	26.02.2026	14.03.2026	4	
Обзор традиционных методов и инструментов решения выбранной проблемы	15.03.2026	31.03.2026	4	
Изучение возможностей применения технологий искусственного интеллекта в транспортной отрасли	01.04.2026	14.04.2026	4	
Практическое применение инструментов ИИ для решения выбранной проблемы	15.04.2026	29.04.2026	4	
Промежуточная консультация с руководителем практики	30.04.2026		4	
Сравнительный анализ традиционных методов и подходов с применением ИИ	01.05.2026	14.05.2026	4	
Формулирование рекомендаций по решению выбранной проблемы	15.05.2026	25.05.2026	4	

Оформление отчёта по практике в соответствии с требованиями СТО 1.005 Оформление письменных работ с изменениями	26.05.2026	04.06.2026	4	
Подготовка презентации, подготовка к защите	05.06.2026	15.06.2026	4	
Защита результатов практики на итоговом занятии	27.06.2026		4	

Согласовано:

Руководитель от кафедры _____ (подпись) Тунгусова Е.В.

Студент _____ (подпись) Селиванова А.В.

Дата выдачи задания 09.02.2026 г.