Раздел 5. ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ ТРАНСПОРТНЫХ СРЕДСТВ

УДК 656.13: 656.25

Харлап Сергей Николаевич, *Белорусский государственный университет транспорта (Беларусь, Гомель), кандидат технических наук, доцент, e-mail: hsn2013@tut.by, 246653, Республика Беларусь, г. Гомель, ул. Кирова, 34*
Конопацкая Анастасия Юрьевна, *ОАО «Конструкторское бюро системного программирования» (Беларусь, Гомель), e-mail: anstsknptsk@gmail.com, 246012, г. Гомель, проспект Речицкий, 135*

ОБЗОР СУЩЕСТВУЮЩИХ МЕТОДОВ ПОВЫШЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

В работе выполнен обзор причин нарушения нормальной работы беспилотных транспортных средств, вызванных некорректной работой систем искусственного интеллекта, а также методов, направленных на повышение их функциональной безопасности. Основное внимание уделяется методам оценки робастности систем искусственного интеллекта в условиях воздействия внешних факторов. Рассмотрены типовые методы оценки робастности, в том числе методы повышения устойчивости систем искусственного интеллекта к воздействию электромагнитных помех.

Ключевые слова: беспилотные транспортные средства; система искусственного интеллекта; функциональная безопасность; робастность.

Беспилотные транспортные средства (БТС) – одна из самых передовых технологий, представляющая собой сложную интеграцию искусственного интеллекта (ИИ), сенсоров и систем управления. Эти системы призваны обеспечить автономное вождение с минимальным вмешательством человека. Однако, несмотря на стремительное развитие, ИИ в беспилотных транспортных средствах подвержен ряду рисков, связанных с отказами. Отказы ИИ могут иметь серьёзные последствия, включая угрозы безопасности участников дорожного движения, повреждения имущества и утрату доверия к технологиям. В данной работе рассматриваются основные причины возникновения отказов ИИ в БТС, их риски, а также способы устранения этих проблем.

Рассмотрим далее основные причины отказов ИИ в беспилотных транспортных средствах.

Ошибки восприятия окружающей среды. ИИ в беспилотных транспортных средствах зависит от множества сенсоров, таких как

камеры, лидары, радары и ультразвуковые датчики, которые собирают информацию о дорожной обстановке. Ошибки в восприятии окружающей среды могут возникать:

– по причинам погодных условий: дождь, снег или туман могут искажать или блокировать сигналы сенсоров, приводя к неверному распознаванию объектов;

– из-за многообразия объектов: сложные или непредсказуемые объекты на дороге, такие как животные или мусор, могут быть неправильно классифицированы системой ИИ;

– из-за сбоев в работе сенсоров: выход из строя или неисправность сенсоров может привести к некорректным данным, что приведет к ошибкам в принятии решений.

Недостатки в алгоритмах принятия решений. Алгоритмы, управляющие движением беспилотных транспортных средств, должны быть высокоэффективными и учитывать множество факторов одновременно.

Технические сбои и отказ оборудования. Ошибки в коде или несовместимость компонентов программного обеспечения могут вызвать отказ в работе системы ИИ. Выход из строя процессоров, оперативной памяти или других критически важных компонентов системы может привести к потере контроля над транспортным средством.

Кибератаки. Беспилотные транспортные средства могут стать целью кибератак, направленных на нарушение работы ИИ. Атаки могут изменить параметры управления транспортным средством или вывести его из строя. Внешние манипуляции с данными, поступающими с сенсоров, например, с помощью лазеров или других устройств, могут нарушить корректное восприятие ИИ окружающей среды.

Функциональная безопасность для ИИ играет ключевую роль в обеспечении корректной и безопасной работы систем, особенно в критических приложениях, таких как беспилотные транспортные средства, медицинские устройства и промышленная автоматизация. Цель функциональной безопасности заключается в предотвращении или смягчении опасных ситуаций, вызванных отказами системы или непредвиденными ошибками, путем реализации мер по снижению рисков.

Функциональная безопасность для ИИ основывается на нескольких ключевых принципах.

Предотвращение отказов системы. ИИ, применяемый в сложных системах, должен быть устойчив к отказам как в аппаратной, так и в программной составляющей. Основная задача функциональной безопасности – минимизация риска возникновения опасных ситуаций в случае сбоя или неправильной работы ИИ.

Моделирование рисков. Для управления рисками, связанными с ИИ, важно идентифицировать все возможные сценарии отказов и опасных ситуаций. Для этого используются методы анализа, такие как: FMEA (Failure Mode and Effects Analysis) – анализ возможных отказов и их последствий; FTA (Fault Tree Analysis) – метод анализа, который помогает идентифицировать основные причины отказов системы.

Устойчивость к непредсказуемым ситуациям. ИИ должен быть спроектирован так, чтобы справляться с неожиданными или нестандартными ситуациями, которые могут возникнуть в реальной жизни. ИИ должен быть обучен на данных, представляющих различные сценарии, включая необычные и опасные ситуации. Система должна адаптироваться к быстро меняющимся условиям, особенно если стандартные алгоритмы не могут дать решение.

Наиболее перспективными направлениями по повышению функциональной безопасности систем искусственного интеллекта являются следующие направления.

Автоматическое обнаружение угроз. Развитие систем автоматического обнаружения угроз (IDS) и систем предупреждения об аномалиях (IPS) для алгоритмов ИИ позволяет оперативно обнаруживать подозрительное поведение и атаки на модели и данные.

Дифференциальная конфиденциальность. Разработка методов дифференциальной конфиденциальности, которые позволяют анализировать данные, не раскрывая личную информацию, что обеспечивает защиту приватности пользователей.

Технологии защиты от уязвимостей. Исследования направлены на разработку методов обнаружения и защиты от уязвимостей в моделях и алгоритмах ИИ, чтобы предотвратить атаки, основанные на выявленных уязвимостях.

Автоматизация безопасности. Разработка инструментов и платформ для автоматического анализа безопасности моделей и алгоритмов ИИ, а также для автоматического внедрения мер безопасности.

Наиболее распространенные ошибки ИИ заключаются в неправильном распознавании окружающей среды, связанном с внешними воздействиями.

Проверка на робастность ИИ для устранения ошибок восприятия окружающей среды является важным шагом в обеспечении надежности и безопасности беспилотных транспортных средств. Под робастностью понимается устойчивость системы к внешним изменениям и возмущениям, которые могут возникать в реальной дорожной среде, включая различные погодные условия, непредсказуемые объекты и искажения данных сенсоров.

Проблемы восприятия окружающей среды. Восприятие окружающей среды является ключевым компонентом работы ИИ в беспилотных транспортных средствах. Ошибки восприятия могут возникать из-за неадекватной обработки данных от сенсоров (камер, лидаров, радаров), неправильного распознавания объектов на дороге, сложных погодных условий (туман, дождь, снег), которые ухудшают видимость, сбоев в работе аппаратуры или программных алгоритмов. Проверка на робастность ИИ заключается в оценке того, как система справляется с этими внешними факторами и насколько устойчиво её поведение в сложных или нестандартных ситуациях.

Рассмотрим типовые методы проверки робастности ИИ:

Моделирование внешних условий. Один из методов проверки робастности заключается в создании симуляций различных внешних условий. В симуляторе можно воспроизвести различные сценарии, включая погодные изменения (снегопад, дождь, густой туман), препятствия на дороге (животные, дорожные работы, разбросанный мусор). ИИ подвергается тестированию в этих условиях, и оценивается его способность правильно идентифицировать объекты и адекватно реагировать на изменения в окружающей среде.

Аугментация данных. Для повышения робастности ИИ применяют аугментацию данных – искусственное создание вариаций исходных данных для обучения. Например, изображение дороги можно обработать для имитации различных погодных условий (дождь, снег) или изменения освещённости (день/ночь). Это помогает ИИ научиться корректно распознавать объекты в различных контекстах и минимизировать вероятность ошибок восприятия.

Тестирование на «загрязнённых» данных. В реальных условиях данные сенсоров могут быть искажены, например, из-за грязи на камерах или осадков на лидарах. Проверка на робастность включает тесты на «загрязнённых» данных – ИИ обучается и тестируется на данных с определёнными искажениями. Это помогает системе развить устойчивость к небольшим потерям или искажениям информации.

Использование конкурирующих моделей. Один из способов устранения ошибок восприятия – применение нескольких параллельных моделей ИИ, каждая из которых анализирует поступающие данные с разных типов сенсоров. Например, лидары могут компенсировать недостатки камер в условиях низкой видимости, и наоборот. Эти модели могут сравнивать свои результаты, повышая общую точность и надёжность системы.

Для устранения ошибок восприятия есть некоторые методы, которые следует детально рассмотреть.

Многосенсорные системы. Надежность восприятия окружающей среды можно улучшить за счёт использования нескольких источников данных: камеры, лидары, радары и ультразвуковые сенсоры. Многосенсорные системы позволяют ИИ компенсировать недостатки одного сенсора данными с другого. Например, лидар может точно определить расстояние до объекта, когда камера не может этого сделать из-за плохой видимости.

Фильтрация и обработка данных. Для устранения ошибок восприятия применяется фильтрация данных, позволяющая отсеивать шумы и искажения. Одним из распространённых методов является фильтр Калмана, который использует поступающие данные для предсказания и корректировки траекторий объектов, помогая уменьшить неопределённость.

Глубокое обучение и регуляризация. Для повышения робастности можно использовать методы глубокого обучения, такие как сверточные нейронные сети (CNN), которые лучше справляются с распознаванием объектов на сложных изображениях. Важно применять методы регуляризации (например, dropout или L2-регуляризация), чтобы избежать переобучения модели на определённых данных и улучшить её способность к обобщению новых ситуаций.

Обратная связь и самообучение. Беспилотные транспортные средства могут быть оборудованы механизмами обратной связи, которые позволяют ИИ обучаться на реальных данных в режиме реального времени. Если система сталкивается с ошибкой в распознавании объекта, она может корректировать свои алгоритмы, улучшая точность работы в будущем.

Проверка на робастность ИИ при воздействии электромагнитных помех (ЭМП) – это важный этап в обеспечении безопасности и надежности работы систем, использующих искусственный интеллект, особенно в критических сферах, таких как беспилотные транспортные средства, авиация, медицина и промышленные устройства. Электромагнитная совместимость (ЭМС) предполагает способность системы нормально функционировать в условиях ЭМП, которые могут возникать как от внешних, так и от внутренних источников.

ИИ-системы, особенно в автономных устройствах, используют множество электронных компонентов, таких как процессоры, сенсоры, антенны, которые могут быть подвержены воздействию электромагнитных полей. Если ИИ-устройства не защищены от электромагнитных помех, это может привести к следующим проблемам: нарушение работы сенсоров и их некорректная интерпретация окружающей среды, сбои в работе ИИ-алгоритмов из-за ошибок в передаче или обработке данных, потеря связи с другими системами или

внешними устройствами, риск полного отказа системы, что особенно критично для беспилотных транспортных средств и медицинских приборов.

Электромагнитные помехи могут возникать из различных источников, как внешних, так и внутренних.

Внешние ЭМП исходят от других устройств, таких как мобильные телефоны, радиопередатчики, линии электропередач и т. д.

Внутренние ЭМП генерируются внутри самой системы из-за работы процессоров, электродвигателей или других электронных компонентов.

Методы проверки робастности ИИ на электромагнитную совместимость включают в себя:

– ***лабораторные испытания на ЭМС.*** Одним из основных методов проверки робастности на электромагнитную совместимость является тестирование в специализированных лабораториях. В лабораторных условиях создаются контролируемые электромагнитные помехи различных частот и интенсивностей, чтобы проверить, как система ИИ справляется с этими условиями;

– ***анализ источников ЭМП.*** Для минимизации рисков электромагнитных помех проводится анализ потенциальных источников ЭМП как внутри системы, так и снаружи;

– ***экранирование и защита от помех.*** Одним из способов повышения устойчивости к электромагнитным помехам является экранирование и использование защитных схем.

Для устранения рисков, связанных с электромагнитными помехами, можно применять следующие меры:

– ***комплексная изоляция систем.*** Все критические компоненты ИИ-системы, включая сенсоры, процессоры и коммутационные устройства, должны быть защищены от внешних и внутренних источников ЭМП с помощью экранирующих материалов и конструкций;

– ***резервирование систем.*** В условиях повышенного риска электромагнитных помех полезно использовать резервные системы, которые могут взять на себя управление, если основная система ИИ столкнется с отказами;

– ***мониторинг и диагностика ЭМП.*** Современные системы могут включать датчики, отслеживающие уровень электромагнитных помех в реальном времени. Это позволит своевременно диагностировать угрозы и адаптировать работу системы для минимизации рисков;

– ***обучение ИИ на данных, подверженных ЭМП.*** Для того чтобы ИИ был готов к работе в условиях помех, можно включить в процесс обучения данные, которые содержат искажения или шумы, вызванные

электромагнитными помехами. Это позволит ИИ лучше адаптироваться к реальным условиям эксплуатации.

Проверка на робастность ИИ – это критически важный процесс для повышения безопасности и надёжности беспилотных транспортных средств. Она включает моделирование различных условий, аугментацию данных, использование многосенсорных систем и применение передовых методов машинного обучения. Только за счёт тщательной проверки на устойчивость можно минимизировать риски ошибок восприятия окружающей среды и обеспечить бесперебойную работу ИИ в реальных дорожных условиях. Комплексное тестирование, экранирование, алгоритмическая обработка данных и защита от электромагнитных помех помогут обеспечить устойчивость и надежность работы ИИ-систем в реальных условиях.

В заключении необходимо отметить, что развитие стандартов, нормативов и технологий безопасности в области ИИ является ключевым элементом обеспечения доверия к этим технологиям и их успешного внедрения в различные отрасли и области применения. Также важно отметить, что вопросы этики и социальной ответственности в использовании ИИ играют все более значимую роль. Необходимо уделять должное внимание обеспечению прозрачности, справедливости и ответственности при разработке и применении систем ИИ.

Следует подчеркнуть, что развитие и внедрение искусственного интеллекта на транспорте представляет собой важный шаг к современной и безопасной транспортной системе. Однако, для успешного осуществления этого процесса необходимо уделить должное внимание функциональной безопасности. Работа в этом направлении должна быть осуществлена с учетом высоких стандартов надежности и безопасности, а также с учетом социальной ответственности перед обществом.

1. Ответственность за причинение ущерба высокоавтоматизированным транспортным средством: состояние и перспективы [Электронный ресурс] – 2019. – Режим доступа: https://cyberleninka.ru/article/n/otvetstvennost-za-prichinenie-uscherba-vysokoavtomatizirovannym-transportnym-sredstvom-sostoyanie-i-perspektivy/viewer. – Дата доступа: 19.08.2024.

2. Беспилотные транспортные средства: новые вызовы общественной безопасности [Электронный ресурс] – 2019. – Режим доступа: https://cyberleninka.ru/article/n/bespilotnye-transportnye-sredstva-novye-vyzovy-obschestvennoy-bezopasnosti/viewer. – Дата доступа: 19.08.2024.

3. Потенциал искусственного интеллекта в беспилотных автомобилях [Электронный ресурс] – 2023. – Режим доступа: vestnik-glonass.ru/~DuD12. – Дата доступа: 20.08.2024.

4. ПНСТ 836 – 2023. Функциональная безопасность и системы искусственного интеллекта. Предварительный национальный стандарт

Российской Федерации. – Москва: Российский институт стандартизации, 2023 – 70 с.

Kharlap Siarhei,
Belarusian State University of Transport (Belarus, Gomel),
Ph.D. in Technical Science, A.P.
e-mail: hsn2013@tut.by, 34, Kirova str., 246653, Gomel
Konopatskaya Anastasia,
Design Bureau of System Programming (Belarus, Gomel),
e-mail: anstsknptsk@gmail.com, 135, Rechitsky ave., 246012, Gomel

REVIEW OF EXISTING METHODS FOR IMPROVING THE FUNCTIONAL SAFETY OF UNMANNED VEHICLES

The work provides an overview of the reasons for disruption of the normal operation of autonomous vehicles caused by incorrect operation of artificial intelligence systems, as well as methods aimed at increasing their functional safety. The main attention is paid to methods for assessing the robustness of artificial intelligence systems under the influence of external factors. Standard methods for assessing robustness are considered, including methods for increasing the resistance of artificial intelligence systems to the effects of electromagnetic interference.

Keywords: autonomous vehicles; artificial intelligence systems; functional safety; robustness.