Краткий отчет по проекту

РФФИ 19-29-06099 мк

«Разработка методов поиска уязвимостей интерфейсов взаимодействия человека с искусственным интеллектом транспортной среды «умного города»

Руководитель проекта

к.т.н. Чечулин А.А.

Современная транспортная среда "Умного города" обширна, она представляет собой совокупность общественного транспорта (поезда, метро, автобусы и троллейбусы), частного транспорта (частные машины и такси), рабочей техники (техника для уборки дорог, вывоза мусора, перевозки груза) и инфраструктуры для их навигации и функционирования (дороги, стоянки, заправочные станции и станции подзарядки, станции техобслуживания), а также людей, состоящих как из пользователей транспортной среды, так и персонала, обеспечивающего ее бесперебойную работу.

Особенностью "Умных городов" является использование искусственного интеллекта для управления транспортной инфраструктурой и оптимизации человеческих потоков. Однако, наряду с повышением эффективности и удобства управления это создает и новые угрозы для общества, так как нарушение работоспособности подобной системы управления может привести к значительному ущербу. Так, существует много различных видов атак на городские "умные" системы. Наиболее известные примеры - это компьютерные атаки на различные общественные платформы: экраны, билборды, банкоматы и другие аппараты, подключенные к интернету. К менее распространенным, но более опасным, относятся атаки на беспилотные транспортные объекты, такие как, например, поезда метро.

Данный проект направлен на исследования в области интеллектуальных транспортных систем в умном городе и решении фундаментальной задачи поиска уязвимостей интерфейсов взаимодействия человека с искусственным интеллектом. Задача данного проекта – описать и классифицировать такие проблемы безопасности (уязвимости), а также предложить пути их устранения или нейтрализации.

Результаты данного проекта помогут создателям "Умных городов" еще на стадии разработки программного и аппаратного обеспечения учесть и устранить возможные уязвимости, а если уязвимость будет обнаружена уже на этапе эксплуатации, то помогут разработать средства защиты, позволяющие ее нейтрализовать. Таким образом, исследование направлено на обеспечение безопасности организаций и граждан, живущих в "Умных городах"

В рамках первого отчетного периода был выполнен:

- анализ современных исследований в области человеко-машинного взаимодействия и выделены типы интерфейсов, применяемые в транспортных системах;
- выделены семь основных требований к устройствам и их интерфейсам в рамках функционирования транспортной среды;
- предложена классификация интерфейсов взаимодействия человека с транспортными системами умного города, состоящая из девяти основных классов;
- разработана концептуальная модель интерфейса взаимодействия пользователь-система, описывающая интеллектуальную транспортную среду при взаимодействии водителя пилотируемого транспортного средства с интеллектуальными системами мониторинга;
- разработана двухуровневая концептуальная модель интерфейса взаимодействия система – пользователь, включающая в себя уровень взаимодействия типов интерфейсов и уровень взаимодействия конкретных устройств;
- выполнена классификация возможных угроз в транспортной инфраструктуре умного города, состоящая из 36 классов;
- выполнена классификация уязвимостей интерфейсов человек - искусственный интеллект на основе анализа природы угроз (кибернетические, физические, киберфизические, психофизиологические и киберпсихофизиологические угрозы);
- разработаны компоненты программного обеспечения для программно-аппаратного стенда, позволяющие провести первичную апробацию предложенных в рамках первого этапа концептуальных моделей.

Также, в рамках первого года выполнения проекта была опубликована новость в ТАСС от 01.05.2020 «Ученые РФ классифицируют уязвимости платформ "Умного города" для создания систем защиты» (https://tass.ru/nacionalnye-proekty/8384481) и на портале “Научно-технологическое развитие Российской Федерации” в разделе “Ключевые

события” (http://нтр.рф/events/v-rf-klassifitsiruyut-uyazvimosti-platform-umnogo-goroda-dlya-sozdaniya-sistem-zashchity/).

В рамках отчетного периода была опубликована статья в журнале Sensors (входит в первый квартиль (Q1) журналов по системе цитирования Web of Science), опубликованы 4 научных статьи в трудах международных конференций, индексируемых в системах цитирования Scopus и WoS, опубликована 1 статья в журнале из перечня ВАК и 5 докладов были представлены на российских конференциях, труды которых индексируются в системе цитирования РИНЦ.