DOI: 10.58168/SAS2025_147-158
УДК 656.13

INTELLIGENT TRANSPORTATION SYSTEMS
ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ

Липовский А.М., студент магистратуры, ФГБОУ ВО «Воронежский государственный лесотехнический университет им. Г.Ф. Морозова», Воронеж, Россия.

Маклакова Е.А., д. филол. наук, профессор, ФГБОУ «Воронежский государственный лесотехнический университет им. Г.Ф. Морозова», Воронеж, Россия.

Lipovsky A.M., student of master courses, Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia.

Maklakova E.A., Doctor of Philological Sciences, Professor, Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia.

Abstract: With the development of intelligent vehicle management systems and road infrastructure, travel has become more efficient and reliable. This article comprehensively classifies security and privacy vulnerabilities in intelligent transportation systems, discusses issues and potential mitigation technologies to address these issues, and suggests directions for future research.

Keywords: intelligent transportation systems, vehicles, personal data, privacy.

Аннотация: С развитием интеллектуальных систем управления транспортными средствами и дорожной инфраструктуры путешествия стали более эффективными и надежными. В этой статье всесторонне классифицируются уязвимости безопасности и конфиденциальности в

интеллектуальных транспортных системах, обсуждаются проблемы и потенциальные технологии их устранения для решения этих проблем, а также предлагаются направления будущих исследований.

Ключевые слова: интеллектуальные транспортные системы, транспортные средства, личные данные, конфиденциальность.

Интеллектуальные транспортные системы (ИТС) меняют внешний вид и функционирование наших дорог и городов. Система обладает потенциалом для создания более эффективных, безопасных и приятных условий для путешественников по всему миру. Многие компании и города приступили к реализации планов по поддержке и продвижению развития технологий интеллектуальных транспортных систем (например, инициатива IBM «Умный город» и проект CityVerve от BT). Благодаря инновационному алгоритму прогнозирования дорожного движения и появлению автономных или полуавтономных транспортных средств безопасность и эффективность дорожного движения будут повышены, а дорожное движение в будущем будет сильно отличаться от сегодняшнего. Кроме того, достижения в области информационно-развлекательных систем (таких как навигационные системы, Bluetooth-соединения, текстовые сообщения громкой связи и телефоны и т.д.) продолжают обеспечивать современный комфорт в автомобилях. Интеграция технологий в транспортную систему открывает новые возможности для работы в мобильной среде и повышает комфортность поездок на большие расстояния. Однако развитие интеллектуальных транспортных систем и внедрение новых технологий в области дорог и инфраструктуры также привели к возникновению новых проблем [1].

Растущая интеграция устройств и приложений с недостаточными мерами безопасности в транспортные системы предоставляет злоумышленникам возможность воспользоваться преимуществами этих систем. Атака на интеллектуальную транспортную систему окажет влияние

на реальный мир и может привести к повреждению инфраструктуры, несвоевременному реагированию на чрезвычайные ситуации, жертвам и даже угрожать национальной безопасности. Из-за возможности серьезного материального ущерба и травмирования персонала люди провели оценку рисков интеллектуальных транспортных систем и создали модели рисков, но многие из этих моделей все еще имеют нерешенные проблемы, поэтому необходимы дальнейшие исследования. Перед лицом этих рисков необходимо разработать безопасную и ориентированную на конфиденциальность структуру для интеллектуальных транспортных систем, чтобы обеспечить безопасность и неприкосновенность частной жизни путешественников по всему миру.

Фигейредо (Figueiredo) и др. обсуждали концепцию и развитие интеллектуальных транспортных систем в конце 1990-х годов. Поскольку исследования в области интеллектуальных транспортных систем являются относительно новыми, многие проблемы до сих пор не решены. Особенно в области безопасности и конфиденциальности, необходимо изучить ряд вопросов, прежде чем интеллектуальные транспортные системы смогут в полной мере выполнять свою роль. Правительство также прилагает усилия и инвестиции в интеллектуальные транспортные системы, предоставляя планы исследований и финансовые средства для проектов, направленных на повышение осуществимости и практичности таких технологий. С выпуском стандарта серии X началась работа по стандартизации. Эти стандарты напрямую связаны с коммуникационными возможностями между транспортными средствами в интеллектуальных транспортных системах. Стандарт, предложенный Институтом инженеров электротехники и электроники (Institute of Electrical and Electronics Engineers), был дополнительно усовершенствован за счет добавления словаря набора сообщений SAE J2735 Directional Short-Range Communication (DSRC), который описывает стандарт, используемый в IEEE 1609. В прошлом такие

проекты, как приложение для электронной защиты транспортных средств от вторжений (EVITA) и Открытая платформа безопасности транспортных средств (OVERSEE), были направлены на повышение безопасности и конфиденциальности интеллектуальных транспортных систем, но эти проекты не успевали за темпами технического прогресса [2].

Следует рассматривать интеллектуальную транспортную систему с точки зрения системы в целом и обсуждать долгосрочные проблемы безопасности и конфиденциальности, которые могут возникнуть в связи с непрерывным развитием области интеллектуальных транспортных систем. Важен всесторонний анализ современных тенденций в области безопасности и конфиденциальности интеллектуальных транспортных систем и будущих направлений исследований в этой области. Необходима исчерпывающая классификация вопросов безопасности и конфиденциальности интеллектуальных транспортных систем, а также разработка потенциальных технологий устранения дефектов и уязвимостей.

Результаты таких научных изысканий помогут инженерам и исследователям интеллектуальных транспортных систем изучить и решить неотложные задачи, направленные на то, чтобы сделать интеллектуальные транспортные системы более безопасными, надежными и ориентированными на конфиденциальность.

Распространенным методом классификации по степени секретности является использование схемы конфиденциальности, целостности и доступности (CIA). Здесь классифицированы общие проблемы безопасности в интеллектуальных транспортных системах в соответствии с аспектами конфиденциальности, целостности и доступности, а также дополнительными аспектами, такими как аутентификация, идентификация и отказ от использования.

При обработке конфиденциальной информации в коммуникационной сети конфиденциальность, очевидно, является одной из необходимых услуг

безопасности, которые необходимо учитывать в интеллектуальной транспортной системе. Конфиденциальность позволяет устройствам и сторонам в интеллектуальной транспортной системе безопасно и конфиденциально взаимодействовать друг с другом, не раскрывая информацию несвязанным сторонам. Например, умный автомобиль и автобус могут передавать друг другу информацию о близком расстоянии, чтобы поддерживать безопасную дистанцию. Конфиденциальность обеспечивает безопасное средство связи для этих компонентов интеллектуальной транспортной системы, позволяющее передавать данные по незащищенным каналам, предотвращая при этом прослушивание обмениваемой информации третьими сторонами и потенциальными противниками. В дополнение к механизмам шифрования, обеспечивающим конфиденциальность, недавние исследования в области стеганографии и скрытых каналов также позволили изучить, как использовать эти альтернативные методы для сокрытия информации, когда злоумышленники могут получить доступ к каналам связи.

Коммуникационные сети имеют уязвимую поверхность для атак, как пассивных, так и активных. В частности, технология Car-Connected Everything должна обеспечивать конфиденциальность, чтобы конфиденциальная информация, передаваемая по каналу связи Car-Connected Everything, не подвергалась различным пассивным и активным атакам. Поскольку интеллектуальные транспортные системы включают в себя множество устройств, от сложных смартфонов и «умных» автомобилей до простых устройств Интернета вещей с чрезвычайно низкой вычислительной мощностью, обеспечение конфиденциальности в интеллектуальных транспортных системах является сложной задачей [3].

Поддержание целостности информации и вычислительных данных между транспортными средствами, инфраструктурой, центрами управления дорожным движением и т.д. имеет существенное значение для правильной

работы интеллектуальных транспортных систем. Целостность каждого узла (функциональной плоскости) интеллектуальной транспортной системы может быть нарушена. Например, вредоносное транспортное средство в интеллектуальной транспортной системе может осуществить атаку «человек посередине», перехватывая информацию о безопасности между двумя транспортными средствами и изменяя ее содержимое перед передачей информации другим транспортным средствам. Таким образом, легальные транспортные средства не смогут получить правильную информацию о местоположении других транспортных средств, что может привести к катастрофическим последствиям, поскольку легальные транспортные средства будут использовать эту неверную информацию в различных расчетах и решениях. В настоящее время доказано, что работа по слиянию датчиков компенсирует влияние неверной информации на расчеты, так что она не превышает допустимого диапазона. Технология Sensor Fusion широко используется во многих современных автомобилях.

Другой доказавшей свою эффективность атакой на целостность данных является подмена глобальной системы позиционирования (GPS). При подмене GPS злоумышленник передает ложный сигнал GPS, чтобы заставить путешественников изменить свои маршруты на основе неверных / вредоносных данных. Sybil Attack – еще одна распространенная форма атаки. Злоумышленник выдает себя за нескольких участников самоорганизующейся сети транспортного средства и вводит в сеть ложные широковещательные сообщения. Этот тип атак был изучен в научной литературе, но он по-прежнему остается одной из распространенных проблем в самоорганизующихся сетях транспортных средств и интеллектуальных транспортных системах.

В недавнем исследовании Сингха и соавторов изучалось использование блокчейна в качестве механизма безопасного обмена данными между сторонами в интеллектуальной транспортной системе. Однако предлагаемый

метод, основанный на блокчейне, нуждается в дальнейших исследованиях, чтобы определить его применимость в среде реального времени [4].

Наличие оборудования для управления и взаимодействия с другими компонентами интеллектуальной транспортной системы имеет огромное значение для обеспечения безопасности путешественников. Атака типа «отказ в обслуживании» является основной атакой на доступность компонентов и сервисов интеллектуальных транспортных систем. Атаки типа «отказ в обслуживании» распространены в большинстве областей применения интеллектуальных транспортных систем. Из-за требований к работе многих компонентов интеллектуальных транспортных систем в режиме реального времени «атаки на доступность» особенно опасны для интеллектуальных транспортных систем.

В интеллектуальной транспортной системе крайне важно аутентифицировать и идентифицировать все стороны, участвующие в коммуникации и передаче данных. Распространенные методы решения проблем аутентификации и идентификации включают использование кода аутентификации сообщения (MAC) или протокола ответа на запрос. Оба решения позволяют проверить личность отправителя, но они также увеличивают вычислительную нагрузку на систему, что создает новые проблемы. Многие устройства в современных интеллектуальных автомобилях требуют аутентификации и идентификации для правильной работы. Однако, как упоминалось ранее, дополнительные вычислительные затраты, связанные с механизмом аутентификации, могут повлиять на работу этих устройств в режиме реального времени или их ресурсные ограничения.

В дополнение к кодам аутентификации сообщений и решениям для реагирования на вызовы во многих исследованиях по аутентификации и идентификации самоорганизующихся сетей транспортных средств рассматривается и идея использования псевдонимов вместо идентификаторов транспортных средств для обеспечения большей конфиденциальности.

Однако этот сдвиг в использовании псевдонимов требует дополнительных затрат и вычислений при обработке информации о безопасности в интеллектуальной транспортной системе, поскольку псевдонимы сначала должны быть проверены надежным агентством.

«Отказ от ответственности» (Non-Repudiation) является ключевой услугой безопасности в интеллектуальных транспортных системах, особенно при изучении самоорганизующихся сетей транспортных средств и связи между автомобилями. «Отказ от ответственности» может помешать участникам системы отрицать вредоносное поведение. В большинстве работ по «отказу от ответственности» участвуют доверенные третьи стороны для проверки подлинности псевдонимов, обычно используемых в самоорганизующихся сетях транспортных средств. Эти третьи стороны называются региональными доверенными учреждениями и могут принимать форму таких групп, как организации физической инфраструктуры или государственные учреждения. Компромисс между «отказом от ответственности» и конфиденциальностью создает дополнительные проблемы для интеграции служб безопасности в интеллектуальные транспортные системы [5].

Конфиденциальность личных данных в интеллектуальных транспортных системах означает конфиденциальность реальных личных данных водителей, путешественников, пассажиров, пешеходов или участников. Эти удостоверения личности могут включать их имена, номера водительских прав, регистрационные номера автомобилей и т.д. Недавние исследования самоорганизующихся сетей транспортных средств выдвинули идею использования псевдонимов (также известных как псевдо-идентификационные коды) для замены практики привязки реальных идентификационных данных к транспортным средствам (часть системы самоорганизующихся сетей транспортных средств). Исследования показали, что псевдонимы могут защитить связь между широковещательной передачей

сообщений, содержащих информацию о безопасности (например, о местоположении транспортного средства) в самоорганизующейся сети транспортного средства, и идентификацией отправителя этих сообщений. Однако исследования также показали, что при использовании базовых псевдонимов злоумышленники все равно могут отслеживать конкретные транспортные средства. В ответ на эту ситуацию, достигнут прогресс в изучении псевдонимов в самоорганизующихся сетях транспортных средств, и были внедрены более специальные методы с точки зрения того, когда и как менять псевдонимы транспортных средств.

В качестве альтернативы использованию псевдонимов для защиты конфиденциальности и идентификации предлагаются учетные данные, основанные на атрибутах. Учетные данные с улучшенной конфиденциальностью на основе атрибутов позволяют пользователям проходить аутентификацию у проверяющих, так что пользователи не будут связаны между событиями аутентификации и будут показывать проверяющим только атрибуты, относящиеся к проверяющему, в своих учетных данных. Однако учетные данные, основанные на атрибутах, требуют больших ресурсов, а также создания общих секретов / атрибутов для всех необходимых служб. Существует компромисс между защитой конфиденциальности участников интеллектуальных транспортных систем и предоставлением безотказных услуг безопасности, которые используются для правильной идентификации пользователей системы в случае дорожно-транспортных происшествий и / или уголовных дел.

Информация о пользователе в интеллектуальной транспортной системе очень богата и подробна, включая финансовую информацию, информацию о местоположении и привычках пользователя в системе, что предоставляет множество возможностей для нарушения конфиденциальности личного поведения. В рамках интеллектуальных транспортных систем поведенческая конфиденциальность относится к конфиденциальности данных, которые

описывают группы или отдельных лиц и их поведение в интеллектуальных транспортных системах. Чтобы сохранить конфиденциальность поведения, система должна иметь возможность анонимно обрабатывать собранные пользовательские данные, предотвращать их раскрытие и маскировать общие модели поведения пользователей интеллектуальных транспортных систем.

Защита конфиденциальности поведения пользователей интеллектуальных транспортных систем необходима для того, чтобы злоумышленники не могли отслеживать и выводить данные о конкретных лицах в системе. Поскольку интеллектуальная транспортная система собирает информацию о маршрутах путешественников, чтобы сделать их более безопасными и эффективными, система также будет фиксировать маршруты передвижения отдельных путешественников. Анализируя эту информацию, можно сделать вывод о личном поведении. Например, отправная точка и пункт назначения одного путешественника могут вызвать проблемы с конфиденциальностью, поскольку злоумышленники могут определить место жительства или работы путешественника.

Согласно определению конфиденциальности, приведенному в статье Финна и соавторов «Семь типов конфиденциальности», конфиденциальность местоположения в интеллектуальных транспортных системах может быть классифицирована как «конфиденциальность местоположения и пространства», то есть пользователи имеют право путешествовать или перемещаться в системе, не беспокоясь о том, что информация об их местоположении может быть учтена. Хотя точная информация о местоположении помогает интеллектуальным транспортным системам предоставлять услуги с учетом местоположения, такая информация также может быть использована для нарушения конфиденциальности личных данных. Злоумышленник может использовать эту информацию о местоположении для начала атаки против физического лица. Для навигационных систем, основанных на глобальных системах

позиционирования, чрезвычайно сложно обеспечить конфиденциальность информации о местоположении пользователей при предоставлении услуг [6].

Поэтому главное – найти баланс между предоставлением пользователям полезных и точных услуг и защитой конфиденциальности местоположения. Размытие местоположения или маскировка местоположения – это технология, используемая в сервисах определения местоположения, защищенных от несанкционированного доступа. Маскировка местоположения защищает конфиденциальность пользователя, слегка изменяя или обобщая местоположение пользователя, чтобы избежать раскрытия его фактического местоположения.

Список литературы

1. Ананенко А. О. Основные направления совершенствования гражданско-правового законодательства в области регулирования беспилотных транспортных средств // Транспортное право и безопасность. 2020. 2(34). С. 76-83.

2. Евстигнеев, И. А. Дорожная инфраструктура и высокоавтоматизированные транспортные средства // САПР и ГИС автомобильных дорог. 2019. 2 (13). С. 44-50.

3. Землин А. И. Проблемные вопросы правового регулирования отношений, связанных с использованием высокоавтоматизированных транспортных средств // Журнал российского права. 2022. Т. 26. № 12. С. 58-69. DOI: 10.12737/jrl.2022.128. – URL: https://elibrary.ru/bsmkwa.

4. Коробеев А. И., Чучаев А. И. Беспилотные транспортные средства: новые вызовы общественной безопасности. Lex Russica (Русский закон), 2019. 2(147). С. 9-28.

5. Кутюр С., Тоупин С. Что означает «суверенитет» в цифровом мире? // Вестник международных организаций: образование, наука, новая экономика. 2020. 15(4). С. 7.

6. Юдкина, В. В. Высокоавтоматизированные транспортные средства как субъект общественной безопасности // Административное право и процесс. 2022. №10. – URL: https://elibrary.ru/xhbcrb.

References

1. Ananenko A. O. The main directions of improvement of civil law legislation in the field of regulation of unmanned vehicles // Transport Law and Security, 2020. 2(34), pp. 76-83.

2. Evstigneev I. A. Road infrastructure and highly automated vehicles / CAD and GIS of highways, 2019. 2(13), pp.44-50.

3. Zemlin A. I. Problematic issues of legal regulation of relations related to the use of highly automated vehicles // Journal of Russian Law. 2022. T. 26. № 12. – P. 58-69. DOI: 10.12737/jrl.2022.128. – URL: https://elibrary.ru/bsmkwa/.

4. Korobeev A. I., Chuchaev A. I. Unmanned vehicles: new challenges to public safety. Lex Russica (Russian Law). 2019. 2(147). Pp. 9-28.

5. Couture S., Toupin S. What does "sovereignty" mean in the digital world? // Bulletin of International Organizations: Education, Science, New Economy. 2020. 15(4), p. 7.

6. Yudkina V. V. Highly automated vehicles as a subject of public safety // Administrative Law and Process. 2022. №10. – URL: https://elibrary.ru/xhbcrb.