Курская региональная общественная организация
Общероссийской общественной организации
«Вольное экономическое общество России»
Северо-Кавказский федеральный университет,
Пятигорский институт (филиал) (Россия)
Совет молодых ученых и специалистов Курской области

ПОКОЛЕНИЕ БУДУЩЕГО: Взгляд молодых ученых-2023

Сборник научных статей
12-й Международной
молодежной научной конференции
09-10 ноября 2023 года

Ответственный редактор *Горохов А.А.*

19-20 октября 2023 года

Ответственный редактор *Горохов А.А.*

ТОМ 3

в 4-х томах

Информационно–телекоммуникационные системы, технологии и электроника.
Технологии продуктов питания.
Строительство. Градостроительство и архитектура.
Безопасность жизнедеятельности и охрана окружающей среды.

Курск 2023

УДК 338: 316:34
ББК 65+60+67
Ш67 МЛ-05

Поколение будущего: Взгляд молодых ученых-2023: сборник научных статей 12-й Международной молодежной научной конференции (09-10 ноября 2023 года), / редкол.: А.А. Горохов (отв. редактор), в 4-х томах, Том 3, - Курск: ЗАО «Университетская книга», 2023, - 404 с.

ISBN 978-5-907776-87-6

Содержание материалов конференции составляют научные статьи отечественных и зарубежных молодых ученых. Излагается теория, методология и практика научных исследований.

Для научных работников, специалистов, преподавателей, аспирантов, студентов.

Материалы в сборнике публикуются в авторской редакции.

ISBN 978-5-907776-87-6
УДК 338: 316:34
ББК 65+60+67

СОДЕРЖАНИЕ

ВАСИЛЬЕВ ЕГОР АЛЕКСАНДРОВИЧ, студент
КНЯЗЬКИНА ОЛЬГА ВЛАДИМИРОВНА, к.т.н., доцент
dmtov@mail.ru
Сибирский государственный индустриальный университет,
г.Новокузнецк, Россия

КИБЕРБЕЗОПАСНОСТЬ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ

Рассмотрены подходы к созданию безопасных беспилотных автомобилей, основанные на трех ключевых составляющих: едином безопасном шлюзе SCU, системе KasperskyOS и сервисах анализа угроз. Описаны особенности применения данных технологий в интеллектуальных транспортных системах, которые позволяют оперативно реагировать на угрозы, тем самым обеспечивая безопасность транспортных систем.

Ключевые слова: кибербезопасность, интеллектуальные транспортные системы, беспилотные автомобили.

Интеллектуальные транспортные системы (ИТС) стали неотъемлемой частью нашей современной дорожной инфраструктуры. Они играют ключевую роль в улучшении безопасности, эффективности и комфорта путешествия для водителей и пассажиров. Однако с ростом использования электронных контроллеров в ИТС возникает все больше уязвимых мест, которые могут стать целью кибератак[1].

Сегодняшние ИТС используют электронные контроллеры для поддержания связи с внешними источниками данных, такими как системы геопозиционирования, диагностики и развлекательные системы. Это позволяет им эффективно контролировать движение, оптимизировать маршруты и даже предупреждать о возможных поломках. Однако с каждым новым контроллером возникает потенциальная уязвимость, которую злоумышленники могут использовать для кибератак. Разработчики должны уделять особое внимание реализации протоколов безопасности и шифрования данных, чтобы предотвратить возможность перехвата или модификации информации злоумышленниками.

Кроме того, важно учесть возможность обновления и модернизации системы безопасности в ИТС, так как киберугрозы постоянно эволюционируют, необходимо иметь гибкую и адаптивную систему, которая может быстро реагировать на новые уязвимости и предоставлять обновления для защиты от них [2].

Рассмотрим новые подходы к созданию безопасных, подключенных и в будущем – беспилотных автомобилей, которые основаны на трех ключевых составляющих: едином безопасном шлюзе SCU, системе KasperskyOS и сервисах анализа угроз, которые являются ключевыми компонентами, обеспечивающими безопасность и надежность подключенных автомобилей [3].

Модуль безопасной коммуникации (Secure Communications Unit, SCU) представляет собой инновационную программную платформу, основанную на технологии KasperskyOS, которая открывает новые возможности для разработки и внедрения безопасных центральных шлюзов для подключенных контроллеров транспортных средств. Это решение позволяет укрепить защиту от цифрового вторжения и усовершенствовать бесконтактную диагностику, обеспечивая надежность и безопасность системы.

SCU представляет собой гибкую программную платформу, которая может быть адаптирована к различным требованиям и потребностям производителей. Она обеспечивает защиту от киберугроз и предотвращает несанкционированный доступ к системе транспортного средства. Благодаря применению технологии KasperskyOS, SCU обладает высоким уровнем безопасности и может эффективно защищать транспортные средства от вредоносного программного обеспечения и хакерских атак.

Одна из особенностей SCU – возможность создания безопасного центрального шлюза, который объединяет и контролирует все подключенные контроллеры автомобиля, что позволяет производителям эффективно управлять всеми аспектами безопасности и диагностики транспортных средств, обеспечивая надежность и защиту от угроз.

Бесконтактная диагностика становится все более популярной в автомобильной индустрии, поскольку она позволяет проводить диагностику транспортного средства без необходимости физического подключения. SCU усовершенствует этот процесс, обеспечивая безопасную связь между транспортным средством и диагностическим центром. Это позволяет операторам более эффективно и точно определять проблемы и выполнять необходимые ремонтные работы.

Кроме того, SCU поддерживает возможность шифрования и аутентификации данных, передаваемых между транспортным средством и внешними системами. Это гарантирует конфиденциальность и целостность передаваемой информации, предотвращая возможность несанкционированного доступа и подмены данных.

Использование SCU в транспортных средствах позволяет производителям создавать безопасные и надежные системы, обеспечивая защиту от киберугроз и повышая уровень безопасности водителей и пассажиров [3].

KasperskyOS предлагает подход к безопасности, основанный на строгом разделении компонентов и принудительном внедрении политик. Это означает, что различные части системы работают независимо друг от друга, что существенно снижает возможность распространения вредоносного кода и его воздействия на другие компоненты системы. Кроме того, операционная система KasperskyOS использует проверенные методологии и патентованные технологии, обеспечивающие дополнительный уровень защиты.

Одной из ключевых особенностей KasperskyOS является его способность предотвращать атаки на уровне ядра операционной системы. Традиционные операционные системы часто становятся уязвимыми для атак, когда злоумышленники находят уязвимости в ядре системы. В KasperskyOS применяются инновационные методы, которые позволяют обнаруживать и предотвращать такие атаки, что делает эту операционную систему особенно надежной.

Кроме того, KasperskyOS предлагает широкий набор инструментов и функций для обеспечения безопасности встроенных систем. Он включает систему контроля доступа, механизмы защиты памяти, а также возможность проверки и анализа программного обеспечения на наличие вредоносного кода. Все это позволяет предотвращать атаки и обеспечивать безопасность системы на всех уровнях.

Сервисы кибербезопасности для автомобилей, поездов и других видов транспорта предоставляют ценную информацию об опасностях и результатах анализа, необходимых для более надежной защиты и противодействия самым опасным атакам. Они позволяют предупреждать и предотвращать возможные кибератаки, обеспечивая безопасность как пассажиров, так и транспортных средств [4].

Одним из ключевых инновационных сервисов является система мониторинга и обнаружения аномалий в работе транспортных систем. Посредством специализированных алгоритмов и анализа больших объемов данных, эта система способна выявить подозрительные активности, которые могут указывать на потенциальные кибератаки. Благодаря этому операторы транспортных систем могут принимать меры по предотвращению возможных угроз, минимизируя риски для пассажиров и обеспечивая непрерывность работы системы.

Еще одним важным сервисом является система шифрования данных. Она защищает конфиденциальность и целостность информации, передаваемой и хранимой внутри транспортных систем. Шифрование данных позволяет предотвратить несанкционированный доступ к важным данным, таким как информация о маршрутах, расписаниях, а также личные данные пассажиров. Такая защита особенно важна в мире растущей зависимости транспортных систем от сетевых технологий. Вместе с тем, сервисы кибербезопасности должны быть способны реагировать на новые угрозы и атаки. Для этого внедряются системы машинного обучения и искусственного интеллекта. Такие инновационные методы позволяют оперативно реагировать на угрозы и обновлять системы защиты.

Кроме того, следует отметить важность сотрудничества между разными участниками транспортных систем. Организации, предоставляющие услуги кибербезопасности, должны активно сотрудничать с производителями транспортных средств, операторами систем и общественными организациями, чтобы обмениваться информацией о новых угрозах и разработке эффективных методов защиты.

Сервисы кибербезопасности играют немаловажную роль в современных транспортных системах, обеспечивая защиту от кибератак и обеспечивая безопасность пассажиров и транспортных средств. Инновационные подходы, такие как системы мониторинга и обнаружения аномалий, шифрование данных и использование машинного обучения, позволяют эффективно противодействовать угрозам и обновлять системы защиты. Сотрудничество между различными участниками транспортных систем также является ключевым фактором в обеспечении кибербезопасности [5].

В заключение можно сделать вывод о том, что безопасность является важнейшим аспектом для современных интеллектуальных транспортных систем. Важно использовать целостный подход, начиная с этапа проектирования, чтоб встроить средства информационной сохранности в саму систему. Только так возможно обеспечить защиту от киберугроз и сохранить эффективность и комфорт ИТС для всех их пользователей.

Список литературы

1. К вопросу внедрения интеллектуальных систем на автомобильном транспорте / К.П. Андреев, И.Н. Горячкина, А.В. Шемякин, А.С. Евтеева // Актуальные вопросы организации автомобильных перевозок и безопасности движения : матер. Междунар. науч.-практ. конф. – 2018. – С. 62-67.

2. Озеров, А.В. Стандарты кибербезопасности интеллектуальных транспортных систем // Интеллектуальные транспортные системы. – Москва: Российский университет транспорта, 2023. – С. 607-613.

3. Кибербезопасность транспортных систем // Kaspersky. – URL: https://www.kaspersky.ru/enterprise-security/transportation-security?referer2=tcid_admitad_3aa04670b9023139c824d5a059c3cfd4_442763_x4&tagtag_uid=3aa04670b9023139c824d5a059c3cfd4 (дата обращения: 22.10.2023).

4. Безопасность интеллектуальных транспортных систем – новая реальность // Интеллектуальные транспортные системы России. – URL: https://www.itsjournal.ru/articles/interview/bezopasnost-intellektualnykh-transportnykh-sistem-novaya-realnost/ (дата обращения: 22.10.2023).

5. Использование интеллектуальных транспортных систем для повышения качества организации дорожного движения / И.А. Новиков, Л.Е. Кущенко, Е.А. Новописный, А.С. Камбур – Текст : электронный // Мир транспорта и технологических машин. – 2022. – № 3-4 (78). – С. 49-54.

ДЕРНОВА КРИСТИНА КОНСТАНТИНОВНА, студент,
КНЯЗЬКИНА ОЛЬГА ВЛАДИМИРОВНА, канд. техн. наук, доцент
(e-mail: kristina191198@mail.ru)
(e-mail: dmtov@mail.ru)
Сибирский государственный индустриальный университет, г. Новокузнецк, Россия

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА ВЫСОКОСКОРОСТНЫХ ЖЕЛЕЗНЫХ ДОРОГАХ

Рассмотрено внедрение искусственного интеллекта в системы высокоскоростной железной дороги. Приведены преимущества применения искусственного интеллекта в системах высокоскоростной железной дороги. Вывялено, что искусственный интеллект имеет огромный потенциал для оптимизации и модернизации железнодорожного транспорта.

Ключевые слова: искусственный интеллект, высокоскоростная железная дорога, интеллектуальное управление, железнодорожный транспорт.

Искусственный интеллект (ИИ) является одной из самых важных и инновационных технологий нашего времени. Он представляет собой системы, способные обучаться и принимать решения, основываясь на аналогии с когнитивными процессами человека. Благодаря постоянному развитию новых технологий и