Лешан А.Д., Вязников Н.А. Обеспечение безопасности данных
в современных автомобилях // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 9(47) с. 9–15

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.55

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В СОВРЕМЕННЫХ АВТОМОБИЛЯХ

[1]Лешан А.Д., Вязников Н.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [1]nekrasov15ig@gmail.com

В данной научной статье рассматривается вопрос роста рисков различных киберугроз в современных автомобилях, который связан с увеличением количества электронных систем и подключенных устройств. Особое внимание уделяется атакам на систему управления автомобилем, систему связи и навигации, а также кражам данных пользователей. Предлагаются практические меры по обеспечению безопасности, такие как сегментация систем, шифрование данных, надежная аутентификация и авторизация, а также мониторинг и обнаружение угроз. В статье подчеркивается необходимость комплексного подхода к обеспечению информационной безопасности в электрокарах для защиты как самих автомобилей, так и их пользователей.

Ключевые слова: Электромобили, хакерские атаки, защита данных, уязвимости, безопасность систем, автомобильные технологии, обновление программного обеспечения, кибератаки, информационная безопасность, удаленное управление, взлом автомобилей, современные транспортные средства, безопасность пользователей, защита личных данных.

ENSURING DATA SECURITY IN MODERN CARS

[1]Leshan A.D., Vyaznikov N.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: [1]nekrasov15ig@gmail.com

This scientific article examines the issue of increasing the risks of various cyber threats in modern cars, which is associated with an increase in the number of electronic systems and connected devices. Special attention is paid to attacks on the car's control system, communication and navigation systems, as well as the theft of user data. Practical security measures are proposed, such as system segmentation, data encryption, reliable authentication and authorization, as well as threat monitoring and detection. The article emphasizes the need for an integrated approach to ensuring information security in electric cars to protect both the cars themselves and their users.

Keywords: Electric vehicles, hacker attacks, data protection, vulnerabilities, system security, automotive technologies, software updates, cyber attacks, information security, remote control, car hacking, modern vehicles, user safety, personal data protection.

Введение

В последние годы стремительное развитие электромобилей и увеличение числа подключенных устройств в этих транспортных средствах привели к возрастанию важности обеспечения безопасности данных. Существующие классические методы защиты информации, такие как брандмауэры и антивирусные программы, имеют свои ограничения и уязвимости. В условиях роста вычислительных мощностей и появления новых видов

киберугроз эти методы могут стать недостаточно надежными для обеспечения конфиденциальности и целостности данных в электромобилях. Поэтому возникает необходимость в разработке новых подходов к защите информации, которые смогли бы противостоять угрозам, исходящим от современных кибератак.[1]

Цель данной статьи — рассмотреть вопросы обеспечения безопасности данных в электромобилях, анализируя современные исследования в области кибербезопасности и обосновывая целесообразность применения новых технологий для повышения безопасности транспортных средств. В статье проводится анализ практических результатов использования современных алгоритмов защиты, обсуждаются преимущества новых методов перед классическими подходами и рассматриваются перспективы их внедрения в автомобилестроении.

Таким образом, данная работа вносит вклад в развитие методов информационной безопасности и открывает новые горизонты для создания надежных систем защиты данных в эпоху умных и подключенных транспортных средств.

Основные виды хакерских нападений

Хакерские атаки совершаются преимущественно на атаки на систему управлений. В случае удаленного доступа, хакеры могут получить доступ к системе управления электромобилем и управлять его функциями, такими как торможение, ускорение и поворот, без физического взаимодействия с объектом атаки.

Также возможны манипуляции с программным обеспечением. Злоумышленники могут изменить программное обеспечение автомобиля, что может привести к неправильной работе систем и созданию аварийных ситуаций.[2]

Атаки могут совершаться на систему связи и навигации. Хакеры могут отправлять ложные GPS-сигналы, что дезориентирует водителя. Злоумышленники могут перехватывать и изменять данные, передаваемые между автомобилем и внешними устройствами, включая навигационные данные и сообщения.

Рассматривая вопрос кражи данных пользователей, стоит учесть, что электромобили собирают и хранят различные данные о пользователях, включая маршруты, предпочтения и данные о платежах. В случае обнаружения уязвимости в системах безопасности, может быть получен несанкционированный доступ к этим данным со стороны третьих лиц.

В некоторых случаях автомобили имеют свои собственные мобильные приложения, которые могут быть уязвимы для кибератак, что позволяет злоумышленникам получить доступ к информации и функциям автомобиля.[3]

Зарядные станции, необходимые для реализации функций электромобилей, могут быть могут быть атакованы. Поскольку зарядные станции часто обрабатывают платежные данные, существует риск их перехвата и использования злоумышленниками.

Последствия хакерских нападений с точки зрения компаний и пользователей электромобилей

Последствия хакерских нападений могут быть крайне разрушительными и многогранными. Прежде всего, такие атаки могут привести к утечке конфиденциальной информации, включая личные данные пользователей, финансовые сведения и корпоративные тайны. Эта информация может быть использована злоумышленниками для совершения

мошенничества, вымогательства или других преступных действий, что наносит прямой ущерб жертвам и подрывает доверие к пострадавшим организациям.

Кроме того, хакерские нападения могут вызвать значительные финансовые потери. Восстановление после кибератаки требует значительных ресурсов, как материальных, так и временных. Организациям приходится инвестировать в повышение уровня кибербезопасности, проведение аудитов, обучение персонала и восстановление систем. Помимо прямых затрат, могут возникнуть косвенные убытки в виде упущенной прибыли, штрафов за несоблюдение нормативных требований и потери репутации.

Не менее важными являются и социальные последствия хакерских нападений. Массовые утечки данных могут вызвать панику среди пользователей, подорвать доверие к цифровым технологиям и вызвать общественный резонанс. В некоторых случаях кибератаки могут повлиять на критически важную инфраструктуру, такую как энергетические сети, транспортные системы или медицинские учреждения, что может привести к реальным физическим угрозам и нарушению нормальной жизнедеятельности общества.[4]

Влияние Интернета вещей (IoT) на безопасность автомобилей

Интернет вещей (IoT) оказывает значительное влияние на автомобильную промышленность, предлагая новые возможности для повышения функциональности и удобства использования автомобилей. Однако, с этими преимуществами возникают и серьезные вопросы касательно безопасности.

С увеличением количества подключенных устройств и систем в автомобиле расширяется поверхность атаки. Теперь злоумышленники могут попытаться получить доступ не только через традиционные точки входа, такие как система управления двигателем или тормозная система, но и через менее защищенные устройства, такие как сенсоры, развлекательные системы или даже подключенные смартфоны.

Многие устройства IoT работают на сложных программных платформах, которые могут содержать уязвимости. Обновления программного обеспечения для устранения этих уязвимостей часто запаздывают или не всегда доступны пользователям. Это создает дополнительные риски, особенно если автомобили не получают своевременные обновления безопасности.

Автомобили, оснащенные IoT-устройствами, собирают и обрабатывают огромное количество данных о водителе и пассажирах. Это включает в себя информацию о местоположении, повадках вождения, а также личные данные, такие как контакты и сообщения. Защита этих данных является критически важной задачей, поскольку их утечка может привести к серьезным последствиям для конфиденциальности пользователей.

Известные случаи атак

В 2015 году исследователи по безопасности Кевин Махеффи и Марк Роджерс продемонстрировали, как можно взломать Tesla Model S. Они смогли удаленно проникнуть в систему автомобиля, управлять его движением, включая торможение и ускорение, а также изменять работу информационно-развлекательной системы. Несмотря на то, что проникновение оказалось возможным лишь на скорости 8 км/ч, этот случай привлек внимание к необходимости усиления мер безопасности в электромобилях. Tesla оперативно выпустила обновление программного обеспечения для устранения уязвимостей.[5]

В том же году исследователи по безопасности Чарли Миллер и Крис Валасек показали, как можно взломать Jeep Cherokee. Они смогли удаленно контролировать функции автомобиля, такие как рулевое управление, торможение и ускорение, через уязвимость в системе. Этот случай продемонстрировал, насколько уязвимы современные автомобили, оснащенные сложными электронными системами.[6]

В 2016 году исследователь по безопасности Трой Хант обнаружил уязвимость в мобильном приложении Nissan Leaf, которая позволяла удаленно получать доступ к информации об автомобиле, такой как данные о поездках и состоянии заряда батареи. Хотя эта уязвимость не позволяла управлять автомобилем, она показала, как легко можно получить доступ к личным данным пользователей через недостаточно защищенные приложения.

На конкурсе Pwn2Own, который был проведен в 2019 году, группа хакеров из сингапурской компании по кибербезопасности смогла взломать Tesla Model 3. Они использовали уязвимость в браузере автомобиля для получения доступа к его системам. В результате Tesla также выпустила обновление программного обеспечения для устранения этой уязвимости.

В 2020 году исследователь по безопасности Ленерт Вутерс из Левенского католического университета в Бельгии продемонстрировал, как можно взломать Tesla Model X с помощью оборудования стоимостью всего $300. Он смог получить доступ к системе бесключевого доступа автомобиля и угнать его. Tesla вновь оперативно выпустила обновление программного обеспечения, чтобы закрыть выявленные уязвимости.

Методы защиты от атак на электронные системы автомобиля

Для защиты электромобилей от хакерских нападений необходимо применять комплексный подход, включающий несколько ключевых методов. Одним из таких методов является сегментация систем, которая предполагает разделение сетей автомобиля на отдельные сегменты. Это позволяет ограничить распространение атаки в случае взлома одной из систем, минимизируя потенциальный ущерб и повышая общую безопасность автомобиля.

Шифрование данных играет важную роль в защите информации, передаваемой между автомобилем и внешними устройствами. Использование сильных методов шифрования позволяет предотвратить перехват и несанкционированный доступ к данным, обеспечивая их конфиденциальность и целостность. Это особенно важно для защиты чувствительных данных, таких как данные о местоположении, доступ к системам управления и платежная информация.

Постоянный мониторинг и обнаружение угроз являются критически важными для своевременного выявления подозрительной активности. Использование технологий мониторинга и обнаружения угроз позволяет оперативно реагировать на потенциальные атаки, обеспечивая безопасность систем автомобиля в реальном времени. Наконец, обучение и осведомленность пользователей также играют важную роль в защите электромобилей. Повышение осведомленности пользователей о возможных угрозах и обучение методам защиты помогает им более эффективно противостоять кибератакам и принимать меры предосторожности.

Проблема повышения безопасности в современных автомобилях

Повышение безопасности может иметь негативную сторону, в основном связанную с ухудшением опыта пользователя. Баланс между удобством использования и высокой

степенью безопасности на данный момент является одной из ключевых задач для производителей автомобилей и разработчиков программного обеспечения.

Одним из подходов является создание удобных интерфейсов, которые интуитивно понятны и просты в использовании, при этом обеспечивая надежную защиту. Например, использование многофакторной аутентификации может значительно повысить безопасность, не создавая при этом значительных неудобств для пользователей. Такие интерфейсы позволяют пользователям легко взаимодействовать с системами безопасности, не испытывая сложностей.

Автоматизация процессов также играет важную роль в достижении баланса между удобством и безопасностью. Снижение необходимости выполнения пользователями множества действий для обеспечения безопасности может быть достигнуто за счет автоматизации и использования предиктивных алгоритмов. Это позволяет минимизировать человеческий фактор и снизить вероятность ошибок, одновременно упрощая процесс для конечного пользователя.

Обучение и информирование пользователей – одни из важнейших мер для достижения баланса между безопасностью и простотой пользования. Проведение образовательных кампаний и предоставление четких инструкций по безопасному использованию функций автомобиля способствует осознанию важности мер безопасности. Пользователи, которые хорошо информированы о рисках и способах их минимизации, с большей вероятностью будут следовать рекомендациям и использовать функции безопасности эффективно.

Наконец, предоставление возможностей для пользователей самостоятельно настраивать уровни безопасности в зависимости от их индивидуальных потребностей и предпочтений позволяет адаптировать систему под специфические условия эксплуатации. Такая персонализация позволяет каждому пользователю настроить защиту в соответствии с его личными требованиями, что повышает общую удовлетворенность и доверие к системе.

Таким образом, баланс между удобством использования и высокой степенью безопасности может быть достигнут путем создания удобных интерфейсов, автоматизации процессов, обучения и информирования пользователей, а также предоставления возможностей для персонализации настроек. Эти меры позволяют обеспечить высокий уровень защиты, не создавая при этом значительных неудобств для пользователей.

Заключение

Обеспечение безопасности данных в современных автомобилях является одной из ключевых задач для автопроизводителей и разработчиков программного обеспечения. В эпоху Интернета вещей (IoT) автомобили становятся сложными системами, собирающими и обрабатывающими огромное количество данных, включая информацию о местоположении, повадках вождения и личные данные водителей и пассажиров.

Для защиты этих данных необходимо применять комплексный подход, который включает в себя использование сильного шифрования, сегментацию сетей, регулярные обновления программного обеспечения и внедрение многоуровневых механизмов аутентификации и авторизации. Также важно внедрять системы мониторинга и обнаружения атак.

Современные автомобили должны не только обеспечивать высокий уровень комфорта и функциональности, но и гарантировать надежную защиту данных своих пользователей. В

конечном итоге, безопасность данных должна стать неотъемлемой частью разработки и эксплуатации современных автомобилей.

Список литературы

1. Косарев А.Н., Новокшонов И.М., Ткаченко Ю.Е., Трофимов М.Л. Электронный контроль устойчивости (EPS): принцип работы и преимущества // Сборник статей Международной научно-практической конференции. Уфа, 2022 С. 35-39.
2. Сальников Е.В. Беспилотные автомобили: массовые предрассудки и футурологический прогноз // Управление деятельностью по обеспечению безопасности дорожного движения: состояние, проблемы, пути совершенствования. 2018. № 1 (1) С. 356-363.
3. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории // Учебник / Сер. 76 Высшее образование. (1-е изд.) Москва, 2024.
4. Сафиуллин Р.Н., Керимов М.А., Григорьева А.С. К вопросу автоматизации электронных систем управления автомобильной техники по информационно-телекоммуникационному взаимодействию // Сборник научных трудов кафедры «Организация перевозок и управление на транспорте» С. 197-203
5. Вострецова Е.В. Основы информационной безопасности // Учебное пособие: рекомендовано методическим советом Уральского федерального университета для студентов вуза, обучающихся по укрупненной группе направлений бакалавриата и специалитета 10.00.00 «Информационная безопасность» / Екатеринбург, 2019.
6. Бессонов Б.А. Электромобили и экология. Перспективы использования электромобилей // В сборнике: Современная техника и технологии в электроэнергетике и на транспорте: задачи, проблемы, решения. Сборник трудов VII Всероссийской (национальной) научно-практической конференции научных, научно-педагогических работников, аспирантов и студентов. Науч. редактор А.Н. Ткачёв. Челябинск, 2023. С. 161-167.

References

1. Kosarev A.N., Novokshonov I.M., Tkachenko Yu.E., Trofimov M.L. Electronic stability control (EPS): the principle of operation and advantages // Collection of articles of the International scientific and practical Conference. Ufa, 2022 pp. 35-39.
2. Salnikov E.V. Unmanned vehicles: mass prejudices and futurological forecast // Management of road safety activities: state, problems, ways of improvement. 2018. No. 1 (1) pp. 356-363.
3. Shcheglov A.Yu., Shcheglov K.A. Information protection: fundamentals of theory // Textbook / Ser. 76 Higher education. (1st ed.) Moscow, 2024.
4. Safiullin R.N., Kerimov M.A., Grigorieva A.S. On the issue of automation of electronic control systems of automotive equipment for information and telecommunication interaction // Collection of scientific papers of the department "Organization of transportation and management in transport" pp. 197-203
5. Vostretsova E.V. Fundamentals of information security // Textbook: recommended by the Methodological Council of the Ural Federal University for university students studying in an enlarged group of bachelor's and specialty areas 10.00.00 "Information security" / Yekaterinburg, 2019.

6. Bessonov B.A. Electric vehicles and ecology. Prospects for the use of electric vehicles // In the collection: Modern equipment and technologies in the electric power industry and transport: tasks, problems, solutions. Proceedings of the VII All-Russian (national) scientific and practical Conference of scientific, scientific and pedagogical workers, graduate students and students. Scientific editor A.N. Tkachev. Chelyabinsk, 2023. pp. 161-167.