DOI: 10.58168/MSTT2025_21-24
УДК 62.788

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПАТРУЛЬНЫХ АВТОМОБИЛЕЙ ГОСАВТОИНСПЕКЦИИ

С.В. Канавин[1]
[1] Воронежский институт МВД России, г. Воронеж, Россия,
sergejj-kanavin@rambler.ru

Аннотация. В статье рассмотрены вопросы проблематики обеспечения информационной безопасности в области эксплуатации современных легковых патрульных автомобилей Госавтоинспекции. На основе проведенного анализа предложены возможные пути решения проблемы в данной предметной области.

Ключевые слова: информационная безопасность, патрульный автомобиль, полиция, критические системы легкового автомобиля, системы безопасности.

INFORMATION SECURITY OF STATE TRAFFIC INSPECTORATE PATROL CARS

S.V. Kanavin[1]
[1] Voronezh Institute of the Ministry of the Interior of Russia, Voronezh, Russia,
sergejj-kanavin@rambler.ru

Abstract. The article examines the issues of information security in the field of operation of modern light patrol cars of the State Traffic Safety Inspectorate. Based on the analysis conducted, possible solutions to the problem in this subject area are proposed.

Keywords: Information security, patrol car, police, critical systems of a passenger car, security systems.

Современные патрульные автомобили Госавтоинспекции МВД России (ГИБДД) оснащены сложными электронными системами, включая средства радиосвязи, видео-регистрации, навигации, устройствами для передачи данных по мобильным каналам связи 3G/4G, средствами удаленной оплаты штрафов и т.д. В настоящее время базовые комплектации современных легковых автомобилей включают такие мультимедийные и информационные системы как: большой экран - тачскрин, датчики слепых зон, электронный помощник при парковке задом, контроль выхода из полосы, автопилот. Этот функционал становится критически важным для автотранспорта и требует разработки дополнительных средств защиты от постороннего вмешательства нарушителя в работу подобных систем [1]. Эти технологии повышают эффективность работы сотрудников полиции, но одновременно создают новые угрозы информационной безопасности. Утечка или несанкционированный доступ к данным этих систем может привести

к серьезным последствиям, включая потерю управления, компрометацию оперативной информации и нарушение конфиденциальности персональных данных граждан. В статье рассмотрены основные риски информационной безопасности и меры защиты информационных систем в том числе патрульных автомобилей ГИБДД.

Патрульные автомобили ГИБДД обрабатывают конфиденциальные данные, такие как персональные данные водителей, номера автотранспортных средств, видеозаписи с камер контроля дорожного движения и переговоры по защищенным каналам радиосвязи. Основные угрозы включают: перехват информации передаваемой по проводным и беспроводным каналам связи; перехват данных навигационных систем ГЛОНАСС/GPS; кибератаки на бортовые компьютеры; внедрение вредоносного программного обеспечения (ПО) для доступа к базам данных; физический доступ к оборудованию; кража или подключение к системам автомобиля злоумышленниками; утечки через сторонние сервисы; уязвимости в облачных хранилищах или мобильных приложениях, используемых сотрудниками органов внутренних дел [2]. Системы легкового автомобиля, через которые может быть реализовано деструктивное воздействие (Рисунок 1).

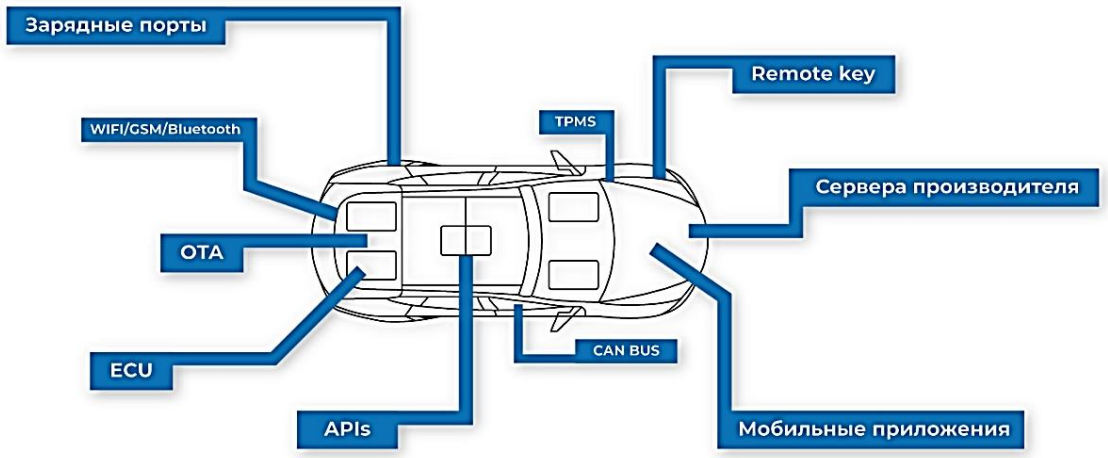

Рисунок 1 – Системы легкового автомобиля, через которые может быть реализовано деструктивное воздействие

Необходимо учитывать, что в современном автомобиле есть хотя бы один модем беспроводной связи (Wi-Fi, Bluetooth, NFC), который может использоваться для работы дополнительных функций. Например для диагностики сбоев и т.д. Такие беспроводные каналы могут быть использованы злоумышленником для реализации деструктивных воздействий [3]. В настоящее время распространены следующие их типы: деструктивные воздействия на приложения и платформы; деструктивные воздействия с непосредственным физическим доступом; деструктивные воздействия через телематику. Например если злоумышленник имеет доступ к CAN шине (Controller Area Network) и, если система слабо защищена, есть вероятность перепрограммирования электронного блока управления (ЭБУ), для разблокировки и угона служебного автотранспорта. Исследователи

называют подобную атаку «CAN Injection». Наиболее подвержены риску легковые автомобили оборудованные системами бесключевого доступа.

Для минимизации рисков информационной безопасности применяются следующие технологические решения и методы защиты: шифрование данных; защита радиопереговоров и передаваемых файлов с помощью криптографических алгоритмов; регулярное обновление ПО; выявление и устранение уязвимостей в бортовых системах и сервисах; многофакторная (биометрическая) аутентификация; ограничение доступа к базам данных и служебным приложениям; физическая защита оборудования; использование защищенных модулей хранения информации и блокировка портов для предотвращения несанкционированного подключения; мониторинг и аудит; анализ логов доступа и выявление подозрительной активности. Системы, на которые может быть оказано деструктивное воздействие нарушителем приведены на рисунке 2.

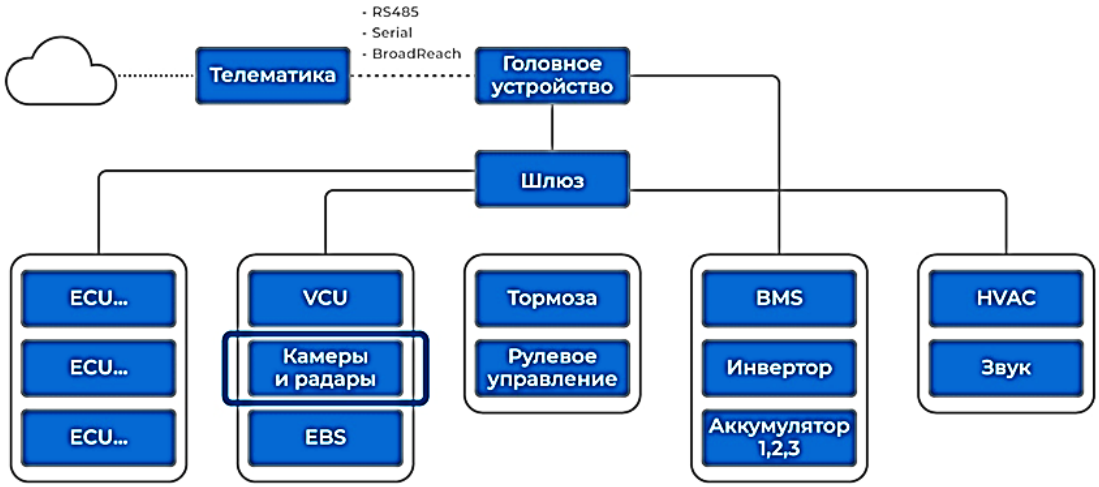

Рисунок 2 – Системы на которые может быть оказано деструктивное воздействие нарушителем

Правовое регулирование в области информационной безопасности патрульных автомобилей Госавтоинспекции. Деятельность ГИБДД в сфере информационной безопасности регламентируется: Федеральным законом № 152-ФЗ «О персональных данных»; руководящими документами регуляторов в области информационной безопасности (ФСТЭК России и ФСБ России), приказами МВД России, устанавливающими требования к защите информации; международными стандартами (ISO/IEC 27001), применяемыми к системам управления безопасностью данных.

Информационная безопасность патрульных автомобилей ГИБДД – критически важный аспект их эксплуатации. Современные технологии помогают предотвращать утечки данных, но требуют постоянного обновления и контроля. Внедрение надежных систем шифрования, строгих правил доступа и регулярный аудит позволяют минимизировать риски ИБ и обеспечить защиту как служебной информации, так и персональных данных граждан. Дальнейшее развитие техно-

логий сегментации и изоляции коммуникационных сетей, применение аппаратных модулей безопасности, регулярные обновления системы безопасности, ограничение сбора и обезличивание персональных данных и ужесточение нормативных требований будут способствовать повышению уровня безопасности в этой сфере. ПО в сфере информационной безопасности внутри автомобиля требует реализации нескольких функций безопасности, таких как защищенные протоколы, управление идентификацией и доступом, обнаружение вторжений и уровни абстракции для криптографических функций. Эти функциональные возможности затем используются функциональными ЭБУ для защиты коммуникаций и предотвращения создания «черных ходов». Поэтому ожидается, что сегмент ПО будет занимать наибольшую долю на рынке автомобильной информационной безопасности в том числе и автотранспорта органов внутренних дел.

Список литературы

1. Характеристика зон уязвимости и источников угроз информационной безопасности эксплуатации беспилотных автомобилей в интеллектуальной транспортной системе // Писарева О.М., Алексеев В.А., Медников Д.Н., Стариковский А.В. / Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2021. Т. 14. № 4. С. 20-36.

2. Автомобильная электроника и угроза ее информационной безопасности // Клиновенко В.В., Колистратов М.В. / E-Scio. 2021. № 9 (60). С. 202-210.

3. Проблемы обеспечения информационной безопасности высокоавтоматизированных транспортных средств // Правиков Д.И., Пономарева Е.А., Куприяновский В.П. / International Journal of Open Information Technologies. 2020. Т. 8. № 6. С. 98-103.

References

1. Pisareva, O.M. Characteristics of vulnerability zones and sources of threats to information security of unmanned vehicles in an intelligent transport system / O.M. Pisareva, V.A. Alekseev, D.N. Mednikov, A.V. Starikovsky // Scientific and technical statements of the St. Petersburg State Polytechnical University. Economic sciences. – 2021. – Vol. 14. – № 4. – Pp. 20-36.

2. Klinovenko, V.V. Automotive electronics and the threat to its information security // V.V. Klinovenko, M.V. Kolistratov / E-Scio. – 2021. – № 9 (60). – Pp. 202-210.

3. Pravikov, D.I. Problems of ensuring information security of highly automated vehicles / D.I. Pravikov, E.A. Ponomareva, V.P. Kupriyanovsky // International Journal of Open Information Technologies. – 2020. – T. 8. – № 6. – P. 98-103.