УДК 004.413.4

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ АВТОМОБИЛЕЙ

Рыбаков С. Д.[1]
Научный руководитель – канд. пед. наук, доцент Авксентьева Е. Ю.[1]
Университет ИТМО
steparyb@yandex.ru

Введение

В ходе длительного пути развития современный автомобиль фактически превратился из механического устройства в цифровой «гаджет» на механической колесной базе. Современное транспортное средство состоит из множества управляющих блоков и цифровых подсистем, может содержать большое количество различных шин данных и интерфейсов взаимодействия, что значительно расширяет его поверхность атаки относительно менее «умных» версий. Использование автопроизводителями технологий удаленного доступа открыло злоумышленникам потенциальную возможность перейти от классических атак на данные к киберфизическим атакам, например, созданию аварийных ситуаций на дорогах общего пользования. При этом, надо отметить, что, хотя возможность таких атак неоднократно доказывалась исследователями безопасности [1], на практике злоумышленниками они пока еще не применялись.

В то же время, национальные и международные регуляторы активно работают над строгой регламентацией кибербезопасности ТС [2]. Например, на уровне ЕЭК ООН приняты правила UN R155 и R156, устанавливающие обязательные стандарты обеспечения информационной безопасности и управления обновлениями ПО для всех поставляемых на рынок ЕС новых ТС. Хотя эти меры признаны во многих странах и побуждают автопроизводителей предусматривать защиту еще начиная со стадии проектирования, надо отметить, что текущие формулировки мер носят скорее декларативный и описательный, нежели технический характер, что дает возможность несознательным производителям ограничиваться формальным соответствием, недостаточно обеспечивающим фактическую безопасность автомобилей.

Основная часть

В работе рассмотрены основные этапы цифровой эволюции автомобиля. Без понимания, что из себя представляет современный автомобиль, невозможно определить ландшафт угроз, сформировать проблемы и пути их решения. При этом, в работе под современными автомобилями понимается в первую очередь общая совокупность транспортных средств, используемых на дорогах общего пользования, и лишь в отдельных, явно обозначенных ситуациях, понимаются автомобили, выпущенные в последние несколько лет и обладающие определенным уровнем цифровизации.

Далее в работе формулируются основные проблемы обеспечения информационной безопасности современных автомобилей, а затем предполагаются и оцениваются возможные способы их решения. В качестве оптимального подхода к защите современных автомобилей предлагается комплекс мер безопасного проектирования, разработки и эксплуатации.

В его основе лежит принцип изоляции критических систем, например, путем разделения бортовой сети на домены с использованием центрального шлюза, реализующего функцию фильтрации сообщений. Корректное использование этого

принципа позволит препятствовать многим продвинутым атакам на безопасность устройства.

Во-вторых, использование принципов безопасной разработки должно стать обязательной составляющей разработки новых версий ПО ТС. Хотя пока это требование как правило не является обязательным с точки зрения нормативно-регулирующих документов, практика показывает, что крупные автопроизводители уже сейчас вкладываются во внедрение соответствующих подходов в своих командах разработки, т.к. выгода более раннего исправления уязвимостей, а тем более недопущения их появления, очевидна.

В-третьих, существует проблема применимости классических мер защиты в автомобилях. С одной стороны, цифровизация существенно снизила порог вхождения для злоумышленников: больше не надо разбираться в низкоуровневых машинных командах, ведь теперь (утрированный пример) можно отправлять обычными и общедоступными инструментами привычные Ethernet-пакеты, чтобы атаковать ТС. Доступные же наложенные механизмы защиты зачастую не поспевают за развитием возможных угроз и самих автомобилей в силу их специфики. Это подтверждает важность разработки новых или адаптации существующих механизмов информационной безопасности к требованиям транспортной отрасли.

Выводы

Проведенный в работе анализ показывает, что проблема обеспечения информационной безопасности современных автомобилей принимается и решается производителями и регуляторами, однако процесс еще далек от завершения.

Ожидается, что в ближайшие несколько лет указанные в работе практики обеспечения информационной безопасности станут фактическим стандартом для подавляющего большинства автоконцернов или регуляторов. Также ожидается и появление на рынке большего числа специализированных инфраструктурных решений, например, удаленных SOC, развития бортовых систем телеметрии и т.д.

Только комплексное применение усилий (со стороны государств и межгосударственных регуляторов, транспортной и ИБ-индустрии) приведет к заметному снижению рисков в обозримом будущем.

В практическом смысле это означает, что автопроизводителям стоит уже вчера начинать инвестировать в кибербезопасность своих продуктов и готовиться к сертификации по новым правилам.

Литература

1. Тренды информационной безопасности современного автомобиля [Электронный ресурс]. – Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2025/07/31/trendy-informacziionnoj-bezopasnosti-sovremennogo-avtomobilya/ (Дата обращения 28.02.2026).
2. С. Мельников, А. Облогина, «Кибербезопасность в автомобильной промышленности: как обеспечить соответствие положениям ЕЭК ООН» cert.kaspersky.ru/publications/reports/2024/02/07/cybersecurity-in-the-automotive-industry-ensuring-compliance-with-unece-regulations/ (Дата обращения 28.02.2026).