Кибербезопасность механизмов обновления по воздуху для транспортных средств

Сергей Мельников, Степан Рыбаков

24.09.2026 Версия 1.0

Оглавление

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Введение

С 1980-х годов, когда в серийных автомобилях появились первые электронные блоки управления (ЭБУ), их количество значительно выросло: в современном транспортном средстве (ТС)[1] таких блоков уже более 100. В 1990-х годах автопроизводители начали применять в ЭБУ микроконтроллеры с перезаписываемой флеш-памятью. Благодаря этому новшеству стало возможно обновлять прошивки блоков в транспортных средствах, которые уже находятся в эксплуатации.

В 2010-х годах автопроизводители стали реализовывать в серийных транспортных средствах функцию обновления блоков по воздуху (Over-the-Air, OTA-обновления). В начале 2020-х годов эту опцию имели минимум 309 моделей 23 производителей. Согласно прогнозам SBD Automotive, в ближайшие 10 лет доля машин с возможностью обновления ЭБУ по воздуху на дорогах США, стран Евросоюза и Китая вырастет более чем в три раза и составит 30–40% от общего автопарка этих стран (рис. 1). Есть основания полагать, что заметно больше таких автомобилей станет и на российских дорогах.

[1] В данной статье рассматриваются транспортные средства, на которые распространяются требования ЕЭК ООН к безопасности обновлений: пассажирские и грузовые ТС (категории M и N), прицепы (категория O), сельскохозяйственное и лесозаготовительное оборудование (категории R, S и T). Подробный список категорий автотранспортных средств, на которые распространяются требования Положений UN 155 и 156, приведен в статье «Кибербезопасность в автомобильной промышленности: как обеспечить соответствие положениям ЕЭК ООН».

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

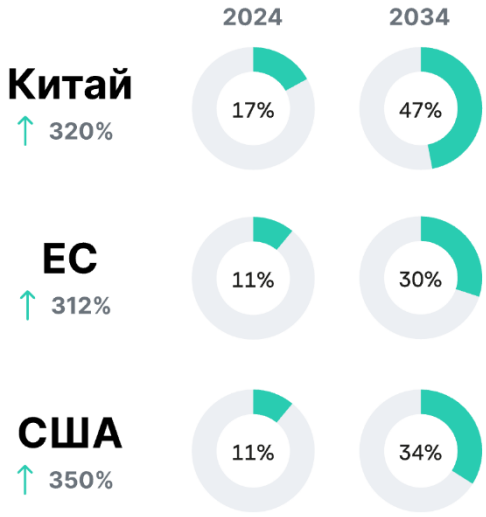

Рис. 1. Текущая и прогнозная доли транспортных средств с возможностью OTA-обновлений от общего автопарка США, стран Евросоюза и Китая

Увеличивается и частота обновлений. По результатам исследования VicOne, еще недавно на одно ТС в среднем приходилось 4–5 OTA-обновлений в год. Ожидается, что совсем скоро частота вырастет до 12–14 обновлений в год.

Зачем нужны обновления по воздуху? Значительная часть функций современного ТС – от взаимодействия пользователя с автомобилем через смартфон до управления режимами коробки передач – строится на основе программного обеспечения. Программный код может содержать ошибки, а обновления по воздуху позволяют оперативно доставлять исправления на все транспортные средства, подключенные к платформе обновлений. Кроме того, разработчики ПО уже на этапе эксплуатации ТС могут дорабатывать какие-либо функции или добавлять новые, подключать автомобиль к новым цифровым облачным сервисам.

Масштабная компьютеризация отрасли создает благотворную почву для роста количества атак на отдельные ТС, автопарки и дорожную инфраструктуру. Атаки непосредственно на транспортные средства пока не получили широкого распространения и в основном сводятся к отдельным случаям угона или нештатной модификации бортового ПО по заказу текущего владельца. А случающиеся атаки на ИТ-инфраструктуру автопроизводителей чаще всего приводят к утечке конфиденциальной информации и финансовым потерям из-за нарушения работы сервисов. Тем не менее исследователи кибербезопасности регулярно

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

обнаруживают в бортовом ПО ТС и бэкенд-инфраструктуре автомобильных сервисов[2] уязвимости, которые могут быть использованы в разрушительных атаках, в том числе выполняемых удаленно. Такие атаки могут быть направлены на парки транспортных средств, подключенных к одному сервису или оснащенных одинаковым дополнительным оборудованием, а также на транспортные средства определенной модели и модификации, объединенные общей архитектурой и наличием определенного штатного электронного блока.

По нашей оценке, вероятные векторы атак на автомобили могут быть связаны с компрометацией инфраструктуры автопроизводителя, его технологических партнеров, провайдеров цифровых сервисов, а также с эксплуатацией уязвимостей в штатных электронных блоках и дополнительном электронном оборудовании, в том числе устанавливаемом для соблюдения требований национального законодательства.

Эта статья состоит из двух частей.

В первой части приводятся примеры атак на системы автопроизводителей, а также примеры отчетов об исследованиях уязвимостей автомобилей и поддерживающей инфраструктуры. Эта часть рассчитана на широкий круг читателей, интересующихся проблемами кибербезопасности современных автомобилей.

Вторая часть описывает архитектурные подходы к решению ключевых проблем безопасности транспортного средства: как обеспечить безопасность на протяжении кампаний обновлений ПО блоков управления, исключить манипуляции с пакетами обновлений и минимизировать возможный ущерб для подключенных транспортных средств в случае компрометации платформы обновлений. Этот раздел будет интересен прежде всего разработчикам, архитекторам платформ обновлений, вендорам автомобильного ПО, поставщикам программных компонентов и цифровых сервисов для поддерживающей инфраструктуры ТС.

[2] Бэкенд-инфраструктура автомобильных сервисов в общем случае представляет собой облачное решение с развернутыми в нем серверами приложений, данных и обновлений. Инфраструктурные сервисы могут быть развернуты как на стороне автопроизводителя, так и на сторонних платформах. Некоторые сервисы могут поддерживаться таксопарками (обработка телеметрии), СТО (ведение электронной сервисной книжки), сетями станций зарядки (поддержка программы лояльности) и т. д.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Как развиваются угрозы для автомобильного ПО

Атаки на инфраструктуру автопроизводителей

Во второй половине 2025 года произошло несколько крупных инцидентов, часть которых пришлась на сектор транспорта и логистики. В сентябре прошлого года производитель автомобилей Jaguar Land Rover (JLR) сообщил об атаке вымогателей, которая затронула деятельность компании и ее поставщиков во всем мире. В результате атаки JLR была вынуждена отключить несколько систем, в том числе используемых на заводах компании. По сообщениям СМИ, несколько поставщиков JLR столкнулись с угрозой банкротства из-за вынужденной приостановки производства в течение нескольких недель.

Представители JLR также заявили, что в результате проникновения злоумышленников в инфраструктуру была скомпрометирована часть данных компании. Злоумышленники опубликовали скриншоты внутренних систем JLR и документацию на автомобили.

В период с 29 сентября по 9 октября JLR удалось справиться с последствиями атаки и поэтапно перезапустить производство. Прямые убытки от атаки на инфраструктуру JLR составили несколько десятков миллионов долларов. Кроме того, для покрытия потерь вследствие остановки производства и нарушения цепочки поставок компания взяла дополнительные кредиты от государства и коммерческих банков на общую сумму в 4,69 млрд долларов. По оценке британского центра мониторинга инцидентов, атака на JLR сказалась на работе около 5000 организаций, нанеся британской экономике совокупный ущерб в 2,5 млрд долларов.

Инциденты со взломом инфраструктуры автопроизводителей и их поставщиков, о которых известно из открытых источников, пока не содержат примеров развития атаки ни на подключенные парки ТС, ни на поддерживающую автомобили инфраструктуру через взлом ТС.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Уязвимости в цифровых сервисах для транспортных средств

Исследователи регулярно обнаруживают уязвимости в цифровых сервисах, к которым подключены современные транспортные средства. Так, в ноябре 2024 года исследователь кибербезопасности Сэм Карри выявил уязвимости на портале администратора Subaru STARLINK – платформе с функциями сопряжения ТС со смартфоном, навигации, удаленного доступа и цифровых сервисов Subaru.

В ходе исследования Сэм Карри сбросил пароль учетной записи одного из сотрудников компании и получил доступ к полномочиям администратора платформы. Через панель администратора можно было не только узнать VIN, регистрационные номера и местонахождение автомобилей в США, Канаде и Японии, но и персональные данные их владельцев: фамилию, адрес, номер телефона и электронную почту. Зная персональные данные владельца, VIN или регистрационный номер автомобиля, администратор платформы мог добавлять новых пользователей с правом удаленного управления ТС. При этом фактический владелец ТС не получал уведомлений ни о добавлении новых пользователей, ни об отправке от их имени удаленных команд на ТС. В качестве демонстрации уязвимости Сэм Кэрри разблокировал автомобиль своей знакомой по его регистрационному номеру. Исследователь утверждает, что аналогичным образом злоумышленники могут запускать или глушить двигатель, а также получать доступ к персональным данным владельцев и информации о ТС (данным о местоположении за 5 лет, пробеге, предыдущих владельцах, истории продаж и пр.).

Цифровые сервисы для современных транспортных средств могут предоставляться не только автопроизводителями, но и сторонними компаниями. Ранее, в январе 2023 года, тот же Сэм Карри продемонстрировал, что транспортные средства могут быть атакованы и через сервисы сторонних вендоров, к которым подключаются крупные автопарки. Он обнаружил уязвимости в инфраструктуре системы Spireon, предоставляющей сервисы телематики и управления автопарком. Использовав простейшую SQL-инъекцию, Сэм получил доступ к CMS этих сервисов и права администратора. А вместе с этим – потенциальный контроль над 15,5 млн транспортных средств, в том числе из автопарков полиции и скорой помощи в нескольких штатах США. Это дало ему возможность отправлять управляющие команды на транспортные

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

средства, отслеживать их текущее местоположение и перепрошивать установленное на них оборудование Spireon.

Отчеты экспертов по информационной безопасности указывают на риск причинения серьезного ущерба миллионам подключенных ТС. Наиболее высок риск несанкционированного доступа к сервисам удаленного управления парками транспортных средств – корпоративными, каршеринга, такси, общественного транспорта, дорожных служб, полиции, скорой помощи.

Отдельные исследования, как правило, закрытые и редко публикуемые, указывают на возможность компрометации функций безопасности ТС – вплоть до удаленного перехвата управления транспортным средством. Это может привести к массовым дорожным инцидентам и созданию затруднений на дорогах общего пользования.

Уязвимости дополнительного электронного оборудования

Еще один вектор атаки на ТС связан с дополнительным электронным оборудованием, которое устанавливается перевозчиками самостоятельно или самим вендором, например для выполнения требований национального законодательства. Такие системы, предназначенные, в частности, для контроля состояния водителей коммерческого транспорта, нередко устанавливаются с нарушением требований информационной безопасности. В результате злоумышленник может получить доступ к каналу удаленного управления важными системами автомобиля.

Исследования безопасности дополнительного оборудования с возможностью подключения к нему по беспроводным каналам связи выявляют большое количество критических уязвимостей и недостатков архитектуры, которые могут быть использованы злоумышленниками для получения контроля над транспортными средствами.

В феврале 2024 года исследователи из Государственного университета Колорадо опубликовали отчет об уязвимостях в прошивке ELD-устройств (Electronic Logging Device). Такие устройства устанавливаются на коммерческий транспорт в США, Канаде и странах Евросоюза для автоматического учета времени, проведенного водителем за рулем, а также для сбора данных о работе двигателя и перемещении транспортного средства, что необходимо для соблюдения законодательных норм этих стран.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Устройство, проанализированное в ходе исследования, имело сравнительно простую архитектуру: оно подключалось к сети ТС через диагностический разъем и отслеживало трафик CAN-шины. Кроме того, оно было оснащено модулем глобальных навигационных спутниковых систем (GNSS) и беспроводными интерфейсами Wi-Fi и Bluetooth для подключения к пользовательским приложениям и мобильным устройствам. В устройстве использовались предсказуемые идентификаторы беспроводных сетей (SSID) и пароли по умолчанию, а также был доступен API, который позволял настраивать устройство и загружать OTA-обновления.

Исследователи загрузили по воздуху в ELD-устройство прошивку, изменившую параметры подачи топливовоздушной смеси в двигатель. В результате тестовый грузовик замедлил ход. Более того, исследователи сумели распространить вредоносную программу типа «червь» с зараженного блока на стоящий неподалеку грузовик (они назвали это ПО Truck-to-Truck Worm). Второй грузовик находился от скомпрометированного ELD-устройства на расстоянии 12 парковочных мест, то есть примерно в 36 метрах. Заражение цели заняло меньше 30 секунд.

В июне 2024 года Kaspersky ICS CERT опубликовал исследование безопасности модемов Telit Cinterion. Такие модемы устанавливаются в том числе в блоки ЭРА-ГЛОНАСС. В ходе исследования были обнаружены семь уязвимостей, для эксплуатации которых необходим локальный доступ, и одна уязвимость, которую можно проэксплуатировать удаленно. Совокупность этих уязвимостей позволяет злоумышленнику полностью скомпрометировать модем, выполнить произвольный код и развить атаку на другие ЭБУ ТС.

От атак на инфраструктуру к атакам на подключенные автопарки

Атаки на ЭБУ требуют от злоумышленника довольно высокого уровня знаний и подготовки: реализовать их сложнее, чем атаковать инфраструктуру цифровых автомобильных сервисов. Атаки на ЭБУ технически сложны, требуют знаний реверс-инжиниринга, опыта поиска и эксплуатации уязвимостей в низкоуровневых компонентах ТС, включая обход встроенных механизмов защиты.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Хотя низкоквалифицированные злоумышленники могут использовать готовые эксплойты, преимущественно для модификации ПО или угона конкретного ТС, самостоятельная разработка эксплойтов им обычно не под силу.

Сейчас наиболее распространенными атаками являются атаки на инфраструктуру автопроизводителей, их поставщиков или сторонние сервисы, используемые владельцами ТС. Последствиями таких атак становятся утечки конфиденциальных данных автопроизводителей и владельцев ТС, простои производства и иные операционные издержки.

Тем не менее, мы полагаем, что в будущем злоумышленники не будут ограничиваться компрометацией серверов и рабочих станций внутри инфраструктуры компании. Исследователи регулярно находят уязвимости в цифровых сервисах и электронных блоках ТС, подключенных к этим сервисам. Такие уязвимости могут использоваться для поиска и реализации векторов атак, целью которых могут стать уже подключенные к этим сервисам парки транспортных средств.

Проблемы безопасности обновлений

Исправление уязвимостей через обновление по воздуху, как и исправление недостатков реализации автомобильных функций, постулируется как одно из преимуществ современных ТС, управляемых программным кодом. На практике же для безопасного обновления ПО ЭБУ автомобилей производители должны решить несколько нетривиальных задач.

Для упрощения поддержки программных модулей разработчики составляют специальные реестры (например, в форме SBOM – Software Bill of Materials), которые учитывают все программные компоненты и описывают связи между ними. Любое обновление ТС может изменить состав программных компонентов и соответствующие зависимости. Поэтому автопроизводитель должен не только формировать такие реестры для производимых моделей транспортных средств, но и актуализировать эти реестры при выпуске обновлений в ходе эксплуатации автомобиля. Без ведения таких реестров и анализа проводимых обновлений трудно представить и выполнение требований

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Правил № 155 ЕЭК ООН[3], о которых идет речь в статье «Кибербезопасность в автомобильной промышленности: как обеспечить соответствие положениям ЕЭК ООН». Согласно этим правилам производитель обязан доводить до сведения органа по официальному утверждению информацию о любой модификации типа транспортного средства, влияющей на его технические характеристики в части кибербезопасности.

Кроме легитимных обновлений от автопроизводителя, владельцы автомобилей или сотрудники сервиса иногда пытаются в обход мер контроля производителей самостоятельно установить несертифицированное электронное оборудование или загрузить в блок управления модифицированную прошивку. Желание некоторых автопроизводителей предотвратить такие манипуляции связано не только с защитой бизнес-модели, предусматривающей доступ к функциям ТС по подписке. Сторонние прошивки могут содержать уязвимый код, вызывать преждевременный износ механических узлов и делать поведение ТС на дороге небезопасным. Автопроизводители стремятся избежать последствий в виде сбоев блоков управления, гарантийного ремонта, штрафов со стороны регулирующих органов и отзыва сертификатов одобрения типа транспортного средства (ОТТС), однако выявлять такие модификации в масштабах всего парка подключенных транспортных средств бывает трудно.

На сегодняшний день существуют технологии для платформ обновлений по воздуху, способные взять на себя задачи управления конфигурацией автомобильного ПО и выявления несанкционированного или модифицированного ПО, установленного на ТС.

В общем случае в архитектуре ТС выделяют один или несколько блоков, отвечающих за взаимодействие с платформой обновлений: они скачивают установочные файлы, проверяют их подлинность и передают на обновляемый блок. В одних публикациях блоки, взаимодействующие с платформой обновлений, называются FOTA Master (Firmware Over-the-Air), в других – Primary. Все блоки, обновляемые через процедуры FOTA при посредничестве таких выделенных блоков, называются FOTA Target или Secondary. В этой статье для обозначения типа блока мы используем

[3] Правила №155 ЕЭК ООН «Единообразные предписания, касающиеся официального утверждения транспортных средств в отношении кибербезопасности и их систем обеспечения кибербезопасности».

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

терминологию FOTA Master – FOTA Target. Процедура обновления FOTA Master – FOTA Target представлена на рис. 2.

Рис. 2. Схема обновления FOTA Master – FOTA Target

Необходимость использования FOTA Master обусловлена как минимум двумя причинами:

1. **Обеспечение кибербезопасности.** Если бы FOTA Master отсутствовал, каждый отдельный блок был бы вынужден самостоятельно взаимодействовать с платформой обновлений по беспроводному каналу, что существенно расширило бы поверхность атаки ТС. Однако FOTA Master сам по себе является приоритетной точкой входа при удаленной атаке, поэтому к нему предъявляются повышенные требования кибербезопасности.
2. **Оптимизация затрат на защиту.** К блокам управления двигателем и трансмиссией предъявляются жесткие требования по времени реакции. Например, блок управления двигателем должен обрабатывать показания датчика положения коленвала и мгновенно, в течение миллисекунды, отдавать команды на открытие или закрытие клапанов. Любое замедление или рассинхронизация управляющих команд блока может привести к ухудшению рабочих характеристик двигателя, снижению его ресурса или поломке. Поэтому в силу специфики выполняемых задач добавление функций безопасности непосредственно в эти блоки либо невозможно, либо приводит к их значительному удорожанию.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Защита процесса обновления на уровне транспортного средства

Защита процесса обновления, а также обеспечение целостности и подлинности обновлений осуществляются за счет мер безопасности на различных уровнях архитектуры ТС: на уровне бортовой сети, FOTA Master и FOTA Target. Выбор и реализация механизмов безопасности проводятся на основе оценки угроз и рисков кибербезопасности для каждого из этих уровней.

В рамках статьи мы приводим меры защиты только для FOTA Master как ключевого блока, поддерживающего процессы обновления. Для FOTA Master актуальны следующие угрозы:

- перехват соединения между ТС и платформой обновлений с изменением передаваемых данных;
- перегрузка FOTA Master и нарушение его доступности (отказ в обслуживании);
- откат к старым и уязвимым версиям ПО;
- загрузка ПО с поддельных серверов обновлений;
- перевод блока в режим отладки с повышенными привилегиями;
- эксплуатация уязвимостей загрузчика для подмены исполняемых файлов и выполнения произвольного кода;
- атаки на конфигурацию блока (параметры подключения и работы);
- компрометация криптографических ключей, подмена корня доверия и атаки на криптографические операции.

Меры защиты

Корень доверия

Защита FOTA Master должна выстраиваться на основе корня доверия (рис. 3), предоставляющего сервисы безопасности, то есть набор базовых неизменяемых функций безопасности. Эти сервисы усиливают меры защиты блоков управления ТС, которые приводятся в последующих подразделах. Корень доверия реализуется на программно-аппаратных модулях безопасности (Trusted Platform Module, TPM или Hardware Security Module, HSM), которые могут быть как частью FOTA Master, так и отдельным модулем.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рис. 3. Корень доверия и меры защиты FOTA Master

Криптографические ключи размещаются в защищенной области памяти и не передаются за пределы программно-аппаратного модуля. Все криптографические операции выполняются внутри его изолированной программно-аппаратной среды, что исключает возможность программного считывания ключей. Защита модуля от атак по побочным каналам исключает перехват промежуточных вычислений и анализ энергопотребления для вычисления ключей шифрования.

Созданию точной копии модуля, то есть его клонированию, препятствуют уникальные ключи устройства (endorsement key), которые генерируются на этапе производства, размещаются в модуле безопасности и связывают конкретный экземпляр прошивки с конкретным модулем. Поэтому прошивка, скопированная с модуля одного ТС, не будет работать на аналогичном модуле другого ТС.

Программно-аппаратная реализация корня доверия защищает FOTA Master от нескольких типов атак, таких как атаки на целостность прошивки или попытки извлечь данные из памяти.

Безопасность соединения с бэкенд-серверами

Шифрование трафика в беспроводных каналах связи при помощи криптографического протокола TLS является базовой мерой, которая обеспечивает конфиденциальность и целостность команд и файлов, поступающих на FOTA Master с серверов платформы обновлений.

Обязательная проверка подлинности серверов платформы на FOTA Master на основе сертификатов X.509 позволяет однозначно верифицировать источники данных и предотвращать атаки типа «человек посредине», направленные на подмену серверов файлов обновлений и команд.

Дополнительными мерами защиты канала связи выступают частный APN и соответствующие политики безопасности, изолирующие обмен данными

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

между ТС и платформой обновлений от публичного сегмента сети провайдера услуг связи. Политики APN могут блокировать попытки подключения к ТС из нетипичной локации или через базовую станцию без поддержки шифрования еще до начала передачи данных.

Аппаратная изоляция и доверенная среда исполнения

Выполнение критически важных операций, таких как дешифрование и проверка подлинности файлов обновлений, должно осуществляться в доверенной среде исполнения (Trusted Execution Environment, TEE). Например, обработка базовой телеметрии выполняется на основных вычислительных ядрах, а проверка подлинности скачанных файлов обновлений – защищенным сопроцессором.

Физическая изоляция операций снижает риск утечки криптографических секретов в случае компрометации верхнеуровневого ПО блока.

Изоляция памяти и периферии[4] микроконтроллера должна выполняться с помощью аппаратных механизмов, например, блоков защиты памяти MPU, которые контролируют взаимодействие между изолированными доменами.

За взаимодействие FOTA Master с бортовой сетью ТС должен отвечать отдельный микроконтроллер. Он берет на себя задачи проверки и обработки сообщений блоков на внутренних шинах данных, предоставляя остальным компонентам FOTA Master интерфейс со строго определенным перечнем доступных команд (API). Компактную прошивку такого микроконтроллера можно сертифицировать по высокому классу автомобильной безопасности.

Комплексные меры изоляции противодействуют попыткам эскалации привилегий, блокируют горизонтальное перемещение атакующего между доменами безопасности и предотвращают несанкционированный доступ к механизмам обновления ТС.

[4] Порты ввода-вывода GPIO; интерфейсы связи UART, SPI; таймеры и счетчики; преобразователи АЦП/ЦАП и пр.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Защита от физического вмешательства и атак по побочным каналам

Отладочные интерфейсы FOTA Master, например JTAG или SWD, должны быть отключены или требовать аутентификации при каждом подключении клиента. Ограничение доступа через отладочный интерфейс блокирует попытки извлечения криптографических ключей и прошивок из памяти блока.

Злоумышленники могут попытаться обойти функции безопасности FOTA Master при помощи лазерного или электромагнитного воздействия на микроконтроллер. Нейтрализовать такие попытки внедрения сбоев помогают аппаратные и программные контрмеры.

1. Аппаратные меры:
   - резервирование ядер (lockstep cores);
   - детекторы сбоев (glitch detectors);
   - аппаратный контроль памяти (ECC и parity check);
   - защитный экран поверх микросхемы;
   - внутренняя рандомизация тактов (clock scrambling и jitter).
2. Программные меры:
   - контроль целостности потока выполнения (CFI);
   - дублирование условных переходов (double checking);
   - многобитовые флаги состояний;
   - искажение времени выполнения (software jitter и dummy cycles);
   - использование сторожевых таймеров (watchdog).

Аппаратные модули безопасности FOTA Master должны быть защищены от физического вмешательства и атак по побочным каналам. Датчики вскрытия корпуса, флуктуаций температуры и скачков напряжения автоматически реагируют на физический взлом и инициируют экстренное стирание секретных ключей или полную блокировку микроконтроллера. Защищенная память модуля безопасности с непрерывным шифрованием содержимого и контролем целостности делает невозможным несанкционированное чтение данных и загрузку произвольного кода.

Аппаратная поддержка жизненного цикла блока

Аппаратная поддержка разделения этапов жизненного цикла блока исключает возможность его возврата в режим разработки или отладки, а также повторного введения устройства в эксплуатацию.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Необратимый переход блока между этапами жизненного цикла реализуется за счет однократно программируемых предохранителей (eFuses). Выжигание предохранителей отладочных интерфейсов на производстве навсегда блокирует доступ к режимам отладки и калибровки блока.

Логика перехода между этапами жизненного цикла может быть реализована с помощью неизменяемых конечных автоматов, как, например, в спецификации EVITA Full HSM. Этап жизненного цикла кодируется не переменной в памяти, а логической схемой из транзисторов и триггеров на микроконтроллере. Этот конечный автомат на основе состояния неизменяемых предохранителей определяет, к каким блокам памяти и периферии разрешен доступ.

В результате злоумышленник не сможет зарегистрировать такой списанный или украденный блок на платформе обновлений под видом легитимного узла. При попытке аутентификации сервер платформы выявит несоответствие подписи блока, сформированной на основе неизменяемых предохранителей, и отклонит сессию.

При выводе из эксплуатации модуль безопасности должен запускать процедуру аппаратного уничтожения информации. Мастер-ключи, сертификаты и сессионные токены, хранящиеся в защищенной памяти, должны перезаписываться случайной последовательностью.

Отказоустойчивость и резервирование критичных данных

Злоумышленники могут намеренно вызывать сбои или отказы в компонентах блока, чтобы исказить или принудительно изменить ключи шифрования, уникальные идентификаторы, метаданные обновлений, файлы конфигурации и т. д.

Для предотвращения модификации таких данных рекомендуется дублировать их в физически и логически независимых областях защищенной энергонезависимой памяти. При выполнении операций целостность данных контролируется при помощи контрольных сумм или хешей. Если обнаруживается повреждение данных, запускается процедура их перезаписи из резервной копии в изолированной области.

В оперативной и энергонезависимой памяти применяются аппаратные коды обнаружения и исправления ошибок, чтобы предотвратить отказы из-за эксплуатационных факторов и целенаправленных воздействий на блок управления.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Блок управления должен поддерживать механизмы атомарной записи данных и журналирования операций. Любые изменения сначала записываются в журнал в энергонезависимой памяти и только потом обновляются в оперативной памяти и основном ПЗУ микроконтроллера. В случае сбоя или нарушения питания запускается процесс восстановления, в ходе которого происходит чтение журнала с последней контрольной точки и выполнение одной из операций: откат к исходному состоянию или повторное внесение изменений.

Управление памятью

Блок управления памятью (MMU) за счет механизмов аппаратной и программной изоляции разграничивает процессы таким образом, что они оперируют исключительно в пределах выделенных им областей памяти.

Некоторые MMU могут ограничивать еще и доступ сопроцессоров или периферийных устройств. Например, графический процессор мультимедийной системы может не иметь доступа к областям памяти, где обрабатывается информация от системы рулевого управления. Области памяти, куда поступают данные из внешних сетей (LTE и Wi-Fi), выделяются только для обработки данных.

Даже если злоумышленник сумеет записать в область данных или стек вызовов свои инструкции, то биты запрета исполнения, установленные в соответствующие страницы памяти (NX-бит или XD-бит), гарантируют, что процессор блока управления откажется исполнять код из этого сегмента.

Дополнительные механизмы защиты могут включать размещение стековых канареек (stack canaries) и рандомизацию адресного пространства (ASLR).

Такое управление памятью нивелирует угрозы атак, связанные с переполнением буфера, несанкционированным чтением данных и исполнением произвольных команд за границами разрешенной области.

Для противодействия атакам, направленным на исчерпание ресурсов блока управления, применяется квотирование вычислительных мощностей и памяти для каждого процесса. Например, квотирование по времени (time-triggered scheduling) не позволяет одному процессу монополизировать все ресурсы и предоставляет время на выполнение важных задач, таких как обработка сигналов от системы экстренного торможения.

Защита конфигурации

Чтобы не допустить несанкционированного изменения конфигурации внутри блока, используются стойкие алгоритмы хеширования, например

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

SHA-256, или контрольные суммы. Конфигурация хранится в защищенной области памяти блока.

Контроль аутентичности команд на изменение конфигурации, направляемых со стороны облачной инфраструктуры на подключенное ТС, минимизирует вероятность их модификации или подмены.

Эти меры защищают от несанкционированного изменения параметров блока.

Журналирование

В журналы заносятся не только события успешной установки, но и промежуточные статусы с указанием версий загружаемых файлов и результатов проверки их подписей. Подозрительные паттерны, такие как множественные неудачные попытки аутентификации или частые отказы доступа, помогают выявить перебор аутентификационных данных и иные следы кибератак. Анализ аномалий на борту позволяет оперативно применить защитные сценарии – блокировку интерфейсов или изоляцию скомпрометированных компонентов.

При проникновении в систему злоумышленники часто стараются скрыть следы присутствия, удаляя или модифицируя записи журналов. Для противодействия этой угрозе журналы следует размещать в защищенной области памяти, выполнив криптографическое связывание содержащихся в них записей.

Проверка подлинности и защита от атак повторного воспроизведения

Источники загрузки обновлений по воздуху необходимо ограничить доверенными ресурсами платформы обновлений[5]. Механизмы цифровой подписи или имитозащиты (MAC) сообщений платформы обновлений снижают риски внедрения вредоносных команд и перехвата управления ТС. Цифровая подпись передаваемых пакетов обновлений минимизирует вероятность модификации или подмены пакетов обновлений, направляемых на подключенное ТС. Проверка пакета осуществляется при помощи открытого ключа разработчика или автопроизводителя, который хранится в защищенном аппаратном модуле (HSM или TPM).

Для противодействия атакам повторного воспроизведения (replay attacks) в трафик, поступающий с платформы обновлений, внедряются штампы

[5] Архитектура и меры защиты платформы обновлений не входят в область рассмотрения данной статьи.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

времени на основе криптографического протокола TSP. Проверив штамп времени, можно подтвердить, что в заданный момент действительно поступили определенные команды и файлы обновлений. При выявлении несоответствий блок управления отвергает входящий трафик от платформы обновлений.

Дополнительной мерой защиты выступает запрет на откат системы к устаревшим версиям. Система находит номер версии в подписанных метаданных устанавливаемого файла и проверяет, превышает ли он текущую версию. Это не позволяет злоумышленникам откатить систему до легитимной, но старой и уязвимой прошивки.

Безопасная загрузка

Безопасная загрузка защищает от эксплуатации уязвимостей низкоуровневого ПО, которые позволяют модифицировать загрузчик и исполняемые файлы, а также обойти защитные механизмы еще до загрузки этих файлов.

Процесс начинается с выполнения верифицированного неизменяемого кода, сохраненного в программно-аппаратном модуле безопасности. Размещение этого кода в однократно программируемой памяти (ROM/OTP) не позволяет злоумышленнику модифицировать или заменить его для обхода проверок на этапе загрузки и для подмены корня доверия. Проверка целостности и подлинности кода загрузчика должна осуществляться при помощи открытого ключа производителя. Блок должен поддерживать процедуры отзыва и обновления открытого ключа производителя.

Этот код последовательно проверяет каждый последующий компонент ПО перед его запуском и передачей управления. Если на любом этапе этой цепочки проверок обнаруживается несоответствие, выполнение кода, не прошедшего проверку, блокируется загрузчиком.

При обновлении злоумышленники могут искусственно вызвать критическую ошибку, которая переводит систему в бесконечный цикл перезагрузки или уязвимое состояние. В такой ситуации загрузчик запускает механизм безопасного отката версии ПО. Он должен распознать некорректный запуск, изолировать поврежденные файлы и восстановить систему на основе верифицированной рабочей версии ПО, хранящейся в защищенной области памяти.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Идентификаторы RxSWIN

Безопасность процесса обновления на стороне ТС обеспечивается рассмотренными выше техническими мерами. Однако их применение не способно гарантировать функционального, а значит и юридического соответствия конкретного экземпляра автомобиля одобрению типа транспортного средства, на основании которого данная модель ТС допускается к продаже и эксплуатации.

ОТТС выдается строго на определенные версии и конфигурации ПО блоков автомобиля. Поэтому, если очередное обновление ПО существенно затрагивает функции блоков управления, потребуется ресертификация для получения нового ОТТС.

Идентификация программных модулей

До недавнего времени автопроизводители по-разному относились к модификациям автомобильного ПО: одни, как BMW, объявили технологическую войну неофициальным прошивкам, тогда как другие заняли более мягкую позицию.

В настоящее время Европейская экономическая комиссия ООН требует от автопроизводителей контролировать, какие именно пакеты обновлений загружаются и как они устанавливаются на транспортные средства.

Правила № 156 ЕЭК ООН[6] обязывают автопроизводителей присваивать специальный идентификатор RxSWIN каждой версии ПО, установка которой влечет сертификацию затрагиваемых типов транспортных средств[7].

Идентификатор состоит из двух частей: Rx (от UN Regulation) указывает на номер Правил ЕЭК ООН, которым должно соответствовать автомобильное ПО, а SWIN (Software Identification) – на конкретную версию данного ПО.

Введение RxSWIN решает сразу несколько задач:

[6] Правила № 156 ЕЭК ООН «Единообразные предписания, касающиеся официального утверждения транспортных средств в отношении обновления программного обеспечения и системы управления обновлениями программного обеспечения».

[7] Про сертификаты одобрения типов транспортного средства можно прочитать в статье «Кибербезопасность в автомобильной промышленности: как обеспечить соответствие положениям ЕЭК ООН».

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- напрямую связывает версию ПО с сертификатом ОТТС;
- обеспечивает контроль установки и конфигурации ПО блоков управления в масштабе всего ТС;
- позволяет выявить «серый» чип-тюнинг;
- формирует доказательную базу при дорожных происшествиях и кибератаках на ТС.

Правила № 156 делегируют обязанности определения формата RxSWIN автопроизводителям. Автопроизводители обязаны определять и присваивать RxSWIN таким образом, чтобы он отвечал следующим требованиям:

- однозначно идентифицировал версии ПО;
- гарантированно обновлялся при каждом обновлении ПО;
- считывался через штатный электронно-коммуникационный интерфейс, например, на СТО, с помощью специального диагностического оборудования через OBD-разъем.

Кроме того, автопроизводитель должен предоставлять и своевременно обновлять всю информацию, связанную с RxSWIN, компетентным органам по официальному утверждению типа ТС[8].

Правила № 156 не содержат подробных инструкций по формированию RxSWIN. Вопрос соответствия формата RxSWIN требованиям Правил № 156 находится на уровне проработки автомобильными инженерами.

Так, японские инженеры предлагают следующий подход к формированию RxSWIN (подробное описание – в материале Report of Japanese Test Phase (Software Update)). Каждой функции электронного блока управления, подлежащего сертификации по какому-либо из правил ЕЭК ООН, присваивается уникальный идентификатор. Такой RxSWIN содержит данные о модели (типе) ТС и идентификатор конфигурации системы – SysID.

[8] В России функции компетентного органа по официальному одобрению типа транспортного (ОТТС) выполняет Росстандарт – Федеральное агентство по техническому регулированию и метрологии.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рис. 4. Пример RxSWIN

Перед выпуском новой версии ПО разработчики должны определить, потребует ли она ресертификации системы. При необходимости изменений в ОТТС разработчики вносят в систему управления конфигурациями новый SysID, состоящий из наименования системы и связанной с ней версии ПО.

Теперь рассмотрим, как происходит обновление соответствующего RxSWIN (рис. 5). Представим, что условная модель ТС поддерживает обновления ПО блоков мультимедиа (IVI), антиблокировочной системы (ABS), системы курсовой устойчивости (ESP) и декоративной подсветки салона. В отношении тормозов действуют Правила № 13-H, в отношении измерения скорости (спидометра) – Правила № 39, а в отношении рулевого оборудования – Правила № 79. Одна система может попадать под действие нескольких Правил ЕЭК ООН или, как в случае с декоративной подсветкой, вообще не регулироваться ими. Поэтому декоративная подсветка не подлежит сертификации, а ПО управления режимами подсветки не требует присвоения RxSWIN.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

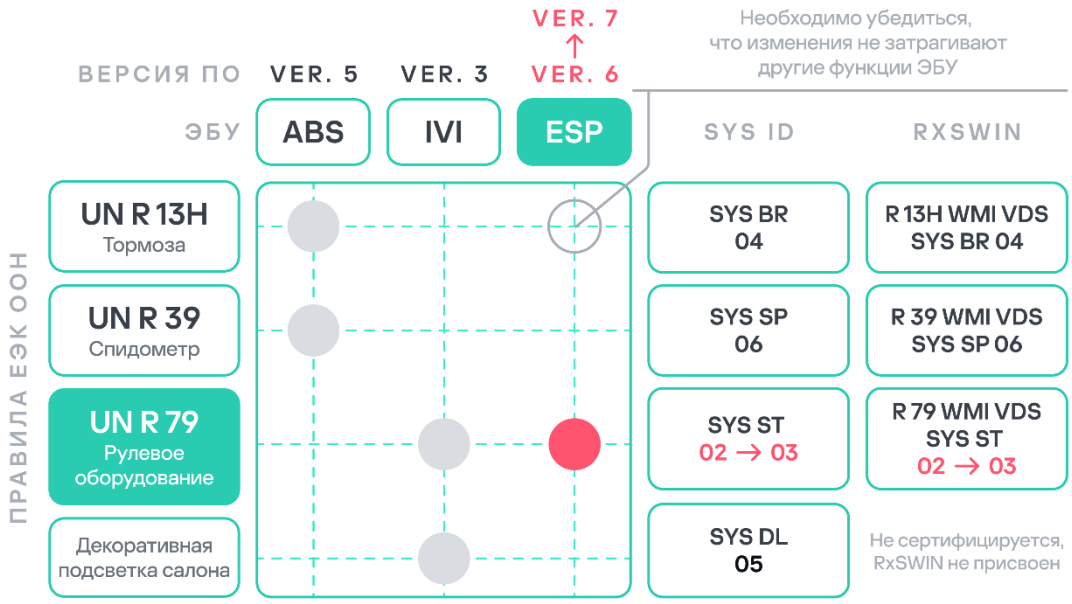

Рис. 5. Обновление ПО и соответствующего RxSWIN

При выпуске очередной версии ПО для ESP, которая включает новые функции управления рулевым оборудованием, необходимо:

1. Присвоить ПО новый идентификатор версии;
2. Обновить SysID, исходя из новой версии ПО;
3. Определить, затрагивает ли новая версия ПО другие автомобильные функции и нужна ли ресертификация других систем;
4. Выполнить ресертификацию системы с присвоением ей нового RxSWIN;
5. Если затронуты смежные автомобильные системы, выполнить их ресертификацию в соответствии с Правилами ЕЭК ООН.

Для соответствия требованиям автопроизводителям недостаточно просто поддерживать в актуальном состоянии перечень версий программных модулей и их зависимостей (SBOM). RxSWIN отличается от простого номера версии ПО, поскольку он требуется только в случаях, когда ПО попадает под сертификацию по какому-либо Правилу ЕЭК ООН. Кроме того, RxSWIN новой версии ПО должен указывать, потребуется ли ресертификация или расширение ОТТС при обновлении до этой версии.

Более того, Правила № 156 усложняют задачу для автопроизводителей, обязывая их обеспечивать защиту от несанкционированных изменений не только установочных пакетов обновлений, но и соответствующих

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

идентификаторов RxSWIN. Помимо этого, для получения сертификата соответствия Правилам № 156, то есть ОТТС, автопроизводители должны предоставить отчет о применяемых методах защиты ТС. Эти методы должны охватывать как блоки и ПО ТС, так и платформу обновлений.

Разные автопроизводители могут использовать разные форматы RxSWIN, и в глобальном масштабе может возникнуть проблема их уникальности. В настоящий момент в отрасли не определен единый механизм разрешения возможных коллизий, например случаев, когда разные автопроизводители декларируют идентичные RxSWIN для различного ПО или, наоборот, разные RxSWIN для одного и того же ПО. Проблема синхронизации и гармонизации RxSWIN приводит к идее о создании единого реестра RxSWIN в масштабах всей отрасли, однако этот вопрос выходит за рамки данной статьи.

Управление журналом RxSWIN для отдельно взятого ТС

Пункт 7.1.2.3 Правил № 156 требует от автопроизводителя ведения журнала учета RxSWIN, в который должны вноситься сведения о связанных с RxSWIN версиях ПО и данных проверки их целостности. В то же время пункт 7.2.1.2.2 допускает хранение журнала как на борту ТС, так и в инфраструктуре автопроизводителя.

Хранение журналов RxSWIN на платформе обновлений может показаться автопроизводителю наиболее приемлемым вариантом, поскольку требует минимальных изменений в архитектуре ТС. В этом случае блок FOTA Master должен загружать пакеты обновлений и проверять их целостность. Дополнительно FOTA Master должен передавать на платформу обновлений версии прошивок обновляемых блоков. Основная нагрузка по планированию кампаний и определению целей обновления[9] выполняется на стороне платформы, где на момент начала кампании могут храниться неактуальные данные. Поэтому бэкенд-серверам обновлений необходимо выполнять актуализацию данных о подключенном парке ТС.

Рассмотрим теперь два полярных варианта хранения RxSWIN на борту ТС:

1. RxSWIN хранятся отдельно на каждом FOTA Target, который получает обновления по бортовой сети от FOTA Master.

[9] Цель обновления (target), по ISO 24089 – модель ТС, автомобильная система или ЭБУ, определяемые на основе данных о конфигурации ТС. Не путать с целью кибербезопасности (cybersecurity goal).

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

2. Журнал RxSWIN хранится на одном или нескольких выделенных блоках (FOTA Master), обладающих необходимыми механизмами безопасности и отвечающих за взаимодействие с платформой обновлений.

RxSWIN хранятся на FOTA Target

Хранение RxSWIN в прошивке каждого блока, как и их хранение на платформе обновлений, также требует минимальных изменений архитектуры ТС. Такая схема в целом соответствует принципам эшелонированной защиты: компрометация любого смежного блока, включая FOTA Master, и доступ к бортовой сети ТС не означает, что злоумышленник автоматически сможет скомпрометировать целевой блок, модифицировав его прошивку и RxSWIN.

Чтобы исключить компрометацию блоков, автопроизводитель должен реализовать более строгие меры защиты для каждого блока. Блоки должны поддерживать защищенные протоколы передачи данных, криптографические механизмы проверки подлинности пакетов обновлений и защиты идентификатора RxSWIN от подмены или изменения.

При таком подходе блоки FOTA Target становятся более сложными и дорогостоящими, их номенклатура ограничивается, а автопроизводитель вынужден тщательно контролировать, насколько ответственно его поставщики подходят к кибербезопасности поставляемых блоков. Роль FOTA Master заключается во взаимодействии с платформой и скачивании обновлений для целевых блоков ТС.

Журнал RxSWIN в этом случае не требуется хранить на автомобиле, он формируется динамически – например, в начале кампании обновления транспортных средств путем опрашивания обновляемого ТС и сохранения итогового перечня идентификаторов на платформе обновлений.

Журнал RxSWIN хранится на FOTA Master

Когда журнал RxSWIN хранится на одном или нескольких FOTA Master, то FOTA Master должен контролировать соответствие идентификаторов прошивок блоков журналу RxSWIN и уведомлять платформу обновлений о несоответствиях. С одной стороны, к обновляемым блокам автопроизводитель может предъявлять менее строгие функциональные требования. С другой стороны, необходимо, чтобы эти блоки поддерживали проверку подлинности и целостности обновлений, поступающих от FOTA Master по бортовой сети.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

FOTA Master должен не только контролировать конфигурацию обновляемых блоков, но и иметь защищенное хранилище для загрузки файлов с платформы обновлений и хранения резервных копий прошивок обновляемых блоков. В журнале RxSWIN FOTA Master агрегирует данные о блоках (идентификатор блока, тип блока, подписи/хеши файлов прошивки, соответствующие RxSWIN и пр.).

Часть функций безопасности, таких как управление криптографическими ключами, защита журнала RxSWIN, проверка подлинности и целостности обновлений, а также безопасная загрузка (secure boot), требует оснащения FOTA Master программно-аппаратным модулем безопасности (например, TPM).

К FOTA Master предъявляются повышенные требования безопасности, поскольку в случае его компрометации злоумышленник сможет успешно развить атаку на любой из управляемых им блоков ТС.

Конструктивная безопасность блоков управления

При определении и реализации требований к электронным блокам автопроизводителям необходимо учитывать как минимум следующие факторы, каждый из которых может стать точкой входа в современные транспортные средства:

- недостатки и ошибки реализации архитектуры блоков, например связанные с доступом к их функциям, конфигурированием, взаимодействием по бортовой сети и беспроводным каналам;
- уязвимости в реализации криптографических процедур и управлении криптографическими ключами;
- уязвимости в компонентах с открытым исходным кодом, сторонних компонентах и компонентах безопасности, устанавливаемых «из коробки»;
- человеческий фактор, выражающийся в стремлении сделать «как удобно», а не как предписывают политики и инструкции безопасности.

При проектировании новой модели ТС недопустимо разрабатывать меры защиты каждого элемента в отрыве от контекста, не учитывая их взаимодействие, в том числе с другими системами. Требования безопасности должны учитываться с самых ранних этапов разработки, в том числе при выборе архитектурных решений. Такая методология разработки описана в ГОСТ Р 72118-2025 «Защита информации. Системы с

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

конструктивной информационной безопасностью. Методология разработки» и применяется при создании конструктивно безопасных систем (Secure by Design), максимально устойчивых к эксплуатации уязвимостей в ходе атак злоумышленников.

Обеспечению кибербезопасности ТС также способствуют практики безопасной разработки. Они помогают своевременно выявить и сократить количество недостатков и уязвимостей в коде, а также избежать внесения новых. За основу при внедрении практик разработки безопасного ПО можно взять ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Заключение

Проблема безопасности удаленного обновления автомобильного ПО признана международными и отраслевыми организациями. Наиболее вероятно, что все больше стран будут стремиться регулировать процессы OTA-обновлений в правовом поле, гармонизируя национальное законодательство с Правилами № 156 ЕЭК ООН.

В этой связи автопроизводителей ожидает ряд сложностей, поскольку количество конфигураций ПО и автомобильного оборудования огромно, а предъявляемые к ним требования объемны и разнообразны. В их числе – требования по внедрению идентификаторов обновлений (RxSWIN). При этом у каждого автопроизводителя собственные требования к идентификации и контролю версий. Это может затруднить достижение согласия об использовании единого формата RxSWIN для участников глобального автомобильного рынка.

Обычно установленный законодательством срок эксплуатации ТС, в течение которого гарантируется безопасная работа всех узлов, составляет 10 лет. Однако на практике ТС часто используются и по истечении этого срока – в течение 15–20 лет и более. Это делает актуальным вопрос о предоставлении обновлений и защите ТС на протяжении фактического срока эксплуатации.

К счастью или, возможно, к несчастью автопроизводителей, ни Правила ЕЭК ООН, ни дополняющий их стандарт ISO 24089:2023 не ограничивают их жестко заданным перечнем технологий реализации. Поэтому, столкнувшись с этими и другими сложностями, автопроизводитель может решить внедрять минимальные меры защиты – только чтобы формально

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

соответствовать международному или национальному законодательству. Однако при таком подходе автопроизводитель рискует оказаться в позиции вечного догоняющего: в кибербезопасности латать дыры при их возникновении – не лучшая стратегия.

Мы считаем, что в динамично развивающейся области обновлений по воздуху в частности и автоматизированного транспорта в целом необходимо занимать проактивную позицию. Проектирование ПО и систем, управляемых ПО, для всех выпускаемых моделей транспортных средств нужно осуществлять с учетом возможности их безопасного обновления. Минимальные меры защиты, способные сегодня обеспечить формальное соответствие нормам стандартов, через несколько лет могут оказаться несостоятельными. Поэтому необходимы конструктивные решения, учитывающие развитие технологий.

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com

© 2026 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»