kaspersky

Тренды информационной безопасности современного автомобиля

31.07.2025 Версия 1.0

Оглавление

Введение

Современные автомобили все активнее стремятся стать полноценными гаджетами на колесах. Они предлагают пользователям массу опций: одни касаются привычного функционала, но теперь доступного в новом формате — вроде подписки на подогрев сидений, другие представляют собой вспомогательные сервисы для жизни — например, по покупке билетов в театр и кино. Расширяется и спектр разнообразных интеллектуальных систем и сервисов, обеспечивающих безопасность участников дорожного движения, — от ставших базовыми систем помощи водителю, таких как электронная система курсовой устойчивости (Electronic Stability Control, ESC), антиблокировочная тормозная система (Anti-lock Braking System, ABS), система помощи при экстренном торможении (Brake Assist System, BAS), до набирающих популярность интеллектуальных систем нового поколения, таких как система предотвращения столкновений (Collision Avoidance System, CAS), система предупреждения о скользкой дороге (Slippery Road Alert, SRA), автоматическая система экстренного вызова eCall, система автономного экстренного торможения (Autonomous Emergency Breaking, AEB) и т. д. Все эти системы, призванные сделать вождение более удобным и безопасным, реализованы с помощью цифровых технологий, которые увеличивают поверхность атаки автомобиля.

Ландшафт угроз современного автомобиля определяется во многом его внутренним устройством. С этой точки зрения автомобиль можно упрощенно представить как набор компьютеров, связанных между собой сетью передачи данных и установленных на передвижную платформу с колесами и двигателем. Но эти компьютеры не только решают какие-то вычислительные задачи во взаимодействии с пользователем через человеко-машинный интерфейс, но и управляют платформой, на которой они установлены. Поэтому, получив удаленное управление автомобилем, злоумышленник может не только украсть данные пользователя, но и создать аварийную ситуацию на дороге.

Несмотря на великое разнообразие возможных целей и последствий кибервоздействия на автомобиль, в реальной жизни встречаются всего два типа сценариев: злоумышленник атакует автомобиль — как правило, для угона, или владелец (или специалист по запросу владельца) делает с ним что-то, не предусмотренное разработчиком, — для тюнинга, дооснащения или нерегламентированного ремонта. Однако угроза преднамеренных действий, нацеленных на функциональную безопасность автомобиля, к счастью для автовладельцев, повседневной реальностью не становится, как минимум пока... Но может ли ситуация кардинально поменяться в обозримом будущем? И что вообще такое современный автомобиль как объект информационной безопасности?

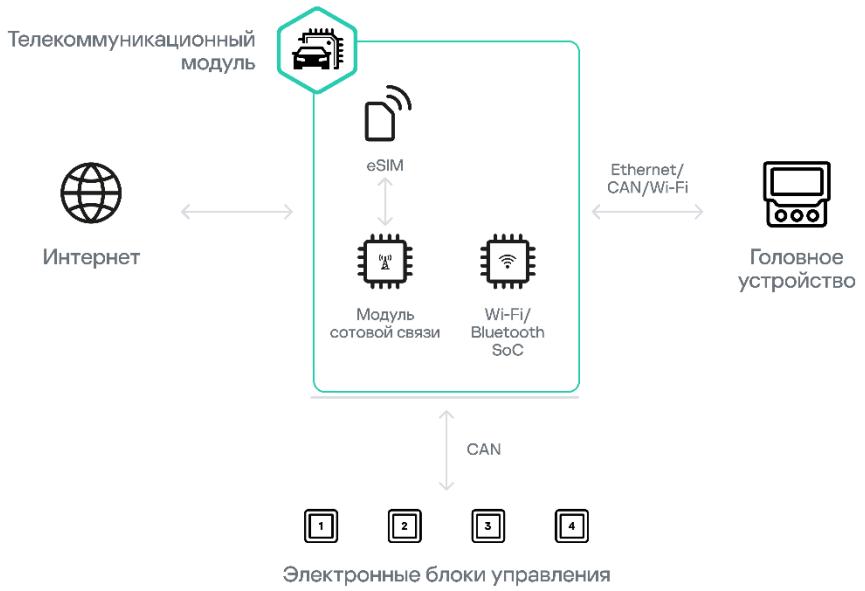
Цифровая эволюция автомобиля

В своем современном виде автомобиль появился относительно недавно. Устанавливать электронные блоки в автомобили начали во второй половине прошлого века, первые цифровые системы, такие как блок управления двигателем и бортовой компьютер, появились в автомобилях в 1970-х годах, а в стандартных комплектациях они заняли место в 1990-х. Эволюция самодвижущейся кареты в то, что мы сейчас называем современным автомобилем, шла по двум основными направлениям: в сторону повышения безопасности вождения и в сторону обеспечения большего комфорта для водителя и пассажиров (если не рассматривать требования защиты окружающей среды и стремление автопроизводителей и прочих игроков автомобильного рынка достичь своих частных коммерческих и политических целей). Эволюционный процесс привел к появлению большого количества узкоспециализированных и технически относительно простых электронных устройств, выполняющих конкретные задачи: замер скорости вращения колеса, управление режимом работы фар, контроль открытия дверей салона и т. д.

Чем ближе к современности, тем больше различных датчиков и контроллеров устанавливалось в автомобиль для наращивания его технических возможностей за счет информационного обогащения уже существующих подсистем управления и создания новых. Для синхронизации и координации работы контроллеров и датчиков используются автомобильные локальные вычислительные сети, исторически строящиеся на базе шин LIN и CAN. С тех пор, как начался этот процесс, прошло около 35 лет, и сейчас автомобиль — это сложное с технической точки зрения устройство. Он обладает богатыми возможностями по удаленному взаимодействию: 5G, V2I, V2V, Wi-Fi, Bluetooth, GPS, RDS.

Компоненты головного устройства (Head Unit, HU) и телекоммуникационного модуля (Telecommunication Unit/Module, TCU/TCM) — штатные точки входа во внутреннюю инфраструктуру автомобиля, поэтому они являются наиболее частыми объектами исследований. Упрощенные архитектуры типовых головного устройства и телекоммуникационного модуля изображены на рисунках ниже.

Архитектура типового телекоммуникационного модуля



С точки зрения функциональных возможностей, оснащения и внутренней архитектуры, а, соответственно, и поверхности атаки разделим условно все автомобили на три категории:

- совсем устаревшие автомобили;
- устаревшие автомобили;
- современные автомобили.

Понятно, что четкую границу между этими категориями, как бы мы ни старались, провести невозможно, и существует много переходных вариантов автомобилей, которые по разным признакам придется отнести сразу к двум категориям.

Совсем устаревшие автомобили

Совсем устаревшими мы называем автомобили, в которых не предусмотрена возможность удаленного взаимодействия с внешними информационными системами по цифровым каналам связи (если не считать подключение диагностического оборудования). Такие автомобили оснащены относительно небольшим набором управляющих блоков. Система коммуникации между блоками управления — примитивна или вообще отсутствует. Об атаках на такие автомобили сложнее угона в результате преодоления механизмов ключевого и бесключевого доступа ничего неизвестно.

Однако следует отметить, что часто такие автомобили дооснащаются более современными головными устройствами и системами экстренной связи. В этом случае автомобили, безусловно, приобретают дополнительные интерфейсы для обмена данными, но в силу того, что сами по себе они имеют устаревшую архитектуру взаимодействия внутренних компонентов, то новые встраиваемые электронные компоненты обычно остаются в замкнутой информационной среде. Это означает, что даже при успешной атаке на них злоумышленник не сможет развить ее на другие компоненты автомобиля.

Устаревшие автомобили

Устаревшие автомобили являются своего рода переходным звеном между простыми автомобилями из прошлого и современными автомобилями, напичканными датчиками и вычислительными блоками. Главное нововведение в таких автомобилях — блок передачи данных через сети беспроводной связи, телематический блок. В большинстве случаев он используется только для сбора телеметрии, но не для осуществления какого-либо удаленного управления (из этого, правда, не следует, что техническая возможность двунаправленной связи отсутствует). Еще одно отличие — более широкая функциональность головного устройства, возможность изменения настроек автомобиля и управления некоторыми его системами. Устаревшие автомобили отличаются и с точки зрения внутренней архитектуры. Во-первых, большинство систем и органов управления в них — цифровые. Во-вторых, подобные автомобили уже нередко оснащаются интеллектуальными системами помощи при вождении. Многочисленные уже электронные блоки объединяются в информационную сеть, обычно «плоскую» или ограниченно разделенную на домены безопасности. Как и в случае с совсем устаревшими автомобилями, штатное головное устройство в этих автомобилях часто заменяют на наделенное современной функциональностью устройство альтернативных производителей, которых вопросы информационной безопасности своих продуктов обычно заботят мало. С точки зрения кибербезопасности устаревшие автомобили, вероятно, представляют собой самую сложную проблему — для них легко достижимы серьезные физические последствия кибератак, вплоть до угрозы жизни и безопасности водителя, пассажиров и других участников дорожного движения. При этом заниматься безопасностью таких автомобилей всерьез никто уже не намерен. Первой публичной демонстрацией факта существования проблем безопасности таких автомобилей стало (каноническое теперь) исследование Чарли Миллера и Криса Валасека с дистанционным взломом Jeep Cherokee. С тех пор в открытом доступе, хоть и не часто, но появляются публикации

результатов похожих исследований, выполненных различными командами, в частности Keen Security Lab[1].

Современные автомобили

Современные автомобили — совсем другое дело. На первый взгляд, технически это — все та же самодвижущаяся платформа со множеством объединенных в информационную сеть электронных блоков управления (Electronic Control Unit, ECU). Однако, как правило, эта сеть уже разделена на домены безопасности при помощи довольно примитивного с точки зрения своей функциональности, но надежно работающего брандмауэра, обычно реализованного внутри центрального шлюза. При этом появление штатных каналов двунаправленного взаимодействия с облачной инфраструктурой производителя принципиально изменяет поверхность атаки. Это заставило исследователей безопасности впервые задуматься о безопасности автомобиля.

Увеличение поверхности атаки автомобиля обуславливается не только ростом числа блоков управления и каналов подключения к внешним системам, но и увеличением количества и сложности сценариев использования. Немалый вклад вносит и увеличение связности системы. Если у исследователя безопасности не получается сходу добраться до какого-то блока одним способом, у него почти всегда есть возможность попробовать «зайти» через другой блок.

Однако автопроизводителям надо отдать должное — большинство из них вынесло урок после нашумевшего исследования Jeep Cherokee. Они доработали архитектуру информационной сети автомобиля, разделили ее на сегменты при помощи центрального шлюза, настроили фильтрацию проходящего через него трафика и изолировали таким образом критически важные системы автомобиля от наиболее доступных для атаки блоков вроде головного устройства и телекоммуникационного модуля. Так автопроизводители существенно усложнили задачу нарушения функциональной безопасности через кибератаку.

Возможное развитие ситуации

В виду вышеизложенных особенностей архитектуры реализовать наиболее опасные для участников движения сценарии атаки, например, удаленно активировать подушку безопасности во время движения на высокой

[1] Некоторые исследования Keen Security Lab:

- Experimental Security Assessment of BMW Cars;
- Experimental Security Research of Tesla Autopilot;
- Experimental Security Assessment on Lexus Cars.

скорости, на современных автомобилях — сложно. А вот достичь других целей — заблокировать запуск двигателя, заблокировать и разблокировать двери, получить доступ к конфиденциальным данным владельца, водителя и пассажиров — часто оказывается значительно проще, ведь в современном автомобиле эти функции доступны через облачную инфраструктуру вендора.

На самом деле, проблем кибербезопасности в современных автомобилях много. Ведущие автопроизводители все чаще обращаются к специализированным командам по анализу защищенности автомобилей. Их задача — провести «нападение» на автомобиль в условиях, приближенных к реальным. Информация из открытых источников о результатах исследований безопасности различных автомобильных брендов и наличие в открытой литературе рекомендаций по проведению анализа защищенности именно этих объектов, например, подробное техническое описание алгоритма проведения исследования безопасности современных автомобилей[2], демонстрируют складывающийся тренд.

При этом важно понимать, что многие исследования остаются под NDA, поэтому о них широкой публике ничего не известно. Хотя бывает и так, что исследователи в погоне за сиюминутной славой публикуют излишне детальные технические отчеты и статьи о результатах исследований безопасности автомобилей и их компонентов, несмотря на возражения производителей. Показательный пример — исследование Keen Security Lab автопилота Tesla.

Но, несмотря ни на что, хакерские атаки на современные автомобили не становятся привычным делом. В таком случае, может, исследователям стоит успокоиться и оставить все как есть?

Кибератака на автомобиль глазами злоумышленника

Киберпреступный мир, или мир нелегального ИТ (да и мир легального ИТ — тоже) можно условно разделить на две касты — неравнозначные по численности и квалификации участников. Первую составляют разработчики и исследователи, которые разрабатывают специфическое ПО, оборудование и сервисы и придумывают новые способы их применения. Вторая объединяет тех, кто все это использует. Массовое распространение продуктов и сервисов для проведения атак позволяет отбивать расходы на исследования и разработку. При определении приоритетов деятельности представители киберпреступного мира руководствуются принципами экономической выгоды и собственной безопасности — все, как в любом бизнесе. При выборе целей, схем и методов работы злоумышленники, закономерно, учитывают:

[2] Alissa Knight. Hacking Connected Cars: Tactics, Techniques, and Procedures, 2020.

- порог вхождения;
- возврат инвестиций;
- риски.

На данный момент отсутствует вредоносное ПО, разработанное специально для атак на автомобили, равно как и схемы монетизации, а значит, порог вхождения для потенциальных злоумышленников — высокий. Масштабируемость атак — плохая, а следовательно, гарантированная доходность — низкая. При этом риски очень высоки — и это, пожалуй, самый важный в данном случае фактор.

Даже такое распространенное нештатное вмешательство в работу систем автомобиля, как чип-тюнинг, требует большой осторожности и четкого понимания действий. Если записать неверные характеристики в блок управления двигателем, то это приведет не к увеличению мощности, а к серьезной поломке. А неправильно запрограммированное дооснащение тормозной системы или системы освещения дороги способно спровоцировать ДТП.

Тем не менее, схема монетизации у такого рода экспертов — вполне рабочая. Риск минимален, поскольку вся ответственность за нештатное вмешательство возлагается на заказчика-пользователя. Однако в случае тяжелых непредвиденных последствий кибератаки на автомобиль переложить ответственность на кого-либо еще окажется проблематично. Преследовать злоумышленника, неосторожные действия которого привели к угрозе жизни и здоровью людей, станут куда жестче, чем кибервымогателя, атаковавшего ИТ-системы компании, имеющей страховку от таких рисков.

Превращение автомобиля в гаджет упрощает его взлом

Однако ситуация медленно, но меняется. Этому, в первую очередь, способствует превращение автомобилей в гаджет (для некоторых автопроизводителей это становится наиболее приоритетным направлением развития их продуктов). В результате в автомобиле появляется множество компонентов, реализованных с использованием распространенных технологий (в первую очередь, операционных систем общего назначения, таких как Linux и Android, во вторую — приложений с использованием кода с открытыми источниками и общих компонентов от третьесторонних ИТ-производителей). Все это делает компоненты автомобиля похожими на прочие ИТ-системы, позволяя реализовывать традиционные техники и тактики атак.

Внедрение средств беспроводной коммуникации делает автомобиль доступным для удаленных злоумышленников

Многие из ключевых компонентов, на основе которых строятся беспроводные коммуникации современных автомобилей, например, LTE-модемы систем телематики, могут содержать критические уязвимости, допускающие возможность удаленного управления. А сим-карты могут использоваться для отслеживания местоположения автомобиля без ведома автовладельца.

Специальный инструментарий становится все более доступным не только для добросовестных исследователей, но и для злоумышленников

Еще 20 лет назад возможность использовать программно-определяемую радиосистему (Software-Defined Radio, SDR) была лишь у специализированных лабораторий, тогда как теперь любой желающий может приобрести это устройство в интернет-магазине. В Сети огромное разнообразие доступного ПО и инструкций по проведению атак на беспроводные сети различных типов: Wi-Fi, GSM, 3G, описаны методики взлома Bluetooth и Bluetooth low energy, а также LTE.

Наблюдаются перемены в киберкриминальной среде и на рынках соответствующих продуктов и услуг

Возможно, в какой-то момент атаки на традиционные цели утратят свою привлекательность. Например, если организации-жертвы вымогателей станут платить меньше или вообще начнут категорически отказываться платить за обещание разблокировать ИТ-системы или не публиковать и не перепродавать украденные у них данные, то злоумышленники, возможно, переключатся на принципиально новые цели.

Какие автомобили в зоне риска

Так станут ли атаки на автомобили логическим развитием атак на классические ИТ-системы? С технической точки зрения, более простыми и потому реалистичными кажутся атаки на наиболее удаленно доступные устройства (головное устройство или телекоммуникационный модуль) или облачные сервисы и мобильные приложения — ради вымогательства или кражи личной конфиденциальной информации (например, записей аудио - и видеопотоков, данных о маршрутах передвижения и прочего). Но и такие сценарии требуют значительных вложений в исследования, разработку

инструментария, а также доработки инфраструктуры и повышения квалификации рядовых исполнителей.

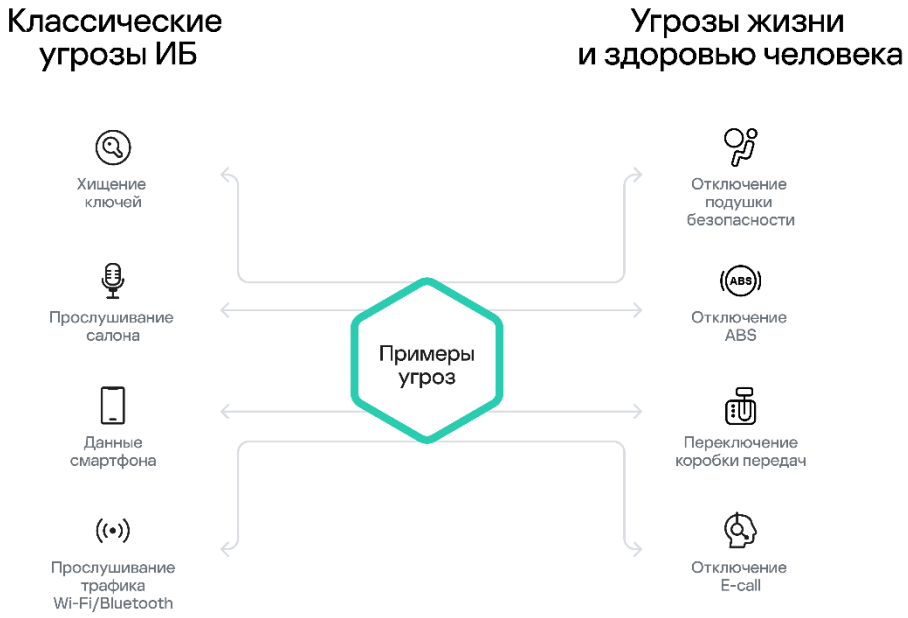
Опять же нужно как-то минимизировать риски на тот случай, если что-то пойдет не так — такую вероятность исключить полностью все же нельзя, даже в случае, если атака не нацелена на критически важные системы автомобиля. При этом успешная реализация атаки тоже не гарантирует, что хотя бы большинство жертв из числа частных владельцев и пользователей автомобилей согласятся заплатить выкуп. Вот и выходит, что частные автомобили в большинстве своем пока малопривлекательны для злоумышленников.

Однако есть еще каршеринговые компании, таксопарки, корпорации и государственные организации с обширными флотами. Автомобили во флоте обычно дополнительно оснащены телеметрическими системами и другим нештатным оборудованием, как правило, однообразным. По уровню безопасности такие дополнительные системы зачастую сильно уступают штатным, да и интегрируются в инфраструктуру автомобиля они тоже далеко не самым безопасным образом. Поэтому атака на подобные системы может иметь значительный масштаб и представлять собой серьезные финансовую и репутационную угрозы для владельцев крупных автопарков. Соблазн сорвать большой куш в данном случае может заставить злоумышленников пойти на риск.

Рассуждая об атаках на нештатные системы сбора телеметрии, важно обратить внимание на грузовики, спецтехнику и городской пассажирский транспорт. Ущерб от атаки на такие машины может быть огромным. К примеру, сутки простоя одного карьерного самосвала могут обернуться убытком в сотни тысяч долларов. Стоимость инцидента, когда такая машина отклоняется от маршрута или утрачивает способность своевременно остановиться, оказывается просто неприемлемой. Информации о результатах исследований безопасности машин такого типа в открытом доступе нет, но это вовсе не значит, что с безопасностью у них все хорошо.

Достоверно известно, что архитектурно такие машины похожи на легковые автомобили и работают на таких же функциональных блоках управления, поэтому имеют схожие проблемы безопасности. Представьте себе, что у всех грузовиков определенной марки и модели одновременно заблокировались тормоза… Опыт, полученный нами в наших исследованиях, говорит о том, что технически такое — вполне реализуемо. Понятно, что подобные атаки тоже дорого стоят и сопряжены с высокими рисками для злоумышленников, а значит, их вероятность стоит рассматривать только в каких-то очень специальных случаях или при резких изменениях геополитической ситуации. На текущий момент об успешных атаках такого рода, к счастью, ничего не известно.

Как и в случае с автомобилями из таксопарков и каршерингов, менее рискованные атаки на грузовики, пассажирский транспорт и спецтехнику могут быть масштабированы и допускают монетизацию через вымогательство. А значит, если злоумышленникам удастся найти способ «все сделать аккуратно» и минимизировать риск неприемлемо тяжелых последствий, то такие атаки вполне могут стать частью реальности. Представьте себе, что после выключения двигателя его включение удаленно заблокировано на всех грузовиках логистической компании, оперирующей на большой территории. Справиться оперативно с таким инцидентом самостоятельно компании может оказаться очень тяжело.



Инвестиции в безопасное будущее

Описанная выше картина, на первый взгляд, не кажется жизнерадостной. И изменить ее можно только через инвестиции в кибербезопасность автомобилей на разных уровнях — от уровня частного пользователя до государственного регулятора. Главных движущих сил — две: забота потребителя (владельца и пользователя автомобиля) о своей безопасности и забота государства о безопасности своей и своих граждан.

К счастью, вопросом обеспечения кибербезопасности автомобилей уже озаботились не только энтузиасты-исследователи, но и вендоры продуктов и поставщики услуг кибербезопасности, а также государственные регуляторы. Требования по кибербезопасности к автомобилям сейчас

закрепляются, в том числе и на законодательном уровне в различных странах. Активно развиваются рекомендации и требования по безопасности к автомобилям, управляемым человеком[3], а в будущем ожидаемо появятся еще и требования по безопасности беспилотных автомобилей.

Под общим давлением инвестировать в тему кибербезопасности начали и автомобильные вендоры (OEM, как их принято называть в индустрии), как минимум, из числа лидеров рынка. Сегодня крупные автопроизводители, как правило, имеют свою собственную команду продуктовой кибербезопасности (Product Security или Product CERT). У них уже налажен процесс реагирования на информацию о новых уязвимостях, а тесты на проникновение являются обязательной частью процесса разработки. Они являются потребителями и активными пользователями информации Cyber Threat Intelligence, пытаются создавать новые продукты методами безопасной разработки и внедряют подходы конструктивной безопасности к разработке наиболее важных компонентов своих продуктов.

В настоящий момент приоритетным направлением для автопроизводителей является внедрение методов безопасной разработки[4]. Это предполагает не только добавление проверок на безопасность кода каким-либо анализатором, например SonarQube, но и общее обеспечение безопасности продукта на каждом этапе его жизненного цикла, от замысла до утилизации. Особенно важным стало обеспечение такой безопасности в цепочке поставки, ведь злоумышленники могут устанавливать свои импланты не только в роутеры. В частности, для решения этой задачи при разработке головного устройства и телекоммуникационного модуля производители выбирают хорошо зарекомендовавшую себя в части ИБ ОС и аппаратную платформу с поддержкой доверенной загрузки.

К этому тренду ежегодно присоединяются несколько автоконцернов, и в течение ближайших 10 лет мы ожидаем, что такой подход станет естественным для доминирующего большинства производителей автомобилей в мире.

Параллельно активно реализуется создание профильных центров мониторинга событий безопасности для автомобилей (SOC). В основе лежит идея удаленного сбора различных данных, доступных со стороны автомобиля, для последующего их анализа на наступление событий информационной безопасности. На основе этих данных теоретически можно выявлять кибератаки на информационные системы автомобиля, создавать базы с информацией об угрозах. Но от теории до практики пока еще далеко. Дело в том, что хотя такая возможность технически доступна на многих автомобилях, на которых установлен телекоммуникационный модуль, данные, которые может предоставить современный автомобиль, пока могут

[3] ISO 26262, SAE J3061, UN R 155/156б, ISO/SAE 21434, ISO 24089.
[4] Dennis Kengo Oka. Building Secure Cars. Assuring the Automotive Software Development Lifecycle, 2000.

лишь косвенно (и не во всех случаях) указывать на его компрометацию, ибо системы сбора телеметрии разрабатывались совсем под другие задачи. Поэтому несмотря на то, что индустрия уверенно движется к разворачиванию таких центров, на текущий момент нет достоверных данных об эффективном применении SOC для управления безопасностью автомобилей. Мы находимся пока в начале пути, который в будущем должен привести к созданию действительно значимых инструментов безопасности.

В любом случае вектор задан, и в ближайшие годы усилия государств, автопроизводителей и специалистов по информационной безопасности должны так или иначе дать свои плоды. Надеемся, это случится до того, как на автомобили как на объект атаки начнет смотреть много злоумышленников.

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