Кибербезопасность в автомобильной промышленности: как обеспечить соответствие положениям ЕЭК ООН

Анастасия Облогина
Сергей Мельников

07.02.2024 Version 1.0

Введение

Кибербезопасность автомобилей традиционно находится в фокусе общественного внимания и внимания регуляторов. Сейчас стадию адаптации на национальном уровне проходят принятые на уровне ЕЭК ООН «Единые положения по сертификации системы управления кибербезопасностью транспортных средств» (далее — Положения UN 155). Эти Положения устанавливают требования кибербезопасности, которые автопроизводители должны соблюдать при производстве всех новых типов автотранспортных средств, начиная с июля 2022 года.

Также были приняты «Единые положения по сертификации системы управления обновлениями ПО транспортных средств» (далее — Положения UN 156), где сформулированы требования к безопасности процесса обновлений прошивок и приложений, установленных в системах автомобиля.

Триггером для принятия Положений 155 и 156, вероятнее всего, послужило появление на потребительском рынке серийных автомобилей с функциями автоматизированного вождения третьего уровня (подробнее об уровнях автоматизации см. рис. 1).

Отличительной особенностью третьего уровня с технологической точки зрения является возможность принятия автопилотом взвешенных решений с учетом окружающей обстановки, хотя в определенных случаях все еще требуется переход на ручное управление автомобилем.

В 2017 году Audi вплотную подошла к реализации функций автоматизированного вождения третьего уровня в модели A8, но впоследствии компания отказалась от этих планов из-за коллизий в законодательстве, существовавших в то время.

Первым автомобилем с третьим уровнем автономности, допущенным на дороги общего пользования в 2021 году, стала Honda Legend, однако аренда автомобиля с такими характеристиками была возможна лишь в Японии.

В начале 2022 Mercedes-Benz запустила продажи серийных машин в премиум сегменте с третьим уровнем автономности (S-class и EQS), сертифицированных по правилам ЕЭК ООН UN 157 для движения в полосе со скоростью, не превышающей 60 км/ч. В 2022 году Mercedes-Benz получила лицензию на использование функций автоматизированного вождения на территории Германии, на 2024 год намечено получение лицензии в ряде штатов США.

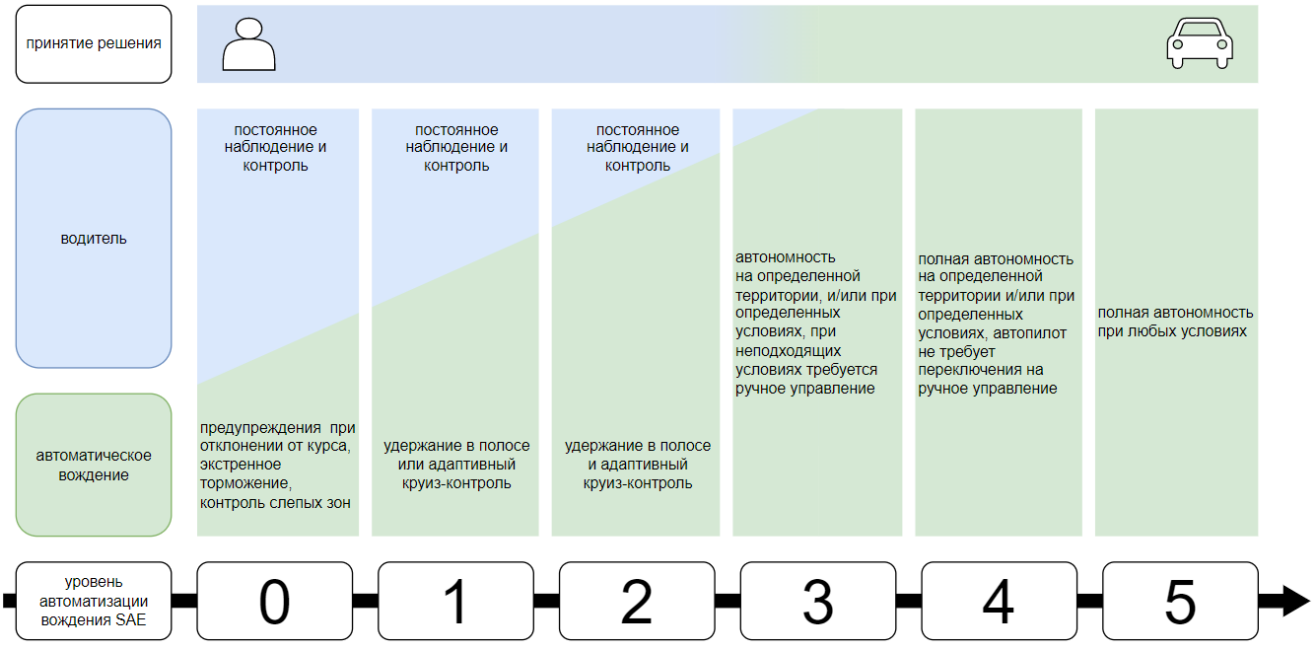

Рис. 1. Уровни автоматизации SAE

Одновременно с появлением серийных машин с третьим уровнем автономности (рис. 1), национальные правительства начали адаптировать законодательную базу для допуска данных автотранспортных средств на дороги общего пользования. Так, в 2017 году Бундестаг внес поправки в Акт регулирования дорожного движения в Германии, разрешающие использование автомобилей, оснащенных системами автоматизации вождения третьего уровня, на немецких автодорогах. В июле 2021 года вступили в силу аналогичные поправки для четвертого уровня автоматизации.

Согласно данному Акту автопроизводитель обязан предоставить контролирующим органам (KBA или уполномоченной технической инспекции) результаты анализа и оценки рисков кибербезопасности и продемонстрировать, что автомобиль должным образом защищен от кибератак на протяжении всего жизненного цикла — от этапа разработки до утилизации.

Однако только национальных законодательных актов о введении ответственности автопроизводителей за кибербезопасность транспортных средств недостаточно, так как рынок транспортных средств глобальный. Именно поэтому требования нужно унифицировать на международном уровне.

Проблемами гармонизации автомобильных стандартов на международном уровне занимается Всемирный форум по гармонизации стандартов для транспортных средств при ЕЭК ООН (WP.29). В нормативных

требованиях к автопроизводителям, разрабатываемых странами — участницами форума, используется принцип взаимного признания результатов сертификации автомобилей и отдельных компонентов. То есть результаты сертификации, проведенной в одной из стран — участниц ЕЭК ООН, признаются остальными странами-участницами.

Положения ЕЭК ООН в области обеспечения автомобильной кибербезопасности действуют в 64 странах, подписавших Соглашение 1958 года[1]. Россия (СССР) присоединилась к Соглашению 1958 года, регламентирующему работу стран — участниц форума, 17 февраля 1987 года.

Страны, не входящие в ЕЭК, для продажи своей автомобильной продукции на рынках стран-участниц должны обеспечить ее соответствие требованиям ЕЭК ООН.

Список категорий автотранспортных средств, на которые распространяются требования Положений UN 155 и 156, приведен в таблице ниже:

Категория ТС	Описание категории	Применяемые требования
L6	Четырехколесные ТС с массой не более 350 кг, объемом ДВС 50 куб. см и максимальной конструктивной скоростью 45 км/ч	UN 155, если ТС соответствует третьему уровню автоматизации или выше
L7	Четырехколесные ТС с массой не более 400 кг и номинальной мощностью при длительной работе не более 15 кВт	UN 155, если ТС соответствует третьему уровню автоматизации или выше
M	ТС с четырьмя и более колесами, предназначенные для перевозки пассажиров	UN 155 и UN 156
N	ТС с четырьмя и более колесами, предназначенные для перевозки грузов	UN 155 и UN 156

[1] Соглашение о принятии согласованных технических правил ООН для колесных транспортных средств, предметов оборудования и частей, которые могут быть установлены и/или использованы на колесных транспортных средствах, и об условиях взаимного признания официальных утверждений, выдаваемых на основе этих правил ООН

O	Прицепы по крайней мере с одним ЭБУ	UN 155 и UN 156
R	Сельскохозяйственные прицепы	UN 156
S	Прицепное (буксируемое) сельскохозяйственное и лесозаготовительное оборудование	UN 156
T	Любое моторизованное, колесное или навесное сельскохозяйственное оборудование с двумя колесными осями, способное передвигаться со скоростью выше 6 км/ч	UN 156

С июля 2024 года Положения UN 155 и 156 станут обязательными не только для разрабатываемых, но и для всех выпускаемых автотранспортных средств. Некоторые производители уже приступили к оценке своей степени соответствия Положениям и к подготовке к прохождению сертификации. Это, однако, может быть затруднительно в отсутствие рекомендаций и технических регламентов по обеспечению соответствия, которые пока не выпущены национальным регулятором.

Мы предлагаем разобраться, как не превратить подготовку к сертификации, потраченное время и ресурсы в чисто «бумажную безопасность», а наоборот, улучшить на практике состояние кибербезопасности автотранспортных средств и предприятий автомобильной промышленности. Для этого прежде всего нужно понять, какие объекты подпадают под эти требования и как для этих объектов можно систематизировать и минимизировать актуальные киберриски.

Мы рассмотрим эти вопросы в настоящей статье. Также мы разберем, чего требуют Положения UN 155 и 156 от автопроизводителя по сути, и покажем, как можно обеспечить соответствие требованиям и при необходимости подготовиться к прохождению сертификации.

Особенности проблемы кибербезопасности в автомобильной отрасли

Проблема кибербезопасности очень значима для всех игроков автомобильного рынка: от крупных межнациональных профессиональных сообществ до небольших поставщиков электронных компонентов. Управление автомобилем сопряжено с высоким риском для всех участников дорожного движения: водителей, пассажиров, пешеходов. Проблема обеспечения кибербезопасности затрагивает и других стейкхолдеров, таких как автопарки, провайдеры услуг каршеринга и такси, сети дилерских центров.

Для автомобильной отрасли характерна распределенная как географически, так и иерархически и функционально сложная цепочка поставок, которая включает:

- *непосредственно автопроизводителя (OEM — Original Equipment Manufacturer);*
- *поставщиков отдельных автомобильных систем и модулей (Tier 1 supplier), таких, например, как коробка передач, информационно-развлекательный модуль или блок управления двигателем;*
- *поставщиков, производящих отдельные компоненты систем и модулей, например микросхемы, датчики, контроллеры, операционные системы, подшипники, приводы и т. п. (Tier 2 supplier);*
- *а также поставщиков различных услуг и сервисов.*

Для перечисленных участников за словами «надежная и безопасная эксплуатация автомобилей» могут стоять разные цели, задачи и сценарии эксплуатации. Тем не менее все эти участники сходятся в общем понимании свойств безопасности, связанных с предсказуемым поведением автомобиля и соответствием этого поведения требованиям безопасности. И все они заинтересованы в том, чтобы сохранить эти свойства.

Помимо этого, автопроизводитель и его поставщики должны быть заинтересованы в обеспечении безопасности не только продукции — автомобилей, комплектующих, ПО, — но и в безопасности собственной инфраструктуры. Проблемы с безопасностью автомобильного производства могут привести к проблемам с автомобилями, а значит потенциально — к ущербу жизни и здоровью людей. Именно поэтому в автомобильной отрасли предъявляется так много требований внешних регуляторов, которые являются обязательными к исполнению.

Актуальные риски кибербезопасности

Требования кибербезопасности в автомобильной отрасли распространяются как минимум на следующие объекты:

1. сама продукция — то есть автомобиль и его компоненты;
2. поддерживающая инфраструктура на этапе эксплуатации (например, серверы обновлений для прошивок электронных блоков управления — ЭБУ);
3. ИКТ-инфраструктура производителя, безопасность которой важна для разработки, производства и последующей поддержки продукции;
4. цепочка поставок отдельных электронных компонентов и систем автомобиля.

Риски для автомобиля

Современные автомобили имеют сложную функционально-ориентированную архитектуру, состоящую из нескольких сотен интегрированных между собой электронных компонентов. Разнообразие функционала (управление двигателем, топливной системой, обеспечение безопасности пассажиров, автопилот, информационно-развлекательная система), архитектуры сопряжения отдельных компонентов (CAN, LIN, Ethernet, Wi-Fi), способов обеспечения связи с внешними сервисами и объектами (Bluetooth, Wi-Fi, LTE) обусловливает большую поверхность кибератаки на автомобили.

Случаи успешных атак на автомобили демонстрируют, что злоумышленники для проникновения в системы автомобиля могут использовать широкий арсенал средств: от физического доступа к разъемам диагностики или электропроводке шин передачи данных до удаленной эксплуатации уязвимостей в приложениях и протоколах передачи данных. Однако в большинстве случаев злоумышленник ограничивается взломом одного или нескольких сопряженных ЭБУ в пределах одного автомобиля.

Результатом успешных атак на автомобиль может стать кража или модификация данных (персональных данных, платежной информации и других пользовательских данных), внедрение вредоносного кода/прошивок, нарушение работы или манипуляция отдельными функциями автомобиля, угон автомобиля, физический ущерб для самого автомобиля, ущерб для жизни и здоровья участников дорожного движения.

Следует отметить, что реализация подобных атак может являться следствием несовершенства архитектуры систем автомобиля,

используемых технологий и программного кода, а также отсутствия необходимых тестов и проверок на ранних этапах разработки и производства автомобиля. Поэтому автопроизводитель должен управлять рисками не только для готового автомобиля или его компонентов, а по возможности приступать к этому как можно раньше — еще на стадии проекта, до начала разработки.

Существуют и опосредованные атаки на автомобиль, которые эксплуатируют недостатки поддерживающей инфраструктуры, уязвимости алгоритмов и протоколов обеспечения связи автомобиля с внешними объектами и сервисами. И наоборот, злоумышленники могут использовать уязвимости в электронных системах автомобиля (например, уязвимости в протоколах аутентификации или передачи данных пользовательских приложений) для проникновения в сервисы поддерживающей инфраструктуры.

Риски поддерживающей инфраструктуры

Поддерживающая (бэкенд) инфраструктура автомобильных сервисов в общем случае представляет собой облачное решение с развернутыми в нем серверами приложений, данных и обновлений. Сервисы поддерживающей инфраструктуры 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. п.

Стоит выделить службу автомобильной телематики, которая не только занимается сбором информации о работе систем автомобиля и анализом полученных данных, но и может иметь в своем составе C&C серверы, которые способны при наступлении определенных условий передавать управляющие сигналы для автомобильных систем (например, команды на дистанционный запуск двигателя или открытие и закрытие дверей).

Можно привести следующие примеры атак на поддерживающую инфраструктуру:

- загрузка и установка поддельного обновления;
- загрузка поддельных резервных копий данных или конфигураций;
- отправка автомобилю нелегитимных команд с C&C сервера злоумышленника;

- атака на серверы поддерживающей инфраструктуры (например, на сервер управления сетью станций зарядки) и последующая утечка персональных данных и платежной информации;
- изменение на небезопасное состояние во время обслуживания на СТО (изменение конфигурации, внедрение руткита и т. п.).

Атаки на серверы и сеть поддерживающей инфраструктуры могут привести к нарушению их работы, краже, подделке, потере или подмене обрабатываемых данных. Примерами атак на поддерживающую инфраструктуру могут служить заражение бэкенд-серверов вредоносным кодом (например, шифровальщиками) или кража данных вследствие эксплуатации уязвимостей в алгоритмах аутентификации или управления сессиями.

Недоступность сервисов или данных поддерживающей инфраструктуры может вызвать недоступность некоторых функций информационно-развлекательной системы или более серьезные последствия: отказ системы помощи при вождении, невозможность открыть автомобиль или завести двигатель.

Для автопроизводителя и других стейкхолдеров любое слабое место компонента будущего автомобиля и поддерживающей инфраструктуры оборачивается долгосрочными рисками. Некачественный код компонентов, небезопасная архитектура инфраструктуры обновлений по воздуху не скажутся на безопасности и непрерывности процессов немедленно. Однако в перспективе автомобиль не сможет противостоять кибератакам, что может повлиять на безопасность и функциональные характеристики. В результате производитель, возможно, будет вынужден отзывать часть продукции или вкладываться в дорогостоящие мероприятия для компенсации рисков.

Риски для ИКТ-инфраструктуры автопроизводителя

Автопроизводитель — это промышленная организация, структура которой сочетает обычную ИКТ-инфраструктуру бэк-офиса, т. е. вспомогательных и обеспечивающих подразделений (бухгалтерии, юридического отдела, материально-технического обеспечения офиса и др.), с инфраструктурой подразделения разработки, промышленным сегментом и серверами поддерживающей инфраструктуры.

Характерной особенностью угроз, связанных с ИКТ-инфраструктурой, являются высокие операционные риски. Проникновение в информационные системы бэк-офиса, R&D или в производственную инфраструктуру через ИКТ-инфраструктуру может привести к нарушению планов выпуска

продукции, задержке или остановке производства, внедрению вредоносного кода в прошивки или обновления, утечке данных о разработке, в том числе утечке интеллектуальной собственности и ноу-хау.

Так, например, 29 августа 2023 года голландский производитель электромагнитных автокомплектующих и блоков управления к ним Kendrion сообщил о взломе своей ИКТ-инфраструктуры и доступе неизвестных злоумышленников к бизнес-системам компании. Kendrion отключил атакованные системы и инициировал расследование инцидента с привлечением внешних экспертов. Представители компании не исключили возможности утечки данных, однако не сообщили подробностей о категории информации, к которой могли получить доступ злоумышленники. Ответственность за атаку взяла на себя группировка вымогателей LockBit, угрожая опубликовать данные утечки 2 сентября. 5 сентября компания Kendrion заявила о восстановлении работы ключевых бизнес-систем.

А 27 марта 2023 года немецкий производитель компонентов шасси для грузовиков и грузовых прицепов SAF-HOLLAND SE сообщил о кибератаке на свои ИКТ-системы. В ходе реагирования на инцидент атакованные системы были отключены, что повлекло остановку производства на нескольких площадках компании — по оценке представителей компании, простои могли составить от 7 до 14 дней. В мае стало известно, что эта кибератака привела к временному дефициту продаж на общую сумму около 40 миллионов евро.

Автомобильному производству и разработке свойственны жесткие плановые сроки выпуска конкретной модели автомобиля. Поэтому при нарушении в результате успешной атаки процессов, обеспечивающих основную операционную деятельность (производство и разработку), возникают серьезные риски нарушения сроков и финансовых потерь.

Нарушение работы обеспечивающих подразделений негативно сказывается на графике разработки, что приводит к переносу сроков и дополнительным затратам на восстановление нормального функционирования как бэк-офиса, так и основных процессов, связанных с разработкой и производством. При фиксированных датах выпуска новых моделей меньше времени и ресурсов остается собственно на разработку и запуск в производство, поэтому фактор «горящих сроков» может негативно сказаться на качестве кода (возникает так называемый технический долг) или привести к выбору неоптимальных или недостаточных мер и средств обеспечения безопасности автомобилей.

Большинство рисков ИКТ-инфраструктуры являются краткосрочными. Исключение составляют угрозы для автомобилей и их компонентов,

реализуемые через взломанную инфраструктуру и внедрение закладок в программный код. Однако в настоящее время более вероятными и актуальными остаются операционные риски, связанные с кибератаками, например, шифровальщиков или стилеров.

Риски кибербезопасности, связанные с цепочкой поставок

Автопроизводители могут не иметь объективной оценки зрелости практик безопасности в цепочке поставок. Это может приводить как к нарушению процессов поставки, так и к компрометации поставляемых компонентов и сервисов.

Поставщики могут не предоставлять информацию об используемых компонентах, разработанных третьей стороной. Автопроизводителю также могут быть недоступны сведения о том, придерживается ли поставщик практик разработки безопасного кода, какие проверки и на каких этапах он выполняет. Могут отсутствовать или несвоевременно публиковаться уведомления об обнаружении уязвимостей, не выпускаться критичные обновления безопасности для компонентов автомобиля, не исправляться уязвимости его поддерживающей инфраструктуры.

При атаке на поставщика сбои в его работе могут оборачиваться невыполнением обязательств по поставкам и нарушением планов выпуска конечной продукции или приводить к остановке производства. Сложные атаки на поставщиков могут иметь своей целью добавление закладок в прошивки устройств.

Отсутствие уверенности в безопасности приобретаемых компонентов и сервисов вынуждает автопроизводителей выделять дополнительные ресурсы на тестирование их безопасности и реализацию мер, компенсирующих выявленные риски.

Следует отметить, что комментарии к Положениям UN 155 рекомендуют автопроизводителям как минимум выявлять и учитывать риски не только своих прямых поставщиков отдельных автосистем и модулей, но и их поставщиков, которые производят компоненты для этих автосистем и модулей.

С учетом определённых выше актуальных рисков кибербезопасности предлагаем посмотреть на требования регулятора и понять, как автопроизводителям можно не только обеспечить формальное соответствие требованиям, но и выработать оптимальный для себя подход к минимизации этих краткосрочных и долгосрочных рисков.

Чего требуют положения ЕЭК ООН и международные стандарты

Положения UN 155 и UN 156 содержат требования верхнего уровня, которые можно разделить на две категории: процессно-ориентированные, то есть касающиеся реализации управления безопасностью на уровне организации, и проектно-ориентированные, то есть касающиеся обеспечения безопасности всей производимой продукции — будь то непосредственно автомобили или отдельные системы и компоненты.

Согласно этим положениям, соответствие требованиям подтверждается аудитами, которые проводятся уполномоченными контролирующими органами или техническими службами и организациями и в результате которых выдается Сертификат одобрения типа транспортного средства (Vehicle Type Approval), или OTTC.

В первую очередь автопроизводителям требуется обеспечить управление кибербезопасностью на уровне организации и получить сертификаты на систему управления кибербезопасностью (Cyber Security Management System, CSMS) и систему управления обновлениями (Software Update Management System, SUMS). Максимальный срок действия этих сертификатов — три года. Для их получения автопроизводитель должен продемонстрировать, что перечисленные ниже организационные процессы в рамках управления кибербезопасностью и обновлениями отвечают предъявляемым требованиям, то есть выполняются:

- анализ угроз и оценка рисков (Threat Assessment and Risk Analysis, TARA);
- непрерывный мониторинг, выявление и реагирование на инциденты;
- управление уязвимостями;
- управление цепочками поставок компонентов и управление сервисами;
- управление обновлениями безопасности;
- уведомление контролирующих органов о результатах мониторинга кибербезопасности, в том числе о кибератаках.

Далее автопроизводители должны получать OTTC для производства каждого отдельного типа автотранспортного средства. Наличие действующих сертификатов для CSMS и SUMS обязательно для получения OTTC, поэтому автопроизводителям придется позаботиться о периодическом обновлении этих сертификатов.

Кроме предоставления действующих сертификатов для CSMS и SUMS, автопроизводитель в рамках каждого проекта (под проектом понимается разработка, производство и обслуживание автомобилей конкретного типа) должен реализовать практики обеспечения кибербезопасности для автомобиля.

К сожалению, UN 155 и UN 156 устанавливают только высокоуровневые требования и не отвечают на вопрос, какие действия и в какой последовательности должны предпринять автопроизводители, чтобы пройти сертификацию и получить разрешение на реализацию своей продукции на рынках стран — участниц ЕЭК ООН.

На помощь может прийти стандарт ISO/SAE 21434, утвержденный в августе 2021 года. На рис. 2 приведена структура стандарта.

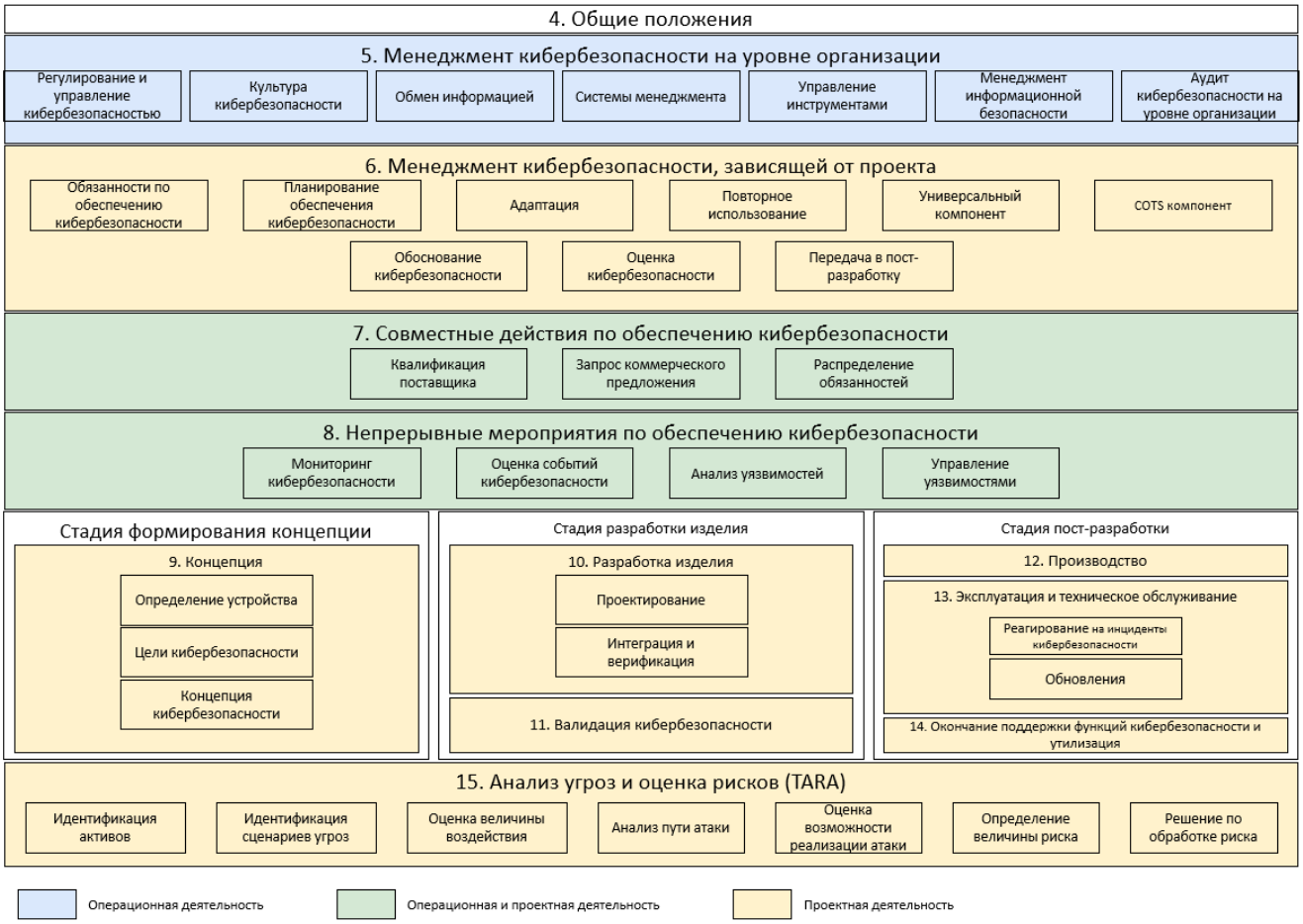

Рис. 2. Структура стандарта ISO/SAE 21434

ISO/SAE 21434 так же, как и UN 155 и UN 156, выделяет управление кибербезопасностью на уровне организации и реализацию практик безопасности в рамках проекта. Выделяются три фазы жизненного цикла проекта: фаза формирования концепции, фаза разработки (включает в себя

действия по разработке и валидации кибербезопасности) и фаза постразработки (включает этапы производства, эксплуатации и технического обслуживания, а также этап окончания поддержки и эксплуатации). Отдельные разделы ISO/SAE 21434 посвящены взаимоотношениям с поставщиками, обеспечению непрерывности киберзащиты, методам анализа угроз и оценки рисков.

ISO/SAE 21434 конкретизирует требования верхнего уровня по обеспечению кибербезопасности, которые содержатся в Положениях UN 155 и UN 156.

ISO/SAE 21434 является хорошим ориентиром не только для внешних аудиторов и представителей уполномоченных органов сертификации, но и для автопроизводителей в части определения границ аудита и полноты и непротиворечивости критериев и свидетельств аудита. Взяв за основу перечень предлагаемых стандартом документов и артефактов, автопроизводитель может подготовиться к прохождению сертификации.

В предыдущем разделе «Актуальные риски кибербезопасности» мы определили объекты, на которые распространяются требования к обеспечению кибербезопасности, и разделили присущие им риски на краткосрочные (операционные) и долгосрочные (рис. 3). Ниже мы рассмотрим подходы к обработке краткосрочных и долгосрочных рисков для обеспечения соответствия требованиям UN 155, UN 156 и ISO 21434.

Рис. 3. Краткосрочные (операционные) и долгосрочные риски

Работа с рисками для обеспечения требований ЕЭК ООН

Процессы обеспечения кибербезопасности автомобиля, цепочки поставок, поддерживающей и ИКТ-инфраструктуры должны быть органично встроены в существующую систему управления организации-автопроизводителя. Роли и обязанности по обеспечению кибербезопасности должны быть распределены согласно зонам ответственности отдельных подразделений.

Обработка рисков для автомобиля и поддерживающей инфраструктуры

Главной целью автопроизводителя является безопасный продукт. Риски и угрозы для автомобиля должны рассматриваться на всех этапах жизненного цикла продукта. Согласно ISO 26262 («Функциональная безопасность — дорожные транспортные средства») жизненный цикл проекта автомобиля разделен на 5 фаз (мы используем именно такое деление, так как фазы определены в ISO 26262 более детально, чем в ISO 21434):

- фаза концепции,
- фаза разработки продукта,
- фаза производства,
- фаза эксплуатации и обслуживания,
- фаза завершения эксплуатации.

Прежде всего необходимо разработать требования кибербезопасности для продукта и заложить их в его архитектуру. Главная сложность состоит в том, что требования могут быть разной степени технической детализации. Они могут колебаться от «нужно, чтобы автомобиль открывался только по сигналу от электронного брелока» до «необходимо в качестве алгоритма проверки сертификата пользователя, заложенного в электронном брелоке, использовать RSA с ключом размером не менее 2048 бит».

Требования проходят ряд преобразований на различных уровнях. На основе требований ISO 21434 можно составить схему, поясняющую, как это должно происходить:

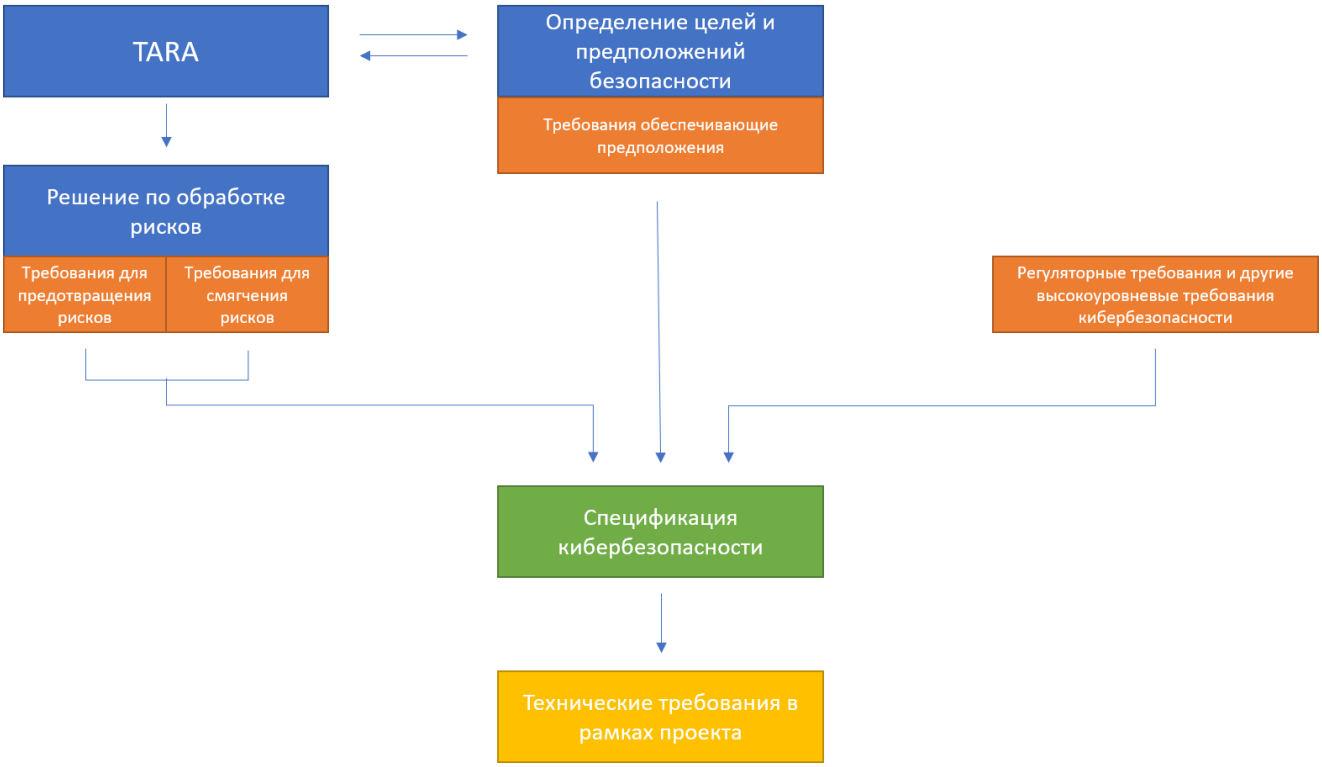

Рис. 4. Выработка технических требований на основе результатов TARA и целей безопасности

Фаза концепции

В рамках фазы концепции необходимо выполнить анализ угроз и оценку рисков (Threat Analysis and Risk Assessment, TARA). TARA выполняется как для отдельных компонентов, так и для автомобиля в целом. Результатом TARA является не только рейтинг рисков безопасности, относящихся к продукту, но и разработка мер, необходимых для минимизации этих рисков.

Согласно стандарту, цели и предположения безопасности определяются по результатам TARA. Цели безопасности описывают желаемое состояние посредством формулировки «Что и от чего мы защищаем?». Их дополняют предположения безопасности, конкретизирующие контекст, который облегчает или осложняет достижение целей безопасности.

Для каждого сценария реализации угрозы принимается решение по обработке соответствующих рисков. Если решение предполагает минимизацию рисков, то формулируется как минимум одна цель безопасности для защиты от угрозы, реализованной по соответствующему сценарию. Если же связанный с угрозой риск принимается, то формулируется предположение безопасности, объясняющее такое решение.

В качестве примера рассмотрим взлом критически важных систем, таких как система помощи водителю ADAS, посредством удаленной атаки и проникновения в информационно-развлекательную систему автомобиля. Цель безопасности при таком сценарии реализации угрозы — защита системы ADAS от проникновения через другие системы автомобиля. Для реализации защиты автопроизводитель разрабатывает доменную архитектуру автомобильной сети, где все взаимодействия между отдельными доменами безопасности контролируются центральным шлюзом с аппаратным корнем доверия. При этом используется предположение безопасности, что взаимодействие отдельных систем автомобиля через центральный шлюз безопасно. Такое предположение вытекает из цели безопасности другого компонента — самого шлюза, — которая заключается в обеспечении безопасного взаимодействия других систем.

На практике TARA и определение целей и предположений выполняются одновременно: цели и предположения отчасти очевидны еще до оценки предполагаемых сценариев атаки; анализ угроз проводится на основе общего понимания задач защиты процессов или активов, после чего цели и предположения уточняются.

К целям и предположениям безопасности добавляются требования регулятора, которые в ходе вышеперечисленных процедур не были учтены, а также другие высокоуровневые бизнес-требования.

Фаза разработки продукта

В начале фазы разработки лидер по кибербезопасности, т.н. security champion, консолидирует все высокоуровневые требования безопасности в спецификацию кибербезопасности для отдельного компонента (или всего автомобиля). Задокументированная спецификация используется им для определения архитектуры, выбора технологий реализации и уточнения технических характеристик.

Далее лидер по кибербезопасности на основе высокоуровневых требований из спецификации для всего компонента (или автомобиля) совместно со специалистами, ответственными за обеспечение безопасности и надёжности кода, формирует перечень требований безопасности к технической реализации и функционированию компонента (или автомобиля). В качестве таких специалистов могут выступать архитекторы решения или ведущие разработчики. Согласование технических требований с ними необходимо, чтобы максимально исключить ошибки при формулировании и реализации требований ещё на ранних этапах разработки. Если устранение выявленных проблем невозможно, то следует вернуться к предыдущим шагам — переработать спецификацию,

скорректировать цели безопасности или повторно выполнить TARA. Перечисленные мероприятия потребуют гораздо меньших ресурсов, нежели внесение кардинальных изменений в почти готовый компонент или автомобиль на поздних этапах разработки.

Согласованный перечень технических требований передается командам разработки. Разработчики должны реализовать все технические требования, определенные лидером по кибербезопасности, чтобы продукт удовлетворял требованиям спецификации кибербезопасности. Необходимо отслеживать качество кода, применяя процедуры и инструменты статического анализа и ревью кода, модульного тестирования, проверки безопасности стороннего кода, функционального тестирования безопасности. Для разработчиков должна быть внедрена программа повышения осведомленности, пропагандирующая принципы безопасной разработки кода, которые помогут свести к минимуму количество уязвимостей в коде, допущенныхв процессе его разработки.

Для верификации достижения целей согласно V-модели разработки (это модель организации процессов, обязывающая выполнять проверку результатов действий на разных этапах разработки, подробнее см. ISO 26262), а также для будущих аудитов нужно обеспечить прослеживаемость требований (traceability) на всех уровнях.

Оканчивается фаза разработки валидационным тестированием. Выполнение установленных требований проверяется для всех сценариев эксплуатации, в том числе чтобы гарантировать функциональную безопасность. Функциональная безопасность занимается непреднамеренными негативными воздействиями и последствиями случайных ошибок, допущенных при разработке, и своевременно не замеченных случайных сбоев на производстве. Однако проводить проверку кибербезопасности теми же методами, что и проверку функциональной безопасности, невозможно. Это связано с тем, что кибератаки являются результатом преднамеренных действий злоумышленников и для них не работают многие предположения, действительные для функциональной безопасности. Притом заранее без дополнительных исследований обычно неизвестно, какие именно предположения не работают. Следовательно, составить по спецификации исчерпывающий набор тестовых сценариев оказывается невозможно, а проверять все возможные сценарии (все возможные входные данные в сочетании со всеми допустимыми условиями эксплуатации) — абсолютно недостижимая цель. Поэтому проверка свойств безопасности — не столько ремесло, сколько искусство, и автопроизводители должны создавать отдельные команды из людей, обладающих специфическими способностями и экспертизой в области практической кибербезопасности,

которые тесно взаимодействуют с подразделениями разработки и функциональной безопасности.

Системная проблема — нехватка таких людей на рынке труда. Единственное решение — дополнительно привлекать сторонние организации для проверки качества кода, поиска уязвимостей в разрабатываемых продуктах и проведения тестов на проникновение.

Еще до начала фазы производства, на этапе заключения контрактов, необходимо определить требования безопасности к сторонним компонентам и к уровню зрелости безопасности их разработчиков и поставщиков. В контракте должно быть прописано, что поставщик должен обеспечивать соответствие продукции данным требованиям и предоставлять автопроизводителю результаты тестирования кибербезопасности или другие подтверждающие свидетельства. В условиях массового промышленного производства автопроизводитель проводит выборочные проверки каждой партии поставляемых компонентов с целью контроля их соответствия требованиям безопасности. Для каждого типа поставляемого продукта может быть разработан план проверок, основой для которого являются требования к поставляемым компонентам из спецификации кибербезопасности.

Фаза производства

Согласно ISO 21434, к началу фазы производства необходимо провести анализ всех производственных операций и разработать План контроля производства (Production Control Plan), который включает:

- описание шагов по реализации требований кибербезопасности для фаз производства, эксплуатации и поддержки и вывода из эксплуатации (в стандарте эти фазы объединены в одну фазу пост-разработки);
- перечень оборудования и инструментов для фазы производства;
- контроли безопасности, которые исключают несанкционированные изменения на производстве;
- процедуры, позволяющие оценить полноту реализации и валидировать требования безопасности для фаз производства, эксплуатации и поддержки и вывода из эксплуатации.

Отметим, что на этапах производства требуется уделить внимание не только самому процессу производства, но и обеспечить безопасность:

- логистики и хранения компонентов и готовой продукции;
- процедур прошивки и загрузки программного обеспечения;
- ИКТ-инфраструктуры сборочных линий.

В случае изменений в номенклатуре поставляемых компонентов или смены поставщика должны быть определены проверки, подтверждающие соответствие новых компонентов требованиям кибербезопасности. Например, в число таких проверок может входить проведение интеграционного тестирования.

Для каждого производственного этапа должны быть запланированы промежуточные проверки качества, т.н. quality gates, которые подтверждают не только требуемое качество и функциональную безопасность, но и надлежащую реализацию требований кибербезопасности. Переход к следующему производственному этапу возможен только после прохождения соответствующей проверки. В качестве примера такой проверки можно привести контроль аутентичности и целостности ПО блока управления после его прошивки.

Фаза эксплуатации и обслуживания

На фазе эксплуатации и обслуживания особое внимание нужно уделить поддержке состояния безопасности автомобиля и поддерживающей инфраструктуры. (Об обеспечении безопасности поддерживающей инфраструктуры см. далее «Обработка рисков для поддерживающей инфраструктуры».)

Для поддержки безопасности автомобиля необходимо:

- отслеживать информацию об обнаруженных уязвимостях и об изменениях ландшафта угроз;
- наладить мониторинг безопасности поддерживающей инфраструктуры и процессы реагирования на инциденты;
- наладить мониторинг информации о компрометации поставщиков и процессы реагирования на инциденты, затрагивающие цепочки поставок и доверенных (авторизованных) партнёров;
- оперативно реагировать на уязвимости и угрозы и инциденты, включая разработку и установку патчей, оповещение пользователей и переоценку рисков.

Часть функционала (мониторинг, безопасное получение и установка обновлений, сценарии смены пользователя/владельца и т.д.) реализуется на стороне автомобиля, а часть — в поддерживающей инфраструктуре.

Фаза завершения эксплуатации

На фазе вывода из эксплуатации нужно, чтобы и пользователи, и их данные оставались в безопасности даже после утилизации или переиспользования

отдельных компонентов. Процедуры предупреждения и оповещения пользователей, удаления пользовательских данных без возможности восстановления, выполнение обязательств по хранению данных и удалению всех остаточных прав доступа определяются заранее.

Обработка рисков для поддерживающей инфраструктуры

Как и в случае с рисками для самого автомобиля, к реализации требований безопасности для поддерживающей инфраструктуры следует приступать на ранних этапах её разработки и создания.

Минимизировать риски атак на поддерживающую инфраструктуру помогут правильно выстроенные топология и сегментация сети, надежные протоколы аутентификации, авторизации, шифрования данных, антивирусная защита, процедуры контроля доступа к системе, управления уязвимостями, мониторинга и реагирования на инциденты.

Справиться с негативными последствиями атак типа «отказ в обслуживании» помогут избыточная архитектура сервисов, балансировка нагрузки между отдельными кластерами и достаточно зрелые с точки зрения безопасности процессы создания резервных копий и восстановления.

На стадии обслуживания поддерживающей инфраструктуры необходимо предусмотреть технологические окна для установки обновлений безопасности и внедрения новых систем защиты. Учения по реагированию на инциденты должны проводиться на регулярной основе.

Если часть поддерживающей инфраструктуры администрируется сторонними организациями, например авторизованными сервисными центрами, или сторонние организации имеют доступ к ее отдельным сегментам, то в таких случаях автопроизводитель для снижения рисков взлома поддерживающей инфраструктуры должен использовать комплексный подход. Он должен сформулировать требования безопасности, на основе которых сторонняя организация обязана самостоятельно принять нужные меры. Если же сторонняя организация не обладает необходимыми ресурсами и компетенцией или просто имеет пользовательский доступ к поддерживающей инфраструктуре, автопроизводитель должен сам найти решение, как защитить поддерживающую инфраструктуру.

Чтобы быть уверенным, что поддерживающая инфраструктура соответствует требованиям безопасности, автопроизводитель регулярно

должен проводить аудиты безопасности и пентесты, учитывая при этом все возможные сценарии использования инфраструктуры сторонними организациями.

Обработка рисков для ИКТ-инфраструктуры производителя

Особенность обработки рисков для ИКТ-инфраструктуры заключается в том, что автопроизводитель должен рассматривать ИКТ-инфраструктуру в качестве отправной точки сложных атак, конечной целью которых является автомобиль, поддерживающая инфраструктура или данные пассажиров и владельцев авто (как физических, так и юридических лиц).

В штатном расписании автопроизводителя должны присутствовать как минимум администратор безопасности и руководитель подразделения безопасности, ответственные за обеспечение безопасности. Для защиты офисной сети и конечных точек применяются корпоративные практики и технические решения обеспечения безопасности. Внутри периметра организации осуществляется процесс мониторинга событий кибербезопасности и определены процедуры реагирования на инциденты. Для всех работников организации проводятся тренинги и обучение в рамках программы повышения уровня знаний в области кибербезопасности и культуры безопасности.

Работа с угрозами также должна учитывать в качестве потенциальных целей нарушителей такие процессы разработки и производства, как управление инструментами разработки или производственной документацией, специфичные для производственных компаний.

Что касается регуляторных требований в этом вопросе, то можно отметить, что UN 155 обращает внимание на необходимость обеспечения безопасности инфраструктуры автопроизводителя, однако требования на этот счет довольно абстрактные. В то же время, стандарт ISO 21434 включает в себя целую главу, посвященную организационной части обеспечения безопасности.

По всей видимости авторы регуляторных документов предполагают довольно высокий уровень зрелости безопасности организации, а может, даже и реализацию серий стандартов по информационной безопасности ISO 27000, которая дополняется рядом специфических требований для автомобильного производства.

Обработка рисков, связанных с цепочкой поставок

Обычно для снижения рисков, связанных с поставками, заключаются соглашения с поставщиками. Часть требований кибербезопасности в этих соглашениях может относиться к предотвращению реализации угроз, а часть — к устранению последствий их реализации. Например, можно потребовать от поставщика свидетельство того, что персонал вовремя проходит курс повышения осведомленности о киберугрозах, и того, что на предприятии реализуются организационные и технические меры предотвращения атак. Остаточные риски в этом случае могут быть снижены с помощью дополнительных рычагов, например, заставляющих поставщика обеспечить защиту от атак или оперативно справляться с их последствиями посредством санкций за неустранённые критические уязвимости и требований к защищённости от кибератак поставляемых компонентов. Такие меры хорошо применять для снижения краткосрочных рисков.

Более комплексный подход должен применяться к долгосрочным рискам, связанным с неочевидными на первый взгляд дефектами и уязвимостями в программном коде поставляемых компонентов. Такие дефекты могут проявить себя позднее даже в готовом автомобиле. Необходимо принять все возможные меры, чтобы исключить появление дефектов на этапе разработки и как можно скорее обнаружить потенциальные уязвимости.

Ответственность за эти мероприятия распределяется между производителем автомобиля и поставщиками компонентов согласно Соглашению о взаимодействии в кибербезопасности (Cybersecurity Interface Agreement). Например, производитель может определить цели и предположения безопасности компонента, а также выдвинуть высокоуровневые требования к компоненту, которые должны войти в его спецификацию. Поставщик в свою очередь эти требования реализует, а также обеспечивает безопасность процесса разработки (все эти моменты должны быть оговорены в контракте). Поставщик в рамках контракта может выполнять оценку рисков для собственного компонента, в то время как производитель примет эти результаты как часть полной, более широкой оценки. Производитель выполняет тестирование полученных компонентов на соответствие требованиям, целям и предположениям безопасности.

Тестирование поставляемых компонентов не должно завершаться вместе со стадией разработки автомобиля. Производителю следует с определенной периодичностью проверять поставляемые компоненты уже по завершении этапа разработки. Это позволяет выявить уязвимости, а также гарантировать, что безопасность не была нарушена, — например вследствие кибератаки на поставщика.

Важно в рамках контракта уделить особое внимание распределению ответственности и плану действий в случае обнаружения несоответствий поставляемых компонентов спецификации или уязвимостей в поставляемых компонентах во время тестирования или эксплуатации. Необходимо четко зафиксировать, в какой срок и как поставщик обязан реагировать на информацию об уязвимостях разной степени критичности. Установленные сроки позволяют поставщику на своей стороне выделить ресурсы и определить бюджет на выполнение обязательств в рамках плана действий.

В контексте устранения уязвимостей нужно иметь в виду проблему контроля поставщиков разного уровня. В автомобильной отрасли структура взаимоотношений различных организаций представляет собой сложную разветвленную сеть: каждый поставщик автомобильных компонентов может иметь одновременно несколько своих собственных поставщиков частей компонентов, ПО, микросхем и материалов.

Помочь решить проблему должны государственные регуляторы, гармонизировав свою законодательную базу в области кибербезопасности с международными регламентами и стандартами, такими как UN 155/156, и заключив партнёрские соглашения с другими государствами о взаимном признании результатов сертификации автомобилей и их компонентов.

В этом случае компаниям-автопроизводителям в контракте достаточно будет сослаться на международные положения, а поставщикам будет проще обеспечивать соответствие своих компонентов унифицированным требованиям по кибербезопасности, не боясь столкнуться со спецификой регионального и местного законодательства.

Стратегия реализации требований безопасности

Рассмотренные в данной статье Положения UN 155, 156 и Стандарт ISO/SAE 21434 имеют достаточно широкую область применения. Они регламентируют обеспечение кибербезопасности не только разрабатываемых и эксплуатируемых автотранспортных средств, но и многих процессов и ИКТ-инфраструктуры в самой компании-автопроизводителе. Определяя необходимые составляющие для обеспечения кибербезопасности, Положения и Стандарт оставляют за самим автопроизводителем свободу в выборе средств и методов для достижения требуемого уровня кибербезопасности (Приложения

ISO/SAE 21434 имеют рекомендательный характер и иллюстрируют один из подходов к идентификации и оценке рисков кибербезопасности.)

На практике автопроизводители могут использовать Положения UN 155, 156 и Стандарт ISO/SAE 21434, как ориентиры, которые помогают выстроить управление кибербезопасностью автомобиля должным образом, даже если перед ними не стоит задача получения Сертификата соответствия ЕЭК ООН.

Для минимизации затрат на обеспечение кибербезопасности следует «заложить» её еще на этапе концепции. Однако, стейкхолдеры компании, внедряющей практики кибербезопасности, как правило, предпочитают использовать ситуативный подход. При этом компании сосредоточены на безопасной разработке и безопасности кода и компонентов самого автомобиля. В этом случае часть долгосрочных рисковможет выпасть из их рассмотрения.

Источником таких рисков могут быть несовершенство архитектуры автомобиля, уязвимости или скомпрометированные сторонние сервисы и компоненты, которые злоумышленники могут в дальнейшем использовать в атаках на автомобиль.

В случае инцидента степень ущерба и затраты на устранение последствий могут оказаться выше затрат, требующихся для разработки защищённой архитектуры и внедрения необходимых практик безопасности на начальных этапах проектирования. К аналогичным последствиям может привести и пренебрежение оценкой влияния компрометации ИКТ-инфраструктуры автопроизводителя при рассмотрении краткосрочных рисков кибербезопасности.

Прежде всего необходимо определить требования кибербезопасности для продукта и заложить их в его архитектуру. Делается это через знакомый автопроизводителям подход из области функциональной безопасности, а именно через определение целей и предположений безопасности (см. раздел «Фаза концепции»).

Цели безопасности должны подкреплять бизнес-цели, цели по обеспечению качества и функциональной безопасности, быть согласованы между всеми стейкхолдерами и зафиксированы для конкретного проекта.
Чёткое формулирование и принятие целей кибербезопасности на этапе концепции поможет исключить многие противоречия и несоответствия между концепцией и реализацией транспортного средства.

Второй важной составляющей на начальном этапе является формирование своей команды, обладающей необходимыми компетенциями для внедрения и поддержания практик кибербезопасности. Часть этих задач можно отдать

третьим организациям, например, если установлены жёсткие сроки разработки и вывода продукции на автомобильный рынок, а развить необходимые компетенции у своей команды в эти сроки не представляется возможным.

В-третьих, надо придерживаться всеобъемлющего и систематического подхода при реализации необходимых практик кибербезопасности. Один и тот же уровень зрелости практик безопасности может быть как достаточным, так и недостаточным или избыточным в зависимости от задач и приоритетов, стоящих перед автопроизводителем.

Одним из приемлемых вариантов реализации практик кибербезопасности может быть следующая последовательность:

1. Создать систему управления кибербезопасностью, то есть разработать и внедрить основные процедуры и политики кибербезопасности в компании;
2. Разработать План кибербезопасности, определяющий перечень и этапы внедрения защитных мер;
3. Обеспечить безопасность ИКТ-инфраструктуры компании, минимизировав риски атаки на подразделения разработки и производственные площадки;
4. Обеспечить безопасность поддерживающей инфраструктуры и внешних сервисов, минимизировав риски атаки на разрабатываемое или эксплуатируемое транспортное средство;
5. Обеспечить соответствие жизненного цикла проекта релевантным требованиям кибербезопасности, начиная с проектирования и безопасной разработки и заканчивая выводом транспортного средства из эксплуатации и переиспользования его отдельных компонентов.

Предлагаемый путь ресурсоёмок, сложен, затрагивает все этапы жизненного цикла транспортного средства и продолжителен по времени. Весьма вероятно, что у автопроизводителей может возникнуть соблазн «срезать углы»: ограничиться анализом непосредственно транспортного средства и фактически выбросить все этапы, кроме Плана кибербезопасности и защиты автомобиля на этапе разработки. К сожалению, с учётом прессинга со стороны киберкриминала и в эпоху подключённых и программно-определяемых транспортных средств (connected and software defined vehicles) такое решение может привести к катастрофическим последствиям и для самой компании, и для владельцев и пассажиров современных автомобилей.

Как же быть автопроизводителям, столкнувшимся с необходимостью внедрения практик кибербезопасности на основе Положений ЕЭК ООН и Стандарта ISO/SAE 21434?

Мы рекомендуем исходить из того, что внедрение практик — не спринт где-то в середине этапа разработки, а марафон длиной в жизненный цикл транспортного средства (или даже продолжительнее), требующий осмысленной стратегии. Перед стартом марафона составляется дорожная карта (или план) дистанции с разбиением на небольшие участки, на преодоление которых с учётом компетенций автопроизводителя тратится минимально необходимое количество ресурсов. В данном случае взвешенный подход к планированию и планомерное продвижение от простого к сложному являются выигрышной стратегией.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com