Международный союз электросвязи

МСЭ-Т X.1373

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2017)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги – Безопасность интеллектуальных транспортных систем (ИТС)

Возможность безопасного обновления программного обеспечения для устройств связи в интеллектуальных транспортных системах

Рекомендация МСЭ-Т X.1373

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных системы (ИТС)	**X.1370–X.1379**
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1373

Возможность безопасного обновления программного обеспечения для устройств связи в интеллектуальных транспортных системах

Резюме

По мере совершенствования технологий интеллектуальных транспортных систем (ИТС) обычным становится взаимодействие автотранспортных средств с другими структурами, такими как другие транспортные средства, связь транспортного средства с транспортным средством (V2V) и транспортного средства с инфраструктурой (V2I). В результате оснащения транспортного средства такими электронными устройствами, как электронные блоки управления (ECU) и электронные системы взимания автодорожных сборов (ETC), более сложными становятся ИТС и автомобильные навигационные системы. Вследствие этого, встроенные в такие электротехнические устройства модули программного обеспечения внутри необходимо соответствующим образом обновлять для устранения ошибок, а также для улучшения работы и повышения безопасности, с тем чтобы избегать крупных аварий.

С целью выполнения указанного выше требования в Рекомендации МСЭ-Т X.1373 представлены процедуры безопасного обновления программного обеспечения между сервером обновления программного обеспечения и транспортными средствами с соответствующими средствами управления безопасностью. Настоящая Рекомендация может на практике использоваться в автомобильной промышленности и отраслях, связанных с ИТС, в качестве набора стандартных возможностей для передового опыта.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1373	30.03.2017 г.	17-я	11.1002/1000/13197

Ключевые слова

Устройства связи, атака типа отказ в обслуживании (DoS), встроенная система, модуль защиты аппаратного оборудования (HSM), интеллектуальная транспортная система (ИТС), вредоносное программное обеспечение, конфиденциальность, анализ рисков, связь между транспортными средствами (V2V), связь транспортного средства с инфраструктурой (V2I), связь транспортного средства с транспортным средством или инфраструктурой (V2X), беспроводная связь.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1373

Возможность безопасного обновления программного обеспечения для устройств связи в интеллектуальных транспортных системах

1 Сфера применения

В контексте обновления программных модулей в электронных устройствах транспортных средств в среде связи интеллектуальных транспортных систем (ИТС) целью настоящей Рекомендации является установление процедуры безопасного обновления программных модулей для устройств связи ИТС для прикладного уровня в целях предотвращения таких угроз, как подделка устройств связи в транспортных средствах и злонамеренное вмешательство в их работу. В частности, Рекомендация содержит описание базовой модели обновления программного обеспечения и мер обеспечения безопасности при обновлении программного обеспечения, а также спецификацию абстрактного формата данных обновляемого программного модуля.

Процедура, касающаяся связи внутри транспортного средства, не входит в сферу применения настоящей Рекомендации. Описание процедуры, применяемой внутри транспортного средства, приводится здесь лишь для сведения.

Данная процедура предназначена для применения к устройствам связи в транспортных средствах ИТС при связи транспортного средства с инфраструктурой (V2I) через интернет и/или выделенные сети ИТС. Рекомендация может применяться на практике в автомобильной промышленности и отраслях, связанных с ИТС, в качестве набора стандартных безопасных процедур и мер управления безопасностью.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.509] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[ITU-T X.1521] Рекомендация МСЭ-Т X.1521 (2011 г.), *Система оценки общеизвестных уязвимостей.*

[ISO/IEC 15408-1] ISO/IEC 15408:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*

[ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный в другом документе.

3.1.1 угроза (threat) [ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 показатель риска (risk score): Количественный показатель, рассчитываемый для каждой угрозы применяемым методом анализа рисков.

3.2.2 бортовой мобильный шлюз (vehicle mobile gateway (VMG)): Модуль, который обеспечивает связь между электронными блоками управления (ECU) в локальной сети контроллеров (CAN) (бортовые шины транспортного средства) и внешними объектами интеллектуальной транспортной системы (ИТС) во внешней сети.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

CA	Certification authority	Орган сертификации
CAN	Controller area network	Локальная сеть контроллеров
CD	Compact disc	Компакт-диск
CRSS	Cvss based risk scoring system	Система оценки рисков на основе cvss
CVSS	Common vulnerability scoring system	Система оценки общеизвестных уязвимостей
DoS	Denial of service	Отказ в обслуживании
DVD	Digital versatile disc	Универсальный цифровой диск
ECU	Electronic control unit	Электронный блок управления
ETC	Electronic toll collection	Электронная система сбора дорожных платежей
FT	Fault tree	Дерево отказов
GPS	Global positioning system	Глобальная система определения местоположения
GUID	Global user id	Глобальный идентификатор пользователя
HSM	Hardware security module	Модуль защиты оборудования
HTTP	Hypertext transfer protocol	Протокол передачи гипертекста
HTTPS	Hypertext transfer protocol secure	Защищенный протокол передачи гипертекста
ID	Identifier	Идентификатор
IT	Information technology	ИТ Информационные технологии
ITS	Intelligent transportation system	ИТС Интеллектуальная транспортная система
LIN	Local interconnect network	Локальная внутрисистемная сеть
MAC	Message authentication code	Код аутентификации сообщений
MOST	Media oriented systems transport	Шина передачи данных мультимедийных систем
OBD	On-board diagnostics	Бортовая диагностика
OEM	Original equipment manufacturer	Производитель оригинального оборудования
PC	Personal computer	ПК Персональный компьютер
RPM	Revolutions per minute	Оборотов в минуту
RSS	Risk scoring system	Система оценки рисков
SD	Secure digital	Стандарт защищенных цифровых носителей
SHA	Secure hash algorithm	Защищенный алгоритм хеширования
SSL	Secure socket layer	Уровень защищенных разъемов
TLS	Transport layer security	Безопасность транспортного уровня
TOE	Target of evaluation	Объект оценки
TPM	Trusted platform module	Модуль доверенной платформы

TV	Television	ТВ	Телевидение
UI	User interface		Пользовательский интерфейс
URL	Uniform resource locator		Универсальный указатель ресурса
USB	Universal serial bus		Универсальная последовательная шина
Usvr	Update server		Сервер обновлений
V2I	Vehicle-to-infrastructure		Связь транспортного средства с инфраструктурой
V2V	Vehicle-to-vehicle		Связь транспортного средства с транспортным средством
V2X	Vehicle-to-x (vehicle/infrastructure)		Связь транспортного средства с транспортным средством или инфраструктурой
VMG	Vehicle mobile gateway		Бортовой мобильный шлюз
Wi-Fi	Wireless-fidelity		Высокая точность беспроводной передачи
XML	Extended markup language		Расширяемый язык разметки

5 Условные обозначения

Отсутствуют.

6 Базовая модель дистанционного обновления программного обеспечения

Для описания практической архитектуры безопасности в настоящем разделе вводится базовая модель традиционной архитектуры обновления программного обеспечения, в рамках которой даются определения основных модулей и типовых процессов обновления программного обеспечения.

6.1 Модули в среде ИТС, участвующие в обновлении программного обеспечения

На рисунке 1 показаны основные относящиеся к транспортному средству модули в среде связи ИТС, участвующие в процессе дистанционного обновления программного обеспечения транспортного средства. К основным модулям относятся установленные в транспортном средстве информационные устройства, электронные блоки управления (ECU) и бортовой мобильный шлюз (VMG), а также сервер обновлений (Usvr) и база данных регистрации производителя транспортного средства и поставщика. Процедура, используемая при связи внутри транспортного средства (например, между ECU и бортовым мобильным шлюзом), не входит в сферу применения настоящей Рекомендации. Модули, используемые для связи внутри транспортного средства (в частности пользовательский интерфейс и ECU), описываются ниже лишь для сведения.

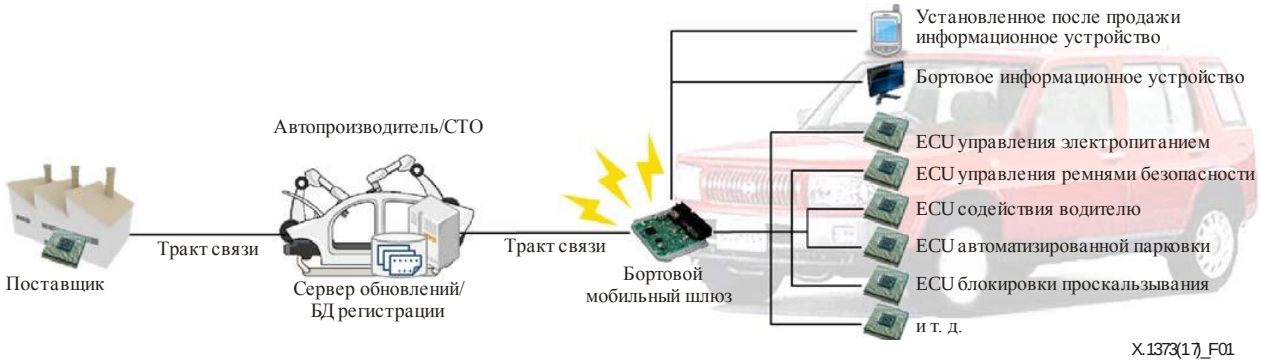

Рисунок 1 – Основные модули, относящиеся к транспортному средству

6.1.1 Пользовательский интерфейс (для сведения)

Пользовательский интерфейс (UI) представляет собой в общем случае установленное в транспортном средстве бортовое или установленное после продажи информационное устройство с дисплеем и устройствами ввода. Такое информационное устройство, соединенное напрямую с другими устройствами транспортного средства, например с VMG или ECU (см. пункт 6.1.2), обеспечивает получение и индикацию различной информации о состоянии транспортного средства – скорости, оборотов в минуту двигателя, уровня топлива в баке и т. д. В частности в контексте настоящей Рекомендации пользовательский интерфейс используется для уведомления водителей о необходимости обновить программное обеспечение.

6.1.2 Электронный блок управления (ECU) (для сведения)

ECU – общий термин, которым обозначаются компьютеры, управляющие различными устройствами в составе транспортного средства. В первые годы после появления ECU их основными функциями были управление временной синхронизацией зажигания и впрыском топлива, регулирование оборотов в холостом режиме и ограничение оборотов в рабочем режиме для повышения экономичности и снижения выбросов выхлопных газов. С ростом компьютеризации транспортных средств область применения ECU распространилась на такие различные функции, как управление электропитанием, управление ремнями безопасности, содействие водителю, автоматизированная парковка, блокировка проскальзывания, управление автоматической коробкой передач и т. д. В последние годы количество различных ECU в транспортном средстве увеличилось с 50 до 100, и особенно растет значимость ECU в сферах обеспечения безопасности и связи. Тем не менее ввиду того что разработка ECU требует создания сложного программного обеспечения, рост в последнее время количества таких блоков в транспортных средствах возлагает нелегкое бремя на автопроизводителей.

6.1.3 Бортовой мобильный шлюз

Бортовой мобильный шлюз – это модуль, задачей которого является взаимодействие с сервером обновлений (пункт 6.1.4) для обновления программного обеспечения транспортного средства. Процесс обновления программного обеспечения, находящегося в транспортном средстве, не входит в сферу применения настоящей Рекомендации. VMG может быть концептуальной единицей, которая реализуется на практике как комплекс из нескольких компонентов. Роль VMG в этом контексте может играть, например, блок управления соединениями (также называемый центральный шлюз, головной блок, головное устройство связи или шлюз транспортного средства (VG)), и для обновления программного обеспечения также могут использоваться любые устройства. В качестве тракта связи между бортовым мобильным шлюзом и наружными объектами ИТС может выступать сеть сотовой (подвижной) или фиксированной беспроводной связи.

6.1.4 Сервер обновлений и база данных регистрации

Сервер обновлений располагается у автопроизводителей или на станциях технического обслуживания для сбора информации о состоянии программных модулей транспортных средств и передачи на транспортные средства обновлений программного обеспечения для этих модулей. Аналогичным образом в большинстве современных компьютеров с поддержкой сетей связи, таких как персональные компьютеры (ПК) и смартфоны, одной из важных функций сервера обновлений является комплексное управление программным обеспечением транспортного средства. Чтобы автоматически управлять состоянием такого программного обеспечения на каждом транспортном средстве, сервер обновлений должен работать вместе с базой данных регистрации, в которой для подтверждения хранится состояние программного обеспечения транспортного средства. Следует отметить, что сервер обновлений может быть размещен не только у производителя транспортных средств, но и у поставщика или третьей стороны.

6.1.5 Поставщик

Автомобиль состоит из тысяч комплектующих, обеспечиваемых различными поставщиками. Автопроизводители устанавливают закупленные у поставщиков бортовые устройства связи и ECU с учетом взаимосвязей между разнообразными устройствами. Ввиду этого и в целом модули обновлений для бортовых устройств связи не производятся заранее автопроизводителями, они производятся поставщиками соответствующих комплектующих. Тщательно протестировав модули обновлений и оценив их работу, автопроизводитель распределяет их транспортным средствам.

6.2 Модель процедуры обновления программного обеспечения

6.2.1 Общая процедура обновления

На рисунке 2 показана типовая модель процедуры обновления программного обеспечения, которую инициирует бортовой мобильный шлюз, проверяя наличие обновлений. Поскольку связь внутри транспортного средства не входит в сферу применения настоящей Рекомендации, относящиеся к ней шаги показаны на рисунке 2 только для сведения – как пример практической реализации процедуры безопасного обновления.

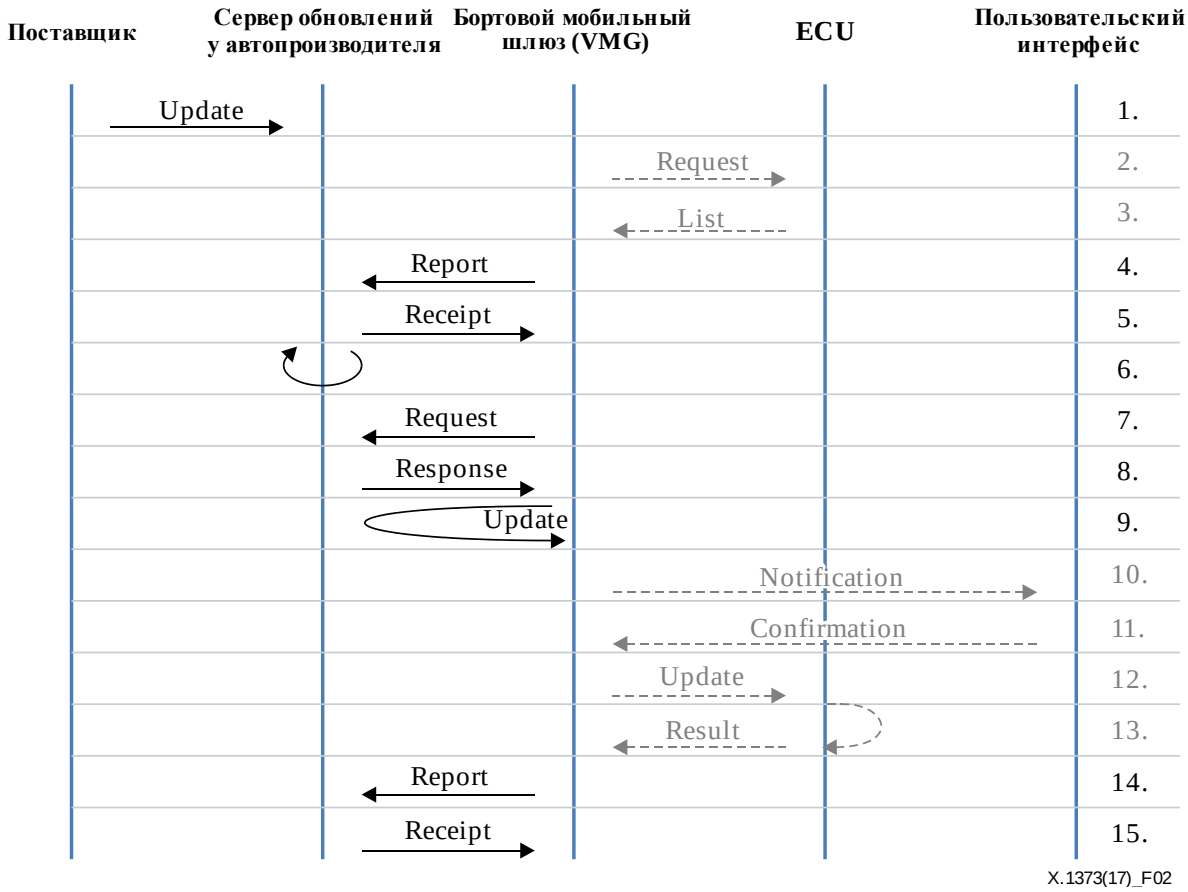

Рисунок 2 – Модель процесса обновления программного обеспечения

Ниже перечислены этапы процедуры обновления, где этапы 2, 3 и 10–13 (обозначены курсивом) приведены для сведения.

1 На первом этапе процесса поставщик комплектующих транспортного средства предоставляет модуль обновления (асинхронно с последующими этапами).

2 *В начале процедуры обновления бортовой мобильный шлюз (VMG) запрашивает у ECU список программных модулей.*

3 *ECU проверяет состояние своего программного обеспечения, генерирует список программных модулей и передает его VMG.*

4 VMG передает полученный список на сервер обновлений, чтобы проверить наличие обновлений для данного транспортного средства.

5 Сервер обновлений передает в адрес VMG сообщение, подтверждающее прием списка.

6 Сервер обновлений анализирует состояние установленного в транспортном средстве программного обеспечения по представленному списку и определяет, есть ли необходимость в обновлении программного обеспечения ECU.

7 Поскольку такой анализ может занять длительное время, VMG периодически проверяет необходимость обновлений для транспортного средства.

8 Если имеются обновления, сервер обновлений передает универсальные указатели ресурса (URL) для доступа к ним; в противном случае отсылает только сообщение о подтверждении.

9 Если для транспортного средства есть обновления, VMG соединяется с сервером обновлений для загрузки модулей обновления для транспортного средства.

10 *Прежде чем устанавливать обновления для ECU, VMG уведомляет водителя для подтверждения применения обновлений.*

11 *Водитель подтверждает и принимает применение обновлений.*

12 *VMG передает файлы обновлений на соответствующие ECU и направляет им запрос на установку обновлений (см. пункт 6.2.3).*

13 *Каждый ECU применяет обновление и сообщает результат применения бортовому мобильному шлюзу.*

14 Бортовой мобильный шлюз передает на сервер обновления отчет о результатах применения.

15 В заключение сервер обновлений возвращает сообщение, подтверждающее прием отчета. Если установить обновления не удалось или остались еще какие-то обновления, сервер обновлений повторяет этапы 6–14 до тех пор, пока установка не будет успешно выполнена (см. пункт 6.2.2).

6.2.2 Ограничение количества повторных попыток

В соответствии с этапом 15 попытки установить обновления предпринимаются до успешного завершения операции, однако следует иметь в виду, что в некоторых случаях установка обновлений может оказаться невозможной, и тогда VMG будет безостановочно предпринимать новые попытки. Чтобы этого избежать, следует ограничить количество повторных попыток некоторым числом N, которое можно определить на основании политики для процедуры обновления. Формулировка политики обновления не входит в сферу применения настоящей Рекомендации.

6.2.3 Ресурсные ограничения

Что касается практического применения программного обеспечения обновления в транспортном средстве (см. приведенный в пункте 6.2.1 для сведения этап 12), в транспортном средстве есть модули, которые не располагают достаточным объемом памяти для единовременного кеширования всего модуля обновления. Такие модули необходимо обновлять с использованием технологии потокового обновления, предусматривающей передачу фрагментированных данных в потоковом режиме.

Вообще говоря, сколько бы модулей ни содержало транспортное средство, в любой системе обновления следует внимательно учитывать ограниченные ресурсы устройств, такие как емкость оперативной памяти, накопителей, а также пропускную способность сети.

7 Спецификация процедуры безопасного обновления программного обеспечения

В настоящем разделе описывается практическая процедура обновления и прикладной формат сообщений, передаваемых между сервером обновлений и транспортным средством (VMG) в процессе обновления программного обеспечения с использованием функций безопасности. Следует отметить, что настоящая Рекомендации не содержит описания функций, обеспечивающих конфиденциальность сообщений. Конфиденциальность может обеспечиваться протоколами более низких уровней (например, защищенный протокол передачи гипертекста (HTTPS) и протокол передачи по защищенному туннелю и т. д.).

Процедура должна учитывать, что разные транспортные средства могут поддерживать неодинаковый набор возможностей защиты. Ввиду этого в настоящей Рекомендации для безопасного обмена сообщениями транспортные средства, использующие асимметричные алгоритмы шифрования, применяют метод цифровой подписи (пункт 7.1.1), а транспортные средства, не использующие асимметричных алгоритмов шифрования, – метод на основе кода аутентификации сообщений (MAC) (пункт 7.1.2).

7.1 Общий формат сообщений с использованием функций безопасности

В этом разделе устанавливается общий формат сообщений с использованием функций безопасности, включая метод аутентификации отправителя и проверки целостности сообщения. Для обеспечения целостности и проверки подлинности могут применяться метод цифровой подписи на основе алгоритма с открытым ключом и/или код аутентификации сообщений на основе алгоритма с общедоступным ключом. В рамках процедуры безопасного обновления программного обеспечения каждое сообщение следует строить с использованием одного из указанных ниже методов защиты.

7.1.1 Метод цифровой подписи

Один из возможных методов аутентификации объектов и проверки целостности сообщений для транспортного средства со способностью ассиметричного шифрования в модуле защиты оборудования (HSM) (например, TPM) – цифровая подпись на базе [ITU-T X.509].

7.1.2 Метод MAC

Поскольку алгоритм с общедоступным ключом дает меньшую нагрузку на процессор, чем алгоритм с открытым ключом, он подходит для устройств с малой вычислительной мощностью. Вместе с тем при алгоритме с общедоступным ключом отправитель и получатель пользуются одним и тем же ключом, из-за чего у большого количества устройств оказывается идентичный ключ. При этом в случае утечки общедоступного ключа необходимо будет обновить ключи на всех устройствах системы. Кроме того, поскольку общедоступный ключ сам по себе не гарантирует подлинности отправителя, каждое сообщение должно содержать идентификатор устройства отправителя, а это предполагает, что идентификатор в устройстве не используется недолжным образом.

7.2 Определение протокола и формат данных

Прикладной формат данных предназначен только для доставки сообщений, относящихся к обновлению программного обеспечения, которые представлены в общем формате сообщений, описанном в предыдущем пункте. В настоящем пункте вначале определены типы сообщений, используемые в ходе обновления программного обеспечения, а затем приведены спецификации типов сообщений. Для сведения приведены примеры сообщений в формате расширяемого языка разметки (XML).

7.2.1 Обзор протокола

На основании модели процедуры обновления программного обеспечения, описанной в разделе 6, сообщения подразделены на несколько типов в соответствии с их назначением, как показано на рисунке 3. Процедуры, используемые при связи внутри транспортного средства, не входят в сферу применения настоящей Рекомендации и показаны на рисунке 3 шрифтом серого цвета.

ПРИМЕЧАНИЕ. – Процедура связи внутри транспортного средства описана в [b-ISO 14229] и [b-ISO 13440].

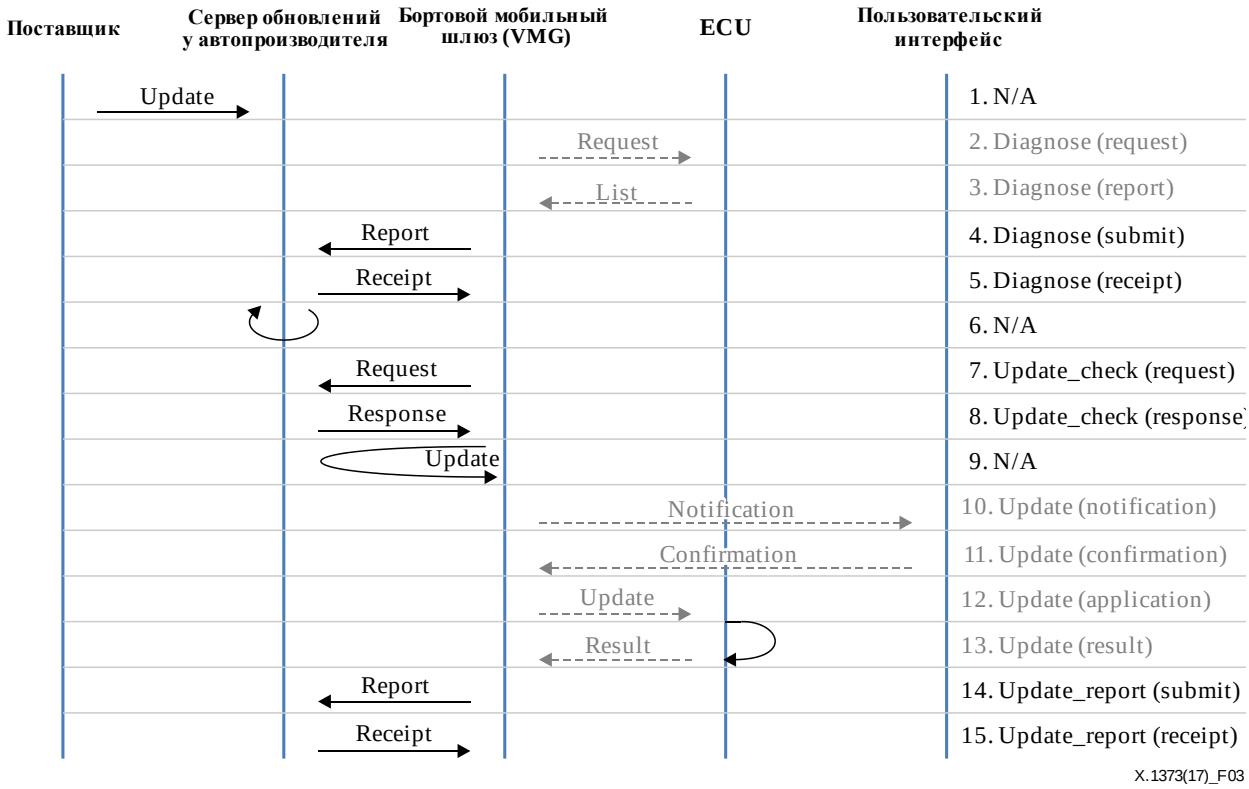

Рисунок 3 – Определение типов сообщений

Сообщения, передаваемые на этапах 2, 3, 4 и 5, относятся к типу diagnose (диагностика), так как предназначены для запроса и сообщения результатов диагностики состояния программного обеспечения в каждом ECU. Аналогичным образом сообщения, передаваемые на этапах 7 и 8, относятся к типу update_check (проверка обновлений). Сообщения, передаваемые на этапах 10, 11, 12 и 13, имеют тип update (обновление), так как служат для подтверждения наличия обновлений и для их установки. Наконец, результаты установки обновлений передаются с использованием сообщений типа update_report (отчет об обновлении) на этапах 14 и 15. Типы, подтипы и коды сообщений приведены в таблице 1.

Таблица 1 – Типы сообщений

Тип	Подтип	От	До	Назначение
diagnose	*request*	*VMG*	*ECU*	*Запрос диагностики состояния программного обеспечения*
	report	*ECU*	*VMG*	*Результат диагностики с указанием состояния программного обеспечения*
	submit	VMG	Usvr	Отчет о результатах диагностики ecu транспортного средства
	receipt	Usvr	VMG	Подтверждение приема отчета о диагностике
update_check	request	VMG	Usvr	Запрос модуля обновления
	response	Usvr	VMG	Модуль обновления предоставлен
update	*notification*	*VMG*	*UI*	*Сообщение об уведомлении водителя об установке обновлений*
	confirmation	*UI*	*VMG*	*Сообщение от водителя с подтверждением установки обновлений*
	application	*VMG*	*ECU*	*Сообщение с запросом, содержащее модуль обновления*
	result	*ECU*	*VMG*	*Результат применения модуля обновления*

Таблица 1 – Типы сообщений

Тип	Подтип	От	До	Назначение
update_report	submit	VMG	Usvr	Отчет об установке обновлений
	receipt	Usvr	VMG	Получение отчета
* Usvr – сервер обновлений. * UI – пользовательский интерфейс.				

ПРИМЕЧАНИЕ. – В таблице 1 серый курсивный текст используется для обозначения элементов, которые не входят в сферу применения настоящей Рекомендации и приведены только для сведения.

7.2.2 Сообщения diagnose

Чтобы определить, какие модули обновления необходимы в транспортном средстве, сервер обновлений и VMG обмениваются сообщениями diagnose для закачки информации об обновлении программного обеспечения транспортных средств на сервер обновлений.

7.2.2.1 Сообщение diagnose (submit)

Получив результаты диагностики транспортного средства, VMG передает список программных модулей на сервер обновлений, расположенный у автопроизводителя (или станции технического обслуживания). Сообщение diagnose (submit) содержит идентификатор транспортного средства (vid) и список программных модулей, извлеченный из сообщений diagnose (report).

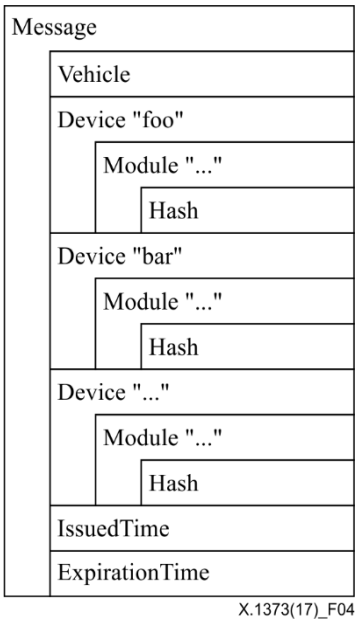

Рисунок 4 – Структура сообщения diagnose (submit)

Таблица 2 – Элементы сообщения diagnose (submit)

Элемент	Атрибут элемента	Описание
Message	–	Контейнер сообщения
	protocol	Всегда равно "1.0"
	version	Номер версии отправителя сообщения
	type	Тип сообщения (всегда равно "diagnose")
	subtype	Подтип сообщения (всегда равно "submit")
	sessionid	Идентификатор сеанса (ID) – случайный глобальный идентификатор пользователя (GUID), присваиваемый сеансу обмена сообщениями diagnose. Такой же идентификатор сеанса присваивается набору сообщений diagnose (request, report, submit и receipt)
	trustlevel	Уровень доверия, определяемый исходя из поддерживаемых возможностей защиты и требований к безопасности устройства, генерирующего это сообщение
	ownerid	Идентификатор владельца, присвоенный производителем транспортного средства/поставщиком
	messageid	Идентификатор сообщения – случайный GUID, присваиваемый отдельному сообщению
Vehicle	–	Контейнер информации о транспортном средстве. Содержит несколько элементов module
	name	Наименование транспортного средства (если таковое имеется)
	model	Наименование модели транспортного средства, присвоенное производителем
	modelid	Наименование модели транспортного средства
	vehicleid	Идентификатор транспортного средства, присвоенный производителем транспортного средства/поставщиком
	locale	Информация о языковой настройке транспортного средства
Device	–	Контейнер информации об устройстве. Содержит несколько элементов module
	name	Наименование устройства (если таковое имеется)
	type	Наименование типа устройства, например "Power management ECU", "Seat belt control ECU" и т. д.
	model	Наименование модели устройства
	deviceid	Идентификатор устройства, присвоенный производителем транспортного средства/поставщиком
	hwversion	Версия аппаратного модуля
Module	–	Контейнер информации о модуле, содержащий элемент hash
	moduleid	Идентификатор модуля – уникальный идентификатор, присвоенный производителем транспортного средства/поставщиком
	version	Версия программного модуля
	nextversion	Устанавливаемая в настоящий момент версия модуля. Используется главным образом при передаче сообщения response в ходе обновления
Hash	–	Контейнер со значением хеша и информацией о применяемом алгоритме хеширования
	algorithm	Алгоритм хеширования (например, SHA-3, SHA-256 и т. д.)
IssuedTime	–	Время генерации сообщения
ExpirationTime	–	Время истечения срока действия сообщения

Таблица 3 – Пример сообщения diagnose (submit)

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="submit"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{BBCE3B0B-2A10-443A-97D0-EF4650457422}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{66E6F81E-F293-4531-B2FC-A93F177373AA }"
version="1.3.23.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion=”HC-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.2.2 Сообщение diagnose (receipt)

После закачки информации о программном обеспечении транспортного средства с сообщением diagnose (submit) сервер обновлений направляет квитанцию с сообщением diagnose (receipt), чтобы транспортное средство было извещено об успешном завершении представления и о возможности перейти к следующей стадии (update_check).

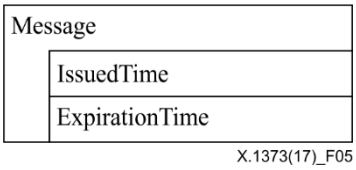

Рисунок 5 – Структура сообщения diagnose (receipt)

Таблица 4 – Элементы сообщения diagnose (receipt)

Элемент	Атрибут элемента	Описание
Message	–	Контейнер сообщения
	protocol	Всегда равно "1.0"
	version	Номер версии отправителя сообщения
	type	Тип сообщения (всегда равно "diagnose")
	subtype	Подтип сообщения (всегда равно "receipt")
	sessionid	Идентификатор сеанса – случайный GUID, присваиваемый сеансу обмена сообщениями diagnose. Такой же идентификатор сеанса присваивается набору сообщений diagnose (request, report, submit и receipt)

Таблица 4 – Элементы сообщения diagnose (receipt)

Элемент	Атрибут элемента	Описание
	trustlevel	Уровень доверия, определяемый исходя из поддерживаемых возможностей защиты и требований к безопасности устройства, генерирующего это сообщение
	ownerid	Идентификатор владельца, присвоенный производителем транспортного средства/поставщиком
	messageid	Идентификатор сообщения – случайный GUID, присваиваемый отдельному сообщению
	status	Подтверждение приема сообщения diagnose (submit)
IssuedTime	–	Время генерации сообщения
ExpirationTime	–	Время истечения срока действия сообщения

Таблица 5 – Пример сообщения diagnose (receipt)

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="receipt"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{E313159C-2081-4A10-B61D-4F81D074D54F}" trustlevel="3"
status=”yes”>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.3 Сообщения update_check

После закачки информации о программном обеспечении на сервер обновлений сообщением diagnose сервер обновлений приступает к ее анализу, чтобы определить подлежащие обновлению модули транспортного средства, что может занять длительное время. Периодически на сервер передается сообщение update_check для запроса о результатах анализа. Сообщения update_check, которыми обмениваются VMG и сервер обновлений, подразделяются на два подтипа – request и response.

7.2.3.1 Сообщение update_check (request)

Сообщение update_check (request) передается от VMG на сервер обновлений и служит для запроса о наличии обновлений. Это сообщение содержит информацию о подлежащих анализу модулях, которая во многом аналогична содержимому сообщения diagnose (receipt).

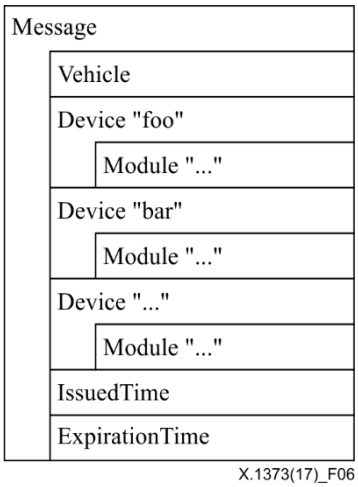

Рисунок 6 – Структура сообщения update_check (request)

Таблица 6 – Элементы сообщения update_check (request)

Элемент	Атрибут элемента	Описание
Message	–	Контейнер сообщения
	protocol	Всегда равно "1.0"
	version	Номер версии отправителя сообщения
	type	Тип сообщения (всегда равно "update_check")
	subtype	Подтип сообщения (всегда равно "request")
	sessionid	Идентификатор сеанса – случайный GUID, присваиваемый сеансу обмена сообщениями update_check. Такой же идентификатор сеанса присваивается набору сообщений update_check (request и response)
	trustlevel	Уровень доверия, определяемый исходя из поддерживаемых возможностей защиты и требований к безопасности устройства, генерирующего это сообщение
	ownerid	Идентификатор владельца, присвоенный производителем транспортного средства/поставщиком
	messageid	Идентификатор сообщения – случайный GUID, присваиваемый отдельному сообщению
Vehicle	–	Контейнер информации о транспортном средстве. Содержит несколько элементов module
	name	Наименование транспортного средства (если таковое имеется)
	model	Наименование модели транспортного средства, присвоенное производителем
	modelid	Наименование модели транспортного средства
	vehicleid	Идентификатор транспортного средства, присвоенный производителем транспортного средства/поставщиком
	locale	Информация о языковой настройке транспортного средства
Device	–	Контейнер информации об устройстве. Содержит несколько элементов module
	name	Наименование устройства (если таковое имеется)
	type	Наименование типа устройства, например "Power management ECU", "Seat belt control ECU" и т. д.
	model	Наименование модели устройства
	deviceid	Идентификатор устройства, присвоенный производителем транспортного средства/поставщиком
	hwversion	Версия аппаратного модуля
Module	–	Контейнер информации о модуле, содержащий элемент hash
	moduleid	Идентификатор модуля – уникальный идентификатор, присвоенный производителем транспортного средства/поставщиком
	version	Версия программного модуля
	nextversion	Устанавливаемая в настоящий момент версия модуля. Используется главным образом при передаче сообщения response в ходе обновления
IssuedTime	–	Время генерации сообщения
ExpirationTime	–	Время истечения срока действия сообщения

Таблица 7 – Пример сообщения update_check (request)

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="request"
sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion=""/>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion=""/>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion=”HC-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion=""/>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.3.2 Сообщение update_check (response)

В ответ на сообщение update_check (request) сервер обновлений направляет результат своего анализа. Если для каких-то модулей транспортного средства имеются обновления, в сообщении update_check (response) передаются URL-адреса для загрузки модулей обновления. Следует обратить внимание, что сообщение update_check (response) не содержит самого двоичного файла модуля – для загрузки этого файла VMG устанавливает новое соединение по URL-адресу, указанному в этом сообщении.

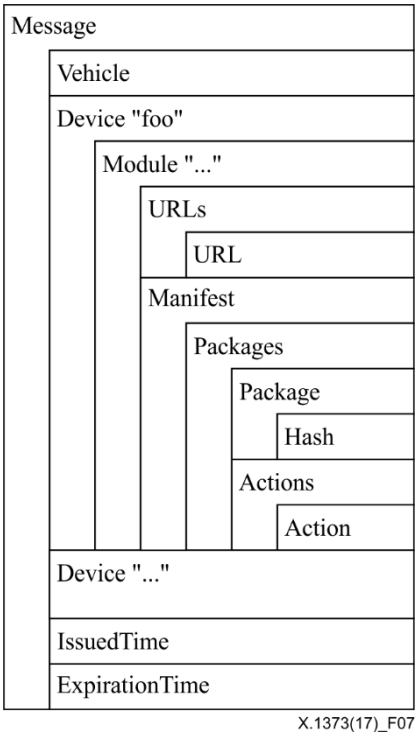

Рисунок 7 – Структура сообщения update_check (response)

Таблица 8 – Элементы сообщения update_check (response)

Элемент	Атрибут элемента	Описание
Message	–	Контейнер сообщения
	protocol	Всегда равно "1.0"
	version	Номер версии отправителя сообщения
	type	Тип сообщения (всегда равно "update_check")
	subtype	Подтип сообщения (всегда равно "response")
	sessionid	Идентификатор сеанса – случайный GUID, присваиваемый сеансу обмена сообщениями update_check. Такой же идентификатор сеанса присваивается набору сообщений update_check (request и response)
	trustlevel	Уровень доверия, определяемый исходя из поддерживаемых возможностей защиты и требований к безопасности устройства, генерирующего это сообщение
	ownerid	Идентификатор владельца, присвоенный производителем транспортного средства/поставщиком
	messageid	Идентификатор сообщения – случайный GUID, присваиваемый отдельному сообщению
Vehicle	–	Контейнер информации о транспортном средстве. Содержит несколько элементов module
	name	Наименование транспортного средства (если таковое имеется)
	model	Наименование модели транспортного средства, присвоенное производителем
	modelid	Наименование модели транспортного средства
	vehicleid	Идентификатор транспортного средства, присвоенный производителем транспортного средства/поставщиком
	locale	Информация о языковой настройке транспортного средства
Device	–	Контейнер информации об устройстве. Содержит несколько элементов module
	name	Наименование устройства (если таковое имеется)
	type	Наименование типа устройства, например "Power management ECU", "Seat belt control ECU" и т. д.
	model	Наименование модели устройства
	deviceid	Идентификатор устройства, присвоенный производителем транспортного средства/поставщиком
	hwversion	Версия аппаратного модуля
Module	–	Контейнер информации о модуле, содержащий элемент hash
	moduleid	Идентификатор модуля – уникальный идентификатор, присвоенный производителем транспортного средства/поставщиком
	version	Версия программного модуля
	nextversion	Устанавливаемая в настоящий момент версия модуля. Используется главным образом при передаче сообщения response в ходе обновления
	status	Результат проверки обновлений – "noupdate", если обновлений нет, и "ok", если для данного модуля имеются обновления
URLs	–	Контейнер для элементов URL в случае, если имеются обновления. Этот элемент содержится в элементе module, если status = "ok"

Таблица 8 – Элементы сообщения update_check (response)

Элемент	Атрибут элемента	Описание
URL	–	URL-адрес файла обновления. Элемент URL должен присутствовать по меньшей мере в двух экземплярах – помимо основного URL-адреса необходимо указать хотя бы один резервный. Максимальное количество элементов URL следует точно определять, учитывая вычислительные ресурсы VMG
	codebase	Местоположение файла обновления
Manifest	–	Описание модуля, подлежащего установке, и действий, которые необходимо предпринять с соответствующими файлами
	version	Номер конкретной новой версии данного программного модуля
Packages	–	Набор файлов, подлежащих установке. Не имеет атрибутов. Содержит один или несколько дочерних элементов Package
Package	–	Одиночный файл, подлежащий установке в рамках данного модуля
	name	Имя файла модуля обновления
	size	Размер модуля обновления в байтах
	description	Описание модуля обновления
Hash	–	Контейнер со значением хеша и информацией о применяемом алгоритме хеширования
	algorithm	Алгоритм хеширования (например, SHA-3, SHA-256 и т. д.)
Actions	–	Описание действий, которые должны быть выполнены для установки модуля, после того как все необходимые файлы из элемента Packages будут успешно загружены
Action	–	Одиночное действие, выполняемое в процессе установки
	event	Фиксированная строка, указывающая, когда следует выполнить это действие: "preinstall", "install", "postinstall" и "update"
	arguments	Аргументы, которые необходимо передать процессу установки
IssuedTime	–	Время генерации сообщения
ExpirationTime	–	Время истечения срока действия сообщения

Таблица 9 – Пример сообщения update_check (response)

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="response
" sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion="" status="ok">
            <Urls>
                <Url
codebase="http://update1.server/this/is/an/example/url/"/>
                <Url
codebase="http://update2.server/this/is/an/example/url/"/>
                <Url
codebase="http://update3.server/this/is/an/example/url/"/>
            </Urls>
            <Manifest version="1.4.0">
                <Packages>
                    <Package name="module1.bin" size="589" description=”This
update provides ...”>
                        <Hash algorithm="SHA-256">hash data here</Hash>
                    </Package>
                </Packages>
                <Actions>
                    <Action arguments="--argument-for-installation"
event="install"/>
                </Actions>
            </Manifest>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="noupdate">
        </Module>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion=”HC-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="noupdate">
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.4 Сообщения update

Процесс обновления, происходящий внутри транспортного средства, не входит в сферу применения настоящей Рекомендации. Определения и спецификации сообщений update не даются.

7.2.5 Сообщения update_report

На последнем этапе процедуры обновления VMG передает на сервер обновлений все собранные отчеты о результатах установки обновлений на устройства, чтобы сделать возможным дальнейшее дистанционное управление программным обеспечением каждого транспортного средства с сервера. Отчет о результатах установки передается в сообщении update_report (submit). В заключение сервер обновлений возвращает в адрес VMG сообщение, подтверждающее прием отчета (update_report (receipt)), обозначая тем самым окончание процесса обновления.

7.2.5.1 Сообщение update_report (submit)

Собрав от устройств отчеты об установке обновлений, VMG передает на сервер обновлений сообщение update_report (submit). Это сообщение содержит результаты установки обновлений, а также информацию о текущем состоянии программного обеспечения, такую, которая передается в сообщении diagnose (submit).

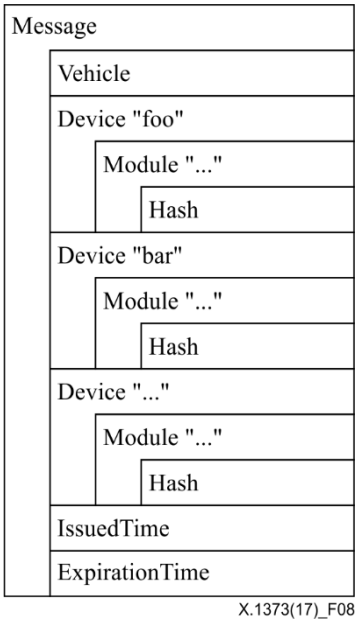

Рисунок 8 – Структура сообщения update_report (submit)

Таблица 10 – Элементы сообщения update_report (submit)

Элемент	Атрибут элемента	Описание
Message	–	Контейнер сообщения
	protocol	Всегда равно "1.0"
	version	Номер версии отправителя сообщения
	type	Тип сообщения (всегда равно "update_report")
	subtype	Подтип сообщения (всегда равно "submit")
	sessionid	Идентификатор сеанса – случайный GUID, присваиваемый сеансу обмена сообщениями update_report. Такой же идентификатор сеанса присваивается набору сообщений update_report (submit и receipt)
	trustlevel	Уровень доверия, определяемый исходя из поддерживаемых возможностей защиты и требований к безопасности устройства, генерирующего это сообщение
	ownerid	Идентификатор владельца, присвоенный производителем транспортного средства/ поставщиком
	messageid	Идентификатор сообщения – случайный GUID, присваиваемый отдельному сообщению
Vehicle	–	Контейнер информации о транспортном средстве. Содержит несколько элементов module
	name	Наименование транспортного средства (если таковое имеется)
	model	Наименование модели транспортного средства, присвоенное производителем
	modelid	Наименование модели транспортного средства
	vehicleid	Идентификатор транспортного средства, присвоенный производителем транспортного средства/поставщиком
	locale	Информация о языковой настройке транспортного средства

Таблица 10 – Элементы сообщения update_report (submit)

Элемент	Атрибут элемента	Описание
Device	–	Контейнер информации об устройстве. Содержит несколько элементов module
	name	Наименование устройства (если таковое имеется)
	type	Наименование типа устройства, например "Power management ECU", "Seat belt control ECU" и т. д.
	model	Наименование модели устройства
	deviceid	Идентификатор устройства, присвоенный производителем транспортного средства/поставщиком
	hwversion	Версия аппаратного модуля
Module	–	Контейнер информации о модуле, содержащий элемент hash
	moduleid	Идентификатор модуля – уникальный идентификатор, присвоенный производителем транспортного средства/поставщиком
	version	Версия программного модуля
	nextversion	Устанавливаемая в настоящий момент версия модуля. Используется главным образом при передаче сообщения response в ходе обновления
	status	Результат обновления модуля
Hash	–	Контейнер со значением хеша и информацией о применяемом алгоритме хеширования
	algorithm	Алгоритм хеширования (например, SHA-3, SHA-256 и т. д.)
IssuedTime	–	Время генерации сообщения
ExpirationTime	–	Время истечения срока действия сообщения

Таблица 11 – Пример сообщения update_report (submit)

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="submit"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{3F7A6438-8306-447E-A1BB-99CED4C2B6AD}" trustlevel="3">
    <Vehicle name="vehicleName" modelid="mid34987130" type="ECU"
model="modelName" vid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok">
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok">
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
    </Device>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status=”ok”>
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.5.2 Сообщение update_report (receipt)

По окончании этой последовательности сервер обновлений передает в адрес VMG сообщение update_report (receipt), сигнализируя транспортному средству о том, что вся процедура обновления завершена. Сообщение update_report (receipt) имеет почти такой же формат, как сообщение diagnose (receipt).

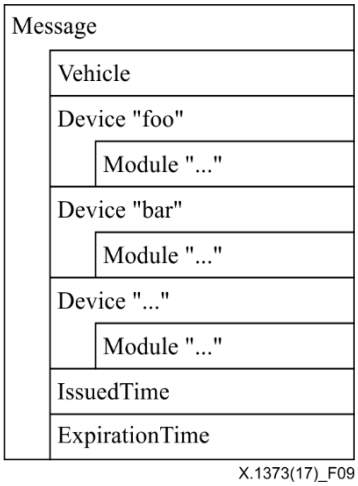

Рисунок 9 – Структура сообщения update_report (receipt)

Таблица 12 – Элементы сообщения update_report (receipt)

Элемент	Атрибут элемента	Описание
Message	–	Контейнер сообщения
	protocol	Всегда равно "1.0"
	version	Номер версии отправителя сообщения
	type	Тип сообщения (всегда равно "update_report")
	subtype	Подтип сообщения (всегда равно "receipt")
	sessionid	Идентификатор сеанса – случайный GUID, присваиваемый сеансу обмена сообщениями update_report. Такой же идентификатор сеанса присваивается набору сообщений update_report (submit и receipt)
	trustlevel	Уровень доверия, определяемый исходя из поддерживаемых возможностей защиты и требований к безопасности устройства, генерирующего это сообщение
	ownerid	Идентификатор владельца, присвоенный производителем транспортного средства/поставщиком
	messageid	Идентификатор сообщения – случайный GUID, присваиваемый отдельному сообщению
Vehicle	–	Контейнер информации о транспортном средстве. Содержит несколько элементов module
	name	Наименование транспортного средства (если таковое имеется)
	model	Наименование модели транспортного средства, присвоенное производителем
	modelid	Наименование модели транспортного средства
	vehicleid	Идентификатор транспортного средства, присвоенный производителем транспортного средства или поставщиком комплектующих
	locale	Информация о языковой настройке транспортного средства

Таблица 12 – Элементы сообщения update_report (receipt)

Элемент	Атрибут элемента	Описание
Device	–	Контейнер информации об устройстве. Содержит несколько элементов module
	name	Наименование устройства (если таковое имеется)
	type	Наименование типа устройства, например "Power management ECU", "Seat belt control ECU" и т. д.
	model	Наименование модели устройства
	deviceid	Идентификатор устройства, присвоенный производителем транспортного средства/поставщиком
	hwversion	Версия аппаратного модуля
Module	–	Контейнер информации о модуле, содержащий элемент hash
	moduleid	Идентификатор модуля – уникальный идентификатор, присвоенный производителем транспортного средства/поставщиком
	version	Версия программного модуля
	nextversion	Устанавливаемая в настоящий момент версия модуля используется главным образом при передаче сообщения response в ходе обновления
	status	Подтверждение приема отчета об установке данного модуля
IssuedTime	–	Время генерации сообщения
ExpirationTime	–	Время истечения срока действия сообщения

Таблица 13 – Пример сообщения update_report (receipt)

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="receipt"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{B5585708-6BDA-4B07-B2CB-5E9241F63271}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok"/>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok"/>
    </Device>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="ok"/>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

Дополнение I

Методика анализа рисков

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Методика анализа рисков на базе [b-JASO TP15002]

В настоящем Дополнении содержится подробная информация, касающаяся Дополнения II. Эта информация основана на руководящих указаниях по обеспечению информационной безопасности транспортных средств [b-JASO TP15002].

Информационная безопасность стала важным аспектом проектирования встроенных систем. На сегодняшний день известны примеры различных атак на безопасность ИТ-систем и накоплена информация по оценке рисков при проектировании ИТ-систем. Основные понятия в области безопасности, необходимые для оценки ИТ-продуктов, даны в [ISO/IEC 15408-1]. В контексте оценки в [ISO/IEC 15408-1] используется термин "объект оценки" (TOE). В этом стандарте вводится также термин "активы", которым обозначаются сущности, предположительно представляющие ценность для владельца TOE. В [ISO/IEC 15408-1] ставится задача определить цели безопасности для TOE, то есть изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям. Угрозы влекут риски для активов, определяемые исходя из вероятности того, что угроза реализуется, и последствий ее реализации для активов. Вместе с тем в [ISO/IEC 15408-1] не содержатся указания относительно методов определения угроз и оценки рисков.

В настоящем Дополнении описаны выявленные угрозы встроенным системам и проводится анализ соответствующих рисков на основе подхода, изложенного в [ISO/IEC 15408-1]. Здесь цель состоит в том, чтобы анализ рисков не зависел от результатов в сфере проектирования защиты. Поэтому в настоящей Рекомендации уровень риска реализации угрозы встроенной системе определяется по методу CRSS [b-JASO TP15002]. Этот метод характеризуется следующим: 1) на этапах определения модели системы и анализа угроз формулируется конечный результат; 2) на основании полученной на предыдущих этапах информации устанавливается значение параметра.

Процесс оценки безопасности согласно [b-JASO TP15002] состоит из следующих этапов.

Этап 1. Определение объекта оценки.

Этап 2. Определение угроз.

Этап 3. Анализ рисков.

Каждый этап поясняется ниже.

I.1.1 Этап 1. Определение объекта оценки

Уточнение объекта, угрозы которому будут определяться на следующем этапе.

Этап 1 состоит из следующих четырех шагов.

Шаг 1. Выработка общего видения

Чтобы все участники проекта выработали общее видение жизненного цикла и устройства рассматриваемой системы, на основе обзорной документации системы подготавливается схема устройства системы, описание ее функционирования и перечень используемых системой данных.

Шаг 2. Построение схемы модели объекта оценки

Составляется схема модели объекта оценки, в которой уточняются состав компонентов системы и потоки информации между ними.

Шаг 3. Определение общего обзора функций модулей

Определяются функции и защищаемые активы каждого составляющего модуля, представленного на схеме модели объекта оценки. Таким образом строится таблица общего обзора функций модулей.

Угрозы безопасности могут описываться применительно к тому, "какие источники угроз существуют и какие негативные действия они могут предпринять в отношении тех или иных активов" в оцениваемой системе. Помимо информации, которая традиционно рассматривается как подлежащий защите актив, в автомобильных встроенных системах к активам также относят встроенное программное обеспечение системы и функции, управляющие работой механизмов (например, двигателя или тормозов).

Модель системы строится исходя из природы активов и схем потоков данных, определяющих потоки данных, относящихся к этим активам.

При определении негативных действий (угроз) рассматриваются все события, которые могут произойти в каждой из исходных точек, а также возможные виды нарушений конфиденциальности, целостности и доступности применительно к каждому типу активов. Например, важно обеспечить правильную, соответствующую ожиданиям работу автомобильной ИТ-системы и предотвратить нарушения целостности и доступности. Столь же важно защитить информацию, которой обмениваются центральные серверы и установленные в транспортном средстве устройства интеллектуальной транспортной системы (ИТС), от несанкционированного раскрытия и изменения, предотвратив нарушения конфиденциальности и целостности. В таблице I.1 приведены примеры информации и других активов, подлежащих защите в транспортных средствах.

Таблица I.1 – Примеры информации и других активов, подлежащих защите в транспортных средствах (информационная безопасность транспортных средств)

Объекты, подлежащие защите	Описание
Деятельность основных функций управления	Координация и доступность основных функций управления, среда выполнения основных функций управления, связь для обеспечения деятельности
Данные, характеризующие конкретное транспортное средство	Данные, характеризующие конкретный физический экземпляр транспортного средства (идентификатор транспортного средства, идентификатор устройства и т. д.), код аутентификации и собранная информация, такая как история поездок и эксплуатации
Данные о состоянии транспортного средства	Данные, характеризующие состояние транспортного средства (местоположение, скорость и пункт назначения)
Данные о пользователе	Личные данные, данные аутентификации, платежные данные, история поездок и эксплуатации конкретного пользователя (водитель/пассажиры)
Программное обеспечение	Программное обеспечение, относящееся к основным функциям управления и расширенным функциям транспортного средства. Пример – программное обеспечение ECU
Контент	Данные приложений (видео, музыка, карты и т. д.)
Информация о конфигурации	Параметры работы аппаратного и программного обеспечения и т. п.

Шаг 4. Определение жизненного цикла объекта оценки

Составляется таблица жизненного цикла, которая описывает весь жизненный цикл объекта оценки.

Источники угроз – это люди, участвующие в жизненном цикле транспортного средства на любом его этапе, включая производство, эксплуатацию приобретающими транспортное средство пользователями (как нового, так и приобретенного на вторичном рынке транспортного средства) и в конечном счете утилизацию. Это связано с тем, что сохранение конфиденциальной информации во встроенных системах транспортного средства и доступ к такой информации осуществляются не только в ходе штатной эксплуатации, но и на других этапах, например при производстве, доставке или техническом обслуживании. Жизненный цикл TOE подробно описывается в таблице I.2.

Таблица I.2 – Жизненный цикл TOE

Этап	Подэтап	Краткий обзор	Потенциальные источники угроз
Эксплуатация	Транспортировка	Персонал производителя оригинального оборудования (OEM) транспортирует готовое транспортное средство в адрес продавца транспортного средства. Эта задача поручается транспортной компании	· Персонал автопроизводителя · Транспортная компания · Персонал продавца транспортного средства · Третья сторона
	Доставка транспортного средства	Персонал продавца транспортного средства доставляет транспортное средство владельцу	· Персонал продавца транспортного средства · Владелец · Третья сторона
	Штатная эксплуатация/ использование	Владелец или пользователь эксплуатирует транспортное средство. Участниками этого этапа являются администратор сервера обновлений, с которого загружается программное обеспечение, и оператор электросвязи, предоставляющий свою сеть	· Владелец или пользователь · Администратор сервера · Оператор электросвязи · Третья сторона
	Штатная эксплуатация/ использование Загрузка программного обеспечения	Для подготовки к обновлению на транспортное средство загружается программное обеспечение с сервера обновлений	· Персонал автопроизводителя · Персонал поставщика · Администратор сервера · Оператор электросвязи · Третья сторона
	Обслуживание (обновление программного обеспечения с сервера обновлений) Обновление программного обеспечения	После парковки транспортного средства выполняется обновление программного обеспечения. Участником этого этапа является администратор сервера обновлений. Оператор электросвязи участвует в качестве поставщика сети связи. Персонал поставщика участвует в качестве поставщика услуг, использующего сеть связи	· Персонал автопроизводителя · Персонал поставщика · Администратор сервера · Оператор электросвязи · Третья сторона
	Обслуживание (обновление программного обеспечения через разъем OBD)	Персонал продавца транспортного средства или станции техобслуживания обновляет программное обеспечение через разъем бортовой диагностики (OBD) в процессе обслуживания транспортного средства	· Персонал продавца транспортного средства · Персонал станции техобслуживания · Владелец или пользователь · Третья сторона

I.1.2 Этап 2. Определение угроз

Выявляются проблемы безопасности применительно к TOE, который был определен на этапе 1.

Этап 2 состоит из следующих трех шагов.

Шаг 1. Формулирование предположений

Чтобы прояснить контекст, в котором определяются угрозы, формулируются предположения на основании схемы модели объекта оценки, сводки функций модулей и таблицы жизненного цикла. Угрозы на этапе 2 определяются в ограниченном контексте. Этот контекст задается предположениями о среде TOE. Каждой выявленной угрозе присваивается идентификатор с префиксом A. Таким образом строят таблицу предположений.

TOE эксплуатируется при следующих предположениях.

A.Reliability_OfficeStaff (надежность персонала автопроизводителя, поставщика, продавца транспортного средства и станции техобслуживания)

Персонал автопроизводителя или персонал поставщика не имеет физического доступа к транспортному средству – объекту атаки. Персонал продавца транспортного средства и станции техобслуживания не имеет физического доступа к транспортному средству на этапе штатной эксплуатации/использования.

A.Reliability_ServiceProvider (надежность администратора сервера/оператора электросвязи)

Администратор сервера обновлений/оператор электросвязи не осуществляет физического доступа к транспортному средству. Наряду с этим администратор сервера обновлений/оператор электросвязи не осуществляет преднамеренных действий, приводящих к возникновению угроз.

A.Reliability_User (надежность владельца/пользователя)

Владелец/пользователь не осуществляет физического доступа к транспортному средству – объекту атаки на этапе обслуживания.

Владелец/пользователь не осуществляет физического доступа к транспортному средству на этапе обслуживания. Наряду с этим владелец/пользователь всегда запирает дверь транспортного средства на этапе штатной эксплуатации/использования. Наряду с этим владелец/пользователь принимает необходимые меры для предотвращения доступа не имеющих разрешений лиц в салон транспортного средства на этапе штатной эксплуатации/использования.

A.Operation_Server (защита сервера вне контекста объекта оценки)

Сервер обновлений эксплуатируется надлежащим образом, то есть лица, являющиеся потенциальными источниками угроз, не имеют возможности считывать/изменять хранящуюся на сервере информацию.

A.Control_OBD-Tool (защита диагностического прибора и т. п. вне контекста объекта оценки)

Диагностический прибор эксплуатируется надлежащим образом, то есть лица, являющиеся потенциальными источниками угроз, не имеют возможности считывать/изменять хранящуюся на нем информацию.

Шаг 2. Определение угроз

На основании схемы модели объекта оценки, сводки функций модулей и таблицы жизненного цикла каждого компонента системы определяются угрозы в отношении ответов на вопросы Где? (исходные точки), Кто? (источники угроз), Когда? (этап жизненного цикла), Почему? (причины) и Что? (негативные действия), как показано в таблице I.3. Каждой выявленной угрозе присваивают идентификатор с префиксом T. Таким образом строят таблицу угроз.

Рассмотрев модель системы, жизненный цикл и негативные действия (анализируемые при определении системы, являющейся объектом оценки, как описано в пункте I.1), можно составить исчерпывающий список источников угроз и негативных действий, которые они могут предпринять в отношении тех или иных активов на различных этапах жизненного цикла.

Таблица I.3 – Аспекты определения угроз

Аспект	Пояснение
Где?	Определить исходные точки атак
Кто?	Определить источники угроз
Когда?	Определить этапы жизненного цикла, на которых происходят атаки
Почему?	Определить причины атак
Что?	Определить негативные действия

Шаг 3. Формулировка политики безопасности организации

Политика безопасности организации определяет требования, которые делают необходимым принятие контрмер в сфере безопасности по иным причинам, нежели угрозы. Примерами могут служить законы и отраслевые руководящие указания, которые необходимо соблюдать при разработке TOE и в среде его эксплуатации. На этом шаге определяются законы и корпоративные правила, относящиеся к разработке системы, которые следует определить как проблемы безопасности TOE. Каждому элементу политики безопасности присваивается идентификатор с префиксом O. Таким образом строится таблица политики безопасности организации.

К TOE не применяется политика безопасности организации.

I.1.3 Этап 3. Анализ рисков

На этом этапе определяют степень риска для всех выявленных угроз.

Для каждого элемента из таблицы угроз вычисляется приоритет.

Этап 3 состоит из следующих двух шагов.

Шаг 1. Оценка рисков

Риск, который представляют угрозы для ИТ-системы, оценивается обычно исходя из ценности активов и стоимости атаки, которая зависит от способа реализации угрозы. Этот подход эффективен, когда есть множество примеров атак и можно прийти к согласию о стоимости конкретного метода атаки с учетом таких факторов, как время, которое необходимо затратить на атаку, и возможности ее исполнителя. На уровне исследований сформулирован ряд теоретических примеров атак на автомобильные встроенные системы, однако такого широкого спектра вариантов методов атаки, который существует для ИТ-систем, в этой сфере не имеется. Ввиду этого затруднительно оценить ущерб от различных методов атак.

I.1.3.1 CRSS

Система оценки рисков на основе CVSS (CRSS) – это метод оценки рисков, связанных с угрозами, в основе которого лежит система оценки общеизвестных уязвимостей (CVSS), то есть система оценки рисков (RSS) по [ITU-T X.1521], используемая для ранжирования уязвимостей ИТ-систем по их степени [b-JASO TP15002]. Система CVSS состоит из трех групп показателей – базовых показателей, временны́х показателей и показателей среды. Эти группы показателей описываются следующим образом.

- Базовые показатели отражают изначальные и основополагающие характеристики уязвимости, которые не изменяются со временем и не зависят от пользовательской среды.
- Временные показатели отражают характеристики уязвимости, которые могут меняться со временем, но не зависят от пользовательской среды.
- Показатели среды отражают характеристики уязвимости, которые относятся к конкретной среде пользователя и свойственны только ей.

В CRSS показатель риска оценивается по *группе базовых показателей* CVSS. Группа базовых показателей отражает характеристики уязвимости, которые не изменяются со временем и не зависят от пользовательской среды. Показатели вектора доступа, сложности доступа и аутентификация отражают способ доступа к уязвимости, а также наличие или отсутствие дополнительных условий, необходимых для ее эксплуатации.

В рамках метода CRSS каждому активу присваивают ценность в отношении конфиденциальности, целостности и доступности, после чего рассчитывают показатель риска исходя из того, насколько легко реализовать атаку и каково ее воздействие.

Степень простоты реализации атаки выводится из показателя, который отражает то, насколько близко источники угроз должны подойти к активам и что им препятствует на этом пути. Пример классификации по степени порстоты реализации атаки приведен в таблице I.4.

Степень воздействия показывает, насколько эксплуатация уязвимости непосредственно скажется на активе, причем воздействие определяется по трем независимым показателям –степень потери конфиденциальности, целостности и доступности. Например, уязвимость может привести к частичной потере целостности и доступности без потери конфиденциальности. Пример классификации по степени воздействия приведен в таблице I.5.

Таблица I.4 – Пример классификации по степени простоты реализации атаки (таблица D.2 [b-JASO TP15002])

Параметр	Принцип учета	Классификация	Примеры
Вектор доступа (Access Vector (AV)): классификация по месту атаки	Классификация по месту атаки, создавшей угрозу (Где?)	Локальный (Local (L))	USB-носитель
		Соседняя сеть (Adjacent (A))	Устройство соединения Wi-Fi
		Сетевой (Network (N))	Линия подвижной связи
Сложность доступа (Access Complexity (AC)): степень сложности выполнения атаки	Классификация по объему навыков и знаний, требуемых для выполнения атаки	Высокая (High (H))	Требуются навыки и знания об атаке
		Средняя (Medium (M))	Требуются знания об атаке
		Низкая (Low (L))	Знания и навыки почти не требуются
Аутентификация (Authentication (Au)): количество уровней аутентификации, необходимое для выполнения атаки	Классификация по количеству уровней аутентификации между активом и источником угрозы	Многократная (Multiple (M))	Несколько уровней идентификации
		Однократная (Single (S))	Один уровень аутентификации
		Отсутствует (None (N))	Аутентификация не требуется

Таблица I.5 – Пример классификации по степени воздействия (таблица D.3 [b-JASO TP15002])

Актив	Классификация	Воздействие на конфиденциальность (Confidentiality impact (C))			Воздействие на целостность (Integrity impact (I))			Воздействие на доступность (Availability impact (A))		
		Отсутствует (None)	Частичное (Partial)	Полное (Complete)	Отсутствует (None)	Частичное (Partial)	Полное (Complete)	Отсутствует (None)	Частичное (Partial)	Полное (Complete)
Функция подвижной связи	Услуга обновления	Да					Да			Да
Функция аутентификации в сети подвижной связи				Да			Да	Да		
Функция загрузки программного обеспечения		Да					Да			Да
Программное обеспечение				Да			Да	Да		
Функция дистанционного обновления программного обеспечения		Да					Да			Да
Программное обеспечение				Да			Да	Да		
Функция GPS-приема	Обработка информации	Да				Да			Да	
Функция подключения к Wi-Fi		Да				Да			Да	
Функция аутентификации в сети Wi-Fi			Да			Да		Да		
Функция подключения по интерфейсу USB		Да				Да			Да	
Функция связи по интерфейсу CAN	Управление транспортным средством	Да					Да			Да
Функция CAN-шлюза		Да					Да			Да
Таблица маршрутизации				Да			Да	Да		
Функция подклю-чения через разъем OBD		Да					Да			Да

Для каждой угрозы, охарактеризованной по пяти аспектам (где, кто, когда, почему, что), можно вычислить количественный показатель риска.

Пример классификации согласно оценке риска приведен в таблице I.6.

Таблица I.6 – Пример вычисления показателей рисков (таблица D.4 [b-JASO TP15002])

№	Угрозы	AV	AC	Au	Степень простоты реализации атаки	C	I	A	Степень воздействия	Значение показателя риска
1	T.control_fcn_Mobile_3rd_ opearation_on_purpose of interfere-function	Сетевой (Network)	Средняя (Medium)	Однократная (Single)		Не требуется (Unnecessary)	Сильное (Large)	Сильное (Large)		
		1	0,61	0,56	6,83	0	0,66	0,66	9,20	7,95
2	T.vehicle_status_WiFi_dealer_ main_purpose_forge	Соседняя сеть (Adjacent network)	Однократная (Single)	Однократная (Single)		Слабое (Small)	Слабое (Small)	Отсутствует (None)		
		0,646	0,71	0,56	5,14	0,275	0,275	0	4,94	4,14
3	T. info_transfer_USB_ 3rd_operation_pursuse_ misop	Локальный (Local)	Низкая (Low)	Отсутствует (None)		Отсутствует (None)	Слабое (Small)	Отсутствует (None)		
		0,395	0,71	0,704	3,95	0	0,275	0	2,86	2,11

Даже в сфере автомобильных встроенных систем, где не хватает сведений об оценке угроз безопасности, метод CRSS позволяет рассчитать риск аналитически по определениям угроз и системе оценки. В числе прочего он позволяет учитывать при оценке риска такие факторы, как риск для жизни, рассматривая функции как активы и присваивая более высокую ценность тем из этих активов, применительно к которым потеря целостности или доступности влечет серьезные последствия.

Шаг 2. Определение причин угроз

Для каждой угрозы с показателем риска, превышающим определенное значение, логически анализируются ее причины с помощью дерева отказов (FT).

I.2 Проверка данных по алгоритмам MAC

Алгоритмы MAC играют важную роль в сфере криптографии и безопасности, обеспечивая целостность сообщения (аутентификацию). Существует ряд важных результатов работы ИСО/МЭК в отношении MAC – это стандарты [b-ISO/IEC 9797-1] (механизмы с использованием блочного шифра), [b-ISO/IEC 9797-2] (механизмы с использованием специализированной хеш-функции) и [b-ISO/IEC 9797-3] (механизмы с использованием универсальной хеш-функции).

Учитывая ограниченность вычислительных ресурсов транспортного средства, целесообразно использовать нересурсоемкие криптографические стандарты. Есть два типа стандартов MAC, отвечающих этому требованию: к первому типу относятся стандарты на базе блочных шифров [b-ISO/IEC 9797-1] и [b-ISO/IEC 29192-2] (легкий блочный шифр), а ко второму – стандарты на базе хеш-функций [b-ISO/IEC 9797-2] и [b-ISO/IEC 29192-5] (легкая хеш-функция).

При выборе наилучших алгоритмов MAC для обеспечения безопасности транспортного средства целесообразно отдавать предпочтение стандартизированным алгоритмам, если другие алгоритмы не обеспечивают явного преимущества в части безопасности или производительности. Основная цель использования алгоритмов MAC – компактная и быстродействующая программная реализация соответствующих функций на микроконтроллерах с обеспечением достаточного уровня безопасности для данной области применения. В частности, может быть желательной разработка высокоэффективного алгоритма MAC, предназначенного для реализации на микроконтроллерах.

Дополнение II

Угрозы, требования безопасности и меры обеспечения безопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

На сегодняшний день известны примеры различных атак на безопасность ИТ-систем и угроз им, и накоплены сведения по оценке рисков при проектировании ИТ-систем. Основные понятия в области безопасности, необходимые для оценки ИТ-продуктов, даны в [ISO/IEC 15408-1]. В контексте оценки в [ISO/IEC 15408-1] используется термин "объект оценки" (TOE). В этом стандарте вводится также термин "активы", которым обозначаются сущности, предположительно представляющие ценность для владельца TOE. В [ISO/IEC 15408-1] ставится задача определить цели безопасности для TOE, то есть изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации. Угрозы влекут риски для активов, определяемые исходя из вероятности того, что угроза реализуется, и последствий ее реализации для актива. Вместе с тем в [ISO/IEC 15408-1] не содержатся указания относительно методов определения угроз и оценки рисков. С другой стороны, существует ряд известных методов определения угроз и оценки рисков. В настоящем разделе определяется TOE для бортового мобильного шлюза (VMG), который рассматривается как один из основных компонентов системы безопасного обновления программного обеспечения, после чего определяются основные угрозы и связанные с ними требования безопасности. В заключение излагаются высокоуровневые меры обеспечения безопасности, позволяющие выполнить эти требования.

II.1 Определение объекта оценки

В настоящем разделе определяется TOE для VMG, который в настоящей Рекомендации рассматривается как один из основополагающих компонентов системы безопасного обновления программного обеспечения.

Для взаимодействия с внешней средой служат бортовой диагностический разъем (OBD), модуль подвижной связи, совмещенный приемник глобальной системы определения местоположения/глобальной навигационной спутниковой системы (GPS/ГЛОНАСС), адаптер беспроводной достоверности (Wi-Fi), радио- и телевизионный (ТВ) приемник, адаптер Bluetooth, адаптер CAN0/1, пользовательский интерфейс с приводом компакт-диска/универсального цифрового диска (CD/DVD), разъем универсальной последовательной шины (USB) и разъем стандарта защищенных цифровых носителей (SD). Хотя для целей настоящего раздела в качестве одной из бортовых шин транспортного средства рассматривается местный разъем контроллеров (CAN), аналогичный анализ можно провести и для других типов бортовых шин, включая шину передачи данных мультимедийных систем (MOST), локальную внутрисистемную сеть (LIN), FlexRay и т. д.

На рисунке II.1 TOE определен как область, обведенная пунктирной линией. Он отвечает за безопасное управление связью, обеспечивая взаимодействие с внешней средой транспортного средства.

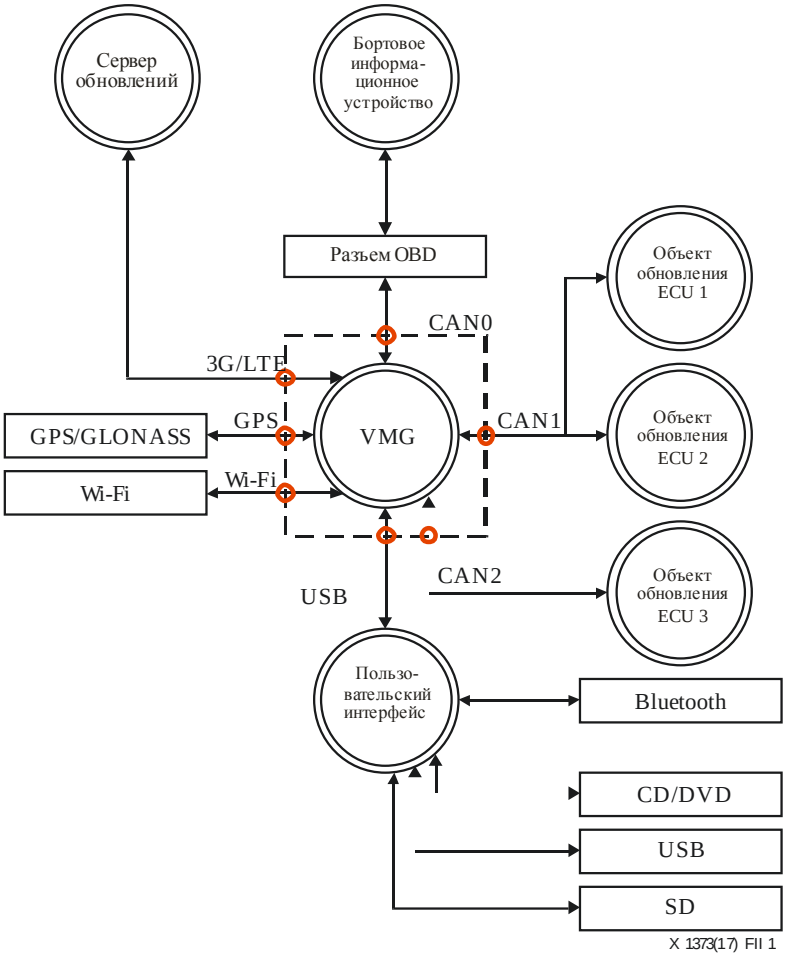

Рисунок II.1 – Модель TOE

Общий обзор функций модулей TOE дан в таблице II.1. В этой таблице также увязываются функции TOE с основными свойствами безопасности конфиденциальности (C), целостности (I) и/или доступности (A), что позволит затем сформулировать требования безопасности TOE в разделе II.3.

Таблица II.1 – Общий обзор функций модулей TOE

№	Модуль	Функция		Актив	C	I	A
1	Бортовой мобильный шлюз	Функция подвижной связи	Взаимодействие с сервером через адаптер подвижной связи. Используются данные аутентификации для проверки подлинности сервера	Функция подвижной связи		Да	Да
				Данные аутентификации	Да	Да	
		Функция загрузки программного обеспечения	Дистанционная загрузка программного обеспечения через адаптер подвижной связи или разъем OBD	Функция загрузки программного обеспечения		Да	Да
				Информация программного обеспечения	Да	Да	
		Функция дистанционного обновления программного обеспечения	Дистанционное обновление программного обеспечения через адаптер подвижной связи или разъем OBD.	Функция дистанционного обновления программного обеспечения		Да	Да

Таблица II.1 – Общий обзор функций модулей TOE

№	Модуль	Функция		Актив	C	I	A
			Если программное обеспечение обновляется дистанционно, используются данные аутентификации обновления для проверки подлинности сервера	Информация безопасности для обновления	Да	Да	
				Информация программного обеспечения	Да	Да	
		Функция GPS-приема	Получение данных от спутника GPS	Функция GPS-приема		Да	Да
		Функция подключения к Wi-Fi	Соединение устройств с интернетом через адаптер Wi-Fi. Использование данных аутентификации через разъем Wi-Fi	Функция подключения к Wi-Fi		Да	Да
				Данные аутентификации	Да	Да	
		Функция подключения по интерфейсу USB	Подключение пользовательского интерфейса с помощью кабеля USB	Функция подключения по интерфейсу USB		Да	Да
		Функция связи по интерфейсу CAN	Отправление/получение данных с ECU/на ECU по шине CAN	Функция связи по интерфейсу CAN		Да	Да
		Функция CAN-шлюза	Маршрутизация данных CAN в соответствии с таблицей маршрутизации. Таблица маршрутизации	Функция CAN-шлюза		Да	Да
				Таблица маршрутизации	Да	Да	
		Функция подключения через разъем OBD	Передача данных по шине CAN через разъем OBD	Функция подключения через разъем OBD		Да	Да

II.2 Определение основных угроз

Исходя из определения TOE для обновления программного обеспечения, приведенного в разделе II.1, в настоящем разделе определены основные угрозы, размещенные в TOE, в рамках подхода, изложенного в стандарте [ISO/IEC 15408-1].

В качестве метода определения основных угроз на основании данной модели TOE в настоящей Рекомендации применяется метод оценки рисков, изложенный (для сведения) в Дополнении I.

Таблица II.2 – Основные угрозы на основании модели TOE

№	Метка	Кто?	Когда? (этап)	Почему?	Где/что?
1	T.DoS-Functions-From-OBD-Device	Третья сторона Персонал СТО	Штатная эксплуатация Обслуживание	Преднамеренно	В отношении функций актива VMG он имитирует устройство соединения разъема OBD, передает большие объемы данных и создает помехи этой функции
2	T.Malfunction-Functions-From-OBD-Device	Третья сторона Персонал СТО	Штатная эксплуатация/ использование/ обслуживание Обслуживание	Преднамеренно	В отношении функций актива VMG он имитирует устройство соединения разъема OBD, передает несанкционированные данные и вызывает сбои в работе рассматриваемой функции

Таблица II.2 – Основные угрозы на основании модели TOE

№	Метка	Кто?	Когда? (этап)	Почему?	Где/что?
3	T.MissDoS-Functions-From-OBD-Device	Персонал авто-продавца Персонал СТО	Обслуживание	Непреднамеренно	В отношении функций актива VMG он по ошибке передает большие объемы данных или несанкционированные данные от устройства соединения разъема OBD и вызывает сбои в работе рассматриваемой функции
4	T.DoS-Functions-From-ECU	Третья сторона Персонал СТО	Штатная эксплуатация/ использование/ обслуживание Обслуживание	Преднамеренно	В отношении функций актива VMG он использует обратное проектирование того же программного продукта, что и встроенная программа ECU на шине CAN0-2, обновляет встроенную программу ECU, соединенную с CAN0-2 с несанкционированной встроенной программой, передает очень большие объемы данных с ECU на шине CAN1-5 и создает помехи в работе рассматриваемой функции
5	T.Malfunction-Functions-From-ECU	Третья сторона Персонал СТО	Штатная эксплуатация/ использование/ обслуживание Обслуживание	Преднамеренно	В отношении функций актива VMG он использует обратное проектирование того же программного продукта, что и встроенная программа ECU на шине CAN1-5, обновляет встроенную программу ECU, соединенную с CAN1-5 с несанкционированной встроенной программой, тем самым передает несанкционированные данные с ECU на шине CAN1-5 и вызывает сбои в работе рассматриваемой функции
6	T.DoS-Functions-From-Mobile-Device	Третья сторона	Штатная эксплуатация/ использование/ обслуживание	Преднамеренно	В отношении функций актива VMG он имитирует сервер, передает большие объемы данных с устройства подвижной связи на VMG и создает помехи в работе рассматриваемой функции
7	T.Spoofing-Server_ToGet-Data	Третья сторона	Штатная эксплуатация/ использование/ обслуживание	Преднамеренно	В отношении информации об активах VMG он передает команду на получение информации об активах VMG от устройства подвижной связи, перехватывая канал связи или имитируя устройство подвижной связи. Таким образом он получает информацию об активах VMG

Таблица II.2 – Основные угрозы на основании модели TOE

№	Метка	Кто?	Когда? (этап)	Почему?	Где/что?
8	T.MissDoS-Functions-From-mobile-Device	Администратор сервера	Штатная эксплуатация/ использование/ обслуживание	Непреднамеренно	В отношении функций актива VMG сервер посылает вследствие неправильного срабатывания большие объемы данных или несанкционированные данные с устройства подвижной связи, создает помехи и сбои в работе рассматриваемой функции
9	T.Leaking-Mobile-Information-From-Mobile-Device	Владелец/ пользователь Администратор сервера/ персонал авто-продавца Администратор сервера	Штатная эксплуатация/ использование/ доставка транспортного средства Штатная эксплуатация/ обслуживание	Непреднамеренно	В отношении информации об активах VMG вследствие неправильного срабатывания он по ошибке передает с устройства подвижной связи команду на VMG на получение актива защиты VMG (информации) и получает и вызывает утечку актива защиты VMG (информации)
10	T.MissUpdate-Mobile-Information-From-Mobile-Device	Владелец/ пользователь Администратор сервера/ персонал авто-продавца Администратор сервера	Штатная эксплуатация/ использование Доставка транспортного средства Штатная эксплуатация/ использование/ обслуживание	Непреднамеренно	В отношении информации об активах VMG вследствие неправильного срабатывания, по ошибке он передает команду на VMG на обновление актива защиты VMG (информации) и обновляет актив защиты VMG (информацию)
11	T.Malfunction-Functions-From-mobile-Device	Третья сторона	Штатная эксплуатация/ использование/ обслуживание	Преднамеренно	В отношении функций активов VMG с устройства подвижной связи он имитирует сервер, передает несанкционированные данные и вызывает сбои в работе рассматриваемой функции
12	T.Spoofing-Server_ToRewrite-Data	Третья сторона	Штатная эксплуатация/ использование	Преднамеренно	В отношении актива защиты (информации) VMG с устройства подвижной связи он имитирует устройство подвижной связи, посылает команду о перезаписи актива защиты (информации) VMG и актива защиты (информации) VMG
13	T.DoS-Functions-From-Wi-Fi-Device	Третья сторона	Штатная эксплуатация/ использование/ обслуживание	Преднамеренно	Для функции подключения к Wi-Fi он имитирует устройство Wi-Fi, передает большие объемы данных и вызывает помехи в работе рассматриваемой функции

Таблица II.2 – Основные угрозы на основании модели TOE

№	Метка	Кто?	Когда? (этап)	Почему?	Где/что?
14	T.Malfunction-Functions-From-Wi-Fi-Device	Третья сторона	Штатная эксплуатация/ использование/ обслуживание	Преднаме-ренно	Для функции подключения к Wi-Fi он имитирует устройство Wi-Fi, передает несанкционированные данные и вызывает сбои в работе рассматриваемой функции
15	T.MissDoS-Functions-From-Wi-Fi-Device	Владелец/ пользо-ватель	Штатная эксплуатация/ использование	Непреднаме-ренно	Для функции подключения к Wi-Fi вследствие неправильного срабатывания устройства подключения к Wi-Fi или инфицирования вредоносным программным обеспечением устройства подключения к Wi-Fi он посылает большие объемы данных или несанкционированные данные и вызывает помехи в работе рассматриваемой функции и сбои в работе рассматриваемой функции
16	T.Spoofing-Wi-Fi-Device_ToGet-Wi-Fi-Information	Третья сторона	Штатная эксплуатация/ использование/	Преднаме-ренно	Для функции подключения к Wi-Fi имитирует устройство подключения к Wi-Fi, посылает команду на получение данных аутентификации подключения к Wi-Fi и эксплуатирует данные аутентификации подключения к Wi-Fi
17	T.Spoofing-Wi-Fi-Device_ToRewrite-Wi-Fi-Information	Третья сторона	Штатная эксплуатация/ использование/ обслуживание	Преднаме-ренно	Для функции подключения к Wi-Fi он имитирует устройство подключения к Wi-Fi, посылает команду на перезапись данных аутентификации подключения к Wi-Fi и перезаписывает данные аутентификации подключения к Wi-Fi
18	T.Leaking-Wi-Fi-Information-From-Wi-Fi-Device	Персонал авто-продавца Владелец/ пользо-ватель	Доставка транспортного средства Штатная эксплуатация/ использование	Непреднаме-ренно	Для информации аутентификации подключения к Wi-Fi передает команду на получение данных аутентификации подключения к Wi-Fi, получает и вызывает утечку данных аутентификации подключения к Wi-Fi
19	T.MissUpdate-Wi-Fi-Information-From-Wi-Fi-Device	Персонал авто-продавца Владелец/ пользо-ватель	Доставка транспортного средства Штатная эксплуатация/ использование	Непреднаме-ренно	Для информации аутентификации подключения к Wi-Fi передает команду на перезапись данных аутентификации подключения к Wi-Fi и перезаписывает данные аутентификации подключения к Wi-Fi

II.3 Требования безопасности для TOE

На основании определения угроз, данного в разделе II.2, в следующих подразделах формулируются три компонента требований безопасности для модели TOE. Каждое требование безопасности основывается на угрозах, определенных в разделе II.2. Каждое требование безопасности в разделе II.3 сопровождается набором идентификаторов угроз (#), которые могут быть получены из таблицы II.2.

II.3.1 Перечень требований безопасности для TOE

II.3.1.1 Защита целостности/доступности функций VMG при связи по шине CAN (SR.integrity/availability protection of VMG functions through CAN communication)

Обеспечить целостность и доступность функций VMG, защитив их от атак типа отказ в обслуживании (DoS) и провоцирующих сбои атак с ECU по шинам CAN0–CAN2 (см. угрозы 4 и 5).

Описание

При связи по шине CAN маршрутизируются только те данные, для которых указаны определенные идентификаторы CAN (ID). VMG не должен выказывать аномалий в работе, если на него поступает большое количество пакетов данных с устройств на шинах CAN0–CAN2 и/или фиксируются необычные сценарии доступа с таких устройств.

II.3.1.2 Защита конфиденциальности данных VMG (SR.confidentiality protection of VMG data)

Необходимо защитить конфиденциальность данных, передаваемых между VMG и сервером, исключив возможность их чтения третьей стороной (см. угрозы 7, 16 и 17).

II.3.1.3 Защита целостности/доступности функций VMG при связи через сеть подвижной связи (SR.integrity/availability protection of VMG functions through mobile communication)

Необходимо обеспечить целостность и доступность функций VMG, защитив их от DoS и провоцирующих сбои атак с мобильных устройств через сеть подвижной связи (см. угрозы 6, 7, 8, 9, 10, 11 и 12).

Описание

При связи с устройством подвижной связи VMG должен подтвердить, что осуществляющее связь устройство является авторизованным устройством подвижной связи. Необходимо защитить VMG от атак с имитацией сервера при приеме несанкционированных/аномальных данных по сети подвижной связи. VMG не должен выказывать аномалий в работе, если на него поступает очень большое количество пакетов данных с устройств подвижной связи и/или подтверждаются необычные сценарии доступа с устройств подвижной связи. Кроме того, VMG должен проверять взаимную согласованность команд, передаваемых с устройств подвижной связи, и контролировать частоту их передачи.

II.3.1.4 Обеспечение отказоустойчивости функций VMG (SR.FaultTolerance of VMG functions)

Необходимо обеспечить работоспособность функций VMG (возможно на сниженном уровне) в условиях аномалий, обусловленных атаками (см. угрозы 1, 2, 3, 4, 5, 6, 8, 11 и 15).

II.3.1.5 Защита целостности/доступности функций VMG посредством OBD (SR.integrity/availability protection of VMG functions through OBD)

Необходимо обеспечить целостность и доступность функций VMG, защитив их от DoS и провоцирующих сбои атак с устройств, подключаемых к разъему OBD (см. угрозы 1, 2 и 3).

Описание

Доступ к ECU при связи по шине CAN через разъем OBD разрешается только определенным устройствам. Необходимо защитить VMG от атак с имитацией устройств соединения OBD при поступлении на него несанкционированных/аномальных данных через разъем OBD. VMG не должен выказывать аномалий в работе, если на него поступают очень большие объемы данных или несанкционированные команды с устройств, подключаемых к разъему OBD.

II.3.1.6 Защита конфиденциальности/целостности/доступности VMG при связи через сеть Wi-Fi (SR.confidentiality/integrity/availability protection of VMG through Wi-Fi communication)

Необходимо защитить VMG от атак с имитацией устройств соединения с Wi-Fi при поступлении на него несанкционированных/аномальных данных через сеть Wi-Fi (см. угрозы 13, 14, 15, 16, 17, 18 и 19).

Описание

При связи с устройством Wi-Fi VMG должен проверить, было ли это устройство предварительно зарегистрировано. VMG не должен выказывать аномалий в работе, если на него поступает большое количество пакетов данных с устройства Wi-Fi и/или фиксируются необычные сценарии доступа с таких устройств.

II.3.2 Требования безопасности среды эксплуатации TOE в отношении ИТ

II.3.2.1 Защита электронных блоков управления (SRE.ECU protection)

Необходимо защитить модуль ECU от анализа встроенной программы ECU путем запутывания кода модуля. Необходимо защитить ECU от атак с передачей несанкционированных данных от датчиков. Необходимо физически защитить ECU от атак с несанкционированной подменой ECU (см. угрозы 4 и 5).

II.3.2.2 Защита данных, передаваемых по шине CAN (SRE.CAN communication protection)

Защитить данные, передаваемые по шине CAN, от анализа протокола связи CAN путем скремблирования данных полезной нагрузки с использованием нересурсоемких операций, таких как перестановка битов и т. п. Необходимо физически защитить шину CAN от атак третьей стороны с несанкционированным присоединением к проводке шины (см. угрозы 4 и 5).

II.3.2.3 Защита сети подвижной связи (SRE.Mobile communication network protection)

Необходимо защитить сеть подвижной связи, используемую для связи VMG с сервером, от атак с несанкционированных устройств. Необходимо защитить информацию о конфигурации сети в отношении конфиденциальности. Следует обеспечить мониторинг сети для обнаружения атак (см. угрозы 6, 7, 11 и 12).

II.3.2.4 Защита данных, передаваемых через беспроводную сеть (SRE.Wireless communication protection)

Необходимо защитить данные, передаваемые через беспроводную сеть, от анализа протокола беспроводной связи путем сведения к минимуму данных полезной нагрузки в пакете связи или скремблирования данных полезной нагрузки с использованием нересурсоемких операций, таких как перестановка битов и т. п. (см. угрозы 7, 12, 16 и 17).

II.3.3 Требования безопасности для среды эксплуатации с позиций эксплуатации/управления, не относящихся к ИТ

II.3.3.1 Предупреждение (SREN.Caution)

Отмечается, что атака на встроенные системы транспортного средства является уголовным преступлением. Наряду с этим следует ограничить продажу продукции, способствующей совершению преступлений (см. угрозы 1, 2, 4, 5, 6, 7, 11, 12, 13, 14, 16 и 17).

II.3.3.2 Обслуживание сервера (SREN.NetworkServicer)

Администратору сервера следует исключить утечку или несанкционированную модификацию хранящихся данных в результате ненадлежащего управления сервером (см. угрозы 7 и 8).

II.3.3.3 Защита инструментов OBD (SREN.OBD tool protection)

Следует защитить подключаемые к транспортному средству инструменты OBD от несанкционированного использования, обеспечив безопасное управление ими. Наряду с этим следует проверить правильность работы подключаемых к транспортному средству инструментов перед их использованием (см. угрозу 3).

II.3.3.4 Информирование пользователей (SREN.User)

При использовании пользователями транспортного средства их необходимо информировать о необходимых мерах предосторожности.

Описание

Необходимо запирать салон транспортного средства, чтобы исключить проникновение в него третьей стороны в отсутствие пользователя. Если транспортное средство не используется, его необходимо ставить на стоянку в таком месте, где доступ к нему третьей стороны будет затруднен. Прежде чем воспользоваться транспортным средством, необходимо убедиться, что в нем нет неопознанных устройств. Пользователю необходимо соблюдать осмотрительность при подключении серийно выпускаемых приборов к разъему OBD, предназначенному для обслуживания (см. угрозы 1, 2, 4, 5, 13, 14, 16 и 17).

II.3.3.5 Сканирование на вирусы (SREN.VirusScan)

Необходимо регулярно проверять на наличие вирусов устройства, подключаемые к системе через сеть подвижной связи/Wi-Fi (см. угрозы 9, 10, 15, 18 и 19).

II.3.3.6 Защита устройств беспроводной связи (SREN.Wireless-Device protection)

Соответствующему лицу необходимо изучить порядок работы с устройством, подключаемым к транспортному средству через сеть подвижной связи/Wi-Fi, прежде чем приступать к его использованию. Наряду с этим соответствующему лицу необходимо соблюдать осмотрительность во избежание утечки пароля устройств, подключаемых через сеть Wi-Fi, и команд (см. угрозы 9, 10, 12, 13, 14, 16, 17, 18 и 19).

II.3.3.7 Подтверждение команд на дисплее беспроводного устройства (SREN.Wireless-Display)

Пользователям устройств, подключаемых через сеть подвижной связи/Wi-Fi, необходимо, выбирая элемент на дисплее устройства, подтверждать или отклонять передачу запросов на чтение и команд на запись информационных активов VMG (см. угрозы 9, 10, 18 и 19).

II.4 Меры обеспечения безопасности

В настоящем разделе излагаются меры обеспечения безопасности, которые удовлетворяют изложенным в разделе II.3 требованиям безопасности (в особенности с позиций ИТ).

II.4.1 Доверенный загрузчик (SC.Trusted boot)

В качестве меры противодействия анализу (например, подделке) изначального программного модуля ECU рекомендуется реализовать в ECU механизмы самопроверки его программного обеспечения, используя для этого механизм защиты загрузчика модуля защиты аппаратного обеспечения (HSM) при каждой загрузке ECU.

Соответствующее требование безопасности

- Защита электронных блоков управления (SRE.ECU protection), пункт II.3.2.1.

II.4.2 Проверка сообщений (SC.Message verification)

В качестве меры противодействия атакам с подделкой, прослушиванием канала связи и повторной передачей эффективен метод проверки сообщений, позволяющий удостоверить подлинность абонентов и целостность передаваемых сообщений.

Для этих целей пригодны два метода – первый с цифровой подписью (метод цифровой подписи), а второй с кодом аутентификации сообщений (MAC).

Пока в отношении практического применения ECU в транспортном средстве криптографические возможности устройств различаются в зависимости от модели транспортного средства. Например, в транспортном средстве класса люкс все ECU могут быть оснащены HSM, а в более массовой модели HSM могут присутствовать только в некоторых ECU. Кроме того, криптографические возможности различаются в зависимости от типа применяемого HSM.

Таким образом в архитектуре безопасности необходимо учитывать, что разные транспортные средства могут поддерживать неодинаковый набор возможностей защиты. Так, в настоящей Рекомендации применяется метод цифровой подписи на базе [ITU-T X.509] для проверки сообщений в транспортных средствах с реализацией асимметричного алгоритма шифрования в HSM (например, доверенного платформенного модуля (TPM)). С другой стороны, для транспортных средств, в которых

не используется асимметричный алгоритм шифрования (например, HSM и смарт-карта), в настоящей Рекомендации для проверки сообщений применяется метод MAC. Подробные сведения о протоколе связи, включая проверку сообщений, см. в разделе 7. Эта мера обеспечения безопасности является важнейшей мерой при дистанционном обновлении программного обеспечения для проверки сообщений согласно настоящей Рекомендации.

Соответствующие требования безопасности

- Защита конфиденциальности данных VMG (SR.confidentiality protection of VMG data), пункт II.3.1.2.
- Защита конфиденциальности/целостности/доступности VMG при связи через сеть Wi-Fi (SR.confidentiality/integrity/availability protection of VMG through Wi-Fi communication), пункт II.3.1.6.
- Защита сети подвижной связи (SRE.Mobile communication network protection), пункт II.3.2.3.
- Защита беспроводной связи (SRE.Wireless communication protection), пункт II.3.2.4.

II.4.3 Аутентификация объектов связи (SC.Authentication)

Чтобы предотвратить имитацию объектов связи (например, ECU, VMG и сервера обновлений), этим объектам рекомендуется организовать взаимную аутентификацию в начале каждого сеанса связи. Эту меру обеспечения безопасности следует реализовать ниже транспортного уровня, а защиту для процедур безопасного обновления, определенных в настоящей Рекомендации, следует обеспечить с использованием более низкоуровневых функций. В качестве конкретной контрмеры аутентификации объектов связи эффективна аутентификация как клиента, так и сервера с использованием протоколов уровня защищенных разъемов/безопасности транспортного уровня (SSL/TLS) под эгидой органа сертификации (CA), являющегося третьей стороной.

Соответствующие требования безопасности

- Защита конфиденциальности/целостности/доступности VMG при связи через сеть Wi-Fi (SR.confidentiality/integrity/availability protection of VMG through Wi-Fi communication), пункт II.3.1.6.
- Защита сети подвижной связи (SRE.Mobile communication network protection), пункт II.3.2.3.
- Защита данных, передаваемых через беспроводную сеть (SRE.Wireless communication protection), пункт II.3.2.4.

II.4.4 Фильтрация сообщений (SC.Message filtering)

Примером DoS-атаки на VMG может служить ситуация, когда скомпрометированный злоумышленником ECU передает на VMG очень большое количество поддельных сообщений, с тем чтобы вызвать непроизводительное расходование его вычислительных ресурсов. Одним из эффективных методов смягчения последствий таких DoS-атак для безопасности является фильтрация сообщений. Рекомендуется реализовать в VMG фильтрование посторонних сообщений по идентификатору отправителя, типу сообщения, размеру, частоте передачи и другим параметрам или их сочетанию.

Соответствующие требования безопасности

- Защита целостности/доступности функций VMG при связи по шине CAN (SR.integrity/availability protection of VMG functions through CAN communication), пункт II.3.1.1.
- Защита целостности/доступности функций VMG при связи через сеть подвижной связи (SR.integrity/availability protection of VMG functions through mobile communication), пункт II.3.1.3.
- Защита целостности/доступности функций VMG при подключении к разъему OBD (SR.integrity/availability protection of VMG functions through OBD), пункт II.3.1.5.

II.4.5 Обеспечение отказоустойчивости функций VMG (SC.FaultTolerance of VMG functions)

Поставщикам VMG настоятельно рекомендуется реализовывать программное обеспечение VMG на базе отказоустойчивой архитектуры, чтобы обеспечить работоспособность VMG в условиях аномалий, обусловленных атаками. В частности, VMG ведет мониторинг своей работы и в случае обнаружения каких-либо аномалий принимает меры (перезагрузку и т. д.) для возвращения к нормальному состоянию. Если же это невозможно, VMG уведомляет водителя о проблеме и приостанавливает работу безопасным образом.

Соответствующее требование безопасности

- Обеспечение отказоустойчивости функций VMG (SR.FaultTolerance of VMG functions), пункт II.3.1.4.

Библиография

[b-ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

[b-ISO/IEC 9797-1] ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50375>

[b-ISO/IEC 9797-2] ISO/IEC 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*. <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51618>

[b-ISO/IEC 9797-3] ISO/IEC 9797-3:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function.* <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51619>

[b-ISO/IEC 29192-2] ISO/IEC 29192-2:2012, *Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552>

[b-ISO/IEC 29192-5] ISO/IEC 29192-5:2016, *Information technology – Security techniques – Lightweight cryptography – Part 5: Hash-functions.* <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67173>

[b-JASO TP15002] JASO TP15002:2015, *Guideline for automotive information security analysis.*

[b-FIPS-202] Federal Information Processing Standards Publication-202 (2015), *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. National Institute of Standards and Technology. <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>

[b-ISO 14229] ISO 14229-1:2013, Road vehicles –Unified diagnostic services (UDS) – Part 1: Specification and requirements.

[b-ISO 13400] Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2018 г.