Международный союз электросвязи

МСЭ-Т X.1371

(05/2020)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасные приложения и услуги (2) – Безопасность интеллектуальных транспортных систем (ИТС)

Угрозы безопасности для соединенных транспортных средств

Рекомендация МСЭ-Т X.1371

ITU-T

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 (1)	
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 (1)	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 (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	**X.1370–X.1389**
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
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
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1371

Угрозы безопасности для соединенных транспортных средств

Резюме

В Рекомендации МСЭ-Т X.1371 описаны угрозы безопасности для соединенных транспортных средств и экосистемы транспортных средств.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1371	29.05.2020	17-я	11.1002/1000/14090

Ключевые слова

Соединенное транспортное средство, угроза безопасности.

* 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 в целях 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 извещения 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.1371

Угрозы безопасности для соединенных транспортных средств

1 Сфера применения

В настоящей Рекомендации содержится описание угроз безопасности для соединенных транспортных средств. На эту Рекомендацию можно ссылаться в будущих Рекомендациях МСЭ-Т, чтобы гарантировать, что в них последовательно учитываются аспекты безопасности интеллектуальных транспортных систем (ИТС).

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.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 готовность (availability) [b-ITU-T X.800]: Свойство быть доступным и годным к использованию по запросу имеющего полномочия объекта.

3.1.2 конфиденциальность (confidentiality) [b-ITU-T X.800]: Свойство, защищающее информацию от доступа к ней или ее раскрытия неуполномоченными лицами, устройствами или процессами.

3.1.3 целостность (integrity) [b-ISO/IEC 27000]: Свойство точности и полноты.

3.1.4 угроза (threat) [b-ISO/IEC 27000]: Возможная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

3G	Third Generation	Третье поколение
4G	Fourth Generation	Четвертое поколение
5G	Fifth Generation	Пятое поколение
ADAS	Advanced Driver Assistance System	Усовершенствованная система помощи водителю
CAN	Controller Area Network	Локальная сеть контроллеров
CAM	Cooperative Awareness Message	Сообщение совместной осведомленности
C-V2X	Cellular-based Vehicle-to-X	Сотовая связь транспортного средства с различными объектами

DENM	Decentralized Environmental Notification Message		Децентрализованное сообщение с уведомлением об окружающих условиях
DRM	Digital Right Management		Управление цифровыми правами
DSRC	Dedicated Short-Range Communication		Выделенная связь на короткие расстояния
ECU	Electronic Control Unit	ЭБУ	Электронный блок управления
GNSS	Global Navigation Satellite System	ГНСС	Глобальная навигационная спутниковая система
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
ID	Identifier		Идентификатор
IT	Information Technology	ИТ	Информационные технологии
ITS	Intelligent Transport Systems	ИТС	Интеллектуальные транспортные системы
IVN	In-Vehicle Network		Бортовая сеть
JTAG	Joint Test Action Group		Объединенная группа по вопросам тестирования
LIN	Local Interconnect Network		Локальная внутрисистемная сеть
MOST	Media Oriented Systems Transport		Шина передачи данных мультимедийных систем
OBD	On-Board Diagnostics		Бортовая система диагностики
ODR	Operating Data Recorder		Регистратор эксплуатационных данных
OEM	Original Equipment Manufacturer		Производитель оригинального оборудования
OTA	Over-The-Air		Канал беспроводной связи
RF	Radio Frequency	РЧ	Радиочастота
RSU	Roadside Unit		Придорожное устройство
SD	Secure Digital		Защищенный цифровой носитель
SQL	Structured Query Language		Язык структурированных запросов
USB	Universal Serial Bus		Универсальная последовательная шина
V2D	Vehicle-to-nomadic Device		[Связь] транспортного средства с перемещаемым устройством
V2I	Vehicle-to-Infrastructure		[Связь] транспортного средства с инфраструктурой
V2P	Vehicle-to-Pedestrian		[Связь] транспортного средства с пешеходом
V2V	Vehicle-to-Vehicle		[Связь] транспортного средства с транспортным средством
V2X	Vehicle-to-X		[Связь] транспортного средства с различными объектами
VIN	Vehicle Identification Number		Идентификационный номер транспортного средства
Wi-Fi	Wireless Fidelity		Высокая точность беспроводной передачи

5 Соглашения

Отсутствуют.

6 Модель соединенного транспортного средства (экосистемы транспортных средств)

На рисунке 1 представлена модель соединенного транспортного средства и его экосистемы. Эта модель является концептуальным представлением экосистемы транспортных средств и не зависит от каких-либо конкретных способов физической реализации и технологий, поскольку имеется понимание того, что они со временем изменятся. В модель вошли не все технологии и системы, используемые в экосистеме транспортных средств, однако она может использоваться в качестве основы для выявления угроз безопасности.

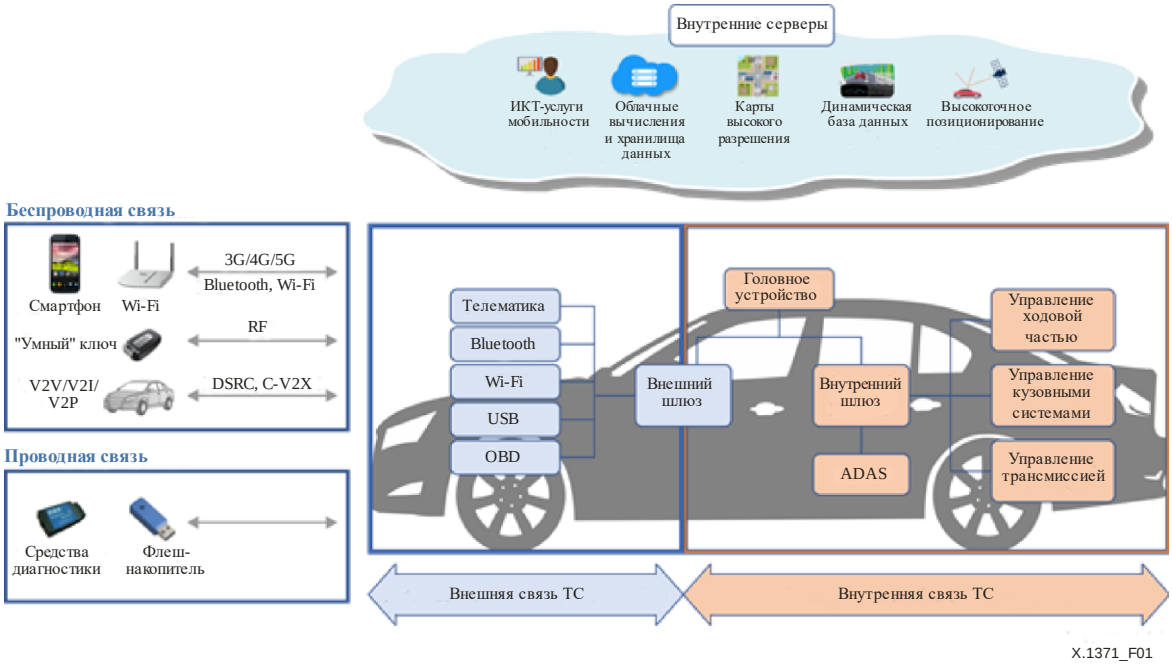

Рисунок 1 – Модель соединенного транспортного средства (экосистемы транспортных средств)

В настоящее время технологии связи имеют большое значение для функционирования транспортных средств. Связь транспортного средства делится на внешнюю и внутреннюю. Внутренняя сеть транспортного средства, известная как бортовая сеть (IVN), состоит из таких компонентов, как датчики и электронные блоки управления (ЭБУ). Эти датчики и ЭБУ используются для управления ходовой частью, управления кузовными системами и управления трансмиссией транспортного средства. Кроме того, эти компоненты используются в рамках усовершенствованной системы помощи водителю (ADAS), которая включает такие функции, как, например, сохранение полосы движения и круиз-контроль. Головное устройство является компонентом информационно-развлекательной системы транспортного средства, которая дает пользователю возможность управления информационно-развлекательными средствами транспортного средства, например аудио- и видеосистемами.

Внешняя связь транспортного средства обозначается термином V2X, что означает режим связи транспортного средства с различными объектами, где под различными объектами понимается все, что имеет отношение к безопасной и эффективной эксплуатации транспортного средства. В частности, V2X – общий термин для режимов связи, обозначаемых как режимы связи транспортного средства с транспортным средством (V2V), транспортного средства с инфраструктурой (V2I), транспортного средствами с перемещаемыми устройствами (V2D) и транспортного средства с пешеходом (V2P). Технология V2X включает в себя выделенную связь на короткие расстояния (DSRC) и связь V2X на основе технологий сотовой связи (C-V2X). Инфраструктура состоит из придорожных устройств (RSU) и внутренних объектов, таких как

системы регулирования дорожного движения и системы контроля. RSU могут быть подключены к внутренним объектам по кабельным или беспроводным сетям. На рисунке 1 показан различный функционал внутренних серверов. К нему относятся услуги мобильности на основе информационно-коммуникационных технологий (ИКТ), облачные хранилища данных, карта высокого разрешения, динамическая база данных по смежной среде и высокоточное позиционирование транспортного средства.

На рисунке 1 проиллюстрирована роль внешних и внутренних шлюзов в вопросах связи транспортных средств. Внутренний шлюз обрабатывает данные во внутренней области транспортного средства. Внешний шлюз отвечает за связь между транспортным средством и внешними устройствами, такими как смартфон и другие транспортные средства, с помощью технологии связи V2X. Внешняя связь делится на проводную и беспроводную. В качестве канала проводной связи, для связи с диагностическими устройствами и обновления ПО или прошивки транспортного средства, может использоваться порт бортовой системы диагностики II (OBD II). Беспроводной канал связи включает в себя технологию сотовой связи, Wi-Fi и Bluetooth, которые используются для соединения транспортного средства с мобильными устройствами, такими как смартфоны.

7 Угрозы безопасности для соединенных транспортных средств или экосистем транспортных средств и возможная информация, связанная с угрозами

7.1 Угрозы безопасности для соединенных транспортных средств или экосистем транспортных средств

7.1.1 Угрозы для внутренних серверов

В последние годы значительно увеличилось разнообразие возможностей установления соединений для транспортных средств и, в частности, весьма востребовано установление соединений с различными серверами ("внутренними серверами"), находящимися внутри транспортного средства. К внутренним серверам относятся серверы, предоставляемые производителями оригинального оборудования (OEM), поставщиками и ИКТ-службами для поддержки экосистем транспортных средств из удаленного центра.

7.1.1.1 Использование внутренних серверов для осуществления атак на транспортные средства или извлечения данных

В экосистеме транспортных средств внутренний сервер обычно ведет сбор данных с транспортного средства, осуществляет их хранение и отправляет информацию на транспортное средство. Для предотвращения взлома внутреннего сервера неавторизованным объектом необходимо учитывать следующие угрозы для внутреннего сервера:

– злоупотребление полномочиями со стороны внутреннего нарушителя. Злоупотребление внутренним нарушителем правами администратора на внутреннем сервере может привести к утечке данных с сервера, отправке транспортному средству ложной информации и т. д.;

– несанкционированный доступ извне к внутреннему серверу. Если на внутреннем сервере остается "лазейка" или известная уязвимость, они могут быть использованы извне для атаки на внутренний сервер с помощью таких методов, как внедрение кода на языке структурированных запросов (SQL) и внедрение вредоносных программ. Если злоумышленник получает права администратора сервера, то следует также рассмотреть ущерб, описанный в предыдущем пункте;

– несанкционированный физический доступ. Существует несколько вариантов физического доступа к внутреннему серверу, например с помощью флеш-накопителя с интерфейсом типа "универсальная последовательная шина" (USB) или в результате входа в здание, где находится сервер, с использованием поддельного идентификатора (ID) работника. В этом случае ущерб и вмешательство в данные, касающиеся транспортного средства, а также в его средства обработки информации являются еще более серьезными.

7.1.1.2 Нарушение функционирования услуг внутреннего сервера

Атаки на внутренний сервер могут вызвать сбои в его работе, нарушить его взаимодействие с транспортными средствами и функционирование услуг, используемых транспортными средствами. Атаки могут оказать серьезное вредное влияние на готовность услуг, связанных с транспортными средствами, таких как управление сертификацией транспортных средств и инфраструктуры.

7.1.1.3 Потеря или компрометация данных внутреннего сервера

Возможна потеря или утечка данных, хранящихся на внутренних серверах, если он был взломан или имело место злоупотребление полномочиями со стороны внутреннего нарушителя, несанкционированный доступ извне или несанкционированный физический доступ, указанные в пункте 7.1.1.1. Помимо этого, существуют следующие дополнительные угрозы:

– потеря информации в облаке. Может произойти утечка или компрометация конфиденциальной информации, такой как идентификационный номер транспортного средства (VIN) или личная информация водителя в случае ее хранения в системах сторонних поставщиков облачных услуг;

– утечка информации в результате непреднамеренного обмена данными. Если сервер находится в пределах неохраняемого периметра из-за неправильной конфигурации администратором, возможны непреднамеренный обмен данными или их утечка.

7.1.2 Угрозы для транспортных средств, связанные с каналами связи

Понятие связи транспортного средства включает в себя связь с внешними объектами, такую как V2V, V2I, V2D и V2P, а также бортовую связь, такую как локальная сеть контроллеров (CAN), локальная внутрисистемная сеть (LIN), шина передачи данных мультимедийных систем (MOST) и FlexRay. Каналы, используемые для этих видов связи, могут быть объектами атак, таких как спуфинг, прослушивание, манипуляция с сообщениями и прочее.

7.1.2.1 Спуфинговые сообщения

Рассылка спуфинговых сообщений может осуществляться на основе принципа подмены участника. В случае сообщений, используемых в режиме связи V2X и в рамках глобальной навигационной спутниковой системы (ГНСС), транспортное средство может принимать недействительные сообщения в результате атаки путем подмены участника. Кроме того, при наличии на определенной дороге большого количества транспортных средств может осуществляться атака Сивиллы с целью спуфинга других транспортных средств.

ПРИМЕЧАНИЕ. – Например, атака Сивиллы происходит, когда одно транспортное средство имитирует многочисленные транспортные средства путем использования нескольких идентификаторов транспортных средств.

7.1.2.2 Несанкционированное манипулирование, удаление или другие изменения кода или данных на транспортном средстве

При наличии уязвимостей или слабых мест в транспортном средстве по его каналам связи могут осуществляться незаконный удаленный доступ или вторжение с помощью вредоносных программ. Таким образом, имеется множество угроз безопасности, связанных с каналами связи, среди которых:

– внедрение кода: например, в поток передачи может быть внедрен взломанный двоичный программный код;

– манипулирование данными или кодом транспортного средства;

– перезапись данных или кода транспортного средства;

– уничтожение или удаление данных или кода транспортного средства.

7.1.2.3 Использование недостоверных или ненадежных сообщений и перехват сеанса или атака повторного воспроизведения

По каналам связи могут поступать сообщения из ненадежного или недостоверного источника. Также по каналам связи возможны атаки через посредника и перехват сеанса. Например, атака на коммуникационный шлюз транспортного средства позволяет злоумышленнику понизить версию программного обеспечения (ПО) ЭБУ или прошивки шлюза, используя известные уязвимости ПО, путем атаки повторного воспроизведения, когда повторная передача достоверных данных осуществляется со злым умыслом.

7.1.2.4 Раскрытие информации

Информация может быть легко раскрыта путем прослушивания сообщений или разрешения несанкционированного доступа к критичным файлам или папкам. То есть информация, которой обмениваются по каналу связи, может прослушиваться путем перехвата со злым умыслом, вмешательства в радиоканал и мониторинга линий связи. Для этого злоумышленник может получить несанкционированный доступ к файлам.

7.1.2.5 Атаки типа "отказ в обслуживании"

Злоумышленник может провести по каналу связи атаку типа "отказ в обслуживании", отправив большой объем информационного мусора в информационную систему транспортного средства, что приводит к нарушению большей части функций транспортного средства. В случае формирования автоколонн или в случае связи транспортного средства с транспортным средством злоумышленник может предотвратить отправку необходимых данных другим транспортным средствам в группе, чтобы они потеряли управление из-за отсутствия необходимых данных от других транспортных средств. Этот вид атаки известен как "черная дыра".

7.1.2.6 Привилегированный доступ у непривилегированного пользователя

Незаконный доступ по каналам связи делает возможным для непривилегированного пользователя получение привилегированного доступа, например корневого доступа к системе. Это носит название "несанкционированное повышение привилегий", и, как только такое повышение происходит, злоумышленник может делать то, чего не могут обычные пользователи.

7.1.2.7 Внедрение вирусов в среду передачи

После обнаружения уязвимостей в системе транспортного средства через каналы связи в систему транспортного средства могут быть внедрены вирусы или вредоносные программы. Вирусы способны стать администратором с привилегированным доступом и намеренно осуществлять любые атаки внутри транспортного средства. Например, так называемая "программа-вымогатель" осуществляет несанкционированное шифрование каких-либо файлов и информации в системе транспортного средства, на которую направлена атака, в результате чего система транспортного средства утрачивает функциональность.

7.1.2.8 Сообщения с вредоносным контентом

Вредоносный контент может содержаться в сообщениях, получаемых транспортным средством (например, диагностические сообщения или сообщения от других транспортных средств) или передаваемых внутри него. В случае IVN злоумышленник может изменить ПО ЭБУ путем внедрения вирусов (см. пункт 7.1.2.7) и присоединиться к сети транспортного средства путем подмены участника.

Вредоносные сообщения V2X, такие как сообщения совместной осведомленности (CAM) и децентрализованные сообщения с уведомлением об окружающих условиях (DENM), могут приниматься находящимися поблизости транспортными средствами. Связь V2X основана на широковещательной передаче, поэтому большое количество вредоносных сообщений V2X может оказывать вредное влияние на все сети транспортных средств, в том числе на IVN самого транспортного средства.

Также возможно получение вредоносных диагностических сообщений. Злоумышленник может записать диагностическое сообщение и использовать его для атаки повторного воспроизведения. Более того, в рамках атаки повторного воспроизведения возможно даже получение команд управления транспортным средством.

Проприетарные сообщения обычно отправляются OEM или поставщиком компонентов, систем или функций. Однако вредоносные проприетарные сообщения могут также направляться злоумышленниками в целях нарушения работы системы транспортного средства.

7.1.3 Угрозы, связанные с процедурами обновления ПО на транспортных средствах

Существует два способа обновления систем транспортного средства, а именно обновление по каналам проводной связи через порт OBD и портативные устройства, такие как защищенная цифровая (SD) карта или флеш-накопитель USB, и беспроводное обновление по каналам

беспроводной связи (OTA). Обновляться может прошивка или данные конфигурации транспортного средства. Большинство неисправностей электроники и ошибок ПО могут быть скорректированы и исправлены электронным образом без физического доступа, например с помощью тестера OBD. Кроме того, обновление по каналам OTA помогает сократить цикл обновления и минимизировать подверженность известных уязвимостей ПО атакам.

7.1.3.1 Злоупотребление процедурами обновления или их компрометация

Вне зависимости от используемого способа обновления – на месте или при наличии физического доступа либо через OTA – процедура обновления может содержать угрозы при использовании поддельных программ обновления систем или скомпрометированной прошивки.

Программным обеспечением можно манипулировать до начала процесса обновления, не нарушая процесса обновления. Поставщик ПО создает или подготавливает ПО для обновления, и оно доставляется в целевые системы, требующие обновления. То есть возможна серьезная угроза манипулирования ПО и его искажения до ввода в действие.

Прежде всего могут быть скомпрометированы криптографические материалы, такие как ключи и сертификаты, используемые в процедуре обновления ПО, следствием чего может стать неверное обновление ПО.

7.1.3.2 Отказ в легальном обновлении

В рамках процедуры обновления ПО возможна атака типа "отказ в обслуживании" на сервер или сеть обновлений в целях предотвращения развертывания критических обновлений ПО или разблокирования пользовательских функций. Также возможен отказ в легальном обновлении.

7.1.4 Непреднамеренные действия человека как угроза для транспортных средств

Действия человека могут непреднамеренно привести к нераспознанным угрозам. К таким угрозам по умолчанию относятся несанкционированная или непреднамеренная модификация ПО. К случайным ошибкам относятся нарушения конфигурации, программные ошибки и искажение данных из-за ошибок пользователя или оператора.

7.1.4.1 Неправильная конфигурация оборудования или систем законным субъектом

Законный пользователь может совершать действия, приводящие к непреднамеренным кибератакам. Он может внести непредусмотренные изменения в настройки системы транспортного средства во время непреднамеренных действий по установке, ремонту или использованию. Кроме того, возможны ошибки в управлении системами или устройствами или ошибки в их использовании, в том числе при обновлении ПО.

7.1.4.2 Непреднамеренное содействие законного субъекта кибератаке

Законный пользователь (например, владелец, оператор или инженер по обслуживанию) может быть невинной жертвой, и его могут склонить к тому, чтобы он совершил действие для непреднамеренной загрузки вредоносного кода (вредоносного ПО) или сделал атаку возможной. Помимо этого, часто бывает, что законный пользователь не выполняет определенные процедуры безопасности.

7.1.5 Угрозы для транспортных средств, связанные с возможностями взаимодействия и соединениями с внешними объектами

Для оказания разнообразных обеспечивающих удобство услуг транспортные средства могут быть оснащены компонентами для связи с внутренними серверами и могут связываться со всеми объектами, которые подключены пользователями дорог через беспроводное соединение. Помимо функций обеспечения комфорта, есть и полезные функции в области безопасности, такие как функция автоматического экстренного вызова и функции, поддерживаемые в режиме связи V2X. Однако, чем больше транспортных средств подключается ко внешним объектам, расширяя возможности взаимодействия, тем больше появляется угроз и уязвимостей, поскольку одновременно с ростом числа дополнительных интерфейсов растет число видов атак.

7.1.5.1 Манипулирование функциями установления соединений для транспортных средств

Манипулирование функциями установления соединений для транспортных средств позволяет осуществлять кибератаки. Такая угроза может проявляться применительно к следующим элементам транспортного средства:

– манипулирование функциями, предназначенными для удаленного управления системами: дистанционный ключ, иммобилайзер и станция зарядки;

– манипулирование телематикой транспортного средства: например, дистанционная разблокировка дверей грузовика;

– манипулирование через интерфейс с беспроводной локальной системой или датчиками.

7.1.5.2 Размещение стороннего ПО

В рамках информационно-развлекательной системы в современных транспортных средствах, подключенной к IVN, возможна установка сторонних приложений. Сторонние приложения могут быть искажены или иметь плохую защиту ПО и использоваться в качестве способа атаки на системы транспортных средств.

7.1.5.3 Устройства, подключенные к внешним интерфейсам

Функции установления соединений предоставляют внешние интерфейсы, а подключенные к ним устройства могут использоваться в качестве средства для атаки на системы транспортных средств со следующими уязвимыми интерфейсами:

– внешние интерфейсы, такие как USB-порт: для атаки путем внедрения кода;

– зараженная вирусом среда связи: вирус может атаковать бортовую систему через зараженную среду связи;

– диагностический доступ: диагностические функции, доступные через устройства Bluetooth по портам OBD, используются для просмотра статуса транспортного средства и управления параметрами, которые включены в ПО транспортного средства.

7.2 Возможная информация, связанная с угрозами

7.2.1 Потенциальные цели или причины атаки

Транспортные средства могут стать целью возможных кибератак, когда они электронным образом подключены ко многим системам или услугам внутри экосистемы транспортных средств. Помимо этого, злоумышленники часто стремятся получить финансовую выгоду, информируя об имеющейся у них возможности атак не просто весь мир, а поставщиков оригинального оборудования. Атаки могут воздействовать на системы транспортных средств, как описано в пунктах 7.2.1.1–7.2.1.7.

7.2.1.1 Извлечение данных или кода транспортного средства

Осуществляются попытки извлечь конфиденциальные или учетные данные, которые могут содержать полезную с точки зрения получения финансовой выгоды информацию, такие как:

– охраняемое авторским правом или проприетарное ПО транспортного средства;

– личная информация владельца, например персональные данные, информация о платежном счете, адресная книга, информация о местонахождении и электронный идентификатор транспортного средства;

– криптографические ключи и так далее.

7.2.1.2 Манипулирование данными или кодом транспортного средства

Манипулируя данными или кодом транспортного средства, злоумышленники могут осуществлять подмену участника или отказ от действий от имени законного владельца. Можно выделить следующие методы манипулирования:

– незаконные/несанкционированные изменения электронного идентификатора транспортного средства;

– мошенничество с персональными данными: в случае если пользователь хочет отображать другие персональные данные при взаимодействии с системами взимания автодорожных сборов и внутренними системами производителя;
– действия по обходу систем контроля: взлом, подделка или блокировка сообщений, например сообщений, содержащих информацию с регистратора рабочих данных (ODR) или о числе поездок;
– манипулирование с целью фальсификации данных о вождении транспортного средства: например, пробег, скорость движения, направление движения и контрольное время транспортного средства;
– несанкционированное изменение диагностических данных системы;
– мошенничество с версией прошивки: последняя версия прошивки, в которой исправлена какая-либо уязвимость, может быть заменена на старую версию, в которой такое исправление отсутствует.

7.2.1.3 Стирание данных или кода

Может произойти несанкционированное удаление журналов системных событий или манипулирование ими. Это часто делает невозможным анализ данных или затрудняет поиск причины атаки.

7.2.1.4 Внедрение вредоносного ПО

Для множества методов атаки внедрение вредоносного ПО в систему транспортного средства является первым шагом злоумышленника. Существуют различные возможности атак в целях внедрения вредоносных программ, среди которых использование внешних интерфейсов и зараженных физических модулей.

7.2.1.5 Внедрение нового или перезапись существующего ПО

Внедрение нового ПО или перезапись вредоносного ПО вместо существующего может привести к серьезным последствиям для кибербезопасности в системе управления транспортным средством или информационной системе.

7.2.1.6 Нарушение работы систем или операций

Атака типа отказ в обслуживании на систему транспортного средства может быть инициирована во внутренней сети из-за переполнения шины CAN сообщениями или из-за высокой скорости передачи сообщений, что вызывает сбои в ЭБУ.

7.2.1.7 Манипулирование параметрами транспортного средства

Манипулирование параметрами транспортного средства может оказать серьезное влияние на систему транспортного средства, например, в результате несанкционированного доступа с целью фальсификации:

– параметров конфигурации ключевых функций транспортного средства, к примеру данных о тормозной системе или пороге срабатывания подушки безопасности;
– параметров зарядки, таких как зарядное напряжение, зарядная мощность, температура аккумулятора и так далее.

7.2.2 Потенциальные уязвимости

7.2.2.1 Уязвимые криптографические технологии

Криптографические технологии могут быть скомпрометированы или применяться в недостаточной степени. Возможно использование уязвимостей криптографических ключей или сертификатов, включая учетные данные, такие как пароль. Например, если используются слабые криптографические ключи или они долго не обновляются, то криптографическая система может быть взломана в результате атаки методом полного перебора. Применение криптографических технологий в недостаточной степени также может привести к утечке криптографических ключей или учетных данных. Кроме того, риск утечки информации может возрасти в связи с использованием уже взломанных и устаревших криптографических технологий.

7.2.2.2 Скомпрометированные автозапчасти или расходные материалы

Аппаратное или программное обеспечение, используемое в экосистеме транспортных средств, может быть сконструировано так, что оно не отвечает проектным критериям для отражения атак. Автозапчасти или расходные материалы транспортного средства могут быть скомпрометированы, что делает возможной атаку на транспортное средство.

7.2.2.3 Уязвимости при разработке программного или аппаратного обеспечения

В основе уязвимостей с возможностью эксплуатации может лежать наличие программных ошибок. Это прежде всего актуально, если ПО не было протестировано, чтобы убедиться в отсутствии известного дефектного кода или ошибок и снизить риск наличия неизвестного дефектного кода или ошибок.

Использование элементов, оставшихся по итогам разработки ПО (например, портов отладки, портов Объединенной группы по вопросам тестирования (JTAG), микропроцессоров, сертификатов разработки и паролей разработчиков), также может обеспечить доступ к электронным блокам управления или позволить злоумышленникам получить привилегии более высокого уровня.

7.2.2.4 Уязвимости при проектировании сети

Если доступ к сети разрешен, а ненужные порты связи оставлены открытыми, то возможна активизация атак типа "несанкционированный доступ".

Кроме того, использование незащищенных шлюзов или точек доступа (например, шлюзов для грузовых автомобилей с прицепом) для обхода средств защиты и получения доступа к другим сегментам сети может привести к выполнению злонамеренных действий, таких как отправка произвольных сообщений по шине CAN.

7.2.2.5 Физическая потеря данных

Конфиденциальные данные, используемые в экосистемах транспортных средств, могут быть потеряны или скомпрометированы из-за физических повреждений в результате дорожно-транспортных происшествий или угона. Также потеря данных может происходить в результате управления цифровыми правами (DRM), например удаления пользовательских данных.

Кроме того, целостность конфиденциальных данных может быть утрачена из-за износа информационно-технологических (ИТ) компонентов, что может вызвать целую череду проблем (например, в случае изменения ключа).

7.2.2.6 Непреднамеренная передача данных

Утечка личных или конфиденциальных данных возможна при смене пользователя транспортного средства (например, когда транспортное средство продано или используется в качестве арендованного транспортного средства другим лицом).

7.2.2.7 Физическое манипулирование системами

Физическое манипулирование системами, например аппаратным обеспечением OEM, может привести к атакам. Например, возможна атака через посредника, если в транспортное средство внедрено неавторизованное ПО.

Дополнение I

Примеры уязвимостей или методов атак, связанных с угрозами

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем Дополнении приведены примеры уязвимостей или методов атак, связанных с угрозами, которые воспроизводятся по таблице 1 [b-UNECE GRVA].

ПРИМЕЧАНИЕ. – Номера пунктов в крайнем левом столбце таблицы I.1 совпадают с номерами пунктов [b-UNECE GRVA].

Таблица I.1 – Список примеров уязвимостей или методов атак, связанных с угрозами

Уязвимости/угрозы – описание высокого и среднего уровней			**Пример уязвимостей или методов атак**	
4.3.1 Угрозы для внутренних серверов	1	Использование внутренних серверов для осуществления атак на транспортные средства или извлечения данных	1.1	Злоупотребление привилегиями со стороны персонала (внутренняя атака)
			1.2	Несанкционированный доступ к серверу через интернет (например, благодаря "лазейкам", неисправленным уязвимостям ПО, SQL-атакам и пр.)
			1.3	Несанкционированный физический доступ к серверу (например, с помощью USB-накопителей или других носителей, подключаемых к серверу)
	2	Нарушение функционирования услуг внутреннего сервера, влияющее на работу транспортного средства	2.1	Атака на внутренний сервер останавливает его работу, например препятствует взаимодействию с транспортными средствами и предоставлению услуг, которые они используют
	3	Потеря или компрометация данных, хранящихся на внутренних серверах (утечка данных)	3.1	Злоупотребление привилегиями со стороны персонала (внутренняя атака)
			3.2	Потеря информации в облаке. Конфиденциальные данные могут быть потеряны из-за атак или происшествий в случае хранения в системах сторонних поставщиков облачных услуг
			3.3	Несанкционированный доступ к серверу через интернет (например, благодаря "лазейкам", неисправленным уязвимостям ПО, SQL-атакам и пр.)
			3.4	Несанкционированный физический доступ к серверу (например, с помощью USB-накопителей или других носителей, подключаемых к серверу)
			3.5	Утечка информации в результате непреднамеренного обмена данными (например, в случае ошибки администратора, хранения данных на серверах в гаражах)
4.3.2 Угрозы для транспортных средств, связанные с каналами связи	4	Спуфинг сообщений или данных, получаемых транспортным средством	4.1	Спуфинг сообщений на базе принципа подмены участника (например, в случае V2X по технологии 802.11p при формировании автоколонн, при рассылке сообщений ГНСС и пр.)
			4.2	Атака Сивиллы (с целью имитировать другие транспортные средства при наличии на дороге большого количества транспортных средств)
	5	Каналы связи, используемые для несанкционированного манипулирования, удаления или других изменений кода/данных на транспортном средстве	5.1	Каналы связи допускают внедрение кода, например, взломанный двоичный программный код может быть внедрен в поток передачи
			5.2	Каналы связи допускают манипулирование данными/кодом транспортного средства
			5.3	Каналы связи допускают перезапись данных/ кода транспортного средства
			5.4	Каналы связи допускают уничтожение данных/ кода транспортного средства
			5.5	Каналы связи допускают введение данных/ кода в транспортное средство (написание кода данных)

Таблица I.1 – Список примеров уязвимостей или методов атак, связанных с угрозами

Уязвимости/угрозы – описание высокого и среднего уровней			**Пример уязвимостей или методов атак**	
	6	Каналы связи допускают использование недостоверных/ненадежных сообщений и перехват сеанса/атаку повторного воспроизведения	6.1	Принятие информации из ненадежного или недостоверного источника
			6.2	Атака через посредника/перехват сеанса
			6.3	Атака повторного воспроизведения, например атака на коммуникационный шлюз транспортного средства позволяет злоумышленнику понизить версию ПО ЭБУ или прошивки шлюза
	7	Информация может быть легко раскрыта, например путем прослушивания сообщений или разрешения несанкционированного доступа к конфиденциальным файлам или папкам	7.1	Перехват информации/вмешательство в радиоканал/прослушивание линий связи
			7.2	Получение несанкционированного доступа к файлам или данным
	8	Атаки типа "отказ в обслуживании" в целях нарушения функций транспортного средства	8.1	Отправка большого количества информационного мусора в информационную систему транспортного средства, так что она теряет способность предоставлять услуги в обычном порядке
			8.2	Атака "черная дыра". С целью нарушить связь между транспортными средствами злоумышленник может блокировать обмен сообщениями между транспортными средствами
	9	Привилегированный доступ к системам транспортного средства у непривилегированного пользователя	9.1	Непривилегированный пользователь способен получить привилегированный доступ, например корневой доступ
	10	Вирусы, внедренные в среду передачи, способны заразить системы транспортного средства	10.1	Вирус, внедренный в среду передачи, заражает системы транспортного средства
	11	Вредоносный контент может содержаться в сообщениях, получаемых транспортным средством (например, в диагностических сообщениях или сообщениях от других транспортных средств) или передаваемых внутри него	11.1	Вредоносные внутренние сообщения (например, CAN)
			11.2	Вредоносные сообщения V2X, в том числе сообщения между инфраструктурой и транспортными средствами либо между транспортными средствами (например, CAM, DENM)
			11.3	Вредоносные диагностические сообщения
			11.4	Вредоносные проприетарные сообщения (например, те, которые обычно отправляются OEM или поставщиком компонентов/системы/функций)
4.3.3. Угрозы, связанные с процедурами обновления ПО на транспортных средствах	12	Злоупотребление процедурами обновления или их компрометация	12.1	Компрометация процедур обновления ПО по каналам беспроводной связи, включая поддельную программу обновления систем или прошивку
			12.2	Компрометация процедур обновления ПО на месте/при наличии физического доступа, включая поддельную программу обновления систем или прошивку
			12.3	Манипуляция ПО происходит до начала процесса обновления (вследствие чего ПО подвергается искажению), хотя процесс обновления не нарушается
			12.4	Компрометация криптографических ключей поставщика ПО с целью сделать возможным его неверное обновление
	13	Возможный отказ в легальном обновлении	13.1	Атака типа отказ в обслуживании на сервер или сеть обновлений в целях предотвращения развертывания критических обновлений ПО и/или разблокирования пользовательских функций

Таблица I.1 – Список примеров уязвимостей или методов атак, связанных с угрозами

Уязвимости/угрозы – описание высокого и среднего уровней			Пример уязвимостей или методов атак	
4.3.4 Непреднамеренные действия человека как угроза для транспортных средств	14	Неправильная конфигурация оборудования или систем законным субъектом, например владельцем или предоставляющим обслуживание лицом	14.1	Неправильная конфигурация оборудования владельцем или предоставляющим обслуживание лицом в процессе установки/ремонта/использования, что вызывает непредвиденные последствия
			14.2	Ошибочное использование или администрирование устройств и систем (в том числе обновление по каналам беспроводной связи)
	15	Законный субъект может совершать действия, не осознавая, что они упрощают кибератаки	15.1	Невинную жертву (например, владельца, оператора или инженера по обслуживанию) могут склонить к тому, чтобы она совершила действие для непреднамеренной загрузки вредоносного ПО или сделала атаку возможной
			15.2	Невыполнение установленных процедур безопасности
4.3.5 Угрозы для транспортных средств, связанные с возможностями взаимодействия и соединениями с внешними объектами	16	Манипулирование функциями установления соединений для транспортных средств делает возможными кибератаки, в том числе в отношении телематики, систем дистанционной эксплуатации и беспроводных локальных систем	16.1	Манипулирование функциями, предназначенными для удаленного управления системами, такими как дистанционный ключ, иммобилайзер и станция зарядки
			16.2	Манипулирование телематикой транспортного средства (например, манипулирование измерением температуры товаров, требующих особого температурного режима, дистанционная разблокировка дверей грузовика)
			16.3	Вмешательство в работу беспроводной локальной системы или датчиков
	17	Размещение стороннего ПО, такого как развлекательные приложения, в качестве способа атаки на системы транспортного средства	17.1	Приложения могут быть искажены или иметь плохую защиту ПО и использоваться в качестве способа атаки на системы транспортных средств
	18	Устройства, подключенные ко внешним интерфейсам, таким как порты USB и OBD, используемые в качестве способа атаки на системы транспортного средства	18.1	Внешние интерфейсы, такие как USB-порт или другие порты, используемые как точка атаки, например для внедрения кода
			18.2	Зараженная вирусом среда связи, соединенная с системой транспортного средства
			18.3	Диагностический доступ (например, через порт OBD), используемый для облегчения атаки, например манипулирования параметрами транспортного средства (прямого или опосредованного)
4.3.6 Потенциальные цели или причины атаки	19	Извлечение данных/ кода транспортного средства	19.1	Извлечение охраняемого авторским правом или проприетарного ПО систем транспортного средства (фальсификация продуктов)
			19.2	Несанкционированный доступ к личной информации владельца, такой как персональные данные, информация о платежном счете, адресной книге, местонахождении, электронном идентификаторе транспортного средства и прочее
			19.3	Извлечение криптографических ключей
	20	Манипулирование данными/ кодом транспортного средства	20.1	Незаконные/несанкционированные изменения электронного идентификатора транспортного средства
			20.2	Мошенничество с персональными данными. Например, в случае если пользователь хочет отображать другие персональные данные при взаимодействии с системами взимания автодорожных сборов и внутренними системами производителя
			20.3	Действия в целях обхода систем контроля (например, взлом/подделка/блокировка сообщений, таких как сообщения, содержащие информацию с ODR или о числе поездок)

Таблица I.1 – Список примеров уязвимостей или методов атак, связанных с угрозами

Уязвимости/угрозы – описание высокого и среднего уровней			Пример уязвимостей или методов атак	
			20.4	Манипулирование в целях фальсификации данных о вождении транспортного средства (например, пробег, скорость движения, направление движения и так далее)
			20.5	Несанкционированное изменение диагностических данных системы
	21	Стирание данных/кода	21.1	Несанкционированное удаление журналов системных событий/манипулирование ими
	22	Внедрение вредоносного ПО	22.1	Внедрение вредоносного ПО или вредоносная программная активность
	23	Внедрение нового или перезапись существующего ПО	23.1	Фальсификация ПО системы управления транспортным средством или информационной системы
	24	Нарушение работы систем или операций	24.1	Атака типа "отказ в обслуживании", например, может быть инициирована во внутренней сети из-за переполнения шины CAN или из-за высокой скорости передачи сообщений, что вызывает сбои в ЭБУ
	25	Манипулирование параметрами транспортного средства	25.1	Несанкционированный доступ в целях фальсификации параметров конфигурации ключевых функций транспортного средства, например данных о тормозной системе, пороге срабатывания подушки безопасности и так далее
			25.2	Несанкционированный доступ в целях фальсификации параметров зарядки, таких как зарядное напряжение, зарядная мощность, температура аккумулятора и так далее
4.3.7 Потенциальные уязвимости, которые могут быть использованы в случае их недостаточной защиты или исправления	26	Возможная компрометация или недостаточное использование криптографических технологий	26.1	Сочетание коротких ключей шифрования и длительного срока действия позволяет злоумышленнику взломать шифр
			26.2	Недостаточное использование криптографических алгоритмов для защиты критичных систем
			26.3	Использование выходящих из употребления или уже устаревших криптографических алгоритмов
	27	Скомпрометированные автозапчасти или расходные материалы делают возможными атаки на транспортные средства	27.1	Аппаратное или программное обеспечение, сконструированное так, что делает атаки возможными, или не отвечающее проектным критериям для отражения атак
	28	Уязвимости при разработке программного или аппаратного обеспечения	28.1	Программные ошибки. Это прежде всего актуально, если ПО не было протестировано, чтобы убедиться в отсутствии известного дефектного кода/ошибок и снизить риск наличия неизвестного дефектного кода/ошибок
			28.2	Использование элементов, оставшихся по итогам разработки ПО (например, портов отладки, портов JTAG, микропроцессоров, сертификатов разработки, паролей разработчиков и прочее), может обеспечить доступ к электронным блокам управления или позволить злоумышленникам получить привилегии более высокого уровня
	29	Уязвимости при проектировании сети	29.1	Лишние интернет-порты остаются открытыми, что обеспечивает доступ к сетевым системам
			29.2	Разделение сети при обходе средств защиты в целях получения контроля над ней. Например, использование незащищенных шлюзов или точек доступа (к примеру, шлюзов для грузовых автомобилей с прицепом) для обхода средств защиты и получения доступа к другим сегментам сети в целях выполнения злонамеренных действий, таких как отправка произвольных сообщений по шине CAN

Таблица I.1 – Список примеров уязвимостей или методов атак, связанных с угрозами

Уязвимости/угрозы – описание высокого и среднего уровней			**Пример уязвимостей или методов атак**	
	30	Возможная физическая потеря данных	30.1	Ущерб, нанесенный третьей стороной. Конфиденциальные данные могут быть потеряны или скомпрометированы из-за физических повреждений в случае дорожно-транспортного происшествия или по причине угона
			30.2	Потеря данных в результате конфликтов по вопросам управления цифровыми правами (DRM). Пользовательские данные могут быть удалены в связи с проблемами, касающимися DRM
			30.3	Конфиденциальные данные (их целостность) могут быть утрачены из-за износа ИТ-компонентов, что может вызвать проблемы каскадирования (например, в случае изменения ключа)
	31	Возможная непреднамеренная передача данных	31.1	Утечка информации. Возможна утечка личных или конфиденциальных данных при смене пользователя автомобиля (например, транспортное средство продано или арендуется новым лицом)
	32	Физическое манипулирование системами может привести к атаке	32.1	Манипулирование аппаратным обеспечением OEM, например внедрение неавторизованного ПО, что делает возможной атаку через посредника

Библиография

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*.

[b-ISO/IEC 27000] ISO/IEC 27000:(2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-UNECE GRVA] UNECE GRVA-01-17 (2017), *Draft Recommendation on cyber security of the Task Force on Cyber Security and Over-the-air* Issues *of UNECE WP.29 GRVA*. Доступно [по состоянию на 07.08.2020] по адресу: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf.

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 протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии,
Женева, 2020 г.