Международный союз электросвязи

МСЭ-Т X. 1372

(03/2020)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

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

Руководящие указания по безопасности систем связи транспортного средства с различными объектами (V2X)

Рекомендация МСЭ-Т X.1372

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.1379**
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.1372

Руководящие указания по безопасности систем связи транспортного средства с различными объектами (V2X)

Резюме

В Рекомендации МСЭ-Т X.1372 содержатся руководящие указания по безопасности систем связи транспортного средства с различными объектами (V2X). V2X – это общий термин для обозначения режимов связи транспортного средства с транспортным средством (V2V), транспортного средства с инфраструктурой (V2I), транспортного средства с перемещаемым устройством (V2D) и транспортного средства с пешеходом (V2P), обсуждаемых в настоящей Рекомендации.

За последние несколько лет произошли значительные изменения в области связи с подвижными объектами в среде интеллектуальной транспортной системы (ИТС). Связь V2X значительно повышает безопасность дорожного движения, уменьшает пробки на дорогах и повышает удобство. Однако связь V2X также делает соответствующие объекты в среде ИТС уязвимыми для разного рода кибератак.

Для решения этой проблемы безопасности в настоящей Рекомендации определены возможные угрозы в среде связи V2X и установлены требования безопасности к связи V2X для смягчения этих угроз. В настоящей Рекомендации также содержится описание возможной реализации связи V2X с обеспечением безопасности.

Хронологическая справка

Издание	Рекомендация	Утверждена	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1372	26.03.2020 года	17-я	11.1002/1000/14091

Ключевые слова

Анализ рисков, анализ угроз, безопасность ИТС, требования безопасности, V2I, V2V, V2D, V2P, V2X.

---

* Для доступа к Рекомендации наберите URL http://handle.itu.int/ в вашем веб-браузере, а затем 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 не 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

			Стр.
1	Сфера применения		1
2	Справочные документы		1
3	Определения		1
	3.1	Термины, определенные в других документах	1
	3.2	Термины, определенные в настоящей Рекомендации	2
4	Сокращения и акронимы		2
5	Соглашения		4
6	Связь V2X		4
	6.1	Обзор	4
	6.2	Связь V2V	5
	6.3	Связь V2I	7
	6.4	Связь V2D	8
7	Выявленные угрозы		10
	7.1	Угрозы для конфиденциальности	10
	7.2	Угрозы для целостности информации	11
	7.3	Угрозы для готовности	12
	7.4	Угрозы для предотвращения отказа от авторства	14
	7.5	Угрозы для подлинности информации	14
	7.6	Угрозы для подотчетности	15
	7.7	Угрозы для авторизации	16
8	Требования безопасности		17
	8.1	Конфиденциальность	17
	8.2	Целостность	17
	8.3	Готовность	17
	8.4	Предотвращение отказа от авторства	18
	8.5	Аутентичность	18
	8.6	Подотчетность	18
	8.7	Авторизация	18
	8.8	Применимость требований безопасности V2X	18
9	Реализация связи V2X с обеспечением безопасности		19
	9.1	Криптографическое обеспечение аутентификации объектов и конфиденциальности сообщений	19
	9.2	Конфиденциальность аварийно-предупредительных сообщений по безопасности дорожного движения	23
	9.3	Аутентификация объекта при формировании автоколонны	23
	9.4	PKI систем связи с подвижными объектами	26

Стр.

Дополнение I – Эталонные модели связи с подвижными объектами 27
I.1 Концепция МСЭ-Т в отношении услуг и приложений для транспортных средств, подключенных к сети, с использованием СПП 27
I.2 Архитектура и функциональные объекты платформ автомобильного шлюза МСЭ-Т 29
Дополнение II – Эталонные модели транспортной PKI 32
Библиография 35

Рекомендация МСЭ-Т X.1372

Руководящие указания по безопасности связи транспортного средства с различными объектами (V2X)

1 Сфера применения

В настоящей Рекомендации содержатся руководящие указания по безопасности связи транспортных средств с различными объектами (V2X). V2X – это общий термин для обозначения режимов связи транспортного средства с транспортным средством (V2V), транспортного средства с инфраструктурой (V2I), транспортного средства с перемещаемым устройством (V2D) и транспортного средства с пешеходом (V2P), обсуждаемых в настоящей Рекомендации. В настоящей Рекомендации перечислены угрозы в среде связи V2X, определены требования к безопасности и дано описание возможной реализации связи V2X при обеспечении безопасности.

Конкретные меры по обеспечению безопасности связи V2X выходят за рамки настоящей Рекомендации.

2 Справочные документы

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

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 Подотчетность (accountability) [b-ITU-T X.800] – свойство, гарантирующее возможность прослеживания действий какого-либо объекта с однозначной привязкой к этому объекту.

3.1.2 Аутентичность, подлинность (authenticity) [b-ITU-T X.641] – защита в виде взаимной аутентификации и аутентификации источника данных.

3.1.3 Аутентификация (authentication) [b-ITU-T X.1252] – процесс, используемый для достижения достаточной меры доверия к связи между объектом и представленной идентичностью.

ПРИМЕЧАНИЕ. – Использование термина "аутентификация" в контексте управления определением идентичности (IdM) означает аутентификацию объекта.

3.1.4 Авторизация (authorization) [b-ITU-T X.800] – предоставление прав, которое включает предоставление доступа на основании прав доступа.

3.1.5 Готовность (availability) [b-ITU-T X.800] – свойство быть доступным и годным к использованию по запросу имеющего полномочия объекта.

3.1.6 Орган по сертификации (certification authority (CA)) [b-ITU-T X.509] – орган, которому один или несколько пользователей доверили разработку и скрепление цифровой подписью сертификатов открытых ключей. Возможен вариант, при котором орган по сертификации разрабатывает ключи для пользователей.

3.1.7 Конфиденциальность (confidentiality) [b-ITU-T X.800] – свойство, защищающее информацию от доступа к ней или ее раскрытия неуполномоченными лицами, устройствами или процессами.

3.1.8 Целостность (integrity) [b-ITU-T X.800] – показатель того, что данные не были изменены или разрушены несанкционированным способом.

3.1.9 Код аутентификации сообщения (message authentication code (MAC)) [b-ITU-T X.813] – криптографическое контрольное значение, используемое для аутентификации источника и целостности данных.

3.1.10 Перемещаемые устройства (nomadic devices) [b-ITU-T F.749.1] – к перемещаемым устройствам относятся информационно-коммуникационные устройства всех типов, а также развлекательные устройства, которые могут быть внесены в транспортное средство водителем и/или пассажирами для использования во время движения. Примерами могут служить мобильные телефоны, портативные компьютеры, планшеты, мобильные навигационные устройства, портативные медиаплееры и многофункциональные смартфоны.

3.1.11 Предотвращение отказа от авторства с подтверждением источника (non-repudiation with proof of origin) [b-ITU-T X.800] – получателю данных предоставляется подтверждение источника данных. Это защищает от любых попыток отправителя ложно отрицать отправление данных или их содержимое.

3.1.12 Псевдоним (pseudonym) [b-ITU-T X.1252] – идентификатор, связь которого с объектом неизвестна или известна лишь в ограниченной степени, в контексте, в котором он используется.

ПРИМЕЧАНИЕ. – Псевдоним может использоваться для предотвращения или снижения рисков, связанных с использованием связей идентификатора, которые могут раскрыть идентичность объекта.

3.1.13 Сертификат открытого ключа (public-key certificate (PKC)) [b-ITU-T X.509] – открытый ключ объекта вместе с некоторой дополнительной информацией, воспроизводимой без возможности фальсификации при помощи цифровой подписи с частным ключом выдавшего его органа по сертификации (CA).

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин.

3.2.1 Ненадлежащее поведение (misbehaviour) – поведение, приводящее к тому, что устройства отправляют неверную информацию, что может вызвать неправильные действия других устройств; либо устройства выполняют неправильные действия, несмотря на получение правильной информации.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AES	Advanced Encryption Standard	Усовершенствованный стандарт шифрования
AVN	Audio, Video, and Navigation	Аудио, видео и навигация
CA	Certification Authority	Орган по сертификации
CAMP	Crash Avoidance Metrics Partnership	Партнерство по измерениям для предотвращения столкновений
CCM	Counter mode with cipher block chaining message authentication code	Протокол блочного шифрования с имитовставкой и режимом сцепления блоков и счетчика
CCU	Central Communication Unit	Центральный узел связи
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
EEBL	Electronic Emergency Brake Light	Электронный аварийный стоп-сигнал
ECDSA	Elliptic Curve Digital Signature Algorithm	Алгоритм цифровой подписи на основе эллиптических кривых

ECIES	Elliptic Curve Integrated Encryption Scheme		Объединенный алгоритм шифрования на основе эллиптических кривых
ECU	Electronic Control Unit	ЭБУ	Электронный блок управления
GPS	Global Positioning System		Спутниковая система навигации
HDMI	High-Definition Multimedia Interface		Мультимедийный интерфейс высокой четкости
ID	Identifier		Идентификатор
ITS	Intelligent Transportation System	ИТС	Интеллектуальная транспортная система
IVN	In-Vehicle Network		Автомобильная сеть
KDF	Key Derivation Function		Функция выработки ключей
LDM	Local Dynamic Map		Локальная динамическая карта
LOS	Line Of Sight		В зоне прямой видимости
LTE	Long Term Evolution		Долгосрочное развитие
MAC	Message Authentication Code		Код аутентификации сообщения, имитовставка
MHL	Mobile High-definition Link		Подвижная связь высокой четкости
NFC	Near Field Communication		Связь ближнего действия
NGN	Next Generation Networks	СПП	Сети последующих поколений
NLOS	Non-Line Of Sight		Вне зоны прямой видимости
OBD	On Board Diagnostics		Бортовая система диагностики
OBU	On-Board Unit		Бортовой блок
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PKI	Public-Key Infrastructure		Инфраструктура открытых ключей
QoS	Quality of Service		Качество обслуживания
RSU	Road-Side Unit		Придорожный блок
SCMS	Security Credential Management System		Система управления удостоверениями безопасности
SHA	Secure Hash Algorithm		Защищенный алгоритм хеширования
USB	Universal Serial Bus		Универсальная последовательная шина
V2I	Vehicle-to-Infrastructure		[Связь] транспортного средства с инфраструктурой
V2D	Vehicle-to-nomadic Device		[Связь] транспортного средства с перемещаемым устройством
V2P	Vehicle-to-Pedestrian		[Связь] транспортного средства с пешеходом
V2V	Vehicle-to-Vehicle		[Связь] транспортного средства с транспортным средством
V2X	Vehicle-to-everything		[Связь] транспортного средства с различными объектами
VGP	Vehicle Gateway Platform		Платформа автомобильного шлюза
VRU	Vulnerable Road User		Уязвимый участник дорожного движения
WAVE	Wireless Access in Vehicular Environments		Беспроводной доступ в условиях автотранспортных перевозок
Wi-Fi	Wireless Fidelity		Высокая точность беспроводной передачи

5 Соглашения

Отсутствуют

6 Связь V2X

6.1 Обзор

К интеллектуальным транспортным системам (ИТС) относится широкий спектр информационно-коммуникационных технологий, предназначенных для повышения безопасности и эффективности транспортной системы. За последние несколько лет произошли значительные изменения, особенно в отношении автомобильных систем связи.

Автомобильные системы связи поддерживают обмен данными между транспортными средствами, между транспортными средствами и инфраструктурой, а также между транспортными средствами и перемещаемыми устройствами. Данные могут относиться к текущему положению, скорости транспортного средства и предупредительным сигналам бортовых датчиков и т. п. Кроме того, с помощью придорожных блоков (RSU) могут обеспечиваться связи с системами регулирования дорожного движения, которые собирают и распространяют среди окружающих транспортных средств предупредительные сигналы об опасных ситуациях. Однако без обеспечения мер безопасности ИТС может стать угрозой для безопасности движения и жизни людей. Поэтому для безопасного и успешного развертывания этой системы она исследуется на безопасность.

На рисунке 1 приведен обзор автомобильной связи. Автомобильную связь можно подразделить на связь внешнюю и внутреннюю по отношению к транспортному средству. Внутренняя сеть транспортного средства, или бортовая сеть (IVN), включает в себя такие компоненты, как датчики и электронные блоки управления (ЭБУ). Внешнюю связь можно, в свою очередь, подразделить на связь V2V, V2I, V2D и V2P. Бортовые устройства (OBU) – это устройства беспроводной связи, установленные на транспортных средствах, а RSU – устройства беспроводного доступа, расположенные вдоль дороги. Инфраструктура состоит из RSU и внутренних объектов, таких как системы регулирования дорожного движения, системы контроля и орган сертификации (CA). RSU могут быть подключены к внутренним объектам по кабельным или беспроводным сетям.

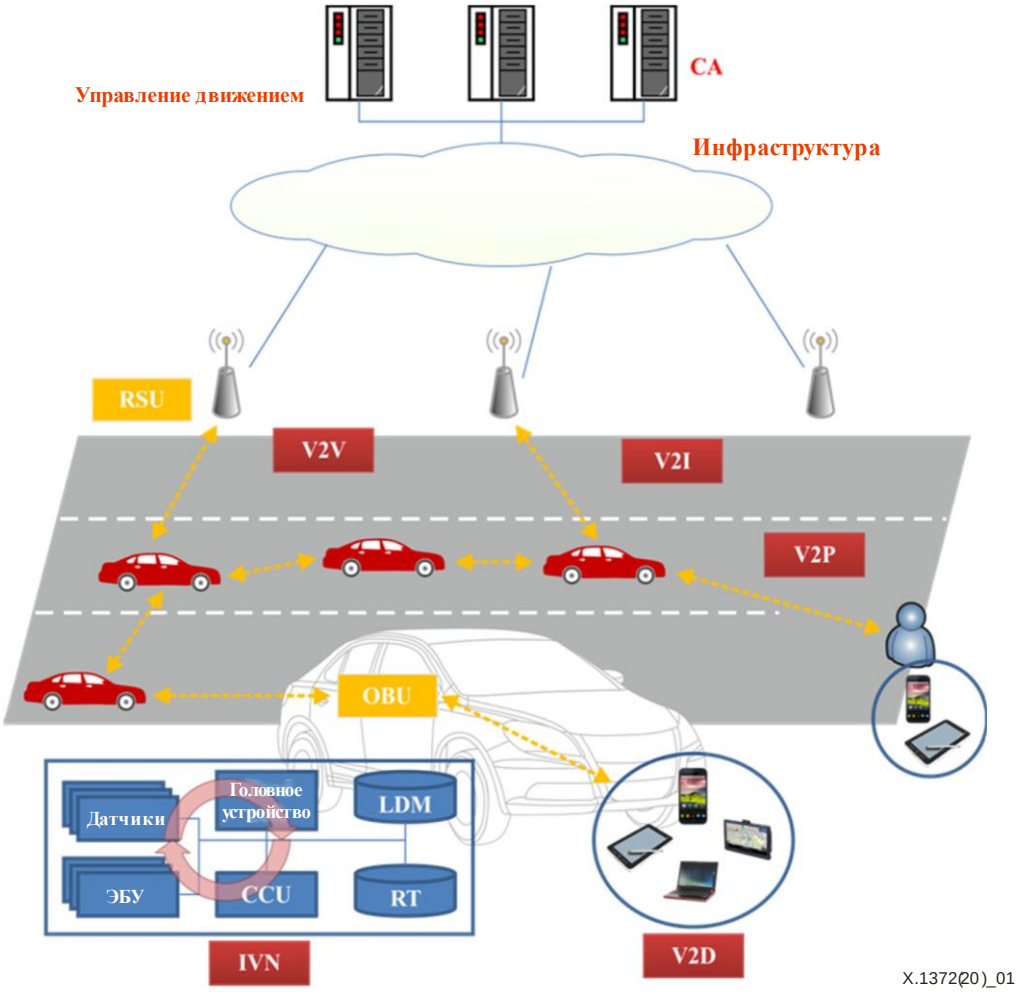


Рисунок 1 – Обзор автомобильной связи

6.2 Связь V2V

К связи V2V относится беспроводная передача данных между транспортными средствами. Целью связи V2V является предотвращение аварий путем обмена информацией и ее распространения между транспортными средствами. В зависимости от того, как реализована технология V2V, транспортное средство может получить предупреждение о возможном риске аварии. В этом случае транспортное средство может принять упреждающие меры, такие как торможение. Групповая связь V2V, обеспечивая обмен информацией о скорости и дорожных условиях, делает возможным движение в колонне. Кроме того, обмен информацией между транспортными средствами с помощью сигнализации способствует легкому и безопасному вождению. Автомобиль с поддержкой связи V2V может собирать информацию, которая обеспечивает полную осведомленность об окружающей обстановке.

Можно выделить следующие сценарии связи V2V.

– Распространение предупреждений по каналам связи V2V

  В сценарии распространения предупреждений по каналам связи V2V предупредительное сообщение передается от одного транспортного средства другому. Например, в случае дорожно-транспортного происшествия предупреждение о том, что впереди произошло столкновение, передается в обратном направлении всем транспортным средствам, приближающимся к месту аварии. С другой стороны, если сзади приближается автомобиль экстренной службы, например полицейский автомобиль, предупредительное сообщение передается всем транспортным средствам, находящимся рядом и впереди, с тем чтобы такой автомобиль мог безопасно двигаться с высокой скоростью. На рисунке 2 показана ситуация, когда предупреждение о произошедшей впереди аварии распространяется против направления движения, а на рисунке 3 – ситуация, когда автомобиль экстренной службы приближается сзади, а предупредительное сообщение распространяется вперед по направлению движения.

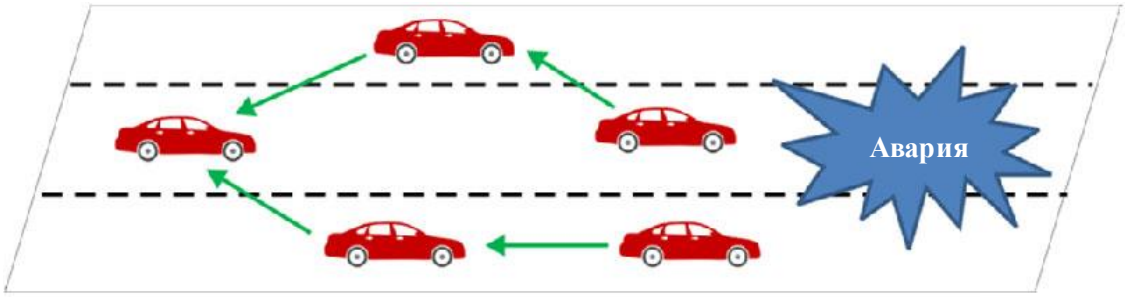


Рисунок 2 – Распространение предупреждения по каналам связи V2V против направления движения

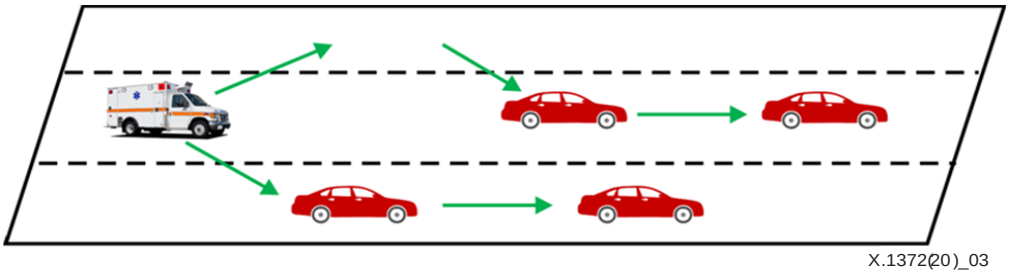


Рисунок 3 – Распространение предупреждения по каналам связи V2V вперед по направлению движения

– Групповая связь V2V

В сценарии групповой связи V2V несколько транспортных средств составляют группу и в ее рамках могут поддерживать связь друг с другом. Например, транспортные средства, движущиеся по одному и тому же маршруту или по крайней мере следующие одним и тем же маршрутом в течение некоторого времени, могут образовывать колонну. В этой колонне может передаваться информация о состоянии автомобилей, что способствует безопасному вождению. Групповая связь V2V иллюстрируется на рисунке 4.

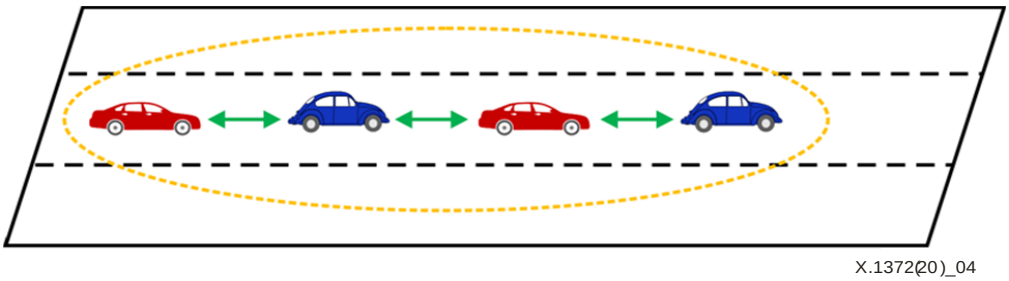


Рисунок 4 – Групповая связь V2V

– Сигнализация по каналам связи V2V

В сценарии сигнализации по каналам связи V2V каждое транспортное средство периодически передает ближайшим транспортным средствам сведения о своем состоянии, такие как текущая скорость, курс и положение. Пример сигнализации по каналам связи V2V показан на рисунке 5.

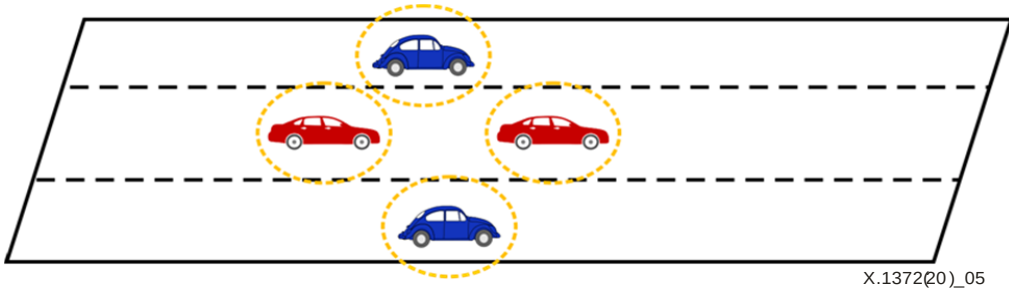


Рисунок 5 – Сигнализация по каналам связи V2V

6.3 Связь V2I

Связь транспортного средства с инфраструктурой (V2I) – это беспроводная передача данных между транспортным средством и объектами инфраструктуры, такими как придорожные блоки (RSU).

Можно выделить следующие сценарии связи V2I.

– Предупреждение по каналам связи V2I

Сценарий предупреждения по каналам связи V2I обеспечивает связь между транспортным средством и объектами инфраструктуры, такими как RSU. Например, если на перекрестке происходит авария, RSU передает предупредительное сообщение приближающимся транспортным средствам. Предупреждения по каналам связи V2I можно использовать и для оповещения о близости транспортного средства при согласовании въезда на полосу при правом или левом повороте и о точках пересечения траекторий движения. Пример сценария предупреждения по каналам связи V2I показан на рисунке 6.

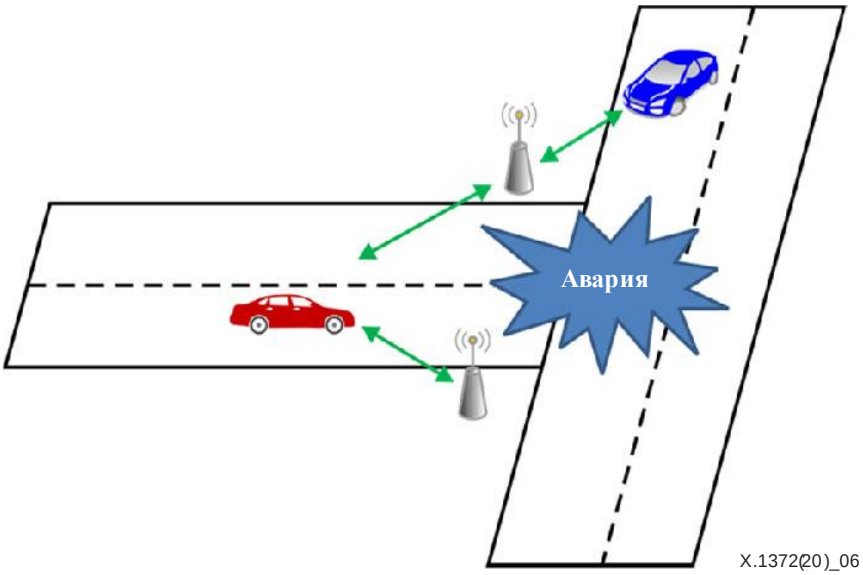


Рисунок 6 – Предупреждение по каналам связи V2I

– Обмен информацией по каналам связи V2I (включая V2V)

Обмен информацией по каналам связи V2I может включать такие сведения, как сигналы/информация внутри транспортного средства, сведения о фазе и длительности сигнала светофора, информация от датчиков транспортного средства, платежная информация (например, о плате за проезд), информация о состоянии дорожного покрытия/погодных условиях/зоне видимости и дорожных работах. Примеры использования.

- Загрузка основных транспортных данных

  В ИТС ряд сообщений по каналам связи V2I может содержать предупреждения. Для работы с такими сообщениями транспортному средству часто требуется карта его местоположения или пункта назначения и может потребоваться информация реального

времени о ситуации вокруг транспортного средства. Такая информация часто загружается из объектов инфраструктуры, таких как RSU.

- Данные, поддерживающие эффективность работы транспорта

  В ИТС транспортное средство может время от времени обращаться к инфраструктуре за информацией, относящейся к дорожному движению, такой как информация об управлении дорожным движением на данный момент и т. п. В результате транспортному средству будет известно, где образуются пробки. Тогда оно может оптимизировать свой маршрут с помощью инфраструктуры, например обновляя его через навигатор, подключенный к сети подвижной связи. Таким образом с помощью связи V2I можно повысить эффективность транспортных средств. В другом примере инфраструктура может обновлять информацию о состоянии дорожного движения на основе сообщений, поступающих от транспортных средств посредством связи V2I. Пример обмена информацией по каналам связи V2I показан на рисунке 7.

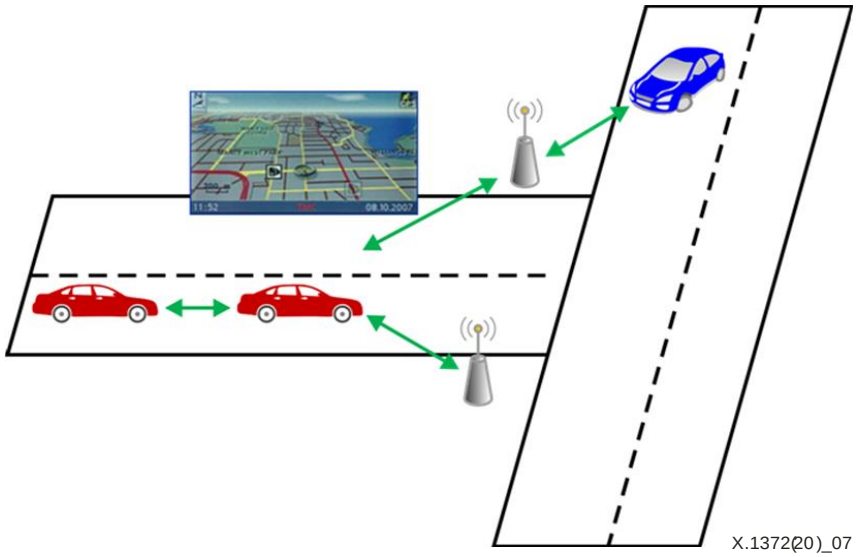


Рисунок 7 – Пример обмена информацией по каналам связи V2I

6.4 Связь V2D

Благодаря технологии V2D обеспечивается подключение транспортного средства к находящимся в нем мобильным устройствам, таким как смартфоны, ноутбуки и автомобильные навигационные системы, осуществляемое либо через открытую архитектуру со стандартизованным интерфейсом к шине локальной сети контроллеров (CAN) транспортного средства, либо через шлюз, который передает запросы и ответы перемещаемых устройств в систему на транспортном средстве. С помощью смартфона или мобильного устройства может предоставляться удаленный доступ к функциям для определения информации о состоянии транспортного средства, такой как наличие деталей для технического обслуживания, и управления ею. Кроме того, ожидается дальнейшее развитие соответствующих услуг.

Например, при планировании поездки водитель выбирает на перемещаемом устройстве пункт назначения, а затем устройство может спланировать маршрут, собирая информацию из разных источников, таких как расписание движения общественного транспорта (поездов, метро, автобусов и т. д.), и информацию реального времени о состоянии дорожного движении. Транспортное средство следует по запланированному маршруту, двигаясь в объезд, если происходят кратковременные изменения дорожной ситуации. Перемещаемое устройство не только принимает решения о маневрах и выполняет их, но и реагирует на местные дорожные ситуации, например решая следовать за другими транспортными средствами, обогнуть препятствие, изменить полосу движения, остановиться на светофоре и т. п. Такое перемещаемое устройство может быть подключено к сетям транспортного средства. Таким образом злоумышленники могут получить доступ к внутренним системам автомобиля. В случае поступления угрозы для безопасности через Bluetooth вредоносный код может быть выполнен

приложением на смартфоне, подключенном к автомобилю. Автомобильные аудио-, видео- и навигационные (AVN) системы уязвимы для атак на встроенное ПО через хранилища мультимедийных данных и могут легко подвергаться взлому через глобальную систему позиционирования (GPS) или спутниковые радиоканалы. Для обеспечения безопасности автомобиля необходимо контролировать атаки через перемещаемые устройства.

Ниже обсуждаются следующие два типа связи V2D.

– Связь V2D по непрямым каналам

  Связь между транспортными средствами и перемещаемыми устройствами может осуществляться через непрямые каналы. Связь по непрямым каналам предполагает наличие стороннего оборудования, такого как узлы доступа и маршрутизаторы, обеспечивающие связь между конечными узлами. В сотовых телефонах и смартфонах используются технологии беспроводного широкополосного доступа, такие как долгосрочное развитие (LTE), высокая точность беспроводной передачи (Wi-Fi) и т. д. Для связи смартфонов с транспортными средствами все чаще используется Wi-Fi. Технология 5G также становится важным носителем таких непрямых каналов связи.

– Связь V2D по прямым каналам

  Связь между транспортными средствами и перемещаемыми устройствами может осуществляться по прямым каналам без какого-либо посредничества или с помощью технологий беспроводной связи, таких как Bluetooth, ZigBee и связь ближнего действия (NFC).

  Транспортные средства и перемещаемые устройства могут поддерживать связь по проводным каналам. Например, перемещаемое устройство может подключиться к транспортному средству по физическому интерфейсу, такому как универсальная последовательная шина (USB), подвижная связь высокой четкости (MHL) или мультимедийный интерфейс высокой четкости (HDMI). Стандарт бортовой системы диагностики II (OBD-II) определяет диагностические интерфейсы, а также предлагает список возможных параметров транспортного средства и процедур передачи данных.

  В частности, связь V2P может рассматриваться как особый случай связи V2D, когда транспортное средство связывается с перемещаемым устройством, находящимся у пешехода.

  Подход V2P применяется для широкого круга уязвимых участников дорожного движения (VRU), включая немоторизованных участников дорожного движения, таких как пешеходы и велосипедисты, а также для мотоциклистов и лиц с ограниченными возможностями или с ограниченной подвижностью.

  Ввиду большого числа дорожно-транспортных происшествий с участием VRU ИТС предлагает решения для повышения безопасности дорожного движения посредством сбора данных от датчиков и таких принципов, как ввод и обеспечение обмена информацией между транспортными средствами и пешеходами. Еще важнее то, что связь V2P может не только предупредить водителя о приближающемся пешеходе, чтобы он успел остановить транспортное средство, но и подать сигнал на мобильный телефон пешехода, чтобы уведомить его о приближающемся транспортном средстве.

  ИТС способна обнаружить VRU и помочь предотвратить столкновение между транспортными средствами и VRU. На рисунке 8 показан пешеход в зоне прямой видимости водителя (LOS), а на рисунке 9 – вне зоны прямой видимости водителя (NLOS). На этих рисунках видно, как ИТС может повысить безопасность VRU на дороге.

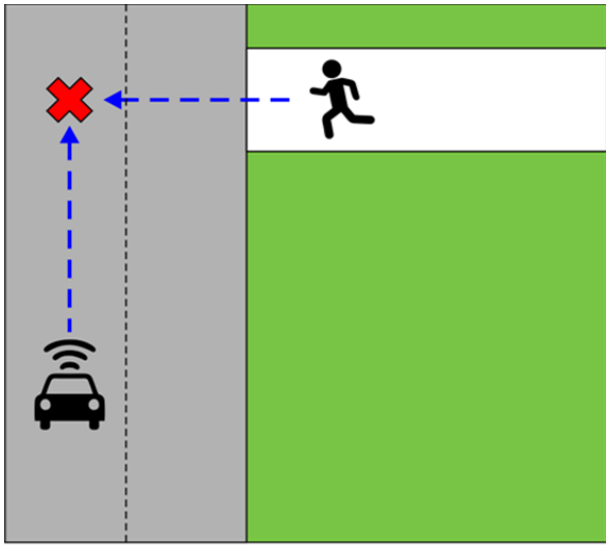


Рисунок 8 – LOS

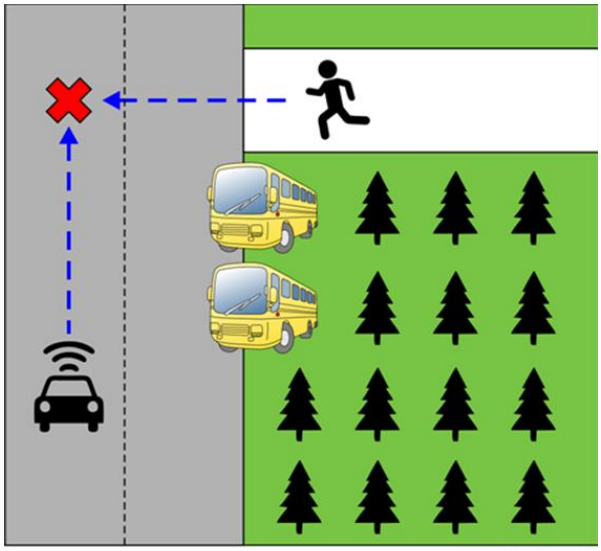


Рисунок 9 – NLOS

- Пешеход в зоне LOS

  Как показано на рисунке 8, активные датчики, такие как радиолокаторы, ультразвуковые датчики, лазерные дальномеры и видеокамеры, действующие на основе машинного зрения, обнаруживают пешеходов, когда они видны из транспортного средства. При приближении пешехода водитель движущегося транспортного средства заметит его и сможет принять критически важное решение. В то же время автомобиль может подать сигнал на сотовый телефон пешехода, чтобы предупредить его о потенциальной опасности.

- Пешеход в зоне NLOS

  Возможность обнаружить пешехода ограничена полем зрения датчиков. На рисунке 9 пешехода загораживают посторонние предметы, такие как деревья и припаркованные автобусы. Однако система связи транспортных средств может получать и распространять информацию и за пределами поля зрения датчиков. Получив предупреждение, система транспортного средства обновит свою локальную динамическую карту (LDM) и оценит критичность ситуации для принятия решения. В то же время на мобильный телефон пешехода поступит предупреждение.

7 Выявленные угрозы

7.1 Угрозы для конфиденциальности

Угрозы для конфиденциальности, описанные в этом пункте, иллюстрируются на рисунке 10.

– Перехват информации

  Злоумышленник может перехватывать (то есть прочесть и/или записать) сообщения по каналам связи V2V от находящихся поблизости транспортных средств и сообщения по каналам связи V2I от RSU, а затем, используя перехваченные сообщения, проанализировать информацию о дорожном движении.

  Злоумышленник может перехватывать сообщения по каналам связи V2D, которыми обмениваются центральный узел связи и перемещаемое устройство. Затем он может проанализировать динамическую информацию о транспортном средстве, включая сведения о текущем местоположении и скорости.

  Злоумышленник может перехватывать сообщения V2P и вводить пешеходов в заблуждение по поводу дорожной ситуации, подвергая их опасности.

– Утечка информации, позволяющей установить личность

Злоумышленник может проанализировать информацию в целях обнаружения владельца транспортного средства, собирая рассылаемые им сообщения по каналам связи V2X и отслеживая местоположение конкретного человека на маршруте его следования.

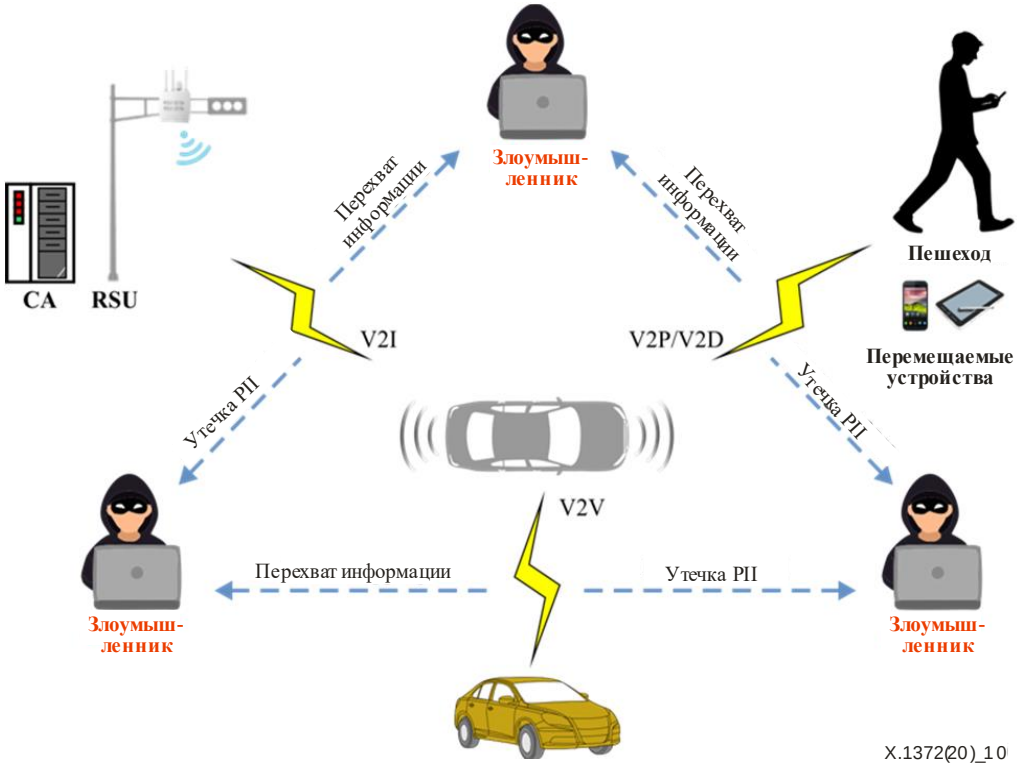


Рисунок 10 – Угрозы для конфиденциальности

7.2 Угрозы для целостности информации

Угрозы для целостности информации, описанные в этом пункте, иллюстрируются на рисунке 11.

– Манипулирование сообщениями о маршруте

Вредоносный промежуточный узел изменяет сообщение о маршруте, и транспортные средства получают ложную информацию.

– Манипулирование удостоверяющей информацией

Манипулирование удостоверяющей информацией предполагает изменение частного ключа или идентификатора транспортного средства, так что злоумышленник может несанкционированно пользоваться удостоверяющей информацией другого транспортного средства.

– Манипулирование информацией датчиков

Злоумышленник может изменить физический адрес модуля связи или манипулировать информацией ЭБУ, например датчика скорости. Кроме того, в автомобиле имеется множество других датчиков оборудования для содействия водителю, таких как радиолокатор и видеокамера. Ложные показания датчиков, включая сведения о широте, долготе, высоте над уровнем моря, скорости, курсе, угле поворота рулевого колеса и ускорение, могут передаваться в другие OBU или RSU. Эти данные, полученные от манипулируемого датчика, могут привести к нарушению дорожного движения. Например, неверное значение ускорения может привести к тому, что соседние транспортные средства включат свои электронные аварийные стоп-сигналы (EEBL), чтобы уменьшить вероятность множественных столкновений транспортных средств, даже при нормальном режиме дорожного движения.

– Манипулирование приложением на перемещаемом устройстве

Манипуляции с приложениями могут оказывать вредное воздействие на транспортное средство через интерфейс связи V2D. Например, манипулируемое приложение может заставить перемещаемое устройство передавать транспортному средству большое количество безобидных сообщений; эта практика называется лавинной рассылкой сообщений. Кроме того, манипулируемое приложение может внедрить в OBU вредоносный код и отправить сообщение, для обработки которого требуется большое количество вычислительных ресурсов. Манипулируемое приложение также может отправлять большее количество сообщений гораздо большего размера, чем объем памяти, доступный на OBU.

– Атака повторного воспроизведения

Злоумышленник может перехватывать сообщения V2V от находящихся поблизости транспортных средств и сообщения V2I от RSU. Позже этот злоумышленник может повторно воспроизвести эти сообщения или информацию для своих злонамеренных целей.

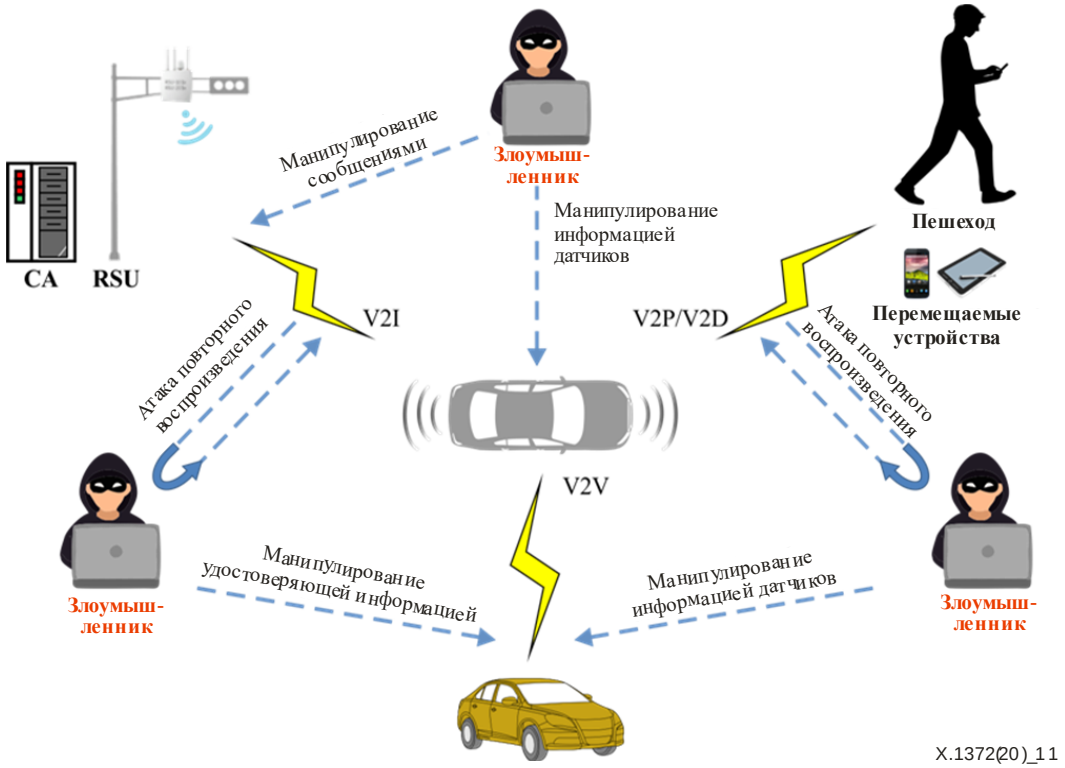


Рисунок 11 – Угрозы для целостности информации

7.3 Угрозы для готовности

Угрозы для готовности, описанные в этом пункте, иллюстрируются на рисунке 12.

– Перегрузка канала и распределенные атаки типа отказ в обслуживании (DDoS) на канал связи V2X

Злоумышленник может отправлять множество бесполезных сообщений; этот метод называется лавинной адресацией. К атакам этого типа можно отнести пересылку узлом маршрутизации лишь определенных сообщений.

– DDoS атака на OBU

Злоумышленник может внедрить в OBU вредоносный код и рассылать сообщения, для обработки которых требуется большое количество вычислительных ресурсов. Этот злоумышленник также может рассылать множество сообщений, совокупный размер которых превышает емкость хранилища OBU. В частности, примером серьезной атаки этого типа могут служить частые несанкционированные обновления программного обеспечения.

– Атака по времени

Атака по времени – это, например, задержка доставки сообщения, относящегося к безопасности, другим транспортным средствам. Таким способом можно помешать предоставлению соответствующих услуг связи V2X, таких как широковещательная рассылка предупредительных сообщений.

– Взлом датчиков

Датчики могут подвергаться атаке и выдать ошибку в результате сбоя. Как правило, неисправности датчиков бывают двух типов – кратковременные сбои и повторяющиеся отказы. Сбой может произойти во время нормальной работы системы, которая после этого быстро восстанавливается. Фактически в большинстве случае неисправность датчиков происходит по модели сбоев, что ограничивает время получения ошибочных результатов измерений. Например, GPS нередко временно теряет связь со спутниками (или получает сигналы помех), особенно в городах с многоэтажными зданиями. Аналогичным образом датчик, передающий данные по перегруженной сети (например, по протоколу TCP/IP с повторными передачами), может доставлять свои показания с запозданием, что приводит к получению сообщений с недостоверной информацией. Однако из-за короткой продолжительности сбоев их не следует рассматривать в качестве угрозы для безопасности системы.

Напротив, повторяющиеся отказы – это неисправности датчиков, которые сохраняются в течение длительного периода времени и могут серьезно повлиять на работу системы. Например, датчик может получить физическое повреждение, вносящее постоянное отклонение в его показания. В таком случае, если отказ не удается устранить программными средствами, системе лучше полностью игнорировать показания этого датчика.

В зависимости от цели злоумышленника атаки на измерения датчиков могут приводить к кратковременным сбоям или повторяющимся отказам. В каждом виде неисправности с точки зрения злоумышленника есть свои преимущества и недостатки. Оказав на датчик воздействие так, чтобы он давал сбои, злоумышленник может помешать своему обнаружению, но будет также ограничен в своих возможностях, тогда как отказ может привести к более серьезным последствиям, но будет быстро обнаружен.

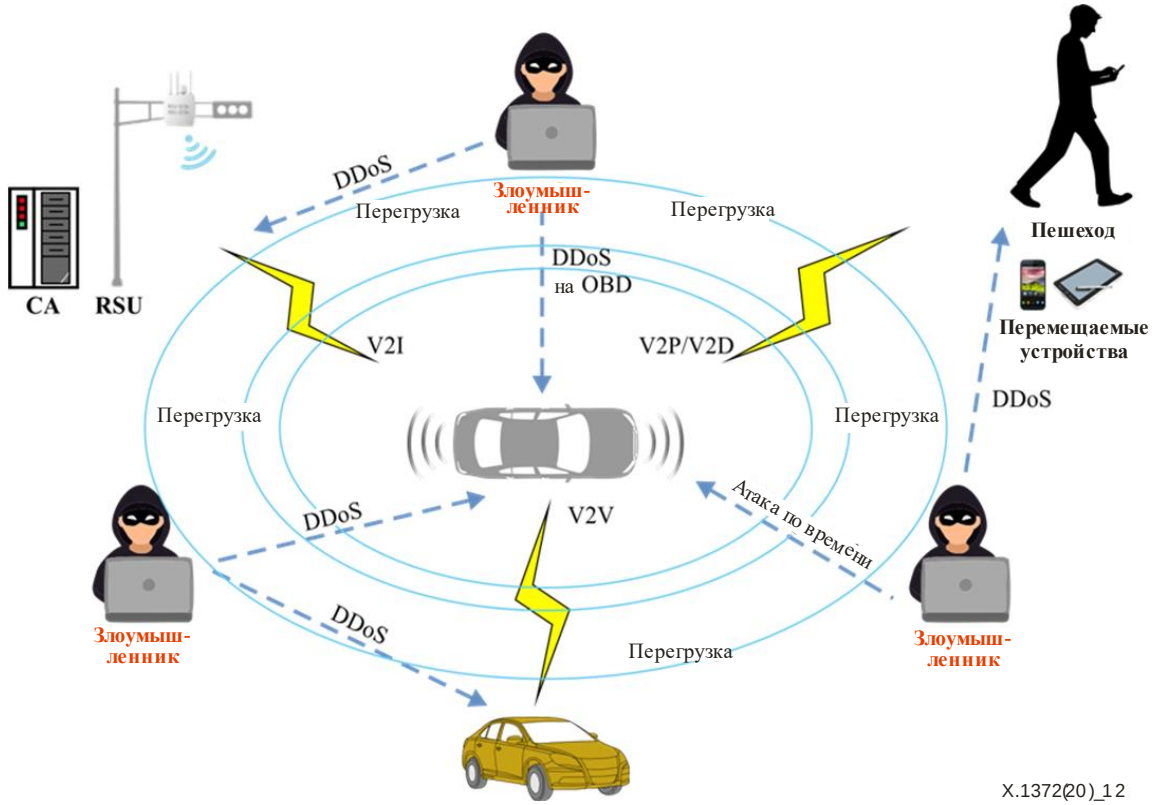


Рисунок 12 – Угрозы для готовности

7.4 Угрозы для предотвращения отказа от авторства

Угрозы для предотвращения отказа от авторства, описанные в этом пункте, иллюстрируются на рисунке 13.

– Манипулирование базой данных сертификатов

  Злоумышленник может манипулировать базой данных псевдонимов в CA. Впоследствии злоумышленник может изменить связь между долгосрочным сертификатом и краткосрочным сертификатом псевдонима.

– Несанкционированный доступ к учетным данным

  Злоумышленник может получить несанкционированный доступ к частному ключу и сертификату. В случае взлома частного ключа предотвращение отказа от авторства для транспортного средства, RSU и перемещаемого устройства не может быть гарантировано.

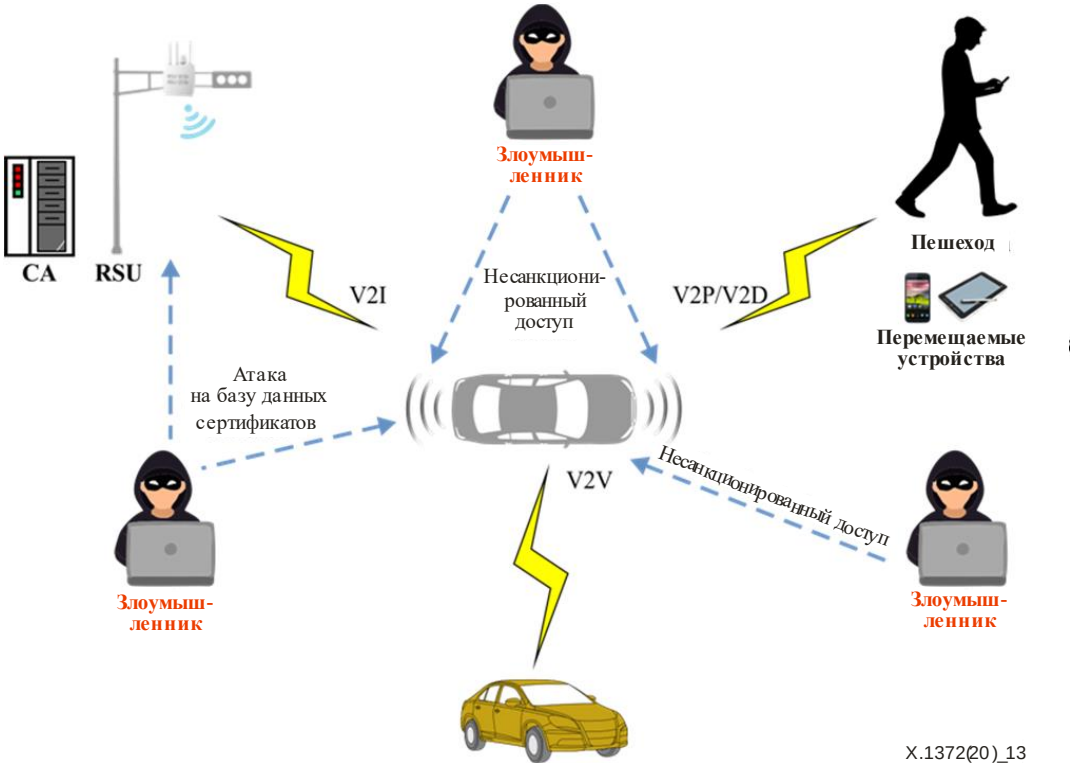


Рисунок 13 – Угрозы для предотвращения отказа от авторства

7.5 Угрозы для подлинности информации

Угрозы для подлинности информации, описанные в этом пункте, иллюстрируются на рисунке 14.

– Атака с изменением таблицы маршрутизации и LDM

  Злоумышленник может подделать информацию GPS транспортного средства и изменить его исходную геопространственную информацию.

– Атака путем подмены участника

  Осуществив кражу идентификационной информации другого объекта, злоумышленник может выдать себя за него. В таком случае злоумышленник может получать сообщения, предназначенные другому объекту, а также отправлять сообщения от чужого имени. Например, если другой объект – это автомобиль экстренных служб, то злоумышленник может отправлять окружающим транспортным средствам сообщения от имени спецавтомобиля с требованием освободить ему путь.

  Злоумышленник также может передать ложный сигнал о неисправности от имени исправного транспортного средства; тогда CA может отозвать сертификат у исправного транспортного средства.

– Атака сивиллы

Атака сивиллы может произойти, когда одно транспортное средство имитирует несколько транспортных средств, используя несколько идентификаторов транспортных средств.

– Атака с использованием анализа псевдонимов

Злоумышленник может проанализировать взаимосвязь между идентификаторами транспортных средств и псевдонимами с целью выявить разные псевдонимы, используемые одним и тем же транспортным средством.

– Манипулирование базой данных сертификатов

Злоумышленник может манипулировать базой данных псевдонимов в CA. В этом случае он может изменить связь между долгосрочным сертификатом и кратковременным сертификатом псевдонима.

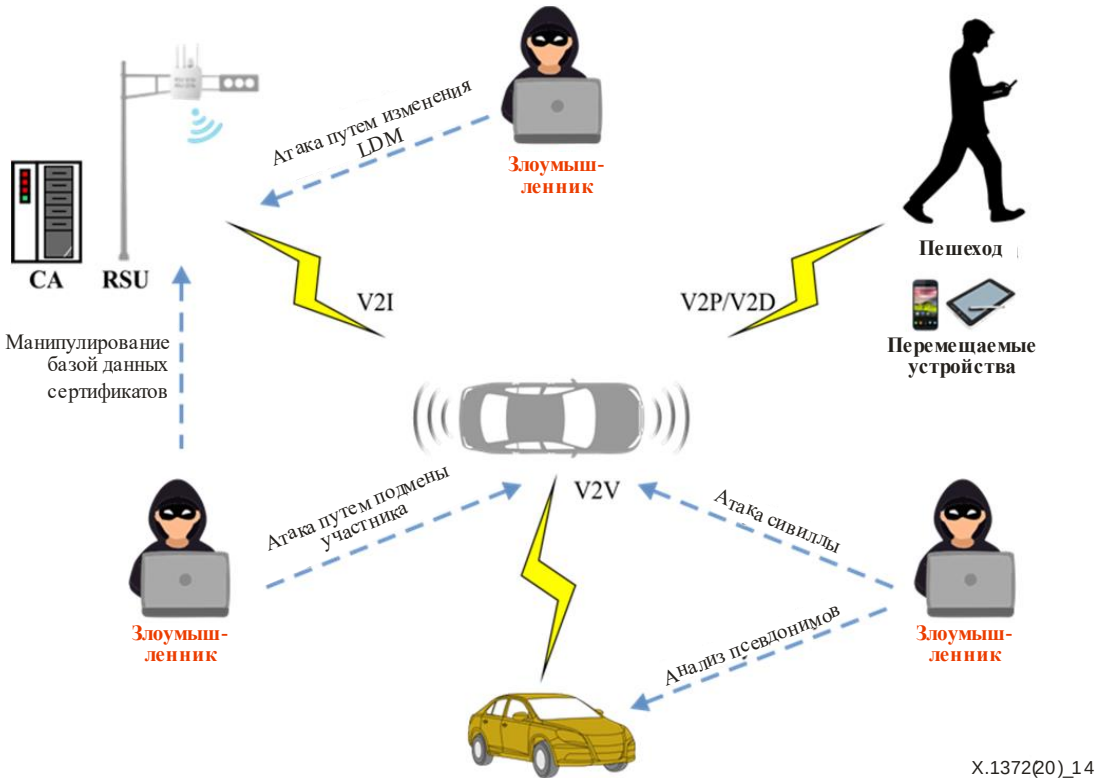


Рисунок 14 – Угрозы для подлинности информации

7.6 Угрозы для подотчетности

Угрозы для подотчетности, описанные в этом пункте, иллюстрируются на рисунке 15.

– Несанкционированное дублирование перемещаемого устройства

Для предоставления некоторых конкретных услуг, таких как диагностика транспортного средства, авторизованное перемещаемое устройство может получать доступ к центральному узлу связи транспортного средства. Однако если его учетные данные скопированы вредоносными устройствами, что может произойти, например когда вредоносное устройство использует учетную запись авторизованного устройства, то и оно может получить доступ к узлу связи. В таком случае неавторизованное перемещаемое устройство может манипулировать этим центральным узлом связи транспортного средства.

– Несанкционированное дублирование транспортного средства и RSU

В случае получения (дублирования) злоумышленником идентификаторов транспортного средства и RSU оригинальное транспортное средство и RSU теряют свою подотчетность.

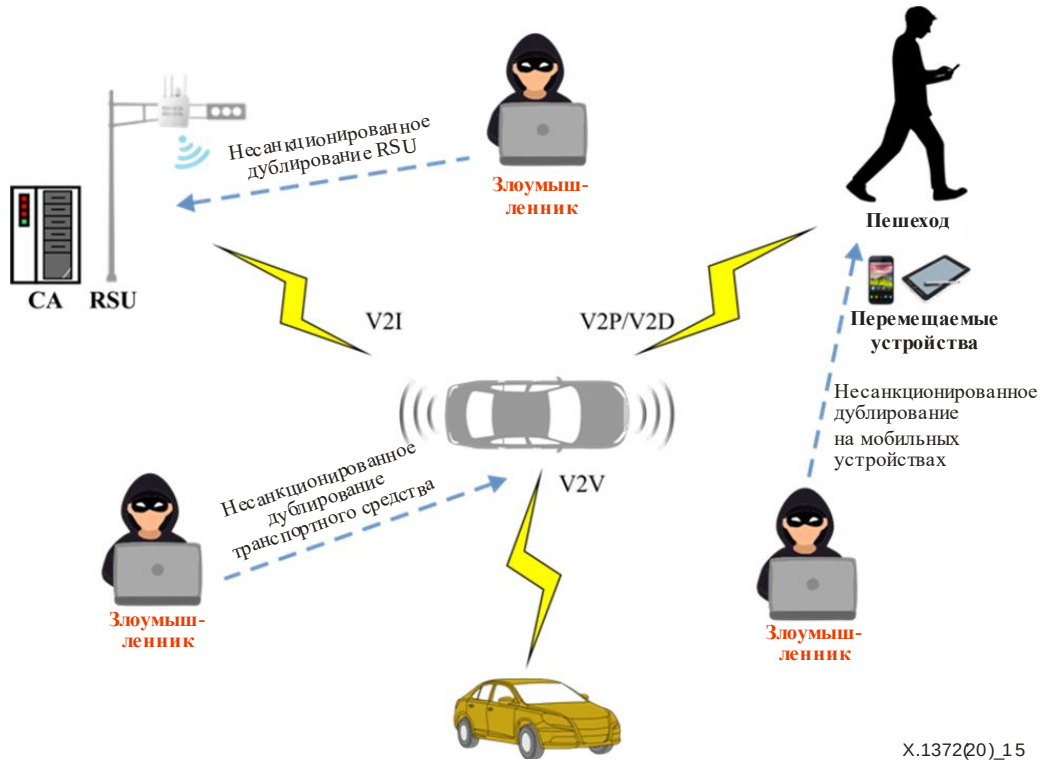


Рисунок 15 – Угрозы для подотчетности

7.7 Угрозы для авторизации

Угрозы для авторизации, описанные в этом пункте, иллюстрируются на рисунке 16.

– Несанкционированный доступ к конфиденциальной информации в транспортном средстве

При отсутствии контроля авторизации злоумышленник или вредоносное приложение могут управлять транспортным средством без авторизации. Например, приложению, которое воспроизводит музыку через динамик в транспортном средстве, не должен предоставляться доступ к важной для безопасности информации, такой как скорость транспортного средства и текущее состояние тормозов.

Злоумышленник также может изменять, стирать и переписывать важные для безопасности данные транспортного средства, включая параметры, касающиеся порога торможения, подушки безопасности и системного журнала.

В электромобилях злоумышленник может манипулировать параметрами конфигурации функций зарядки аккумуляторов.

– Несанкционированный доступ к определенным функциям в автомобиле с использованием перемещаемых устройств

Важнейшее значение имеет обеспечение функций контроля доступа для перемещаемых устройств, которые подключаются к транспортному средству. Обычно перемещаемые устройства используются в автомобиле в качестве аудио-, видео- и навигационного инструментария. Содержимое подвижных устройств также может отображаться на головном мультимедийном устройстве. Несанкционированные функции, такие как связь с центральным шлюзом транспортного средства с использованием этого перемещаемого устройства, могут иметь серьезные последствия для безопасности.

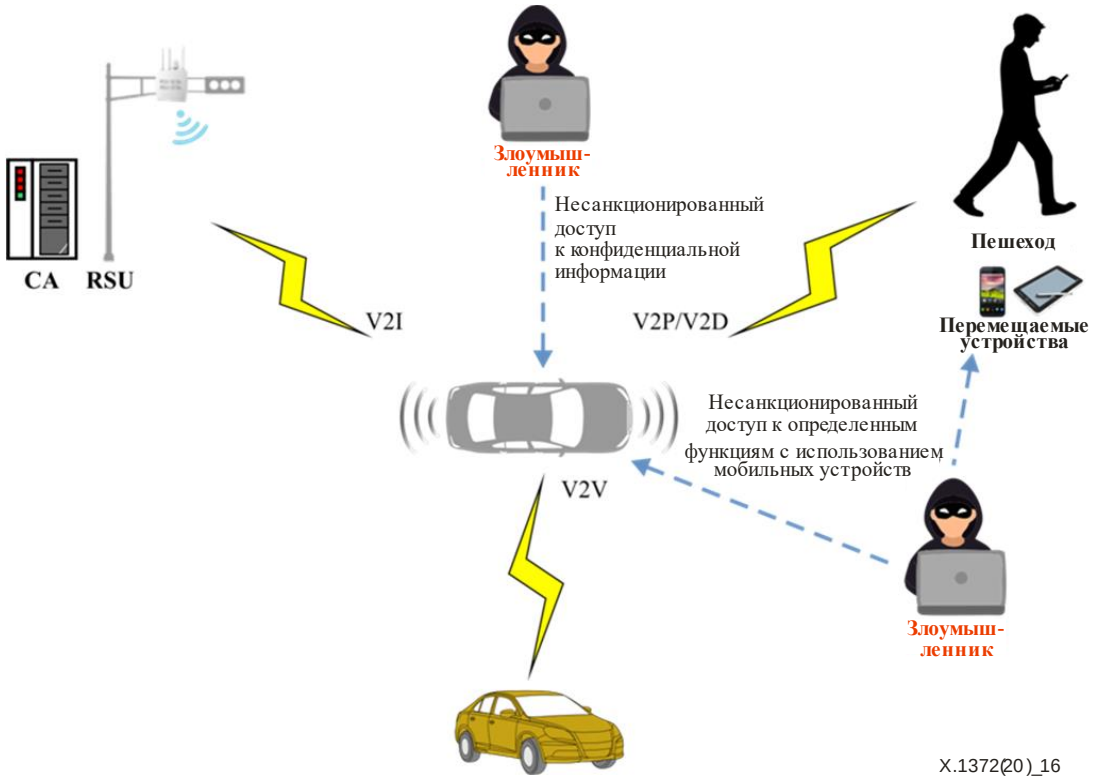


Рисунок 16 – Угрозы для авторизации

8 Требования безопасности

В этом разделе приведены требования безопасности связи V2X. В пунктах 8.1–8.7 описаны требования безопасности к системе связи V2X, а в пункте 8.8 приведены дополнительные сведения об этих требованиях.

8.1 Конфиденциальность

Неавторизованный объект не должен иметь возможность раскрывать сообщения, пересылаемые между транспортными средствами и транспортными средствами, между транспортными средствами и инфраструктурой, транспортными средствами и перемещаемыми устройствами, а также между транспортными средствами и пешеходами.

Неавторизованное лицо не должно иметь возможность анализировать идентификационную информацию человека, используя содержащиеся в сообщениях связи сведения, позволяющие установить личность (PII), такие как местонахождение или маршрут движения.

8.2 Целостность

Сообщения, передаваемые на транспортное средство, RSU или перемещаемое устройство или от них, должны быть защищены от несанкционированного изменения и удаления.

8.3 Готовность

Сообщения должны передаваться и приниматься с приемлемой задержкой. Например, предупредительное сообщение о произошедшем впереди столкновении должно поступать на приближающееся транспортное средство прежде, чем оно достигнет места аварии. Если предупредительное сообщение не будет доставлено на приближающийся автомобиль из-за атаки типа глушения, то приложение безопасности V2V/V2I может оказаться бесполезным.

Должна быть предусмотрена возможность обработки поступающей информации в режиме реального времени; для этого следует использовать упрощенные криптографические алгоритмы с малым объемом служебных данных.

8.4 Предотвращение отказа от авторства

У объекта не должно быть возможности отрицать факт отправления сообщения. Это требование может быть реализовано с использованием цифровых подписей в системах связи V2X.

8.5 Аутентичность

В системе связи V2V/V2I такие объекты как OBU и RSU должны быть в состоянии представить подтверждение того, что ни являются законными владельцами законных идентификаторов. Это требование называется аутентификацией объекта. Аутентификация также необходима для связи между транспортным средством и перемещаемым устройством.

В случае групповой связи транспортное средство не должно доказывать подлинность своего идентификатора. Оно лишь должно доказать, что является подлинным участником группы. Это требование называется атрибутивной аутентификацией.

8.6 Подотчетность

Объект должен иметь возможность обнаруживать и/или предотвращать любое ненадлежащее функционирование OBU или датчиков транспортных средств путем проверки их данных.

Например, OBU может проверить некоторую информацию, содержащуюся в полученном сообщении, на кинематическую корректность по сравнению с ранее полученным сообщением. Если данные о местоположении в полученном сообщении указывают на недопустимые изменения динамического поведения транспортного средства, это может быть вызвано аномальным поведением другого объекта. Следовательно, эту информацию необходимо отфильтровать или проигнорировать.

8.7 Авторизация

Очень важное значение имеет обеспечение контроля доступа и авторизации для разных объектов. Предоставление или запрет доступа тем или иным объектам и/или использование определенных функций или данных должны регулироваться особыми правилами.

8.8 Применимость требований безопасности V2X

В таблице 1 перечислены требования безопасности, описанные в пунктах 8.1–8.7, с указанием их применимости к различным формам связи V2X.

Таблица 1 – Требования безопасности связи V2X

	Распространение предупреждений по каналам связи V2V	**Групповая связь V2V**	**Сигнализация V2V**	**Предупреждение по каналам связи V2I**	**Обмен информацией по каналам связи V2V/V2I**	**Связь V2D**	**Связь V2P**
Конфиденциальность (общая)	–	O	–	–	O	O	O
Конфиденциальность (PII)	O	O	O	▲	O	O	O
Целостность	O	O	O	O	O	O	O
Готовность	O	O	O	O	O	▲	O
Предотвращение отказа от авторства	O	O	O	O	O	O	O
Аутентичность/ подлинность	O	▲	O	O	O	O	O
Подотчетность	O	O	O	O	O	O	O
Авторизация	–	O	–	–	O	O	–

O Обязательное – Необязательное ▲ Частично обязательное

В ситуации распространения предупреждений по каналам связи V2V конфиденциальность не является обязательным требованием, поскольку сообщения, передаваемые одним транспортным средством другому, уже содержат общедоступную информацию, например об аварии впереди или приближении транспортного средства экстренной службы. В ситуации распространения предупреждений по каналам связи V2V распространяемые сообщения не содержат никакой информации, требующей авторизации.

В сценарии групповой связи V2V требуется лишь частичная аутентификация транспортного средства, что означает, что каждому транспортному средству не обязательно требовать аутентификацию каждого транспортного средства из группы. Аутентификация – это процесс, с помощью которого объект проверяет идентичность другого участника обмена данными. Однако в сценарии групповой связи V2V каждому транспортному средству не требуется точная аутентификация объекта из группы. В этом случае достаточно доказать, что транспортное средство является участником группы. Другими словами, гарантируется не идентичность транспортного средства, а только то, что это транспортное средство является участником группы. Этот вид аутентификации можно назвать атрибутивной аутентификацией. Сообщения в этом сценарии также содержат информацию авторизации относительно ведущего колонны или участия в группе.

В сценарии сигнализации по каналам связи V2V распространяемая информация должна быть защищена от несанкционированного изменения и удаления. Однако если сообщение не содержит идентификационной информации о транспортном средстве, его не обязательно шифровать. Кроме того, отсутствие в сценарии сигнализации по каналам связи V2V требования об авторизации объясняется тем, что передаваемая информация не используется для целей управления.

В сценарии передачи предупреждений по каналам связи V2I информация, которой обмениваются транспортные средства и объекты инфраструктуры, такие как RSU, обычно представляет собой общедоступную информацию о дорожном движении. Поэтому конфиденциальность в системе предупреждений V2I не требуется. В ситуации передачи предупреждений по каналам связи V2I защита PII частично необходима в том смысле, что защита PII требуется транспортному средству, но не требуется RSU. Если водитель связан с транспортным средством, должны быть защищены сведения о его текущем местоположении и истории поездок. Однако у RSU нет PII, так как RSU не связан с людьми.

Сценарий связи V2D предусматривает использование перемещаемого устройства в транспортном средстве. В случае когда перемещаемое устройство поддерживает связь с транспортным средством, его готовность не оказывает такого же влияния, как в сценарии связи V2V, так как в реальных условиях число устройств в транспортном средстве обычно меньше, чем количество транспортных средств на дороге.

В сценарии связи V2P перемещаемое устройство у пешеходов или VRU не имеет никаких функций, требующих авторизации транспортного средства.

9 Реализация связи V2X с обеспечением безопасности

В этом разделе представлены возможные варианты реализации связи V2X для выполнения требований безопасности, описанных в разделе 8, таких как конфиденциальность, целостность, готовность и т. д. Приведен краткий обзор основных криптографических алгоритмов, пригодных для систем связи между транспортными средствами, а также дано описание способов их использования в сценариях связи V2X, таких как предупреждение о чрезвычайных ситуациях и взаимодействие в группе.

9.1 Криптографическое обеспечение аутентификации объектов и конфиденциальности сообщений

Функция аутентификации объектов V2X может быть обеспечена с помощью алгоритмов цифровой подписи. Функция обеспечения конфиденциальности сообщений может выполняться с использованием симметричных криптографических алгоритмов и алгоритмов с открытым ключом. В настоящей Рекомендации приведены примеры реализации этих функций. Адаптация и выбор механизмов и параметров, относящихся к функциям аутентификации объектов и обеспечения конфиденциальности сообщений, зависят от политики развертывания.

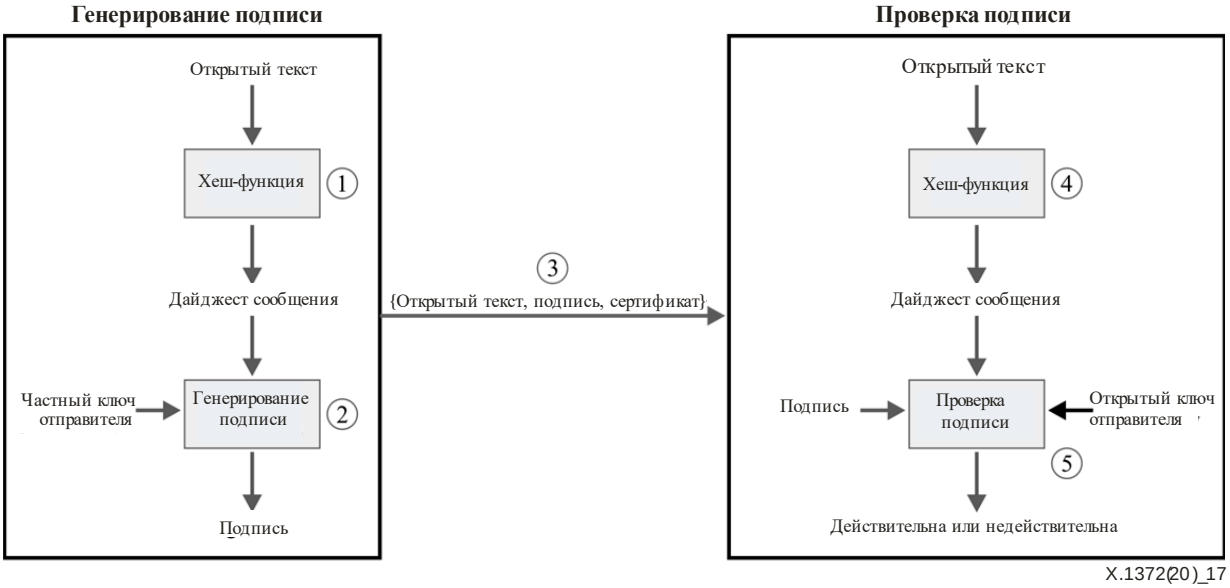


Рисунок 17 – Генерирование и проверка подписи

Алгоритм цифровой подписи включает в себя процесс генерирования подписи и процесс ее проверки, как показано на рисунке 17. Подписант использует процесс генерирования для создания цифровой подписи, защищающей данные. Проверяющий использует процесс проверки подлинности подписи. У каждого подписанта имеются открытый и частный ключи. Как показано на рисунке 17, в процессе генерирования подписи используется частный ключ, а в процессе проверки подписи используется открытый ключ подписанта.

Общая процедура генерирования и проверки подписи включает следующие шаги.

– Шаг 1. С помощью хеш-функции (такой как защищенный алгоритм хеширования-256 (SHA-256)) вычисляется дайджест открытого текстового сообщения. Например, дайджест вычисляется по версии протокола, заголовку, полезной нагрузке и длине заключительной части.

– Шаг 2. С помощью частного ключа отправителя генерируется подпись дайджеста сообщения.

– Шаг 3. Открытый текст, подпись и сертификат отправителя передаются получателю.

– Шаг 4. Получатель вычисляет дайджест сообщения, используя полученный от отправителя открытый текст.

– Шаг 5. Получатель вычисляет проверочное значение, используя дайджест сообщения из шага 4, полученную подпись и открытый ключ отправителя. Если проверочное значение совпадает со значением в подписи, то полученная подпись действительна. Если проверочное значение отличается от значения в подписи, то полученная подпись недействительна.

В качестве алгоритма цифровой подписи в системе связи V2X может использоваться алгоритм цифровой подписи на основе эллиптических кривых (ECDSA).

Для обеспечения конфиденциальности сообщений V2X используются алгоритмы шифрования. Для передачи ключа в алгоритме с симметричными ключами, таком как усовершенствованный стандарт шифрования (AES), используется асимметричный алгоритм шифрования, такой как объединенный алгоритм шифрования на основе эллиптических кривых (ECIES). Процедура шифрования ECIES показана на рисунке 18. В ECIES на рисунке 18 используются следующие функции:

– соглашение о ключах (KA) – функция, используемая для генерирования двумя объектами общего секретного ключа;

– функция выработки ключа (KDF) – механизм, производящий из ключевого материала комплект ключей с некоторыми дополнительными параметрами;

– шифрование – алгоритм шифрования с симметричными ключами;

– имитовставка (MAC) – алгоритм генерирования MAC.

На рисунке 18 используются следующие условные обозначения:

– ***u*** – частный ключ отправителя;

– ***U*** – открытый ключ отправителя;

– ***v*** – частный ключ получателя;

– ***V*** – открытый ключ получателя.

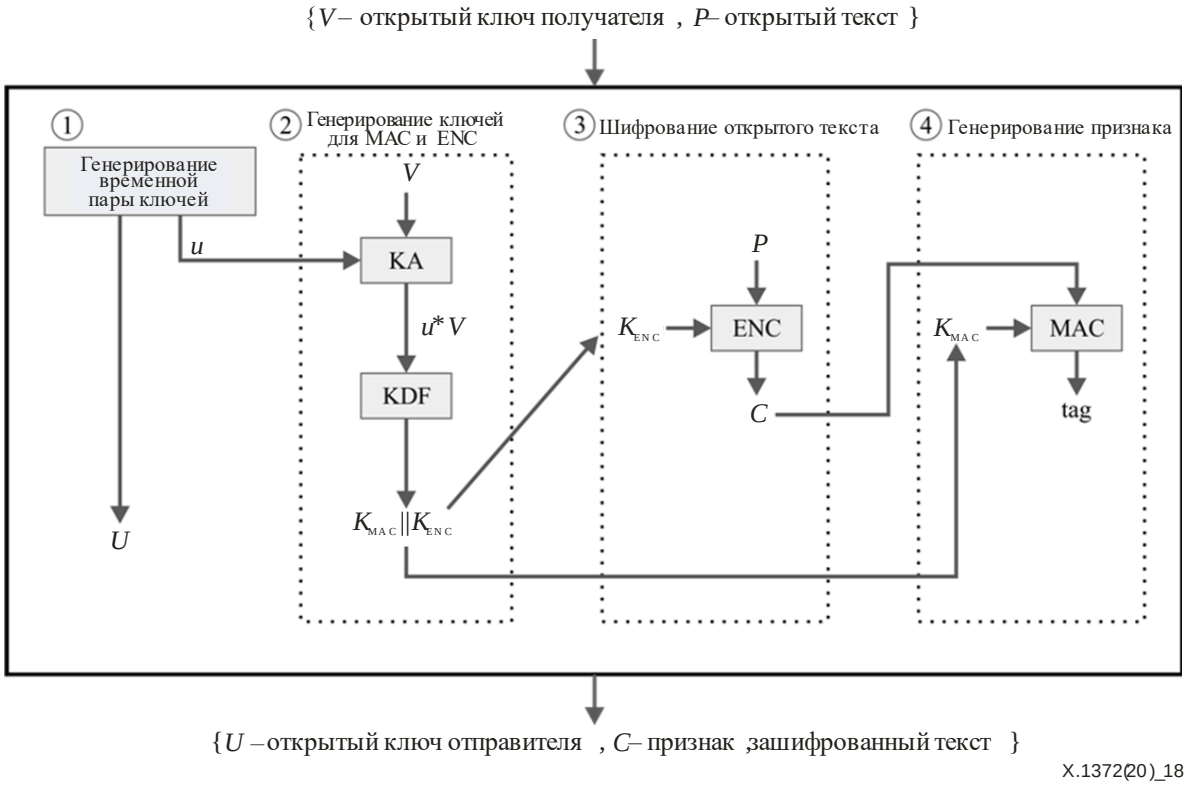


Рисунок 18 – Процедура шифрования ECIES

Как показано на рисунке 18, входными данными процедуры шифрования служат открытый ключ получателя ***V*** и открытый текст ***P***. Выходными данными процедуры шифрования являются открытый ключ отправителя ***U***, признак и зашифрованный текст ***C***. Процедура шифрования сообщения включает следующие шаги.

– Шаг 1. Генерирование временной пары ключей

Отправитель генерирует частный ключ ***u*** и открытый ключ ***U***. Рекомендуется, чтобы для каждой операции шифрования открытый ключ ***U*** создавался заново.

– Шаг 2. Генерирование ключей для MAC и ENC

Функция согласования ключей (KA) с помощью временного частного ключа отправителя ***u*** и открытого ключа получателя ***V*** генерирует общий секретный ключ. Функция выработки ключа (KDF) на основе SHA-256 принимает этот общий секретный ключ для получения конкатенации ключа имитовставки (MAC) (***K*MAC**) и ключа шифрования (***K*ENC**).

– Шаг 3. Шифрование открытого текста

Открытый текст ***P*** шифруется с помощью ***K*ENC** с использованием симметричных алгоритмов шифрования.

ECIES используется для шифрования симметричного ключа шифрования сообщений V2X с использованием протокола блочного шифрования с имитовставкой и режимом сцепления блоков и счетчика на основе расширенного стандарта шифрования (AES-CCM). Таким образом открытый текст фактически представляет собой ключ шифрования для AES-CCM.

– Шаг 4. Генерирование признака

Для обеспечения целостности сообщения функция MAC с помощью SHA-256 генерирует признак зашифрованного текста, который представляет собой симметричный ключ AES-CCM.

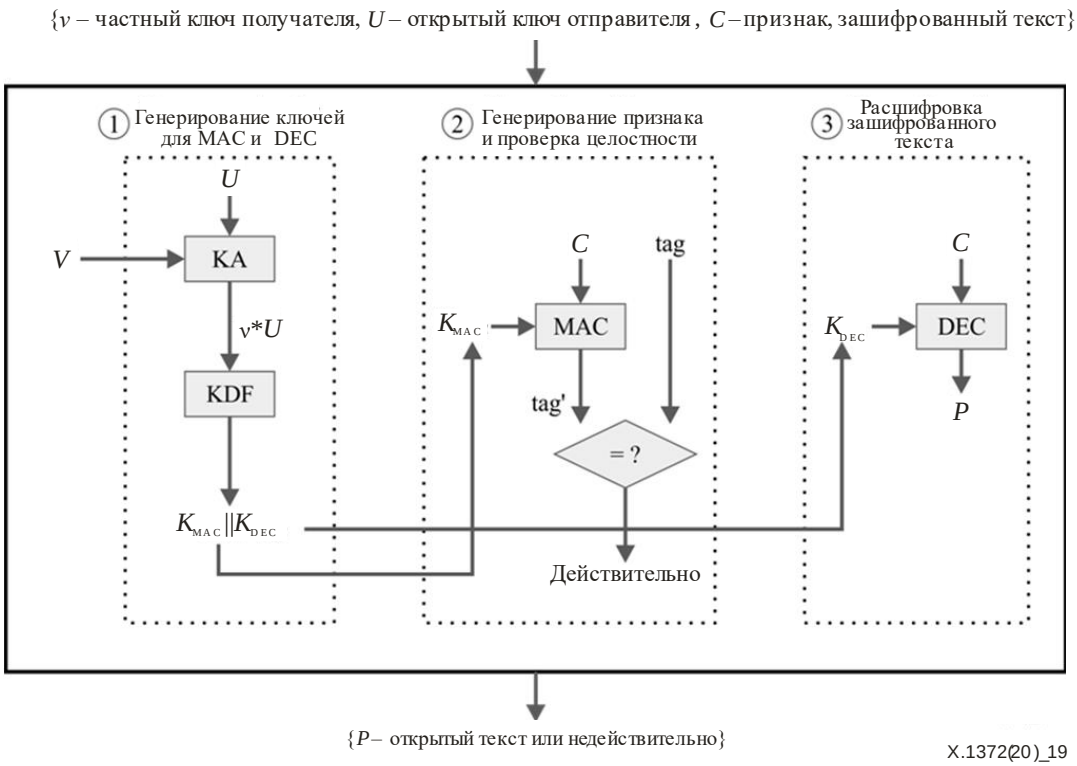


Рисунок 19 – Процедура расшифровки ECIES

Процедура расшифровки ECIES показана на рисунке 19. Как видно на рисунке 19, входными данными процедуры расшифровки являются частный ключ получателя *v*, открытый ключ отправителя ***U***, признак и зашифрованный текст ***C***. Выходными данными процедуры расшифровки являются открытый текст ***P*** или результаты проверки целостности сообщения. DEC на рисунке 19 означает процедуру расшифровки на основе алгоритма с симметричными ключами. Процедура расшифровки сообщения включает следующие шаги.

– Шаг 1. Генерирование ключей для MAC и DEC

Функция согласования ключей (KA) с помощью временного частного ключа отправителя ***U*** и частного ключа получателя ***v*** генерирует общий секретный ключ. Функция выработки ключа (KDF) на основе SHA-256 принимает этот общий секретный ключ, чтобы получить конкатенацию ключа имитовставки (MAC) ($\boldsymbol{K}_{\mathbf{MAC}}$) и ключа дешифрования ($\boldsymbol{K}_{\mathbf{DEC}}$). Отметим, что в алгоритмах с симметричными ключами $\boldsymbol{K}_{\mathbf{ENC}}$ и $\boldsymbol{K}_{\mathbf{DEC}}$ имеют одинаковые значения.

– Шаг 2. Генерирование признака и проверка целостности

Функция MAC с помощью $\boldsymbol{K}_{\mathbf{MAC}}$ генерирует признак полученного зашифрованного текста ***C***. Вычисленный признак сравнивается с полученным. Если значения не идентичны, полученное сообщение отвергается по причине неудачной проверки целостности сообщения.

– Шаг 3. Расшифровка зашифрованного текста

Зашифрованный текст ***C*** расшифровывается с помощью $\boldsymbol{K}_{\mathbf{DEC}}$ с использованием алгоритмов симметричного шифрования.

ECIES используется для шифрования симметричного ключа шифрования сообщений V2X с использованием AES-CCM. Таким образом открытый текст фактически представляет собой ключ шифрования для AES-CCM.

9.2 Конфиденциальность аварийно-предупредительных сообщений по безопасности дорожного движения

На рисунке 20 показан общий вариант использования аварийных предупреждений. ЭБУ торможения передает сообщение в блок связи V2X транспортного средства через его центральный узел связи (CCU). Соответствующее приложение ИТС в блоке связи V2X получает сообщение от ЭБУ торможения и генерирует предупредительное сообщение V2X. Сгенерированное сообщение направляется на сетевой и транспортный уровни. Это сообщение подписывается или шифруется уровнем безопасности. Затем физический уровень отправляет подписанное или зашифрованное сообщение в канал беспроводной связи. По каналу беспроводной связи сообщение передается приемному устройству. В приемном устройстве сообщение проверяется или дешифруется уровнем безопасности и, наконец, передается на верхний уровень соответствующему приложению ИТС. Соответствующее приложение ИТС может обновить LDM или предупредить водителя с помощью человеко-машинного интерфейса и отправить в ЭБУ команду торможения для понижения скорости транспортного средства.

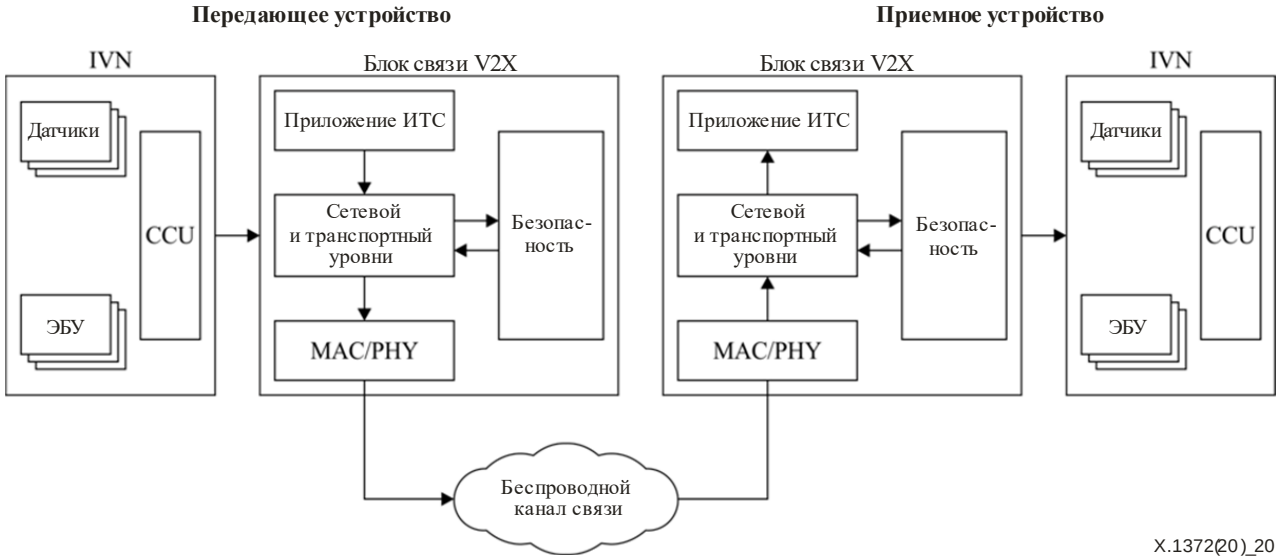


Рисунок 20 – Процедура аварийного предупреждения

9.3 Аутентификация объекта при формировании автоколонны

Формирование автоколонны – это эффективный подход, меняющий схему вождения с индивидуального на групповое. В общем случае групповое вождение предполагает группу транспортных средств, которые движутся в одном направлении одно за другим, сохраняя небольшую почти постоянную дистанцию, как показано на рисунке 21. В процессе формирования колонны выделяют три основных этапа – вливание в колонну, сотрудничество/сохранение колонны и отделение от колонны.

Рисунок 21 – Использование группового подхода

– Вливание в колонну: транспортное средство, которое не входит в состав колонны, движется к ней и вливается в колонну на ближайшем перекрестке.

– Сотрудничество/сохранение колонны: транспортные средства, движущиеся в колонне, должны поддерживать связь и сотрудничать друг с другом, чтобы сохранять колонну и решать такие задачи, как освобождение пути для высокоприоритетных транспортных средств, корректировка положения в соответствии с планом маршрута, пересечение транспортных развязок и смена полос движения.

– Отделение от колонны: транспортное средство отделяется от своей колонны, переместившись на другую полосу движения на ближайшем перекрестке.

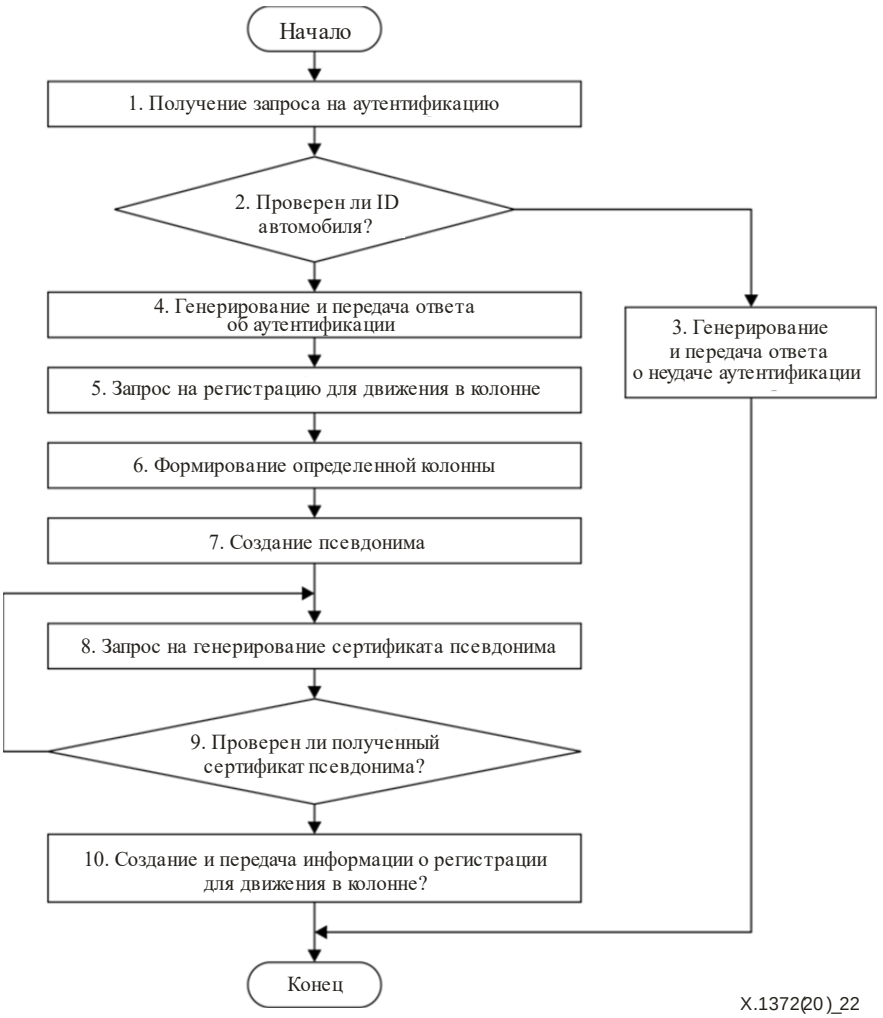


Рисунок 22 – Процедура регистрации колонны

На рисунке 22 показан пример аутентификации для движения в колонне. Как видно на рисунке 22, на этапе 1 от транспортного средства поступает запрос аутентификации для его регистрации для движения в колонне, на этапе 2 идентификатор этого транспортного средства проверяется, например, с использованием алгоритма цифровой подписи криптосистемы с открытым ключом. Запрос аутентификации транспортного средства может быть выполнен посредством передачи сообщения, подписанного частным ключом транспортного средства, в систему обслуживания колонны. Если в результате проверки на этапе 2 идентификатор транспортного средства определен как недействительный, то система обслуживания колонны генерирует соответствующий ответ о неудаче аутентификации и передает его транспортному средству, как показано на этапе 3.

Если в результате проверки на этапе 2 идентификатор транспортного средства определен как действительный, то система обслуживания колонны генерирует соответствующий ответ об аутентификации и передает его транспортному средству, как показано на этапе 4.

После получения ответа об аутентификации, то есть удачной аутентификации транспортного средства, пользователь вводит и выбирает информацию о регистрации в колонне, включая сведения о квалификации вождения в колонне, отправном пункте назначения, предполагаемом времени отправления, предполагаемом времени прибытия и желаемом месте отдыха, и транспортное средство передает информацию о регистрации в колонне в систему обслуживания колонны, тем самым запрашивая регистрацию в колонне, как показано на этапе 5.

Затем в случае поступления от транспортного средства запроса на регистрацию в колонне, включающего информацию о регистрации в колонне, система обслуживания колонны формирует определенную колонну на основе информации о регистрации в колонне, указывающей на один и тот же пункт назначения, одно и то же место отправления, одно и то же предполагаемое место прибытия

и т. д., после чего сохраняет/регистрирует информацию об определенной колонне в групповой информационной базе, как показано на этапе 6.

Определенная колонна может состоять из по меньшей мере одного лидера колонны, то есть ведущего транспортного средства, и по меньшей мере одного участника, то есть транспортного средства – участника колонны. После этого система обслуживания колонны назначает каждому участвующему транспортному средству псевдоним, генерирует запрос на получение сертификата псевдонима, назначенного каждому транспортному средству – участнику колонны, как показано на этапе 7, и передает запрос на сертификат в центр аутентификации, как показано на этапе 8.

На этапе 9 система обслуживания колонны отслеживает получение сертификата псевдонима из центра аутентификации. Если сертификат псевдонима получен, система обслуживания колонны сохраняет его в базе данных информации о колонне. Сертификат псевдонима может представлять собой сообщение из центра аутентификации с цифровой подписью. Обоснованность псевдонима удостоверяется его сертификатом. Псевдоним – это открытый ключ, назначаемый системой обслуживания колонны каждому транспортному средству.

Каждому транспортному средству может быть присвоено несколько псевдонимов. Поскольку псевдоним не содержит информации, связанной с идентификатором каждого транспортного средства, участвующего в колонне, идентификатор такого транспортного средства не раскрывается, так что его PII может быть защищена.

При получении соответствующего уведомления система обслуживания колонны на этапе 10 генерирует информацию о регистрации определенной колонны, сохраняет ее в базе данных колонны и передает каждому транспортному средству в составе колонны. Информация о регистрации колонны может включать в себя идентификатор колонны, псевдоним каждого транспортного средства, сертификат псевдонима и т. п. В зарегистрированной колонне каждое транспортное средство, то есть пользователь транспортного средства, может выполнять движение, поддерживая связь с другими транспортными средствами в колонне с помощью предоставленной ему регистрационной информации колонны.

9.4 PKI систем связи с подвижными объектами

Для создания доверительных отношений между участниками систем связи с подвижными объектами необходима инфраструктура открытых ключей (PKI), которая обеспечивает работу с цифровыми сертификатами и их администрирование. PKI систем связи с подвижными объектами отличается от обычной PKI с учетом ряда аспектов. Наиболее важным является использование псевдонимов для защиты от раскрытия местоположения транспортного средства, связанного с местоположением его владельца. По сравнению с обычной PKI число сертификатов PKI систем связи с подвижными объектами огромно. Поэтому основная задача состоит в том, чтобы предоставить эффективные методы запроса сертификатов и обработки их отзыва.

Более подробное описание эталонных моделей PKI систем связи с подвижными объектами приведено в Дополнении II.

Дополнение I

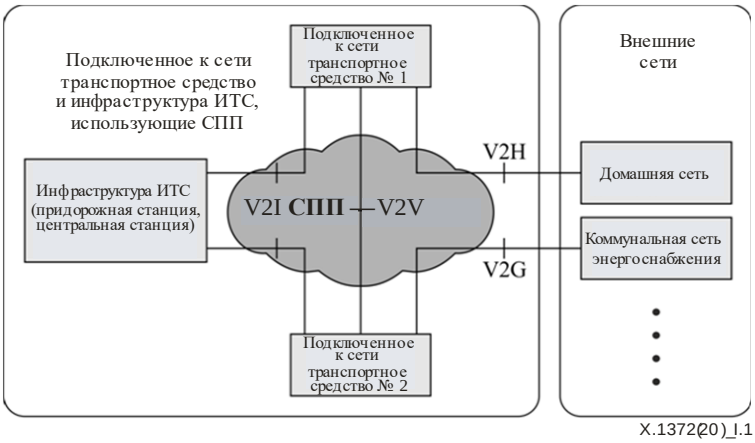
Эталонные модели связи с подвижными объектами

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Концепция МСЭ-Т в отношении услуг и приложений для транспортных средств, подключенных к сети, с использованием СПП

Концепция услуг и приложений для транспортных средств, подключенных к сети, в контексте сетей последующих поколений (СПП) описана в [b-ITU-T Y.2281]. Транспортное средство является одним из важных компонентов, использующих возможности сети для связи между транспортным средством и инфраструктурой (V2I), между транспортными средствами (V2V) и между транспортным средством и домом (V2H). В этом контексте транспортное средство, подключенное к сети, может взаимодействовать с сетями последующих поколений (СПП) для поддержки более сложных услуг и приложений, например связанных с безопасностью дорожного движения, регулированием дорожного движения, мультимедийными услугами и реализацией этих услуг в зависимости от местоположения.

В [b-ITU-T Y.2281] определена взаимосвязь между СПП и транспортным средством, подключенным к сети, а также требования, учитывающие необходимость поддержки услуг и приложений для таких транспортных средств, использующих СПП. Кроме того, описана общая архитектура инфраструктуры для подключенных к сети транспортных средств и интеллектуальных транспортных систем (ИТС) с поддержкой СПП и для поддержки особенностей связи СПП, согласованных с транспортными средствами, подключенными к сети.



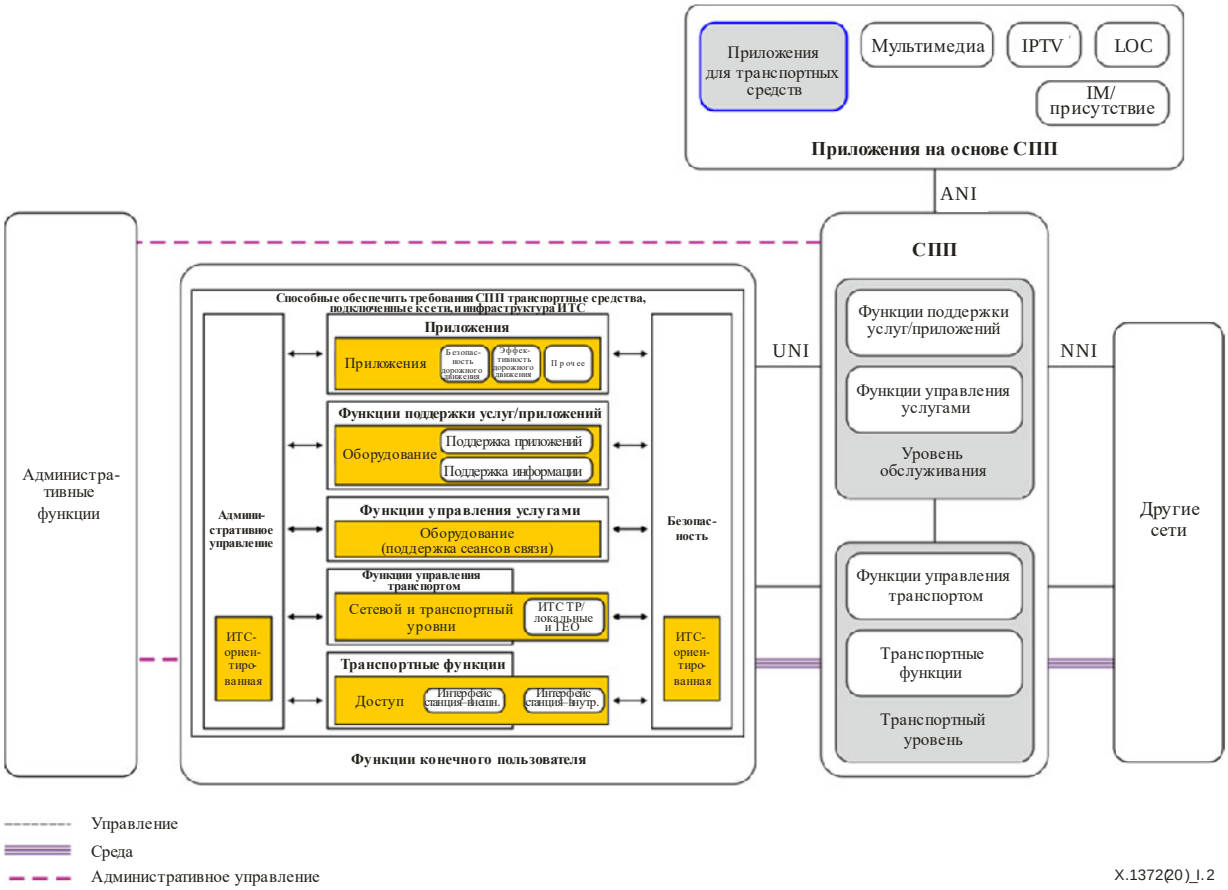
ПРИМЕЧАНИЕ. – Источник рисунка [b-ITU-T Y.2281].

Рисунок I.1 – Общая модель конфигурации инфраструктуры для транспортных средств, подключенных к сети, и ИТС

На рисунке I.1 показана модель конфигурации из Рекомендации МСЭ-Т Y.2281, из которой видно, как транспортные средства, подключенные к сети, связаны с инфраструктурой ИТС, а также с внешними сетями, к которым относятся домашние сети и коммунальные сети энергоснабжения, использующие СПП. В отличие от других стандартов ИТС [b-ITU-T Y.2281] ориентирована на использование СПП в средах ИТС. [b-ITU-T Y.2281] определяет использование СПП в системах ИТС для минимизации проблем функциональной совместимости одноранговых систем связи ИТС и сети общего пользования. Такая функциональная совместимость особенно важна для поддержки качества обслуживания (QoS), мобильности и безопасности при использовании различных мультимедийных услуг.

На рисунке I.2 общая архитектура способных обеспечить требования СПП транспортных средств, подключенных к сети, и инфраструктуры ИТС в сочетании с СПП. СПП включает функции конечного пользователя, уровня обслуживания, транспортного уровня, уровня управления и СПП-приложения. Функция способного обеспечить требования СПП транспортного средства, подключенного к сети, и инфраструктуры ИТС относится к функциям конечного пользователя с учетом СПП.

В [b-ITU-T Y.2281] описан способ поддержки с помощью СПП ориентированных на транспорт приложений СПП, таких как экстренный вызов.



ПРИМЕЧАНИЕ. – Источник рисунка [b-ITU-T Y.2281].

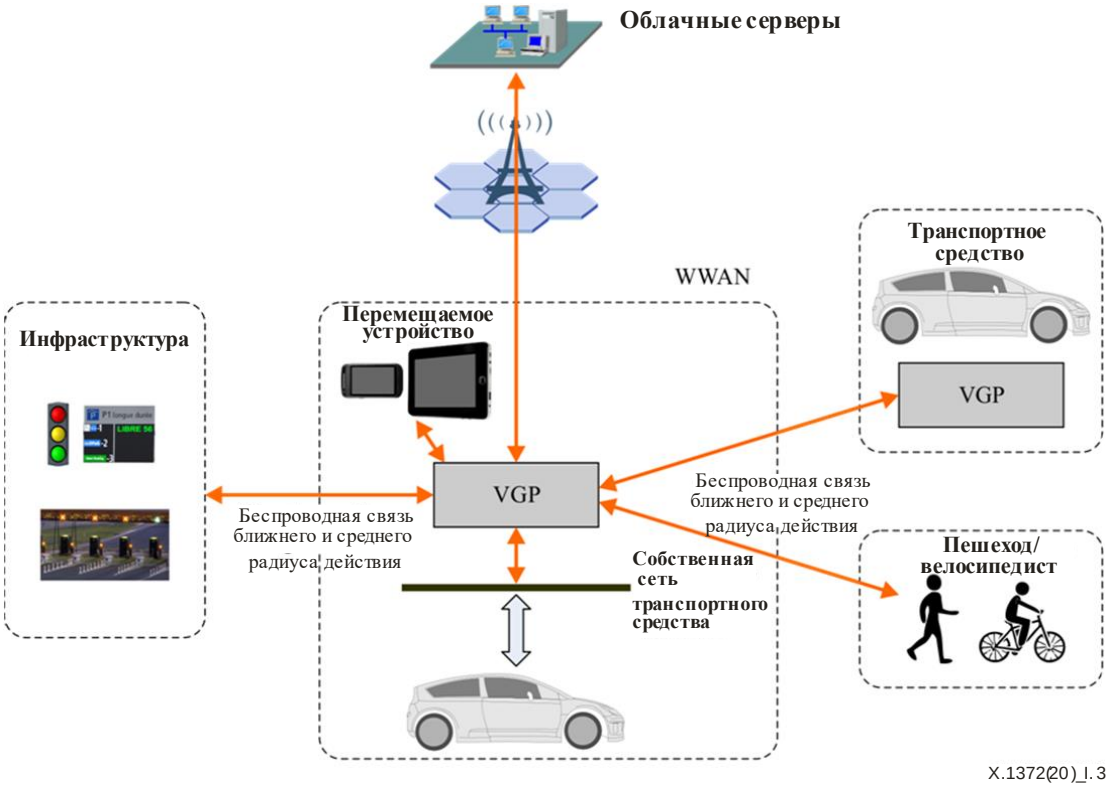
Рисунок I.2 – Общая архитектура способных обеспечить требования СПП транспортных средств, подключенных к сети, и инфраструктуры ИТС в сочетании с СПП

Вопросы безопасности [b-ITU-T Y.2281] рассматриваются в [b-ITU-T Y.2201]. Вопросы безопасности необходимо рассматривать в связи с сетью, к которой подключены транспортные средства. Однако в [b-ITU-T Y.2281] рассматриваются только вопросы безопасности СПП, а требования безопасности для других случаев выходят за рамки этой Рекомендации.

Концепция МСЭ-Т в отношении услуг и приложений для подключенных к сети транспортных средств, использующих СПП, ориентирована на адаптацию СПП к условиям движущихся транспортных средств. В [b-ITU-T Y.2281] не рассматриваются аспекты безопасности в условиях автотранспортных перевозок. Архитектура IEEE беспроводного доступа в условиях автотранспортных перевозок (WAVE), описанная в [b-IEEE WAVE], ориентирована на радиоинтерфейс 5,9 ГГц, поскольку в нее не включено явным образом приложение для связи с другой сетью. Архитектура ИТС ЕТСИ, описанная в [b-ETSI EN 302 665], относится к прикладному уровню, который представляет собой стек протоколов связи. С учетом того, что уровень доступа включает IEEE 802.x, сотовую связь 3G и Bluetooth, архитектура ИТС ЕТСИ предназначена для поддержки нескольких стеков сетевых протоколов.

I.2 Архитектура и функциональные объекты платформ автомобильного шлюза МСЭ-Т

В 16-й Исследовательской комиссии МСЭ-Т изучаются архитектура и функциональные объекты платформ автомобильного шлюза (VGP). Архитектура, структура функциональной архитектуры и функциональные объекты платформ автомобильного шлюза описаны в [b-ITU-T H.550]. Термин VGP определен в [b-ITU-T F.749.1]. VGP – это аппаратно-программный комплекс ИКТ для транспортных средств, который представляет собой открытую платформу для создания интегрированной среды исполнения для услуг связи автомобильного шлюза. VGP также может предоставлять услуги связи более высокого уровня, такие как взаимодействие с водителем через услуги доступа водитель – транспортное средство и т. п. Подсистемы, предназначенные исключительно для эксплуатации транспортных средств, не считаются частью VGP.



ПРИМЕЧАНИЕ. – Источник рисунка [b-ITU-T H.550].

Рисунок I.3 – Расположение VGP в эталонной модели ИТС

На рисунке I.3 показано расположение VGP в эталонной модели интеллектуальной транспортной системы (ИТС). Существует шесть основных сценариев связи: транспортное средство – транспортное средство, транспортное средство – инфраструктура, транспортное средство – облачный сервер, транспортное средство – перемещаемое устройство, транспортное средство – пешеход/велосипедист и сценарий взаимодействия с собственной сетью транспортного средства.

– Сценарий транспортное средство – транспортное средство (V2V) в основном относится к безопасности и автоматическому вождению, когда транспортные средства поддерживают связь друг с другом.

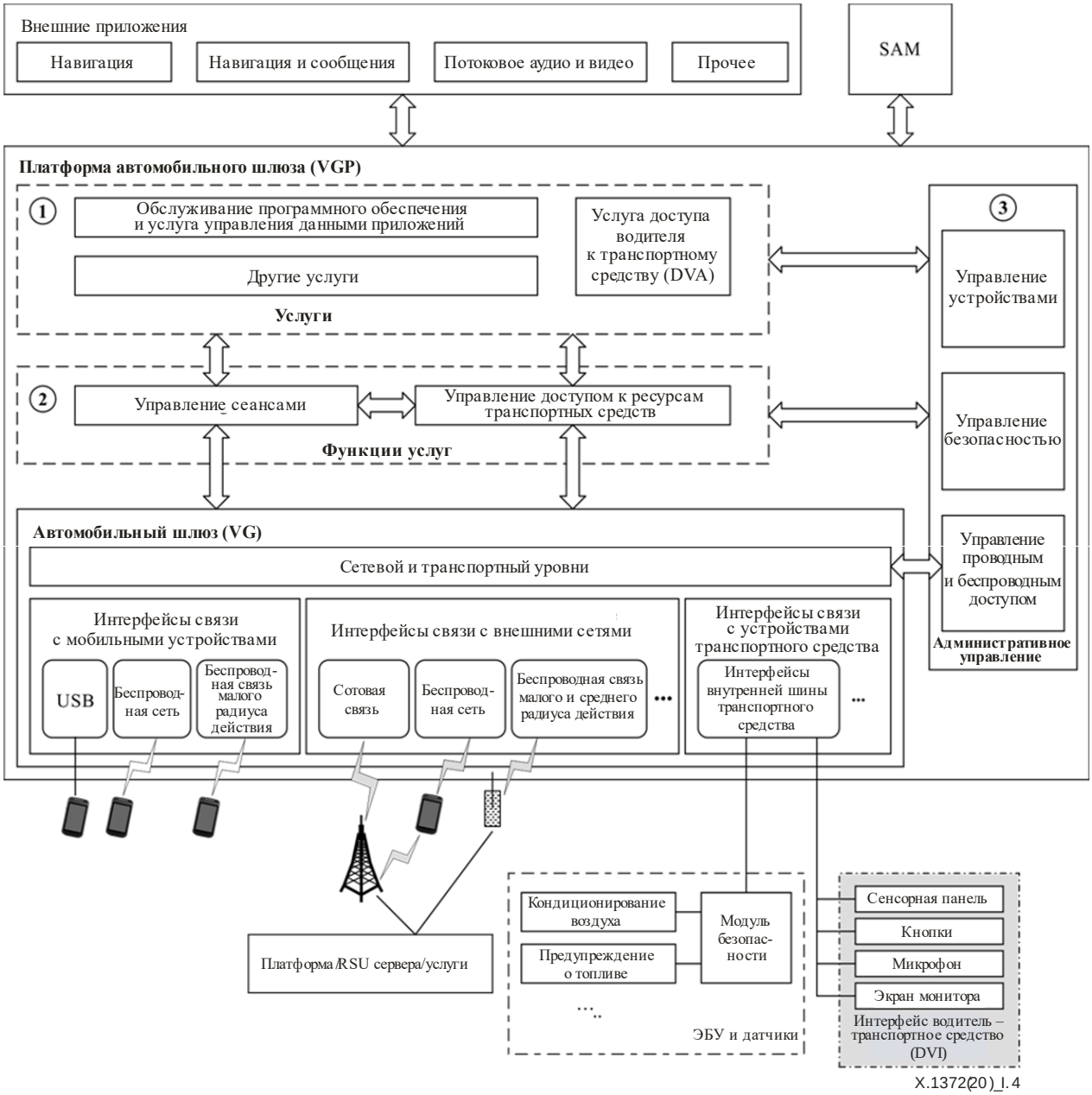
– Сценарий транспортное средство – инфраструктура (V2I) в основном относится к безопасности, электронному сбору платы за проезд (ETC) и обмену информацией о дорожном движении, когда транспортные средства поддерживают связь с придорожной инфраструктурой.

– Сценарий транспортное средство – облачный сервер в основном относится к экстренным вызовам и телематике, когда транспортные средства поддерживают связь с облачными службами.

– Сценарий транспортное средство – перемещаемое устройство в основном относится к связи и интерфейсу дистанционного доступа пользователей (UI), когда транспортные средства устанавливают связь с перемещаемыми устройствами.

– Сценарий транспортное средство – пешеход/велосипедист в основном относится к предупреждениям об опасности, когда транспортные средства связываются с устройствами пешеходов/велосипедистов.

– Сценарий взаимодействия с собственной сетью транспортного средства в основном относится к диагностике транспортного средства, дистанционному сбору данных и дистанционному управлению транспортным средством, когда VGP поддерживает связь с собственной сетью транспортного средства.



ПРИМЕЧАНИЕ. – Источник рисунка [b-ITU-T H.550].

Рисунок I.4 – Общая архитектура VGP

На рисунке I.4 представлена общая архитектура VGP. К услугам VGP относятся обслуживание программного обеспечения и услуга управления данными приложений, услуга доступа водитель – транспортное средство и другие услуги (см. блок 1 на рисунке I.4). К функциональным возможностям услуг относятся управление сеансами и управление доступом к ресурсам транспортных средств (см. блок 2 на рисунке I.4). К административному управлению относятся функции управления устройствами, управления безопасностью и управления проводным и беспроводным доступом (см. блок 3 на рисунке I.4). Имеются услуги поддержания внешних приложений, таких как система навигации и информационно-развлекательная система, обеспечивающие установление сеанса, преобразование форматов данных и специальную обработку.

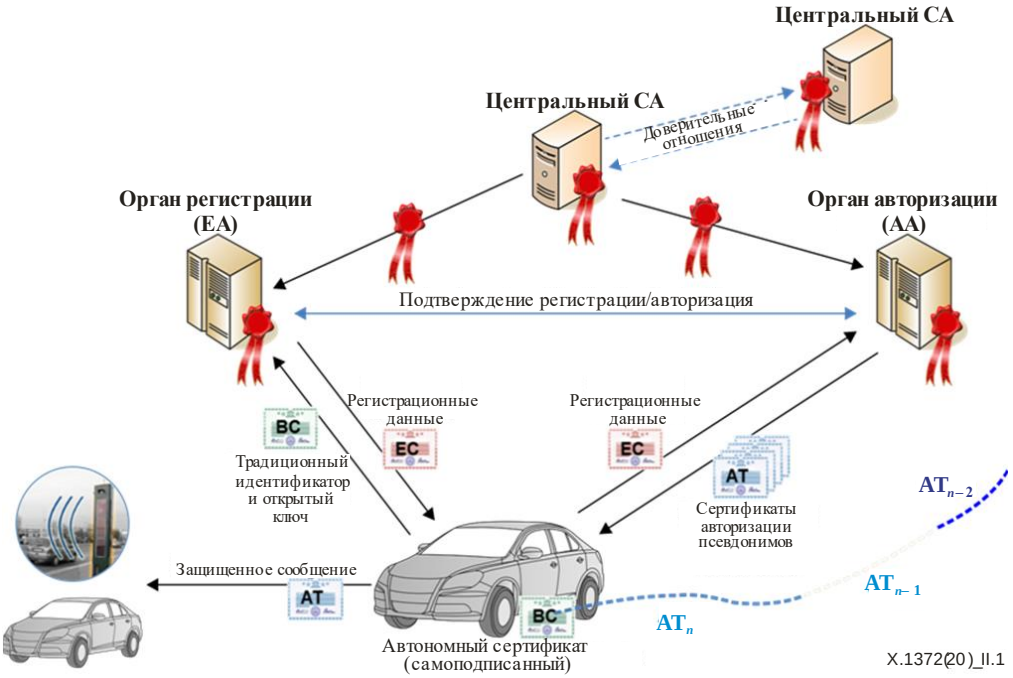
Аспект безопасности в VGP описан как часть уровня управления в [b-ITU-T H.550]. Общее описание функции безопасности содержится в пункте 8.4.1 "Управление безопасностью" [b-ITU-T H.550]. Оно включает функции управления безопасностью на уровне доступа, куда входят транспортный и сетевой уровни, и управление безопасностью услуг/приложений.

Дополнение II

Эталонные модели транспортной PKI

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

К функциям безопасности связи современной ИТС относится аутентификация сообщений, которая обеспечивает конфиденциальность информации о транспортных средствах и водителях. На европейском уровне Европейский институт стандартизации электросвязи (ETCИ) разработал механизм аутентификации сообщений, основанный на использовании инфраструктуры открытых ключей в качестве транспортно-ориентированной PKI, как показано на рисунке II.1.



ПРИМЕЧАНИЕ. – Источник рисунка [b-ETSI TS 102 940].

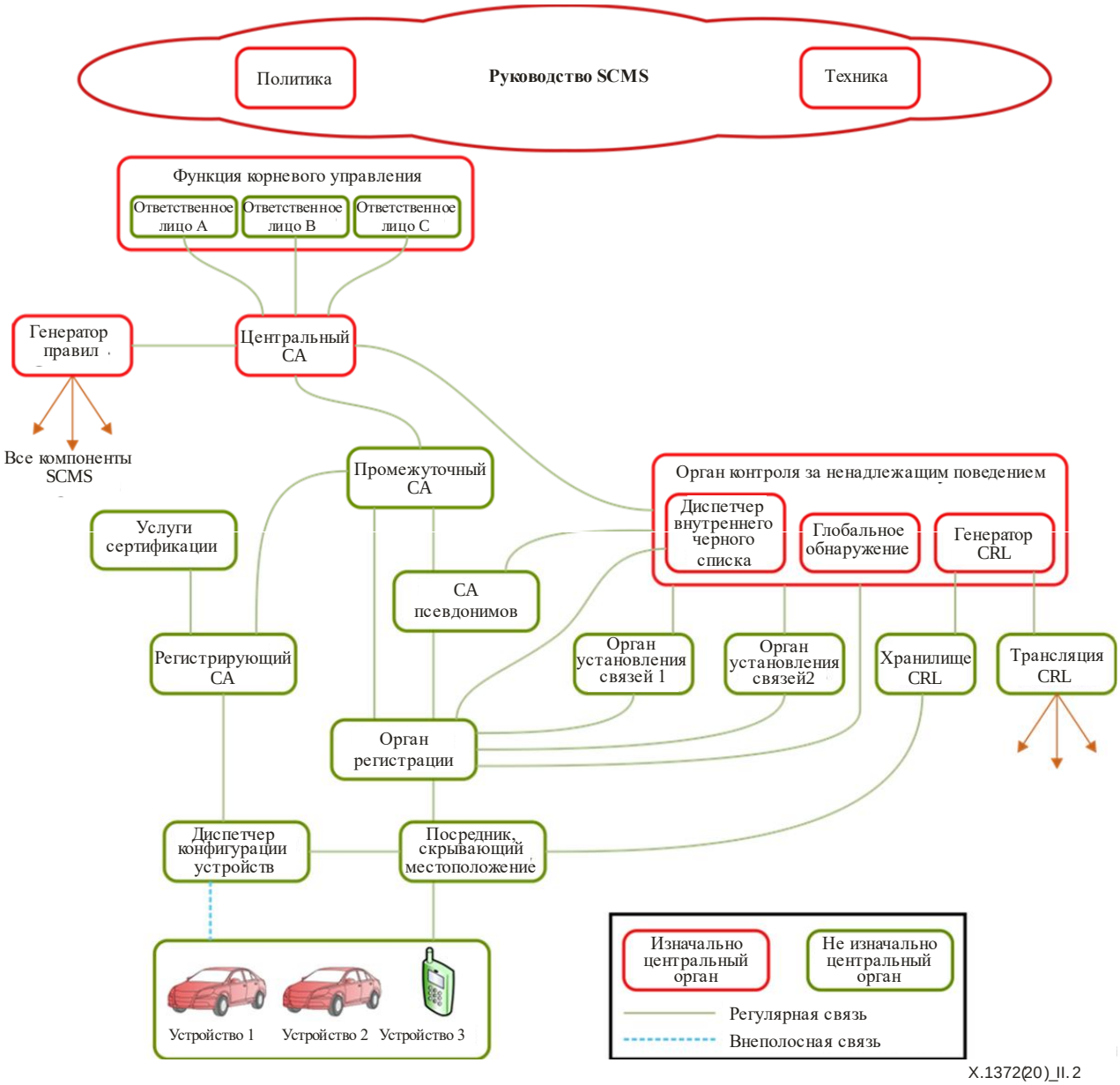
Рисунок II.1 – Транспортная PKI ETCИ

Отправной точкой цепочки доверительных сертификатов является центральный орган сертификации (RCA), который подписывает сертификаты других органов (например, органа авторизации (AA) и органа регистрации (EA)), а также создает и поддерживает список аннулированных сертификатов (CRL). В контексте оперативного управления RCA администрируется субъектом, способным гарантировать высокий и стабильный уровень доверия и быть в достаточной мере единым, таким как государство или группа государств. EA – это орган, который выдает сертификаты регистрации (EC) и оценивает обоснованность запросов на билеты авторизации (AT). AA представляет собой доверенную третью сторону, которая выдает AT станциям ИТС. AA не известен идентификатор станции ИТС, и он поручает EA провести проверку наличия у станции ИТС разрешения на AT. Запрос AT содержит идентификатор EA, в котором зарегистрирована станция ИТС.

Эта архитектура предназначена для обеспечения конфиденциальности станций ИТС и предотвращения возможности отслеживания: EA известен идентификатор станции ИТС, но не известны сертификаты псевдонимов (AT), которые та использует, тогда как AA известен сертификат псевдонима станции ИТС, но не известен ее идентификатор. Станция ИТС самостоятельно регистрируется в EA и получает EC. EC используется для запроса псевдонимов (AT) для AA; когда станция ИТС запрашивает AT, она передает в сообщении запроса свои идентификационные данные, зашифрованные с помощью EC и идентификатора EA. AA получает запрос на псевдоним, считывает идентификатор EA и проверяет

точку доступа EA, чтобы подтвердить запрос AT. EA проверяет EC станции ИТС и подтверждает либо не подтверждает запрос. Если запрос подтвержден, AA генерирует и отправляет AT на станцию ИТС.

С другой стороны, для защиты связи V2X Партнерство по измерениям для предотвращения столкновений (CAMP) разработало систему управления удостоверениями безопасности (SCMS) (см. [b-SCMS]). Она основана на PKI, обеспечивающей безопасность V2X, и в настоящее время находится в стадии перехода от исследований к проверке концепции. SCMS поддерживает процедуры самонастройки, предоставления сертификатов, сообщения о ненадлежащем поведении и отзыва сертификатов.



ПРИМЕЧАНИЕ. – Источник [b-SCMS].

Рисунок II.2 – Архитектура V-PKI CAMP

На рисунке II.2 представлен обзор архитектуры SCMS. Взаимоотношения между различными компонентами SCMS обозначены линиями, которые показывают, что компонент передает информацию или сертификаты другим компонентам.

Основные компоненты SCMS

– Регистрирующий CA (ECA) выдает сертификаты регистрации устройств и может использоваться для запроса сертификатов псевдонимов для различных географических регионов, производителей или типов устройств.
– Промежуточный CA (ICA) – вторичный CA, который освобождает центральный CA от высокой нагрузки; его сертифицирует центральный CA.
– Орган установления связей (LA) занимается предварительным определением ссылок для формирования ссылок, которые указываются в сертификатах для обеспечения их эффективного отзыва. Кроме того, имеются разделительные LA, предназначенные для того, чтобы оператор LA не мог выдавать ссылки на сертификаты, принадлежащие определенному устройству.
– Посредник, скрывающий местоположение (LOP), изменяет исходный адрес, чтобы скрыть местоположение запрашивающего устройства и предотвратить привязку сетевых адресов к местоположениям.
– Орган контроля за ненадлежащим поведением (MA) получает и обрабатывает сообщения устройств о ненадлежащем поведении для выявления потенциального ненадлежащего поведения или неисправности. Кроме того, он отзывает сертификат устройства и помещает его в CRL. MA также инициирует процесс привязки идентификатора сертификата к соответствующим регистрационным сертификатам и его внесения во внутренний черный список RA.
– Генератор правил (PG) поддерживает обновления глобального файла правил для RA. Глобальный файл правил содержит информацию о глобальной конфигурации и файл глобальной цепочки сертификации, в котором указаны все цепочки доверия SCMS.
– CA псевдонимов (PCA) выдает краткосрочные псевдонимы, идентификаторы и сертификаты приложений для устройств. Каждый PCA ограничен конкретным географическим регионом, конкретным производителем или типом устройств.
– Орган регистрации (RA) проверяет и обрабатывает запросы устройств и обеспечивает отсутствие у отозванных устройств возможности выдавать новые сертификаты псевдонимов. Кроме того, RA не выдает устройству более одного комплекта сертификатов в течение определенного периода времени. Более того, RA перетасовывает запросы или отчеты перед отправкой запросов на подписание сертификата псевдонима в PCA или пересылкой информации в MA.
– Центральный орган сертификации (RCA) – корень и вершина цепочки сертификации в SCMS. Выдает сертификаты ICA, PG и MA.

Библиография

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

[b-ITU-T H.550] Recommendation ITU-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

[b-ITU-T X.641] Recommendation ITU-T X.641 (1997), *Information technology – Quality of service: framework*

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

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks in open systems: Non-repudiation framework*

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 год), *Базовые термины и определения в области управления определением идентичности*

[b-ITU-T X.1371] Recommendation ITU-T X.1371 (2020), *Security threats to connected vehicles*

[b-ITU-T Y.2201] Рекомендация МСЭ-Т Y.2201 (2009 год), *Требования к СПП МСЭ-Т и возможности этих сетей*

[b-ITU-T Y.2281] Recommendation ITU-T Y.2281 (2011), *Framework of networked vehicle services and applications using NGN*

[b-ETSI EN 302 665] ETSI EN 302 665 V1.1.1 (2010-09), *Intelligent Transport Systems (ITS); Communications Architecture*. <https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf>

[b-ETSI TS 102 940] ETSI TS 102 940 V1.3.1 (2018-04), *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*. <https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf>

[b-IEEE WAVE] Станд. IEEE 1609.2 (2016 год), *Стандарт IEEE для беспроводного доступа в условиях автотранспортных перевозок – Услуги безопасности для сообщений приложений и управления*

[b-ISO 13185-1] ISO/TR 13185-1:2012, *Intelligent transport systems – Vehicle interface for provisioning and support of ITS services – Part 1: General information and use case definition*

[b-OVERSEE] Open Vehicular Secure Platform, OVERSEE Project. (Website). <https://www.oversee-project.com/>

[b-RITA] United States Department of Transportation, FHWA-JPO-11-130 (2011), *An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues*. <https://rosap.ntl.bts.gov/view/dot/3334/Share>

[b-SCMS] Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium, *Security Credential Management System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.1, 04*. May. 2016. <https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf>

[b-UNECE GRVA] United Nations Secretary of the Informal document GRVA-01-17, *Draft recommendation on cyber security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA*

[b-US DOT] United States Department of Transportation, Safety Pilot Program. <https://www.its.dot.gov/research_archives/safety/safety_pilot_plan.htm>

[b-USDOTHS812014] United States Department of Transportation, National Highway Traffic Safety Administration, DOT HS 812 014 (2014), *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application.* <https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>

[b-US GOV] United States Senator for Massachusetts, Edward J, Markey, Staff Report (2015), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk.* <http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.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 год