ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1383 (03/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

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

Требования безопасности для категоризованных данных в процессе связи транспортных средств с различными объектами (V2X)

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	X.1000-X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	X.1100-X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200-X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	X.1300-X.1499
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.1350-X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	**X.1370-X.1399**
Безопасность технологии распределенного реестра (DLT)	X.1400-X.1429
Безопасность приложений (2)	X.1450-X.1459
Безопасность веб-среды (2)	X.1470-X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500-X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600-X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700-X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750-X.1799
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800-X.1819

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

Рекомендация МСЭ-Т X.1383

Требования безопасности для категоризованных данных в процессе связи транспортных средств с различными объектами (V2X)

Резюме

Обеспечение безопасности данных – один из важнейших вопросов организации связи транспортных средств с различными объектами (V2X). Однако система защиты данных в среде с ограниченными ресурсами, такой как платформа бортовой связи в транспортных средствах, потребляет слишком много ресурсов, поскольку для нее требуются криптографические функции.

В Рекомендации МСЭ-Т X.1383 данные, используемые в процессе связи V2X, делятся на ряд категорий, таких как данные о свойствах объектов, данные о состоянии транспортного средства, данные о восприятии окружающей среды, данные управления транспортным средством, данные приложений и персональные данные потребителя, и этим категориям данных присвоены три уровня безопасности. На основе этих категорий данных и присвоенных им уровней безопасности в настоящей Рекомендации представлены требования безопасности для категоризованных данных в процессе связи V2X.

Хронологическая справка *

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1383	03.03.2023 г.	17-я	11.1002/1000/15108

Ключевые слова

Категоризованные данные, безопасность данных, связь V2X.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL https://handle.itu.int/ после которого укажите уникальный идентификатор Рекомендации.

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 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

Рекомендация МСЭ-Т X.1383

Требования безопасности для категоризованных данных в процессе связи транспортных средств с различными объектами (V2X)

1 Сфера применения

В настоящей Рекомендации данные, используемые в процессе связи транспортных средств с различными объектами (V2X), подразделяются на ряд категорий; для каждой категории данных определяется уровень безопасности. На основе этих категорий данных и присвоенных им уровней безопасности в настоящей Рекомендации представлены требования безопасности для категоризованных данных в процессе связи V2X.

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.

[ITU-T X.1641] Рекомендация МСЭ-Т X.1641 (2016 г.), *Руководящие указания по безопасности данных потребителей облачных услуг.*

[ITU-T X.1603] Рекомендация МСЭ-Т X.1603 (2018 г.), *Требования к безопасности данных для услуги мониторинга облачных вычислений.*

[ITU-T X.1372] Рекомендация МСЭ-Т X.1372 (2020 г.), *Руководящие указания по безопасности систем связи транспортного средства с различными объектами (V2X).*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 десенсибилизация данных (data desensitization) [b-ITU-T X.1217]: Процесс сокрытия конфиденциальных данных.

3.1.2 жизненный цикл данных (data lifecycle) [b-ITU-T X.1751]: Весь жизненный процесс данных после их создания, включая сбор данных, их передачу, хранение, использование (в том числе анализ и визуализацию), обмен данными и их уничтожение.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ABS	Anti-skid Braking System	Противоскользящая тормозная система
BSM	Basic Safety Message	Базовое сообщение безопасности
CAM	Cooperative Awareness Message	Сообщение совместной осведомленности
DoS	Denial of Service	Отказ в обслуживании
GDPR	General Data Protection Regulation	Общий регламент по защите персональных данных

ICV	Intelligent Connected Vehicle	Интеллектуальное соединенное транспортное средство
TLS	Transport Layer Security	Безопасность транспортного уровня
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 между транспортными средствами
V2X	Vehicle-to-Everything	Связь транспортного средства с различными объектами

5 Соглашения

В настоящей Рекомендации приняты следующие соглашения:

ключевое слово "**требуется**" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящему документу;

ключевое слово "**следует**" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом, для заявления о соответствии это требование не является обязательным;

ключевое слова "**может"** означает необязательное требование, которое допустимо, но не имеет какого бы то ни было рекомендательного значения;

ключевые слова "**не должен**" или "**запрещается**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

6 Жизненный цикл данных в процессе связи V2X

6.1 Жизненный цикл данных

Жизненный цикл данных определяется на основе потока данных в соответствующих подразделениях организации в системе связи транспортного средства с различными объектами (V2X). Основываясь на реальной ситуации в области связи V2X, жизненный цикл данных по безопасности можно считать аналогичным представленному в [ITU-T X.1641] и состоящим из описанных ниже этапов сбора, передачи, хранения, использования, перемещения, уничтожения и резервного копирования и восстановления данных.

- **Сбор данных** – процесс создания новых данных во внутренней системе организации и получения данных извне. В системах связи V2X применяются две формы сбора данных: создание данных в ходе различных рабочих процессов связи V2X и сбор данных от соответствующих потребителей, партнеров и других третьих сторон.
- **Передача данных** – процесс передачи данных от одного объекта к другому внутри организации. В процессе связи V2X передача данных главным образом включает в себя организацию потока данных между системами и оборудованием, относящимся к услугам связи V2X.
- **Хранение данных** – процесс физического или облачного хранения данных в любом цифровом формате. Этот этап обычно почти совпадает по времени с этапом сбора данных.
- **Использование данных** – последовательность действий организации с динамическими данными в процессе связи V2X, таких как запрос, анализ и обработка данных. На этом этапе осуществляется обновление данных и создание новых данных.

– **Перемещение данных** – процесс передачи данных внешним сторонам. В него входят отображение данных и их предоставление потребителям услуг связи V2X. Он также включает в себя процесс обмена данными между предприятиями и учреждениями, сотрудничающими в области связи V2X.

– **Уничтожение данных** – процесс, выполняемый с помощью физических или технических средств, в результате которого данные становятся постоянно или временно недоступными. Уничтожение данных может производиться как из соображений экономии, так и из-за внешних требований соответствия или бизнес-требований. В частности, при наличии соответствующих правил хранения данных следует учитывать, что поставщики услуг должны надлежащим образом стирать или анонимизировать собранные данные, для которых истек срок хранения или на хранение которых потребители больше не дают согласия, так чтобы их было невозможно восстановить.

– **Резервное копирование и восстановление данных** – процесс копирования всех или части данных на другие носители для предотвращения потери данных и восстановления исходных данных с помощью резервной копии в случае потери данных.

6.2 Анализ угроз

Данные, участвующие в процессе связи V2X, также подвержены угрозам и проблемам безопасности, аналогичным тем, какие определены в [ITU-T X.1603] и [ITU-T X.1641]. Некоторые из этих угроз и проблем безопасности, возникающих в процессе связи V2X, представлены в таблице 6-1.

Таблица 6-1 – Угрозы и проблемы в течение жизненного цикла данных в процессе связи V2X

Жизненный цикл данных	Угрозы и проблемы безопасности
Сбор данных	a) Несанкционированный сбор данных b) Уязвимости интерфейса сбора данных c) Спуфинг d) Взлом и перехват e) Незащищенный доступ к услуге f) Несанкционированный административный доступ
Передача данных	a) Перехват b) Подлог c) Прослушивание d) Несанкционированный доступ e) Атака типа отказ в обслуживании (DoS)
Хранение данных	a) Потеря и утечка данных b) Неготовность услуги
Использование данных	a) Неправомерное использование данных b) Внутренние угрозы c) Уязвимости системы d) Прослушивание
Перемещение данных	a) Неправомерное использование данных b) Уязвимости системы c) Искажение данных d) DoS-атака
Уничтожение данных	a) Спуфинг b) Уязвимости системы
Резервное копирование и восстановление данных	a) Уязвимости системы

7 Категоризованные данные в процессе связи V2X

В этом разделе представлена политика в отношении категоризации данных, участвующих в процессе связи V2X. В разделе 7.2 описаны шесть категорий данных: данные о свойствах объектов, данные о состоянии транспортного средства, данные о восприятии окружающей среды, данные управления транспортным средством, данные приложений и персональные данные потребителя.

7.1 Идентификация данных на основе сценариев связи V2X

Данные, участвующие в процессе связи V2X, могут различаться в зависимости от фактического сценария связи. В [ITU-T X.1372] сценарии связи V2X классифицируются следующим образом: связь транспортного средства с транспортным средством (V2V), связь транспортного средства с инфраструктурой (V2I), связь транспортного средства с перемещаемым устройством (V2D) и связь транспортного средства с пешеходом (V2P). В этом разделе описываются соответствующие процессы связи и данные для каждого сценария связи.

7.1.1 Данные в процессе связи V2V

В [ITU-T X.1372] определены три сценария связи V2V: распространение предупреждений по каналам связи V2V, групповая связь V2V и сигнализация по каналам связи V2V. В сценарии распространения предупреждений V2V предупредительные сообщения передаются от одного транспортного средства к другому. В сценарии групповой связи V2V группы транспортных средств обмениваются друг с другом информацией о состоянии транспортного средства. В сценарии сигнализации по каналам связи V2V каждое транспортное средство передает информацию о своем состоянии. Данные, участвующие в процессе связи V2V, приведены в таблице 7-1.

Таблица 7-1 – Данные, участвующие в процессе связи V2V

Категория	Сценарий	Данные
Связь между транспортными средствами	Распространение предупреждений по каналам связи V2V	• Предупредительные сообщения • Базовые сообщения безопасности (BSM) • Сообщения совместной осведомленности (CAM)
	Групповая связь V2V	• BSM • CAM
	Сигнализация по каналам связи V2V	• BSM • CAM

Технические характеристики BSM и CAM описаны соответственно в [b-SAE J2735] и [b-ETSI TS 102 637-2].

7.1.2 Данные в процессе связи V2I

В [ITU-T X.1372] определены два сценария связи V2I: предупреждение по каналам связи V2I и обмен информацией по каналам связи V2I. Сценарий предупреждений по каналам связи V2I позволяет транспортным средствам обмениваться предупредительными сообщениями с инфраструктурой. При обмене информацией по каналам связи V2I транспортное средство и инфраструктура взаимодействуют друг с другом, обновляя сведения о дорожном движении и/или информацию, относящуюся к информационно-развлекательным услугам. Данные, участвующие в процессе связи V2I, приведены в таблице 7-2.

Таблица 7-2 – Данные, участвующие в процессе связи V2I

Категория	Сценарий	Данные
Связь между транспортным средством и инфраструктурой	Распространение предупреждений по каналам связи V2I	• Предупредительные сообщения
	Обмен информацией по каналам связи V2I	• Бортовая система отображения дорожных знаков • Бортовая система отображения информации • Сигналы светофора • Информация о времени переключения светофора • Состояние дорожного покрытия • Метеоусловия • Условия видимости • Информация о ремонте дороги

7.1.3 Данные в процессе связи V2D

В сценарии связи V2D транспортное средство взаимодействует с перемещаемыми устройствами, такими как смартфоны, ноутбуки и бортовая система навигации. В [ITU-T X.1372] определены два сценария связи V2D: связь V2D по непрямым каналам и связь V2D по прямым каналам. Разница между этими сценариями заключается в способе связи, и в обоих случаях участвуют данные одного и того же типа. В [ITU-T X.1372] связь V2P рассматривается как частный случай связи V2D. Данные, участвующие в процессе связи V2D, приведены в таблице 7-3.

Таблица 7-3 – Данные, участвующие в процессе связи V2D

Категория	Сценарий	Данные
Связь транспортного средства с перемещаемым устройством	Связь V2D по прямым/непрямым каналам	• Данные об аппаратном обеспечении транспортного средства • Данные о программном обеспечении транспортного средства • Данные об аппаратном обеспечении устройства • Данные о программном обеспечении устройства • Данные о платформе услуг • Данные приложений

7.2 Категоризация данных

В этом разделе содержится описание категоризации данных в отношении данных, участвующих в процессе связи V2X.

На данные V2X-сообщения распространяются законы и положения о защите персональных данных, такие как Общий регламент по защите персональных данных (GDPR), и данные, описанные в этой Рекомендации, не могут указывать на информацию о конкретном или идентифицируемом физическом лице.

7.2.1 Данные о свойствах объектов

Данные о свойствах объектов относятся к свойствам объектов, участвующих в процессе связи V2X, которые можно разделить на три типа: свойства транспортных средств, свойства мобильных устройств и свойства платформ облачных услуг.

– Данные о свойствах транспортных средств относятся к характеристикам транспортных средств, таким как марка, тип, логотип или цвет.

– Данные о свойствах мобильных устройств относятся к характеристикам мобильных устройств, таким как марка, тип или цвет.

– Данные о свойствах платформы услуг относятся к характеристикам платформы услуг, таким как версия, производитель и т. д.

7.2.2 Данные о состоянии транспортного средства

Данные о состоянии транспортного средства относятся к состоянию транспортных средств и тесно связаны с информационной службой в системе связи V2X. К ним относятся данные о рабочем состоянии и параметрах систем, таких как система автомобильной трансмиссии, система шасси, система безопасности транспортного средства, система кузова, система комфорта и электрическая система транспортного средства.

В частности, к данным о состоянии транспортного средства относятся данные, поступающие от контроллера транспортного средства (например, сигнал управления насосом, аварийный сигнал датчика давления воздуха, электрический сигнал торможения двигателя и т. д.), системы трансмиссии (например, крутящий момент, расход топлива и т. д.), системы охлаждения (например, температура охлаждающей жидкости), системы коробки передач (например, данные о начале движения, ускорении и т. д.), системы безопасности (например, данные о состоянии подушки безопасности, использовании ремня безопасности и т. д.), системы шасси (например, данные, отражающие состояние бортовой сети или системы рулевого управления, параметры торможения с использованием ABS, сигналы контроля давления в шинах и т. д.), системы комфорта (например, данные об открытии заслонок кондиционера воздуха, регулировке положения сидений, системе управления окнами, использовании освещения и т. д.) и других вспомогательных систем.

Основываясь на описании рабочих состояний транспортного средства, данные о состоянии транспортного средства можно разделить на два типа: динамические данные о состоянии транспортного средства и статические данные о состоянии транспортного средства.

– Динамические данные о состоянии транспортного средства связаны с рабочими состояниями систем транспортного средства. В качестве примера можно привести систему кондиционирования воздуха, которая зависит от температуры и относительной влажности воздуха внутри транспортного средства.

– Статические данные о состоянии транспортного относятся к статическим состояниям системы кондиционирования воздуха, таким как использование ремня безопасности, включение системы кондиционирования и т. д.

7.2.3 Данные о восприятии окружающей среды

Данные о восприятии окружающей среды связаны главным образом с внешней средой, в которой находится транспортное средство, и включают в себя информацию о внешнем оборудовании, терминалах, пешеходах, а также информацию о соединениях транспортного средства и о взаимодействиях информационных служб в процессе связи V2X, в том числе, помимо прочего, информацию о скорости, сигналах светофоров и дорожной инфраструктуре в процессе связи между транспортными средствами. К данным об окружающей среде также относится собираемая радарами скорости и видеокамерами информация о дорожной инфраструктуре, направлении движения, состоянии движения, скорости и расстоянии; возможные соответствующие статические данные о наличии столкновения; а также информация о зарядных станциях ("столбах") и другом оборудовании, собираемая для электромобилей.

7.2.4 Данные управления транспортным средством

Данные управления транспортным средством относятся к управлению транспортным средством в процессе связи V2X и обычно включают в себя три подтипа: данные управления транспортным средством для автоматического вождения/интеллектуальной системы помощи при вождении, дистанционного управления и дистанционного вождения.

– Данные управления транспортным средством для автоматического вождения/интеллектуальной системы помощи при вождении – это данные команд, связанных с автоматическим вождением или вождением с помощью искусственного интеллекта. Эти данные основаны на обработке данных о восприятии окружающей среды и интеллектуальных систем принятия решений и используются для интеллектуального управления поведением

транспортного средства посредством системы электронного торможения и вождения, автоматической коробки передач, встроенной системы управления шасси и др.

– Данные управления транспортным средством для дистанционного управления относятся к командам управления транспортным средством с помощью приложений, платформ услуг и т. д. и включают в себя данные по дистанционному управлению запиранием/отпиранием дверей, системой кондиционирования воздуха, окнами и освещением и т. д.

– Данные управления транспортным средством для дистанционного вождения, в рамках которых сценарий использования дистанционного вождения подразделяется на несколько вариантов путем проведения различия между человеком в качестве дистанционного водителя и облаком в качестве возможного дистанционного водителя. Данные управления транспортным средством для дистанционного вождения относятся к внешним видеопотокам, показывающим ситуацию на полосе движения вокруг транспортного средства, или внешним аудиопотокам, передаваемым дистанционному водителю для поддержки принимаемых им решений. Помимо этого, данные для дистанционного вождения могут относится к внутреннему видео- или аудиопотоку, передаваемому дистанционному водителю для отслеживания ситуации. Кроме того, данные управления транспортным средством для дистанционного вождения относятся к данным команд дистанционного управления от дистанционного водителя к транспортному средству, например инструкций по ускорению или маневрированию, которые могут быть генерированы и отправлены при срабатывании соответствующего события, например инструкция по торможению [b-ETSI TR 126 985], [b-3GPP TR 22.886].

7.2.5 Данные приложений

Данные приложений относятся к обмену информацией приложений в процессе связи V2X. Это данные, относящиеся к информационным услугам в процессе связи V2X, помимо информации о свойствах объектов, состоянии транспортного средства и восприятии окружающей среды, данных управления транспортным средством и персональных данных потребителя. Они включают, в частности, данные информационно-развлекательной системы, данные систем управления и контроля безопасности дорожного движения, данные по обслуживанию транспортного средства и т. д.

– Данные информационно-развлекательной системы относятся к развлекательным услугам, предоставляемым в процессе связи V2X, таким как загрузка мультимедиа, просмотр веб-сайтов и подписка на передачи для определенных групп населения, а также прогноз погоды и т. д.

– Данные систем управления и контроля безопасности дорожного движения относятся к системам обеспечения безопасности дорожного движения и управления дорожным движением, таким как механизм раннего предупреждения системы обеспечения безопасности дорожного движения, аварийно-спасательная служба, система дистанционного контроля и управления транспортными средствами и т. д.

– Данные по обслуживанию транспортного средства – это информация, связанная с послепродажными услугами в процессе связи V2X, такими как техническое обслуживание транспортного средства, обращение с подержанным транспортным средством, финансовое страхование и соответствующие услуги электронной коммерции. Например, к данным по обслуживанию транспортного средства относится периодичность технического обслуживания определенных типов деталей автомобилей определенной марки.

7.2.6 Персональные данные потребителя

Персональные данные потребителя – это личная информация, относящаяся к потребителю, которая используется и/или генерируется в процессе связи V2X. Классификация и защита персональных данных потребителя в этом разделе не рассматривается.

Если данные, приведенные в качестве примера в таблице 7-4, соответствуют определению персональных данных потребителя, содержащемуся в законах и положениях о неприкосновенности частной жизни, таких как Общий регламент по защите персональных данных (GDPR), то подход к категоризации определяется этими положениями.

7.3 Уровни безопасности данных

Основываясь на анализе с учетом целей обеспечения безопасности данных, степени важности данных и последствий возможных событий, связанных с безопасностью, данные каждой категории можно разделить на три уровня:

– **уровень 1** (наименее защищенные данные) включает общедоступные данные, участвующие в процессе связи V2X, такие как версия программного обеспечения платформы V2X;

– **уровень 2** (умеренно защищенные данные) включает данные, которые необходимо защищать с помощью определенных мер безопасности, такие как данные о транспортном средстве, полученные в процессе связи V2V, учетная запись и пароль в системе связи V2X;

– **уровень 3** (надежно защищенные данные) включает данные, требующие более надежной защиты в процессе связи V2X, чем данные уровня 2 (умеренно защищенные данные), такие как информация о финансовых транзакциях в процессе связи V2D, данные о важнейших характеристиках транспортного средства и информация, позволяющая установить личность в процессе связи V2X.

К конфиденциальным данным относятся только конфиденциальные данные предприятий, участвующих в процессе связи V2X; персональная информация потребителя здесь не рассматривается.

В таблице 7-4 представлены подробные сведения об уровнях безопасности данных и примеры, относящиеся к связи V2X.

Таблица 7-4 – Примеры уровней безопасности данных в процессе связи V2X

Категория данных, участвующих в процессе связи V2X		**Уровень безопасности данных, участвующих в процессе связи V2X**	**Примеры**
Данные о свойствах объектов	Данные о свойствах транспортного средства	Уровень 1	Марка, тип, логотип, цвет автомобиля.
		Уровень 2	Эксплуатационные характеристики транспортного средства определенного типа.
		Уровень 3	Конкретные характеристики конфигурации аппаратного и программного обеспечения транспортного средства определенного типа.
	Данные о свойствах мобильного устройства	Уровень 1	Марка, тип, логотип, цвет мобильного терминала.
		Уровень 2	Данные о состоянии оборудования, относящиеся к некоторым важным функциям связи V2X.
		Уровень 3	Важнейшие характеристики и информация о конфигурации мобильного устройства.
	Данные о свойствах платформы облачных услуг	Уровень 1	Тип и наименование платформы облачных услуг.
		Уровень 2	Информация об аппаратном обеспечении, операционной системе и прикладном ПО.
		Уровень 3	Важнейшие характеристики и информация о конфигурации платформы услуг.
Данные о состоянии транспортного средства	Динамические данные о состоянии транспортного средства	Уровень 1	Состояние системы кондиционирования воздуха. Температура внутри транспортного средства.
		Уровень 2	Рабочее состояние подушки безопасности и ремней безопасности и т. д. Данные, получаемые от внутренних датчиков транспортного средства и тесно связанные с важными параметрами управления транспортным средством, такими как давление в шинах.

Таблица 7-4 – Примеры уровней безопасности данных в процессе связи V2X

Категория данных, участвующих в процессе связи V2X		**Уровень безопасности данных, участвующих в процессе связи V2X**	**Примеры**
		Уровень 3	Основные ходовые технические показатели транспортного средства. Данные, получаемые от внутренних датчиков транспортного средства и тесно связанные с важнейшими функциями управления транспортным средством, например данные от датчиков столкновения.
	Статические данные о состоянии транспортного средства	Уровень 1	Периодичность использования системы кондиционирования воздуха в определенное время.
		Уровень 2	Средний расход топлива автомобиля.
		Уровень 3	Конфиденциальные данные систем автомобиля.
Данные о восприятии окружающей среды	Данные о восприятии окружающей среды транспортным средством	Уровень 1	Тип дороги (шоссе, проселочная дорога или тротуар), состояние дорожного покрытия (неповрежденное, мокрое или скользкое), ограничение скорости на дороге, информация о расположении и состоянии светофоров, загруженности дорог, дорожно-транспортных происшествиях и т. д.
		Уровень 2	В сценарии связи между транспортными средствами – данные после десенсибилизации о соседних транспортных средствах, такие как физическое местоположение, географические координаты, время обновления данных, скорость движения, направление движения, информация о смене полосы движения. В сценарии связи транспортного средства с пешеходом – данные после десенсибилизации, такие как местоположение, расстояние, скорость и характер движения приближающихся пешеходов, а также вероятность столкновения.
		Уровень 3	В сценариях связи между транспортными средствами – данные о соседних транспортных средствах за определенный период времени после десенсибилизации, такие как маршрут движения, местоположение, время, информация о парковке и т. д.
Данные управления транспортным средством	Данные управления транспортным средством для автоматического вождения/интеллектуальной системы помощи при вождении	Уровень 1	Звуковые сигналы подсказки при движении задним ходом.
		Уровень 2	Когда транспортное средство имеет тенденцию отклоняться от заданной полосы движения, функция удержания на полосе движения интеллектуальной системы помощи при вождении подает предупредительный сигнал, такой как дрожание рулевого колеса и сигнал красного или зеленого светового индикатора на приборной панели.
		Уровень 3	Инструкции на подтверждение от интеллектуальной системы парковки при автоматической парковке.

Таблица 7-4 – Примеры уровней безопасности данных в процессе связи V2X

Категория данных, участвующих в процессе связи V2X		**Уровень безопасности данных, участвующих в процессе связи V2X**	**Примеры**
	Данные управления транспортным средством для дистанционного управления	Уровень 1	Обычные данные, относящиеся к удаленному мониторингу в процессе связи V2X.
		Уровень 2	Инструкция на дистанционное трогание с места или запуск системы рулевого управления автомобиля.
		Уровень 3	Выполнение инструкций, относящихся к дистанционному управлению несколькими транспортными средствами, например автоколонной, через платформу связи V2X.
	Данные управления транспортным средством для дистанционного вождения	Уровень 1	Для мониторинга состояния внутри транспортного средства дистанционный водитель может использовать внутренние видео- и аудиопотоки, требования к задержке которых более мягкие, чем к внешним видео- и аудиопотокам.
		Уровень 2	Внешние аудиопотоки могут доставляться дистанционному водителю для передачи информации о шумах от других транспортных средств и звуков их клаксонов.
		Уровень 3	Датчики или воспроизводящие устройства, такие как экран или звуковая система, используются для получения инструкций маневрирования от дистанционного водителя. Инструкции должны предоставляться с высокой надежностью и малой задержкой, а также требовать подтверждения, особенно при возникновении аварийного события (например, инструкций по торможению). Данные видеодатчика (камеры) и аудиодатчика (микрофона) (также возможны данные радара или лидара), фиксирующие внешние звуки и изображения для ранней и невизуальной идентификации препятствий на трассе, например машин скорой помощи, пешеходов и т. д. Данные датчика состояния транспортного средства (ускорение, скорость, направление движения, местоположение и т. д.) могут передаваться от транспортного средства к дистанционному водителю с фиксированным интервалом и высокой надежностью, поскольку некоторые потоки данных, передаваемых датчиками, могут быть необходимы для правильного управления транспортным средством.
Данные приложений	Данные информационно-развлекательной системы	Уровень 1	Данные по радиовещанию
		Уровень 2	Просмотр записей об онлайн-покупках после десенсибилизации
		Уровень 3	Голосовые и видеозаписи после десенсибилизации в информационных приложениях
	Данные систем управления и контроля безопасности дорожного движения	Уровень 1	Предупреждения о пробках на дорогах, предупреждения о дорожно-транспортных происшествиях в режиме реального времени и т. д.

Таблица 7-4 – Примеры уровней безопасности данных в процессе связи V2X

<table>
<tr><th colspan="2">Категория данных, участвующих в процессе связи V2X</th><th>Уровень безопасности данных, участвующих в процессе связи V2X</th><th>Примеры</th></tr>
<tr><td rowspan="5"></td><td rowspan="2"></td><td>Уровень 2</td><td>Предупреждения о возможном столкновении при остановке впередиидущего транспортного средства в транспортном потоке.</td></tr>
<tr><td>Уровень 3</td><td>Данные дистанционного контроля транспортных средств в процессе дорожного движения.</td></tr>
<tr><td rowspan="3">Данные по обслуживанию транспортного средства</td><td>Уровень 1</td><td>После десенсибилизации записываются данные по использованию и эксплуатации развлекательной системы транспортного средства и другие связанные с ней данные.</td></tr>
<tr><td>Уровень 2</td><td>После десенсибилизации – данные о поведении транспортного средства, связанные с его управляемостью.</td></tr>
<tr><td>Уровень 3</td><td>Данные после десенсибилизации, такие как личные предпочтения и поведенческие привычки владельца транспортного средства, относящиеся к длительности поездок, маршрутам и местоположению, а также поведенческие данные по использованию информационно-развлекательной системы или основные характеристики транспортного средства, основанные на данных о восприятии им своего собственного состояния и состояния окружающей среды, и т. д.</td></tr>
<tr><td>Персональные данные потребителя</td><td>Н/П</td><td>Н/П</td><td>Н/П</td></tr>
<tr><td colspan="4">Пояснения к таблице 7-4:
1) Н/П – неприменимо.
2) Указание в таблице 7-4 на данные после десенсибилизации означает, что после обработки анонимизатором и другими техническими средствами эти данные не позволяют прямо или косвенно установить личность и не указывают на персональную информацию физических лиц. К методам десенсибилизации данных, помимо прочего, относятся анонимизация, деидентификация, внесение разнообразия, исключение, искажение, дифференцированное засекречивание и т. д. Организации, участвующей в процессе связи V2X, следует принять соответствующие меры по десенсибилизации данных, основанные на всестороннем рассмотрении характеристик субъекта данных, уровня конфиденциальности данных и требований к работе с данными.</td></tr>
</table>

8 Требования безопасности

В этом разделе представлены требования безопасности базового, среднего и высокого уровней в строгом соответствии с уровнями безопасности данных 1–3.

8.1 Уровень требований безопасности

На основе классификации категоризованных данных для каждого уровня безопасности указываются методы или меры обеспечения безопасности. Существует три возможных уровня требований безопасности: базовый, средний и высокий. Требования безопасности базового уровня, как правило, используются для уровня защиты 1 (наименее защищенные данные), среднего – для уровня защиты 2 (умеренно защищенные данные), а высокого – для уровня защиты 3 (надежно защищенные данные). В таблице 8-1 описываются требования безопасности в зависимости от уровня безопасности данных в системе связи V2X.

Предприятия также могут выбирать меры безопасности в соответствии со своими условиями или степенью конфиденциальности данных.

Таблица 8-1 – Требования безопасности в зависимости от уровня безопасности данных в системе связи V2X

Уровень безопасности данных в системе связи V2X	Уровень требований безопасности		
	Базовый	**Средний**	**Высокий**
Уровень 1 (наименее защищенные данные)	*	Н/П	Н/П
Уровень 2 (умеренно защищенные данные)	*	*	Н/П
Уровень 3 (надежно защищенные данные)	*	*	*
* – охватывает Н/П – неприменимо			

8.2 Требования безопасности базового уровня

1) Сбор данных

- Данные в системе связи V2X следует классифицировать в зависимости от сочетания целей защиты данных, степени важности данных и последствий возможных событий, связанных с безопасностью.
- В процессе сбора данных следует соблюдать принцип минимизации. Можно собирать только данные, относящиеся к производственной деятельности.
- Собранные данные следует классифицировать и администрировать в соответствии с классификацией данных и методами классификации, описанными в разделах 6 и 7. Для данных разных уровней следует сформулировать и реализовать разные меры защиты.

2) Передача данных

- Общие требования безопасности при передаче данных в системах связи V2X не должны быть ниже, чем в обычной сети связи.
- Следует принять разные стратегии и меры безопасности при передаче данных в зависимости от категории данных, технологического процесса и риска безопасности в сценариях связи V2X.
- Для обеспечения безопасности при передаче данных в сценариях связи транспортного средства с разными объектами следует использовать такие протоколы безопасности, как безопасность транспортного уровня (TLS).
- Следует обеспечивать возможность обнаружения искажения данных в процессе передачи.

3) Хранение данных

- Следует обеспечить, чтобы в оборудовании и системах связи V2X присутствовали механизмы шифрования данных, хранящихся в терминалах и на платформах услуг транспортных средств. В разных вариантах конфигурации следует обеспечить поддержку таких параметров, как алгоритм, надежность и режим шифрования.
- Следует предусмотреть, чтобы платформы услуг и системы транспортного средства обеспечивали безопасность кешированных данных. Следует шифровать данные, хранящиеся в системе кеширования.
- Для предотвращения несанкционированного доступа, модификации и удаления информации, а также междоменного доступа следует применять механизмы управления доступом к данным, хранящимся в терминалах и на платформах услуг транспортных средств.
- Следует обеспечить возможность проверки целостности данных в процессе хранения во избежание фальсификации, удаления и вставки данных. В случае нарушения целостности данных следует подавать пользователю предупредительный сигнал.

4) Использование данных

- Данные следует обрабатывать в рамках полученного разрешения в объеме, ограниченном минимальным кругом производственных потребностей.
- Следует получить и проверить разрешение на использование данных.
- Следует обеспечить, чтобы цель и объем использования данных удовлетворяли требованиям соответствующих государственных законов и положений.
- В ходе анализа и извлечения данных следует обеспечить, чтобы исходные данные и результаты анализа данных были подписаны для предотвращения злонамеренного удаления, подлога или злоупотребления.
- Следует принять административные и технические меры для обеспечения безопасности при передаче или экспорте данных между устройствами, системами и платформами интернета транспортных средств.

5) Перемещение данных

- Перед перемещением данных следует провести оценку средств безопасности, чтобы гарантировать безопасное перемещение данных.
- При перемещении данных между различными устройствами следует обеспечить непрерывность производственных процессов и работы приложений.
- В ходе подготовки к перемещению данных следует составить схему перемещения, оценить ее достоинства и недостатки и возникающие риски, а затем разработать соответствующие меры по управлению рисками.

6) Уничтожение данных

- Следует выбрать стратегию уничтожения данных и систему управления, чтобы определить объекты и конкретизировать процесс уничтожения. Следует установить механизм проверки и утверждения операций уничтожения данных, а также учредить соответствующий надзорный орган для контроля за процессом уничтожения.
- Следует предусмотреть меры для удаления данных при наступлении предельного срока их хранения, и когда пользователи больше не дают согласия на обработку своих данных, эти данные следует немедленно уничтожать.
- Следует предусмотреть меры, помогающие очистить данные, оставшиеся после перемещения данных или производственного процесса.
- Следует предусмотреть меры по удалению всех копий резервной копии данных.

7) Резервное копирование и восстановление данных

- Перед перемещением данных следует создать механизмы резервного копирования и восстановления данных.
- Следует производить локальное резервное копирование и восстановление данных.
- Следует установить механизм регулярного полного резервного копирования данных, причем рекомендуемый временной интервал должен составлять не менее одного раза в неделю.
- Следует обеспечить, чтобы права доступа и требования к безопасному хранению резервных копий данных были такими же, как и для оригинальных данных.

8.3 Требования безопасности среднего уровня

Требования безопасности среднего уровня представляют собой набор дополнений к базовым требованиям безопасности. На каждом этапе жизненного цикла данных к базовым требованиям безопасности добавляются следующие требования.

1) Сбор данных

В дополнение к базовым требованиям безопасности следует также выполнять нижеперечисленные требования:

- во время сбора данных уровня 2 следует создать резервную копию оригинальных данных во избежание пропуска и потери данных;

- следует применять механизмы идентификации для обеспечения достоверности при сборе данных;
- следует применять механизмы проверки данных для обеспечения целостности при сборе данных.

2) Передача данных

В дополнение к базовым требованиям безопасности следует также выполнять нижеперечисленные требования:

- при передаче данных посредством основной платформы услуг для транспортных средств и интернета транспортных средств следует использовать частную сеть или виртуальную частную сеть для изоляции от интернета;
- при использовании связи V2V/V2I необходимо наличие авторитетного удостоверяющего сертификата, подтверждающего подлинность узла передачи данных, и в данных аутентификации не должна раскрываться конфиденциальная информация;
- следует обеспечить, чтобы транспортное средство могло выявлять незаконные запросы на установление соединений из сотовых сетей, с тем чтобы отфильтровывать вредоносные пакеты;
- следует проверять надежность источников данных уровня 2, таких как данные команд дистанционного управления, чтобы гарантировать невозможность подлога.

3) Хранение данных

В дополнение к базовым требованиям безопасности следует также выполнять нижеперечисленные требования:

- следует обеспечить возможность проверки целостности данных в процессе хранения для предотвращения фальсификации, удаления и вставки данных; следует предусмотреть необходимые средства восстановления в тех случаях, когда целостность данных нарушена;
- следует снабдить файлы данных, хранящиеся в интеллектуальном соединенном транспортном средстве (ICV), на платформах услуг и в приложениях, идентификационной информацией во избежание использования таких файлов в неавторизованных устройствах и системах;
- следует хранить специальные операционные записи для защиты кешированных данных уровня 2 в процессе связи V2X в системе кеширования платформы услуг;
- для предотвращения угроз, связанных с отказом от авторства, следует наладить целостный процесс управления журналом регистрации данных.

4) Использование данных

В дополнение к базовым требованиям безопасности следует также выполнять нижеперечисленные требования:

- при запросах данных уровня 2 следует выполнять такие операции, как запрос, внешнее отображение, статистическая обработка, обработка нечеткой информации;
- следует проверить характер использования данных уровня 2 и создать контрольный журнал.

5) Перемещение данных

В дополнение к базовым требованиям безопасности следует также выполнять нижеперечисленные требования:

- для подготовки к перемещению данных следует составить схему перемещения, оценить ее достоинства и недостатки и возникающие риски, а затем разработать соответствующие меры по управлению рисками.

6) Уничтожение данных

В дополнение к базовым требованиям безопасности следует также выполнять нижеперечисленные требования:

- следует гарантировать, что пространство хранения ресурсов, относящихся к системе связи V2X, таких как файлы, каталоги и записи базы данных, не будет высвобождено или перераспределено другим пользователям до полного удаления этих ресурсов;
- во избежание утечки данных через бортовой терминал в результате замены компонентов транспортного средства следует предусмотреть функцию стирания данных бортового терминала, гарантирующую невозможность восстановления стертых данных.

7) Резервное копирование и восстановление данных

В дополнение к базовым требованиям безопасности следует также выполнять нижеперечисленные требования:

- при локальном или удаленном резервном копировании данных следует не реже одного раза в неделю создавать полные резервные копии и не реже одного раза в день – добавочные резервные копии. Кроме того, следует создать механизм многократного резервного копирования;
- резервные копии данных следует хранить в зашифрованном виде.

8.4 Требования безопасности высокого уровня

Требования безопасности высокого уровня представляют собой набор дополнений к требованиям безопасности среднего уровня. На каждом этапе жизненного цикла данных следует применять все перечисленные ниже требования безопасности.

1) Сбор данных

- Требования к защите данных аналогичны требованиям безопасности среднего уровня.

2) Передача данных

В дополнение к требованиям безопасности среднего уровня следует также выполнять нижеперечисленные требования:

- следует обеспечить возможность выявления нарушений целостности данных во время передачи и принятия необходимых мер для восстановления данных;
- для конфиденциальных данных уровня 3 следует обеспечить взаимную аутентификацию, чтобы предотвратить возможность несанкционированного доступа и утечки данных в результате подмены идентичности внешних объектов.

3) Хранение данных

В дополнение к требованиям безопасности среднего уровня следует также выполнять нижеперечисленные требования:

- следует принять схему хранения данных с аппаратным шифрованием для обеспечения секретности конфиденциальных данных транспортных средств, платформ услуг, приложений интеллектуальных мобильных терминалов и придорожной инфраструктуры;
- следует обеспечивать возможность проверки целостности данных в процессе хранения для предотвращения фальсификации, удаления и вставки данных; следует предусмотреть необходимые средства восстановления в тех случаях, когда целостность данных нарушена.

4) Использование данных

В дополнение к требованиям безопасности среднего уровня следует также выполнять нижеперечисленные требования:

- следует осуществлять утверждение вторым должностным лицом в режиме коллективной авторизации;
- следует устранять корреляцию данных для предотвращения утечки данных в результате ассоциативного анализа данных различными системами, платформами или приложениями;
- следует поддерживать динамическую десенсибилизацию при использовании конфиденциальных данных.

5) Перемещение данных

Требования к защите данных аналогичны требованиям безопасности среднего уровня.

6) Уничтожение данных

В дополнение к требованиям безопасности среднего уровня следует также выполнять нижеперечисленные требования:

- следует предусмотреть средства для предотвращения возможности восстановления уничтоженных данных.

7) Резервное копирование и восстановление данных

В дополнение к требованиям безопасности среднего уровня следует также выполнять нижеперечисленные требования:

- следует обеспечить средства аутентификации, такие как аутентификация идентичности, чтобы операции локального и удаленного резервного копирования и восстановления данных могли выполняться только с ведома или под контролем авторизованных пользователей.

Библиография

[b-ITU-T X.1217] Рекомендация МСЭ-Т X.1217 (2021 г.), *Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи.*

[b-ITU-T X.1751] Рекомендация МСЭ-Т X.1751 (2020 г.), *Руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных операторами электросвязи.*

[b-3GPP TR 22.886] 3GPP TR 22.886 V16.2.0 (2018), *Study on enhancement of 3GPP Support for 5G V2X Services (Release 16).*

[b-ETSI TR 126 985] ETSI TR 126 985 V16.0.0 (2020), *5G Vehicle-to-everything (V2X) Media handling and interaction (3GPP TR 26.985 version 16.0.0 Release 16).*

[b-ETSI TS 102 637-2] ETSI TS 102 637-2 (2011), *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.*

[b-SAE J2735] *V2X Communications Message Set Dictionary*, (July 2020).

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, 2023 г.