ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1380 (03/2023)

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

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

Руководящие указания по обеспечению безопасности облачных регистраторов данных о событиях в автомобильной среде

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.1399**
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.1380

Руководящие указания по обеспечению безопасности облачных регистраторов данных о событиях в автомобильной среде

Резюме

Регистраторы данных о событиях (EDR) – один из важнейших компонентов, устанавливаемых на средствах автодорожного транспорта для записи состояния транспортного средства, его передвижений и действий водителя при аварии. Анализируя данные о событиях, можно определить причину аварии и впоследствии использовать эти знания для повышения безопасности в автомобильной среде. Еще одним важным компонентом, необходимым для записи данных, дающих четкое представление о взаимодействии между водителем и автоматизированной системой вождения, является система хранения данных для автоматизированного вождения. Однако обычные регистраторы данных о событиях записывают все данные и управляют ими локально, так что эти данные могут оказаться под угрозой потери или уничтожения.

Считается, что важную роль в обеспечении сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу играют облачные вычисления. Облачные услуги уже пытаются применять системах регистрации данных о событиях в таких отраслях промышленности, как авиастроение, для повышения безопасности в авиационной среде. В соответствии с текущей тенденцией к подключению транспортных средств к сети следует ожидать, что для повышения их безопасности будут внедряться EDR и системы хранения данных для автоматизированного вождения. Однако процессы сбора, передачи, хранения, администрирования и использования регистрируемых данных чреваты различными уязвимостями, связанными с особенностями автомобильной среды. И следовательно, эти уязвимости, а также требования безопасности и сценарии использования облачных регистраторов данных в автомобильной среде необходимо изучать.

В Рекомендации МСЭ-Т X.1380 представлены руководящие указания по безопасности облачных регистраторов данных в автомобильной среде. В ней содержится описание угроз, уязвимостей, требований безопасности и сценариев использования облачных регистраторов данных в автомобильной среде.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1380	03.02.2023 г.	17-я	11.1002/1000/15106

Ключевые слова

Облако, облачная DSSAD, облачный регистратор данных о событиях (EDR), регистраторы данных, DSSAD, EDR, требования безопасности, угрозы безопасности.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

На момент утверждения настоящей Рекомендации МСЭ 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.1380

Руководящие указания по обеспечению безопасности облачных регистраторов данных о событиях в автомобильной среде

1 Сфера применения

В настоящей Рекомендации содержатся руководящие указания по безопасности облачных регистраторов данных, таких как регистратор данных о событиях (EDR) и система хранения данных для автоматизированного вождения (DSSAD), в автомобильной среде. В настоящей Рекомендации рассматриваются технические аспекты систем регистрации данных, EDR и DSSAD. Кроме того, в этом проекте Рекомендации также содержатся требования безопасности и сценарии использования.

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.1371] Рекомендация МСЭ-Т X.1371 (2020 г.), *Угрозы безопасности для соединенных транспортных средств*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 аутентификация (authentication) [b-ITU-T X.1252]: Формализованный процесс проверки, при успешном прохождении которого идентичность объекта считается установленной.

3.1.2 автоматизированная система удержания полосы движения (automated lane keeping system) [b-UN R157]: Система, активируемая водителем и удерживающая транспортное средство в пределах своей полосы движения.

3.1.3 авторизация (authorization) [b-ITU-T X.800]: Предоставление прав, которое включает предоставление доступа на основании прав доступа.

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

3.1.5 аутентичность, подлинность (authenticity) [b-ITU-T X.641]: Защита в виде взаимной аутентификации и аутентификации источника данных.

3.1.6 подотчетность (accountability) [b-ITU-T X.800]: Свойство, гарантирующее возможность прослеживания действий какого-либо объекта с однозначной привязкой к этому объекту.

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 система хранения данных для автоматизированного вождения (data storage system for automated driving (DSSAD)) [b-UN R157]: Система, позволяющая определять взаимодействие между автоматизированными системами удержания полосы движения (ALKS) и водителем.

3.1.9 регистратор данных о событиях (event data recorder (EDR)) [b-UN R160]: Устройство или функция в транспортном средстве, регистрирующие динамику транспортного средства в форме временных рядов данных за промежуток времени непосредственно перед событием

(например, скорость транспортного средства в зависимости от времени) или во время аварийной ситуации (например, изменение характеристической скорости со временем), которые предназначены для извлечения после аварии. Для целей этого определения к данным о событиях не относят звуковые и видеоданные.

3.1.10 целостность данных (data integrity) [b-ITU-T X.800]: Показатель того, что данные не были изменены или разрушены несанкционированным способом.

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

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 облачный интерфейс (cloud interface): Шлюз облачной системы, представляющий собой интерфейс для связи между облачной системой и транспортными средствами, пользователями и третьими лицами.

3.2.2 главный диспетчер (general manager): Компонент облачной системы, который управляет основными процедурами хранения и извлечения данных регистраторов данных о событиях (EDR)/системы хранения данных для автоматизированного вождения (DSSAD), а также проводит проверку основных требований запросов, поступающих от пользователя, другого лица или транспортного средства.

3.2.3 нейтральный сервер (neutral server): Сервер, не зависящий от производителей транспортных средств, который может предоставлять анонимизированную информацию или информацию, позволяющую идентифицировать транспортное средство (VII), либо данные регистраторов данных о событиях (EDR)/системы хранения данных для автоматизированного вождения (DSSAD), из которых удалена информация, позволяющая идентифицировать транспортное средство (VII).

3.2.4 диспетчер правил/политики (rule/policy manager): Компонент облачной системы, обновляющий правила/политику в составе главного диспетчера.

3.2.5 координатор хранения данных (storage coordinator): Компонент облачной системы, который разделяет данные регистраторов данных о событиях (EDR)/системы хранения данных для автоматизированного вождения (DSSAD) и информацию, позволяющую идентифицировать транспортное средство (VII), для их хранения в облачном хранилище и последующего извлечения с применением заранее определенной политики.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ALKS	Automated Lane Keeping Systems		Автоматизированные системы удержания полосы движения
API	Application Programming Interface		Интерфейс прикладного программирования
CAN	Controller Area Network		Локальная сеть контроллеров
DoS	Denial of Service		Отказ в обслуживании
DSSAD	Data Storage System for Automated Driving		Система хранения данных для автоматизированного вождения
ECU	Electronic Control Unit	ЭБУ	Электронный блок управления
EDR	Event Data Recorder		Регистратор данных о событиях
FIFO	First-in-first-out		В порядке очередности
GDPR	General Data Protection Regulation		Генеральный регламент ЕС о защите персональных данных

IVN	In-Vehicle Network	Бортовая автомобильная сеть
JTAG	Joint Test Action Group	Объединенная группа по вопросам тестирования
MAC	Message Authentication Code	Код аутентификации сообщений
MRM	Minimum Risk Manoeuvre	Минимально рискованный маневр
OBD	On-Board Diagnostic	Бортовая диагностическая система
OTA	Over-the-air	Беспроводная связь
PII	Personally Identifiable Information	Информация, позволяющая установить личность
TLS	Transport Layer Security	Безопасность транспортного уровня
UDS	Unified Diagnostic Services	Единая диагностическая служба
V2X	Vehicle-to-everything	Связь транспортного средства с различными объектами
VII	Vehicle Identifiable Information	Информация, позволяющая идентифицировать транспортное средство
VIN	Vehicle Identification Number	Идентификационный номер транспортного средства

5 Соглашения по терминологии

В настоящей Рекомендации используются следующие условные обозначения.

Ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии это требование не является обязательным.

6 Облачные системы регистрации данных

6.1 Облачная система регистрации данных о событиях

Облачный EDR – это EDR, подключенный к облачным системам (внутренним серверам) для повышения доступности и безопасности данных EDR в среде соединенных и автономных транспортных средств.

EDR – это устройство для записи информации, связанной с автомобильными авариями или дорожно-транспортными происшествиями (ДТП), которое сегодня установлено в большинстве автомобилей в целях повышения уровня безопасности и комфортабельности транспортных средств.

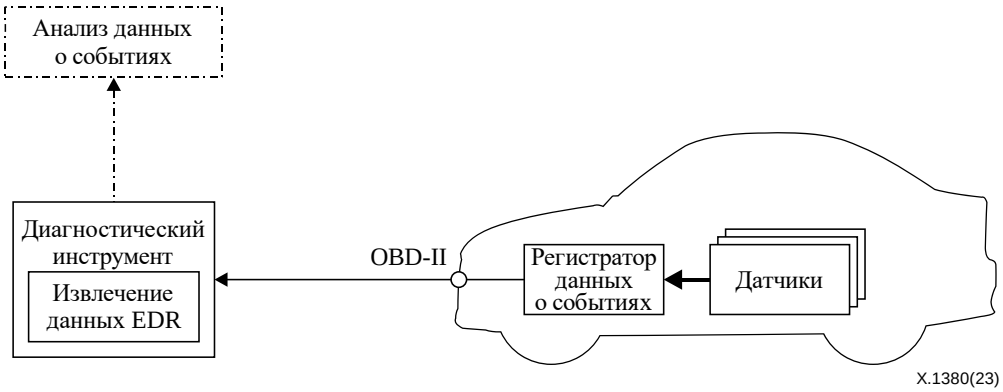

Рисунок 1 − Обычный автомобильный EDR

Обычный EDR, показанный на рисунке 1, запускается, когда происходит событие, при котором состояние автомобиля отвечает определенным условиям, таким как срабатывание фронтальной подушки безопасности, превышение порога ускорения/замедления движения, опрокидывание и т. д. Когда EDR включен, он собирает предопределенный набор данных от датчиков и сохраняет их в энергонезависимой памяти внутреннего хранилища данных (накопителе). На практике данные записываются с момента –5 с перед запуском (обычно обозначаемого как T_0) до момента +500 мс после запуска. Вместо "–5 с" и "+500 мс" могут использоваться другие значения в зависимости от национальных правил или производителя транспортного средства.

Как правило, EDR, установленный на транспортном средстве, может хранить более одного события. Когда хранилище данных заполняется данными прошлых событий, новые данные записываются поверх самых старых. В особых случаях, таких как срабатывание подушки безопасности, обычный EDR сохраняет собранные данные и блокирует хранилище данных, предотвращая возможность манипулирования данными или их перезаписи.

Сохраненные данные извлекаются через порт бортовой диагностической системы (OBD)-II с помощью диагностического инструмента или специальной системы восстановления данных и используются для анализа ситуации. Минимальный набор собираемых данных определяется национальными правилами эксплуатации транспортных средств или конструкцией транспортного средства. Формат записанных данных о событиях обычно также бывает свой у каждого производителя транспортных средств и часто различается от модели к модели. Поэтому при извлечении и анализе данных о событиях требуется использовать специализированное программное обеспечение для восстановления данных.

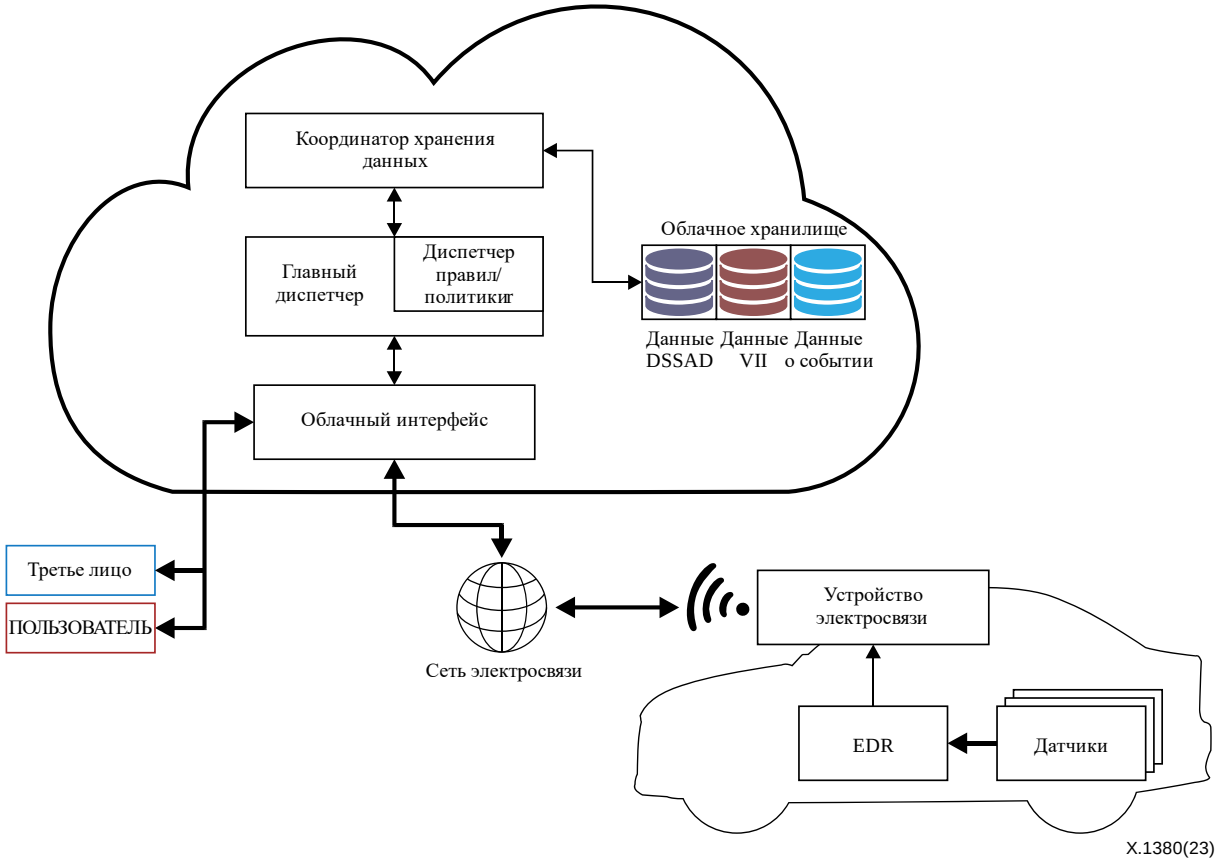

Рисунок 2 − Облачный EDR

Облачный EDR, показанный на рисунке 2, сохраняет данные о событиях в облачных системах с помощью устройства электросвязи, подсоединенного к EDR.

Набор регистрируемых данных облачного EDR может отличаться от набора данных обычного EDR вследствие системных и эксплуатационных различий между ними. Кроме того, может быть добавлен новый тип данных от электронного блока управления (ЭБУ), обеспечивающего автономное вождение, поскольку это критически важные данные, которые помогают анализировать дорожно-транспортные происшествия с участием автономных транспортных средств.

В отличие от обычного EDR, который записывает новые данные о событиях поверх незаблокированных данных, облачный EDR может записывать в облачное хранилище все данные без необходимости перезаписи. Таким образом, облачный EDR способен хранить полную запись данных по транспортному средству, ничего не удаляя. Это одно из главных преимуществ облачного EDR, которое значительно помогает в исследованиях по безопасности дорожного движения с использованием полных данных EDR.

Собранные данные EDR, хранящиеся в облачных системах, должны быть доступны пользователям или третьим лицам, если какая-либо сторона запрашивает такие данные, выполнив надлежащую процедуру авторизации. При предоставлении запрашиваемых данных EDR должен быть предусмотрен процесс аутентификации для проверки правомерности запроса.

В дополнение к функциям хранения и предоставления данных EDR облачный EDR также обеспечивает возможность обновления правил/политики в системе. Любой пользователь или третье лицо может инициировать обновление правил/политики для устройства EDR в транспортном средстве и соответствующей политики в облачной системе. Такой запрос требует более высоких полномочий и строгой проверки безопасности, чем любые обычные процедуры хранения и извлечения информации.

В облачной системе EDR, показанной на рисунке 2, объекты облачных систем работают поверх функциональных возможностей облачного EDR. Облачный интерфейс служит шлюзом облачной системы и ведет журнал обращений к данным. Главный диспетчер управляет основными процедурами хранения и извлечения данных EDR. Он проверяет основные требования запроса от

пользователя/третьего лица или транспортного средства, а также выполняет обновление правил/политики с помощью встроенных диспетчеров правил/политики. Координатор хранения данных обеспечивает хранение и извлечение данных о событиях в соответствии с заданной политикой. Политика может включать проверку данных EDR, извлеченных из облачного хранилища, в соответствии с полномочиями запрашивающей стороны. Она также может включать схему процесса сохранения данных в облачном хранилище EDR и их извлечения.

6.2 Облачная система хранения данных для автоматизированного вождения

Система хранения данных для автоматизированного вождения (DSSAD) – это система, цель которой дать представление о том, кто именно запросил управление и кто находился за рулем (это могут быть разные субъекты, особенно во время передачи управления), благодаря сохранению набора данных, позволяющего получить четкую картину взаимодействия водителя с автоматизированной системой вождения. DSSAD рассматривается в [b-UN R157]. В этом регламенте DSSAD признается обязательным компонентом автоматизированных транспортных средств.

DSSAD хранит такую информацию, как время включения и выключения автоматизированной системы вождения, требования, предъявляемые при передаче управления, экстренные маневры и т. д. Когда автоматизированная система выключена или затребована передача управления, в DSSAD сохраняется причина изменения состояния. Проанализировав данные DSSAD, в которых зафиксирован весь процесс взаимодействия между автоматизированной системой и водителем, заинтересованные стороны могут выяснить, кто именно запросил управление и кто фактически управлял транспортным средством.

Облачная DSSAD, показанная на рисунке 3, сохраняет данные DSSAD в облачных системах через устройство электросвязи, подсоединенное к DSSAD. Процесс передачи данных DSSAD в облачную систему тот же, что и для облачного EDR. Разница в том, что вместо данных EDR передаются данные DSSAD. DSSAD периодически передает данные в облачную систему. Таким образом, DSSAD может гибко реагировать на проблемы, вызванные ограничениями хранилища данных DSSAD.

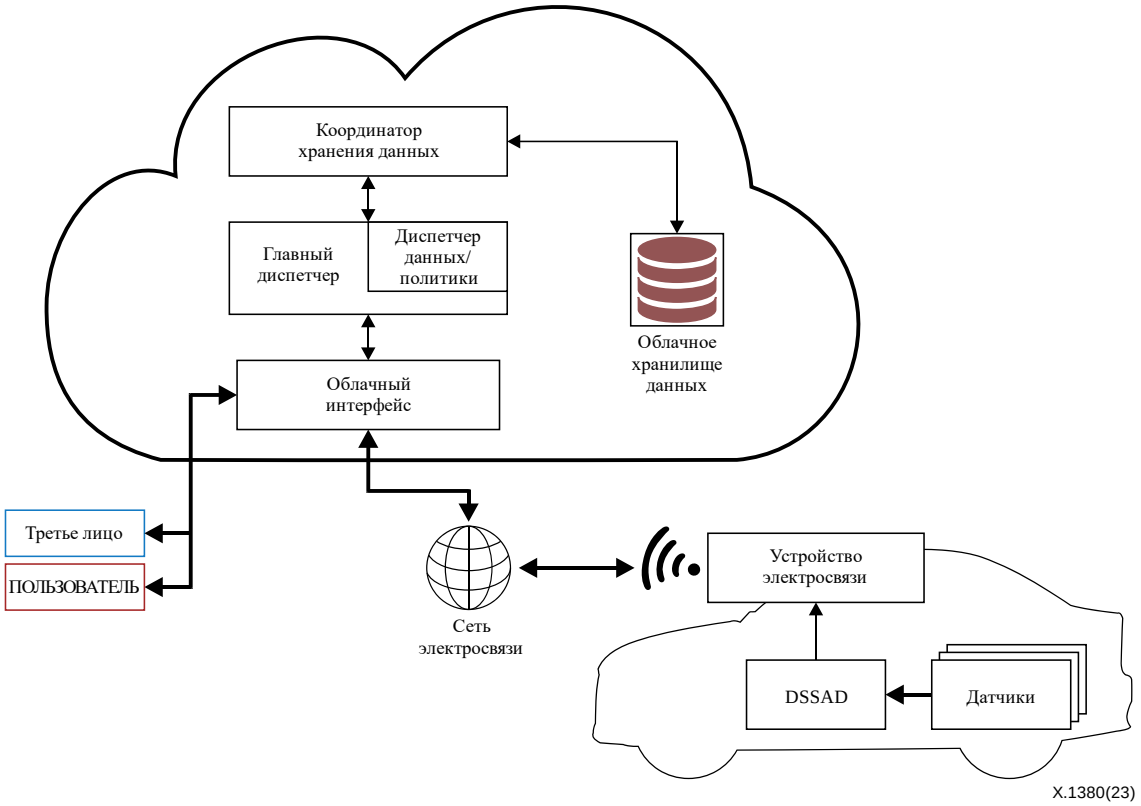

Рисунок 3 − Облачная DSSAD

6.3 Сравнение EDR и DSSAD

В таблице 1 сравниваются системы EDR и DSSAD.

Таблица 1 − Сравнение систем EDR и DSSAD

	EDR	DSSAD
Назначение	Анализ и реконструкция дорожно-транспортных происшествий	Определение степени ответственности транспортного средства в определенный момент времени; кто затребовал управление и кто вел машину
Условия запуска	Событие (например, авария) – физическое происшествие, приведшее к достижению порога срабатывания	Взаимодействие – изменение рабочего состояния системы или запрос на изменение рабочего состояния системы
Собираемые данные	Предопределенный набор данных, относящихся к анализу аварийных ситуаций	Предопределенный набор данных, относящихся к управлению транспортным средством и ответственности
Время хранения	Запись данных при запуске устройства (одномоментно)	Запись данных в течение всего времени вождения
Момент загрузки	Каждый раз при сохранении данных, включении/выключении зажигания	

7 Конструкция облачной системы регистрации данных

7.1 Управление данными EDR

EDR предназначен для записи информации о транспортном средстве при определенных событиях, таких как срабатывание подушки безопасности. Записанные EDR данные используются для анализа и реконструкции аварийных ситуаций. Поэтому EDR записывает время события и состояние транспортного средства в этот момент.

7.1.1 Время записи данных о событии

На рисунке 4 показано, как EDR регистрирует событие. Обнаружив конкретное событие, EDR отмечает время события T_0 и собирает определенные данные в течение предопределенного интервала времени записи. Символом T_0^n обозначено время n-го события. Время записи может различаться в зависимости от типа событий, поскольку событиям каждого типа соответствуют разные условия запуска. Символом T_{pre} обозначено время перед конкретным событием. Символом T_{post} обозначено время после конкретного события. Интервал времени можно обозначить как $[(T_0 - T_{pre}) \sim (T_0 + T_{post})]$.

В случае нескольких последовательных событий EDR записывает данные независимо от перекрывающихся интервалов времени, как показано на рисунке 4. На рисунке 4 (a) показаны интервалы времени записи неперекрывающихся событий. На рисунке 4 (b) показаны интервалы времени записи перекрывающихся событий.

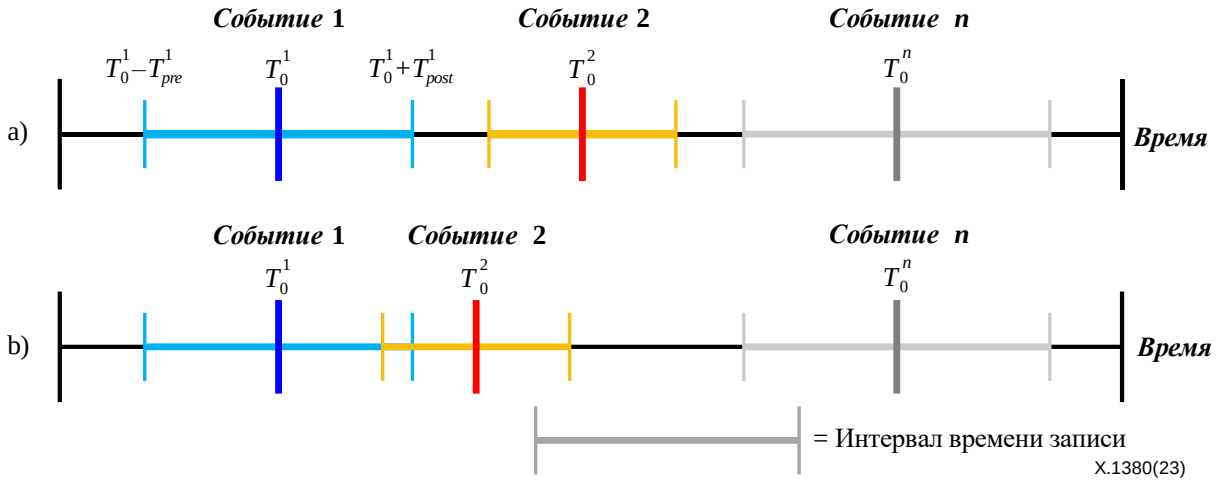

Рисунок 4 − Интервал времени записи EDR: a) неперекрывающиеся события; b) перекрывающиеся события

7.1.2 Блокировка данных в бортовом накопителе

Для хранения данных EDR используется несколько бортовых накопителей. Поскольку заданные условия могут быть разными, может произойти несколько последовательных событий. Запись событий EDR производится в порядке очередности (FIFO). Если все накопители EDR уже заполнены, данные новых событий записываются поверх старых. Однако в некоторых случаях, таких как срабатывание фронтальной подушки безопасности, требуется блокировка накопителя данных после записи, чтобы сохраненные данные было невозможно перезаписать. На рисунке 5 приведен пример процедуры записи EDR с двумя накопителями. На рисунке 5 (a) показан процесс записи информации о последовательных событиях без условия блокировки данных. Информация о событии 3 записывается вместо информации о наиболее старых событиях. С другой стороны, на рисунках 5 (b) и 5 (c) показаны процессы сохранения информации о последовательных событиях с условием блокировки данных, так что в накопителе с блокировкой данных информация о следующем событии переписана не будет. В частности, в случае процесса (c) событие 3 нельзя сохранить ни в одном накопителе, потому что оба устройства заполнены данными предыдущих событий, то есть события 1 и события 2, и заблокированы. Поэтому в политике необходимо установить приоритет, в соответствии с которым будут блокироваться данные в накопителях.

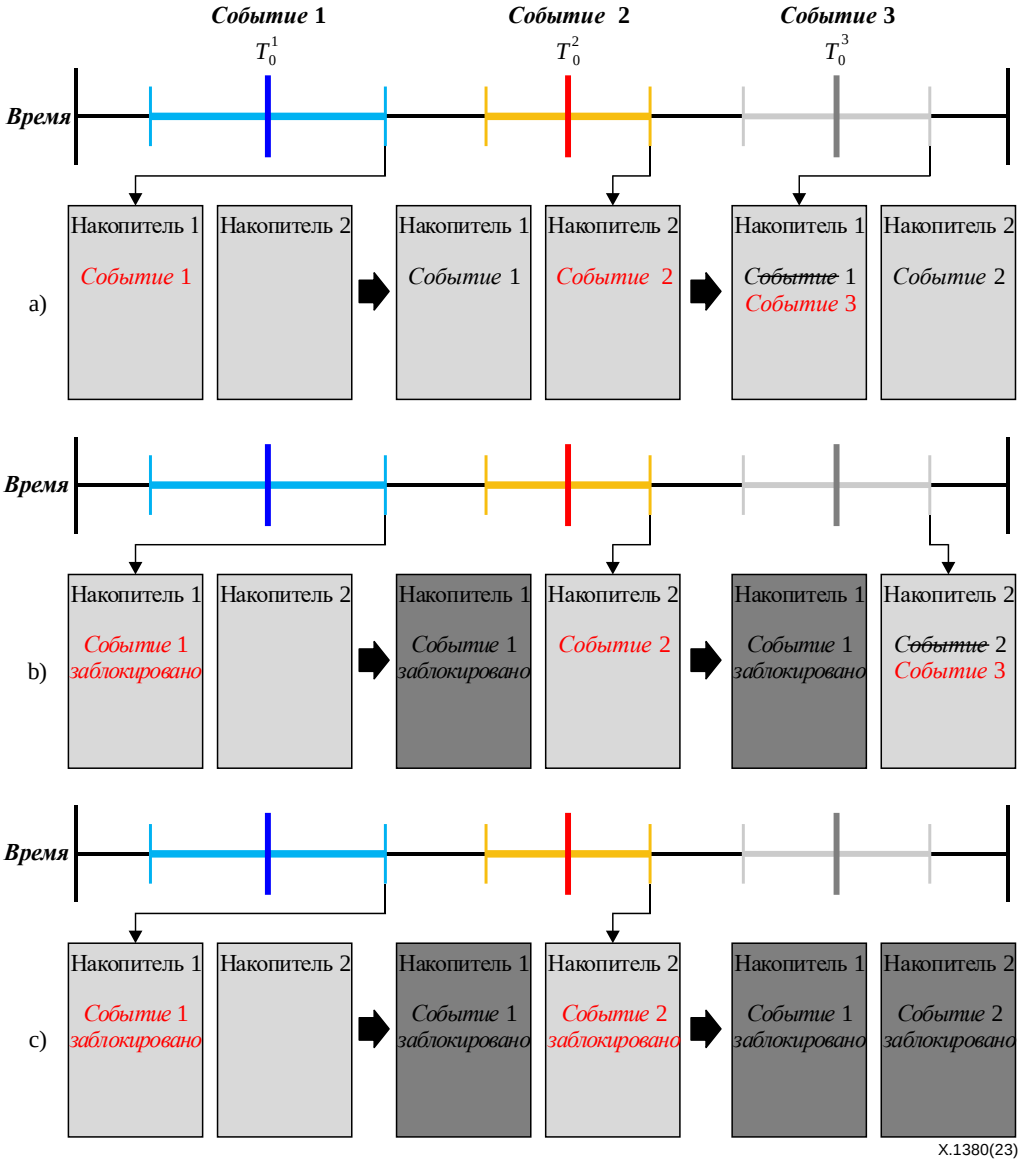

Рисунок 5 – Пример записи EDR с двумя накопителями: a) без блокировки данных; b) с условием блокировки данных только для события 1; c) с условием блокировки данных для событий 1 и 2

7.1.3 Расширение набора данных

Набор данных обычного EDR, как правило, регулируется национальными администрациями или производителями транспортных средств. Для работы с соединенными и автономными транспортными средствами набор данных обычного EDR необходимо расширить. Например, решающее значение для расследования причин дорожно-транспортного происшествия могут иметь данные датчиков, используемых в автономном транспортном средстве, таких как радар и лидар. Кроме того, важное значение для соединенного транспортного средства могут иметь сертификаты, которые использовались во время сеанса связи транспортного средства с различными объектами (V2X) в течение происшествия. А решающее значение для выяснения того, не произошло ли событие в результате кибератаки, имеют журналы событий в системе обнаружения вторжений (IDS), где регистрируются аномалии и сигнатуры при попытках вторжения через сеть.

7.2 Управление данными DSSAD

7.2.1 Регистрация времени в DSSAD

На рисунке 6 показаны различия между EDR и DSSAD, относящиеся ко времени записи данных. DSSAD осуществляет запись всех взаимодействий определенного вида между автоматизированной системой и водителем, в то время как EDR записывает данные в течение заданного интервала времени всякий раз, когда происходит запускающее событие. Таким образом данные, записанные в EDR и DSSAD, полезны для определения того, кто управлял транспортным средством в момент аварии.

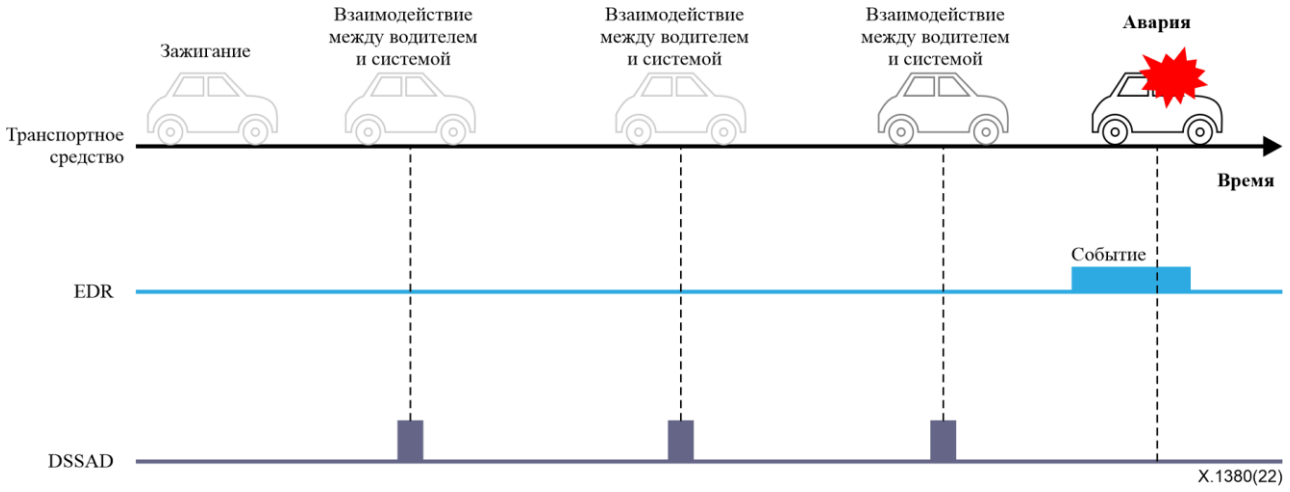

Рисунок 6 − Время записи данных EDR и DSSAD

Облачная DSSAD должна передавать данные в облачную систему в соответствии с предопределенной политикой. Когда накопитель DSSAD в транспортном средстве заполняется до предела, последние данные могут записываться поверх предыдущих в порядке процедуры FIFO.

7.2.2 Блокировка данных в бортовом накопителе

Запись данных DSSAD также производится в соответствии с процедурой FIFO, как и процесс записи данных EDR. Если накопитель DSSAD заполнен, новые данные записываются поверх самых старых. Однако заданное условие запускающего события блокировки данных в накопителе EDR требует блокировки накопителя данных DSSAD после записи данных и отклонения попыток перезаписи уже сохраненных данных. Формат заблокированных данных DSSAD определяется политикой хранения данных DSSAD. Формат заблокированных данных DSSAD может отличаться от обычного формата данных DSSAD.

После блокировки данных DSSAD заблокированные данные DSSAD могут быть переданы в облачную систему. Передача заблокированных данных DSSAD может иметь приоритет перед другими операциями передачи данных, такими как передача обычных данных DSSAD и заблокированных данных EDR. Если подтверждено завершение передачи, переданные данные могут быть удалены из бортового накопителя DSSAD.

7.2.3 Формат данных

Если целью EDR является запись данных о событиях, то цель DSSAD состоит в обеспечении определения ответственного за управление транспортным средством в определенный момент времени (обычно во время ДТП).

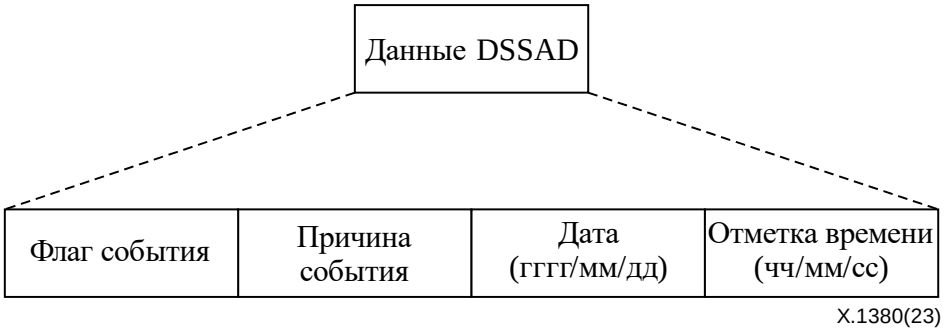

Рисунок 7 − Формат данных DSSAD

Данные DSSAD состоят из четырех полей, как показано на рисунке 7 (см. [b-UN R157]).

Флаг события – это поле, указывающее тип взаимодействия между водителем и системой, такой как требование передачи управления или экстренные маневры.

Поле причины события указывает, почему появился флаг события. Это поле содержит подробное описание причины передачи управления. Возможные причины событий перечислены в пункте 8.2 документа [b-UN R157].

В поле даты заносится дата создания флага события. Данные в этом поле представлены в формате год/месяц/день.

В поле отметки времени фиксируется время создания флага события. Данные в этом поле представлены в формате часы/минуты/секунды часового пояса. Требуется высокая точность отметок времени, что обусловлено характеристиками DSSAD. Может быть разрешена одна отметка времени для нескольких записей данных DSSAD, сделанных одновременно в пределах временно́го разрешения конкретных данных DSSAD. Если происходит несколько событий в течение одной секунды, они могут иметь одну и ту же отметку времени. В этом случае в данных DSSAD должна указываться временна́я последовательность.

7.3 Информация, позволяющая идентифицировать транспортное средство (VII)

Когда EDR/DSSAD загружает свои данные в облачные системы, следует рассматривать информацию VII как идентифицирующую данные. VII может быть номерным знаком, сертификатом транспортного средства, VIN или чем-либо еще, что можно использовать для идентификации транспортного средства. VII можно рассматривать как информацию, позволяющую установить личность (PII).

В отношении будущих систем транспортных средств следует рассмотреть ситуации, когда одно и то же транспортное средство используется несколькими пользователями, например каршеринг. В ситуациях, когда каждый пользователь желает применять при вождении облачные системы EDR/DSSAD, транспортное средство общего пользования должно иметь возможность различать каждого пользователя за рулем. Однако идентифицировать каждого пользователя трудно из-за отсутствия обязательного процесса, позволяющего транспортному средству собирать информацию о пользователях (например идентификаторы пользователей). Информацию о пользователе можно получить с помощью персонализированных систем, таких как цифровой ключ смартфона, который использует процесс аутентификации с применением уникального сертификата пользователя. Таким способом можно собирать информацию о пользователях и передавать ее в составе VII.

Как описано в пункте 6.1, EDR собирает данные, когда транспортное средство сталкивается с предопределенными запускающими EDR ситуациями, а DSSAD – всякий раз при взаимодействии водителя с транспортным средством. Поскольку EDR и DSSAD привязаны к транспортному средству,

а сбор данных осуществляется для каждого транспортного средства, идентификация каждого транспортного средства представляет собой важную задачу для облачной системы EDR/DSSAD. Таким образом, VII состоит из следующих элементов:

– **информация о транспортном средстве** (обязательная) – идентификационные данные конкретного транспортного средства, такие как VIN;

– **информация о пользователе** (факультативная) – идентификационные данные пользователя или водителя.

На рисунке 8 показан процесс передачи данных EDR/DSSAD из транспортного средства в облако.

Система EDR/DSSAD собирает данные от каждого датчика и ЭБУ бортовой сети в соответствии с предопределенными правилами, а затем передает их в устройство электросвязи. Устройство электросвязи добавляет VII к собранным данным EDR/DSSAD и отправляет их в облачную систему. Данные EDR/DSSAD и VII, полученные через облачный интерфейс, передаются координатору хранения данных и далее сохраняются в соответствии с политикой облачной системы.

Возможность доступа к данным EDR/DSSAD, хранящимся в облачной системе, имеют только авторизованные пользователи. Поэтому пользователи, желающие получить информацию из облачной системы, должны представить аутентификационную информацию, чтобы удостоверить свою личность. Облачная система предоставляет аутентифицированным пользователям данные EDR/DSSAD.

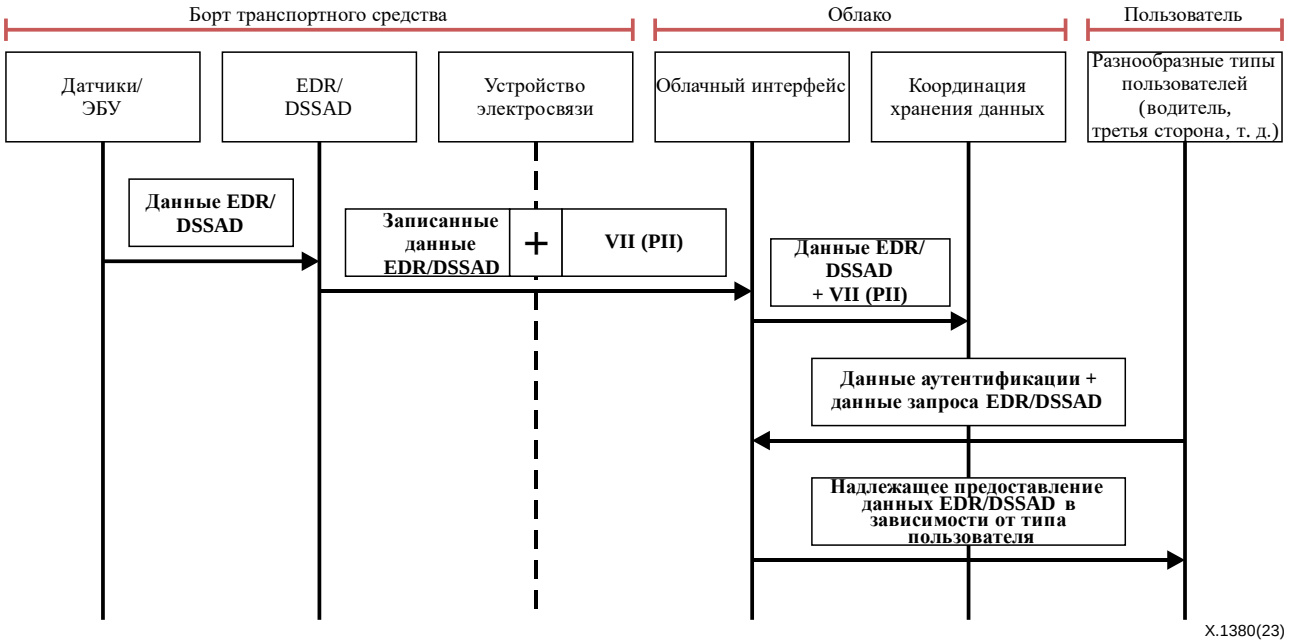

Рисунок 8 − Поток данных облачной системы EDR/DSSAD

7.4 Облачные системы EDR и DSSAD

7.4.1 Повышение доступности зарегистрированных данных

Точка доступа обычного EDR – это порт OBD-II. Получить и использовать данные EDR можно только через порт OBD-II и диагностический инструмент транспортного средства. По этой причине владельцы транспортных средств редко используют данные EDR, хотя и имеют к ним доступ.

А вот облачная система EDR/DSSAD повышает доступность данных EDR/DSSAD для пользователей, загружая такие данные в облачную среду. Пользователи или третьи лица могут применять VII или специальные идентификаторы для загрузки своих данных EDR/DSSAD в целях дальнейшего использования. Это может привести к широкому распространению данных EDR/DSSAD и повысить безопасность дорожного движения.

7.4.2 Обновление правил/политики

Облачная система EDR/DSSAD обеспечивает функцию обновления правил/политики. Правило определяет, как обращаться с данными в транспортном средстве, а политика – как обращаться с данными в облаке. Правило состоит из условий события, типа регистрируемых данных, времени записи данных определенного типа и процедуры загрузки данных в транспортное средство. Политика в контексте облачных EDR/DSSAD представляет собой полномочия доступа к данным, предоставляемые сторонам. В облачных системах хранения данных EDR/DSSAD политикой управляет координатор хранения данных.

Облачные системы EDR/DSSAD предоставляют функцию обновления правил/политики. Как правило, национальные регуляторные органы определяют обязательный набор данных о событиях и его условия. После обновления регуляторным органом по надлежащему запросу пользователя/третьего лица облачная система EDR/DSSAD выполняет обновление правил/политики на транспортном средстве и в облаке.

8 Анализ угроз безопасности

8.1 Активы безопасности и соответствующие цели по обеспечению безопасности

Актив безопасности – это любой информационный объект, функция или ресурс, которые должны быть защищены. В таблице 2 приведены относящиеся к облачным системам EDR/DSSAD активы безопасности и цели по обеспечению безопасности.

Таблица 2 − Активы безопасности и соответствующие цели по обеспечению безопасности

Актив безопасности	Описание	Соответствующие цели по обеспечению безопасности
Данные EDR/DSSAD, хранящиеся на борту транспортного средства	Данные EDR/DSSAD, собранные в транспортном средстве	Целостность
Правила EDR/DSSAD, хранящиеся на борту транспортного средства	Правила EDR/DSSAD, которые могут обновляться в соответствии с политикой облачной системы	Целостность
Микропрограммное обеспечение EDR/DSSAD	Микропрограммное обеспечение устройств EDR/DSSAD	Целостность
Пакет данных беспроводной связи (OTA)	Пакет данных OTA, используемый для обновления правил EDR/DSSAD	Конфиденциальность, целостность
Трафик шины передачи данных	Трафик, передаваемый по шине передачи данных в бортовой сети транспортного средства (IVN)	Конфиденциальность, целостность
Журнал событий EDR/DSSAD	Журнал событий устройства EDR/DSSAD	Целостность, подотчетность
Связь со средствами отладки/диагностики	Связь устройства EDR/DSSAD со средствами отладки или диагностики	Конфиденциальность, подлинность
Связь с внутренним сервером	Связь между внутренним сервером и транспортными средствами или пользователями/третьими лицами	Конфиденциальность, подлинность, готовность
Облачная политика	Облачная политика	Целостность
VII	Личные данные, используемые для идентификации пользователей/транспортных средств	Конфиденциальность
Журнал событий облачной системы	Журналы регистрации изменений облачной политики, запросов от пользователей/третьих лиц и других событий, которые могут повлиять на безопасность облачной системы	Целостность, подотчетность
Данные EDR/DSSAD, хранящиеся в облаке	Данные EDR/DSSAD, полученные от транспортных средств	Целостность

8.2 Угрозы безопасности

В этом разделе описаны угрозы безопасности в облачных системах регистрации данных. Общие выявленные угрозы для соединенных транспортных средств описаны в [ITU-T X.1371].

8.2.1 Угрозы для конфиденциальности

Данные, предоставляемые внутри облачных систем регистрации данных, как правило, представляют собой личные данные пользователей. Право владения данными и допустимый масштаб сбора данных зависят от регуляторного поля, в котором находится транспортное средство; однако обычно данные системы регистрации событий рассматриваются как VII. Несоблюдение условия конфиденциальности данных в облачных системах регистрации событий может рассматриваться как вторжение в частную жизнь пользователей. Например, типичными примерами угроз для конфиденциальности данных могут служить подслушивание и перехват информации посредством подсоединения к проводной линии связи в сети.

– **Подслушивание**. В беспроводных сетях, таких как облачная служба, подслушивание является легкоосуществимой потенциальной атакой. В облачных системах регистрации данных злоумышленник может подслушать сообщения, в том числе содержащие VII, двумя способами. Во-первых, это может иметь место между транспортным средством и облачным сервером. В этом случае возможна утечка данных о событиях из транспортного средства и данных об обновлении правил/политики из облачного сервера.

  Во-вторых, атака подслушивания может быть осуществлена между системой пользователя/третьего лица и облачной системой. В этом случае возможна утечка данных о событиях из облачной системы и запросов на обновление правил/политики из системы пользователя/третьего лица.

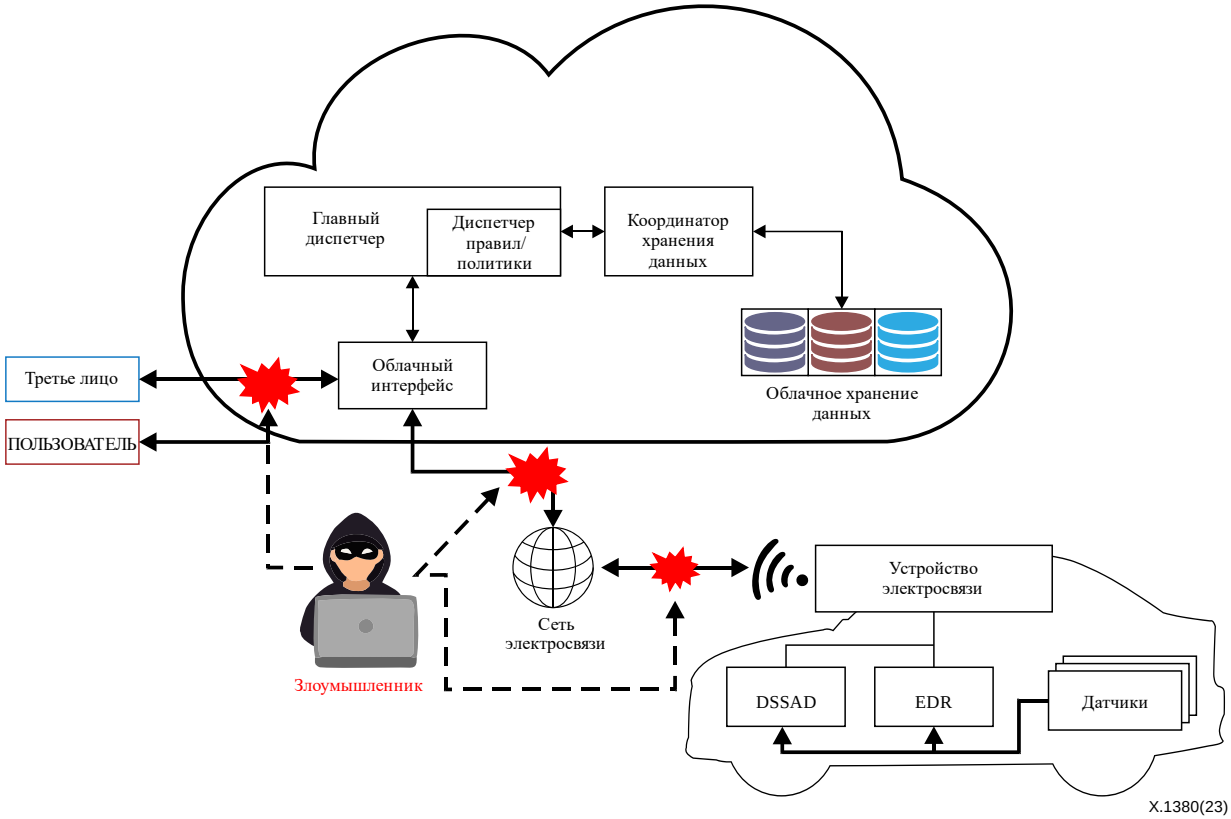

Рисунок 9 – Подслушивание в облачных системах регистрации данных

В-третьих, злоумышленник может перехватить и проанализировать пакет данных OTA, переданный для обновления правил EDR. В этом случае он может передать подложные правила, чтобы получить возможность взломать систему безопасности.

– **Перехват информации посредством подсоединения к проводной линии связи**. Одним из примеров физической атаки может служить прямое подсоединение к бортовой автомобильной сети. В современных транспортных средствах имеется несколько шин передачи данных локальной сети контроллеров (CAN); доступ к любой шине строго контролируется шлюзом безопасности (или межсетевым экраном транспортного средства). Весь трафик всех шин CAN контролировать невозможно, если только злоумышленник не получит право доступа к шлюзу безопасности. Поэтому он может попытаться получить физический доступ к целевому транспортному средству путем подсоединения к проводной линии связи, чтобы перехватить весь трафик шин CAN, включая данные EDR/DSSAD.

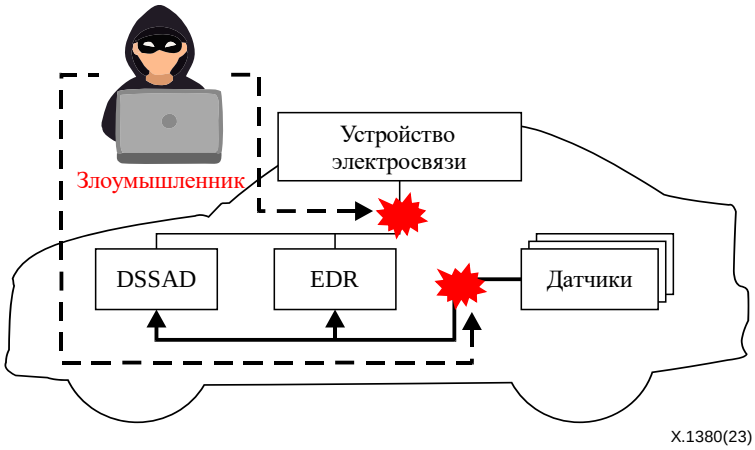

Рисунок 10 − Перехват информации посредством подсоединения к проводной линии связи в облачных системах регистрации данных

8.2.2 Угрозы для целостности данных

Данные EDR используются для анализа аварий или дорожно-транспортных происшествий, а данные DSSAD – для определения ответственных за них. Поэтому необходимо обеспечить, чтобы при хранении и передаче эти данные не были изменены. Сохранение целостности – одна из важнейших задач обеспечения безопасности журналов регистрации событий, таких как данные EDR/DSSAD. Злоумышленники стремятся нарушить целостность данных EDR/DSSAD, используя описанные ниже методы.

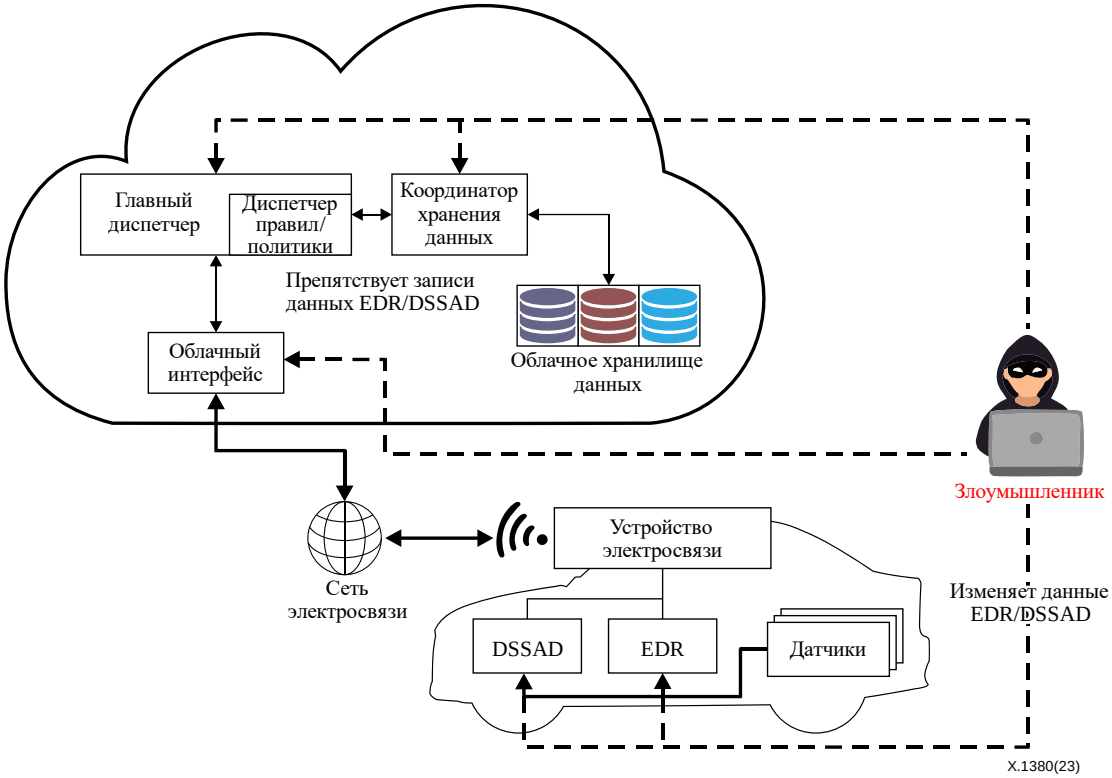

Рисунок 11 − Манипулирование потоком команд в облачных системах регистрации данных

Манипулируя потоком команд в облачной системе регистрации данных, злоумышленник может изменить данные EDR/DSSAD или воспрепятствовать записи данных в EDR/DSSAD. Например, злоумышленник идентифицирует интерфейс отладки на печатной плате (PCB) EDR/DSSAD и получает доступ к нему, после чего использует этот интерфейс для управления исполняемым кодом. Злоумышленник также может внести изменения в микропрограммное обеспечение или правила EDR/DSSAD. Кроме того, он может внести изменение в трафик шины передачи данных и подделать журнал событий EDR/DSSAD.

В случае облачной системы злоумышленник может получить доступ к хранилищу данных и манипулировать данными EDR, журналами событий и политикой облака, используя вредоносное ПО и небезопасные интерфейсы прикладного программирования (API).

На рисунке 11 показан процесс манипулирования потоком команд в облачных системах регистрации данных.

8.2.3 Угрозы для подлинности информации

Типичными угрозами для аутентификационной информации являются атаки через посредника, путем подмены участника и атака с дублированием.

– **Атака через посредника**. В облачной системе регистрации данных злоумышленник может перехватывать сообщения, передаваемые между транспортным средством и облаком или между облаком и пользователем, а затем ретранслировать их с произвольно измененным содержанием. Отправитель не знает, что получателем является неизвестный злоумышленник, который пытается получить доступ к сообщению или изменить его и только после этого передать получателю. Таким образом, злоумышленник в состоянии контролировать весь процесс связи.

– **Атака путем подмены участника**. Атака путем подмены участника в облачной системе регистрации данных может осуществляться четырьмя способами:

  • подача подложного запроса в облачную систему на извлечение данных EDR/DSSAD;

  • подача подложного запроса в облачную систему на обновление правил для определенного транспортного средства;

- подача запроса на сохранение подложных данных EDR/DSSAD в облачной системе;
- фальшивое обновление правил в системе EDR/DSSAD транспортного средства.

Атаки путем подмены участника могут нанести серьезный ущерб целостности всей облачной системы регистрации данных, поскольку они позволяют создавать подложные данные о событиях или фальсифицировать правила/политику в отношении событий. Кроме того, с помощью атаки путем подмены участника злоумышленник может похитить личные данные, хранящиеся в облачной системе.

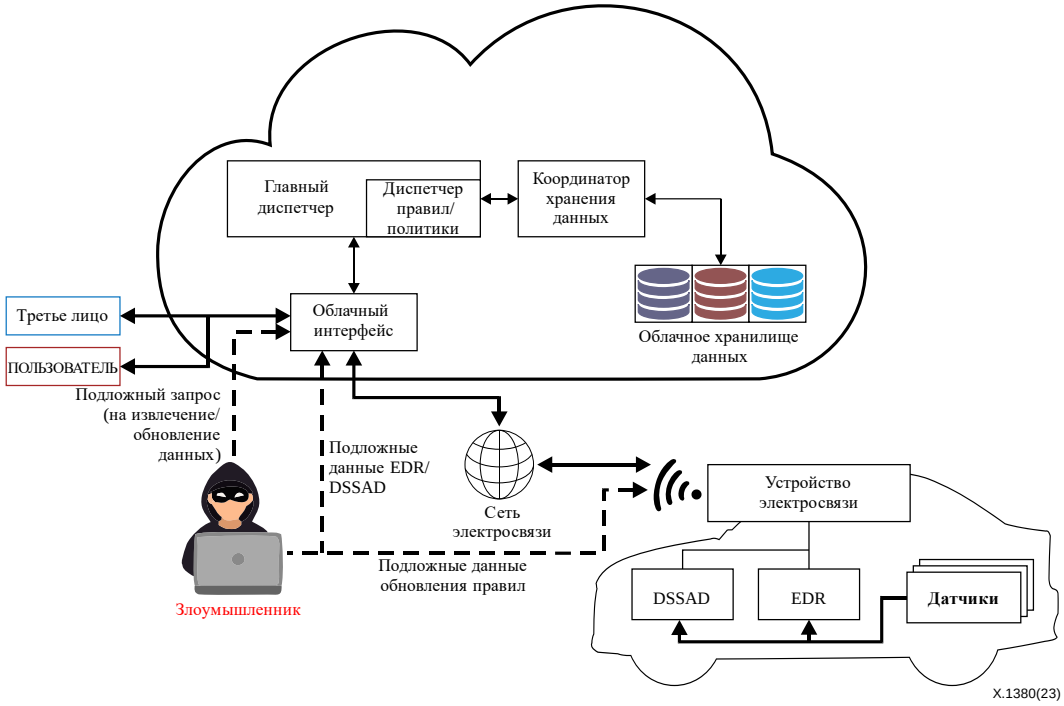

Рисунок 12 – Атака путем подмены участника на облачные системы регистрации данных

– **Атака с дублированием**. При атаке с дублированием данные EDR/DSSAD дублируются и может быть выполнен нежелательный откат правил/политики.

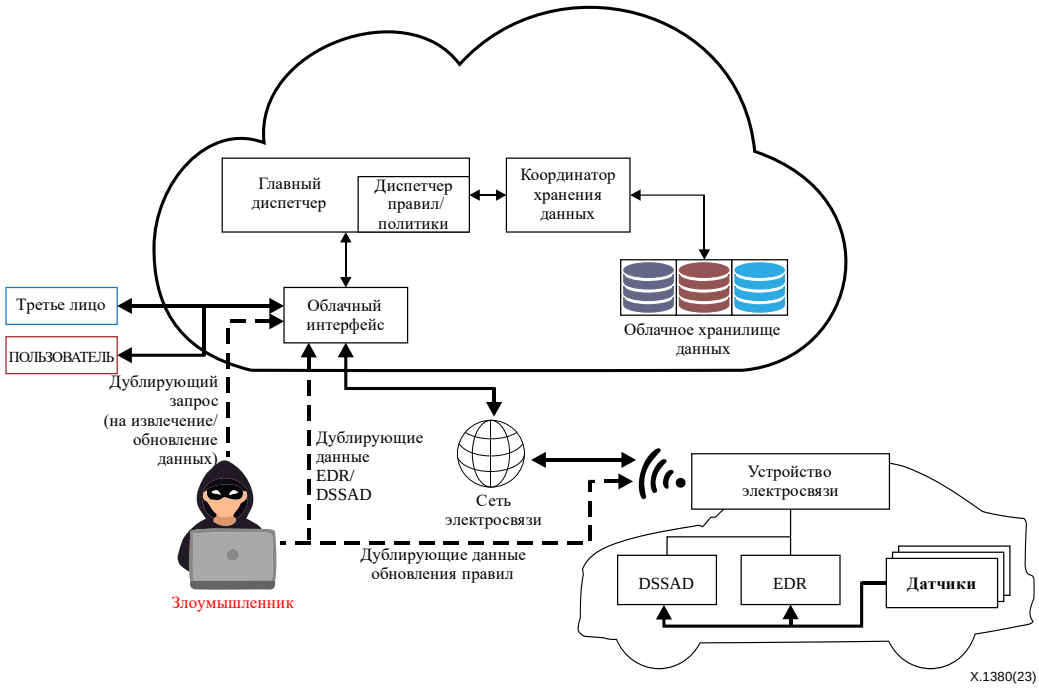

Рисунок 13 – Атака с дублированием на облачные системы регистрации данных

– **Физический доступ**. При наличии у злоумышленника возможности доступа к транспортному средству через порт отладки может быть осуществлена еще одна группа атак. Наиболее распространенным интерфейсом, используемым в качестве порта отладки, является интерфейс Объединенной группы по вопросам тестирования (JTAG). Доступ через интерфейс JTAG обеспечивает возможность чтения содержимого памяти и записи в память, что позволяет злоумышленникам вносить изменения в микропрограммное обеспечение и нарушать меры безопасности.

Еще одним путем получения физического доступа к транспортному средству является диагностика. С помощью диагностических инструментов злоумышленник может получить доступ к порту OBD-II или непосредственно к шлюзу, снабженному функциями удаленной диагностики. Единая диагностическая служба (UDS) – это стандартный протокол диагностики, который позволяет контролировать и администрировать бортовую сеть и ЭБУ транспортного средства.

8.2.4 Угрозы для готовности

Готовность – критически важная характеристика облачной системы регистрации данных, поскольку полезная информация о происшествиях или авариях может сохраняться в любое время. Самая известная угроза для готовности – это атака типа отказ в обслуживании (DoS).

– **DoS-атака**. DoS-атаки могут иметь серьезные последствия для облачных систем регистрации данных, поскольку злоумышленник пытается заблокировать основные средства связи/хранения данных/управления данными EDR/DSSAD, что приводит к тому, что облачная система регистрации данных становится непригодной для анализа происшествий. Примером DoS-атаки может служить переполнение сетевого канала большим объемом сообщений, генерируемых злоумышленником, чтобы парализовать сетевые узлы или всю облачную систему. Сетевые узлы (транспортного средства или облачной системы) не смогут обработать огромное количество поступающих данных, что вызовет сбой при сохранении данных EDR/DSSAD в облачной системе или обновлении правил/политики в бортовой и облачной системах.

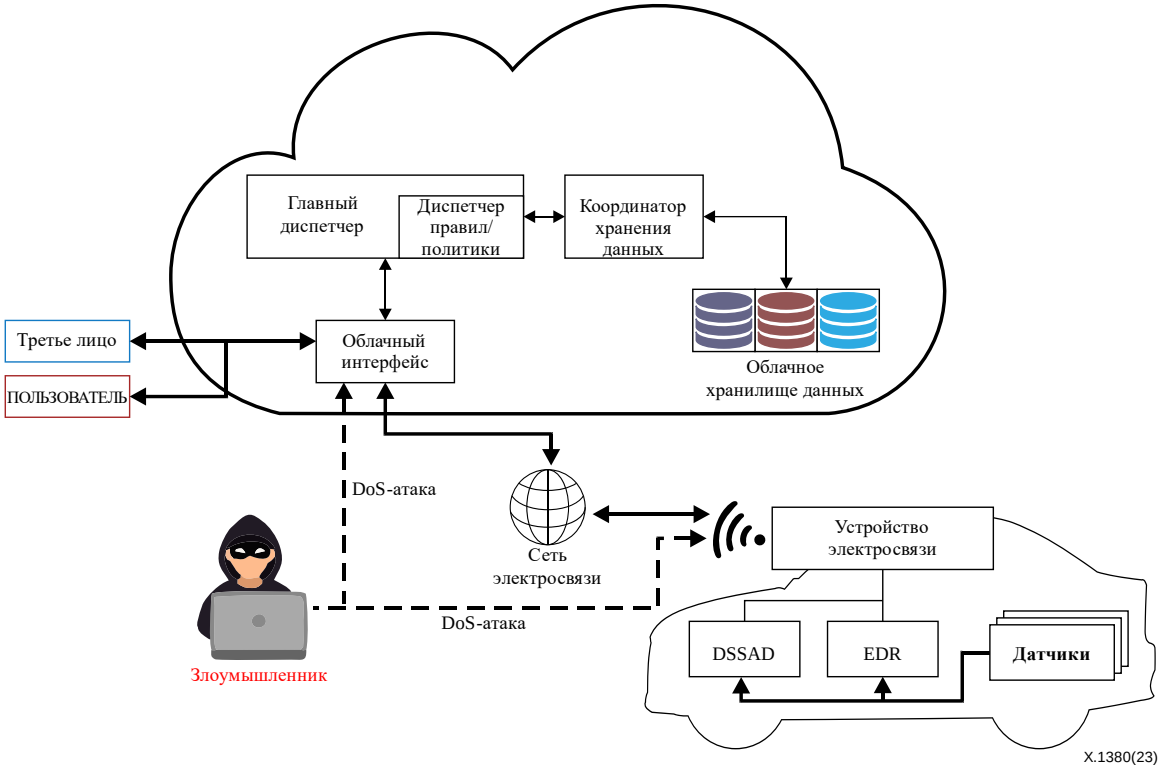

Рисунок 14 – DoS-атака на облачные системы регистрации данных

8.2.5 Угрозы для подотчетности

– **Потеря отслеживаемости событий**. Такие компоненты облачной системы, как диспетчер правил/политики и координатор хранения данных, работают в соответствии с набором правил/политикой, установленными пользователем, обладающим соответствующими полномочиями. Поэтому ведение журнала изменений правил/политики чрезвычайно важно с точки зрения подотчетности. Изменив или удалив содержимое журнала событий, злоумышленник может внести в систему путаницу.

9 Требования безопасности

9.1 Безопасная загрузка

Рекомендуется проверять целостность микропрограммного обеспечения, хранящегося в памяти устройств EDR/DSSAD, перед его выполнением или во время него. Также рекомендуется проверять целостность правил EDR/DSSAD соответствующей конфигурации и данных калибровки.

Процесс защиты микропрограммного обеспечения и правил состоит из двух шагов. Сначала при установке микропрограммного обеспечения и правил их следует проверить на подлинность перед записью во внутреннюю память и настроить в качестве действующих. Затем действующие микропрограммное обеспечение и правила проверяются на целостность при каждой загрузке.

Для проверки целостности микропрограммного обеспечения и правил с надлежащим уровнем безопасности рекомендуется использовать в механизме безопасной загрузки симметричные или асимметричные криптографические средства. Для безопасного хранения криптографических ключей и ускорения вычисления криптографических алгоритмов в устройствах EDR и DSSAD также рекомендуется использовать аппаратный якорь доверия, такой как аппаратный модуль безопасности (HSM).

9.2 Безопасная регистрация в журнале событий

Необходимо обеспечить целостность регистрируемых данных с применением методов криптографической защиты. Поскольку данные EDR/DSSAD могут служить доказательством в конкретных ситуациях, они должны быть защищены от несанкционированных манипуляций.

В случае облачной системы главный диспетчер должен создавать регистрационную запись в каждом из перечисленных ниже случаев:

– попытки аутентификации со стороны пользователей/третьих лиц;

– обновление политики.

Рекомендуется надежно хранить журналы. Криптографические средства, такие как код аутентификации сообщения (MAC), могут присоединяться к журналам и/или храниться в безопасном хранилище с надлежащим контролем доступа. Минимальный срок хранения журнала должен определяться в соответствии с политикой поставщика облачных услуг или законодательством каждой страны.

9.3 Безопасная связь

Облачные системы регистрации данных используют следующие каналы связи:

– между облачной системой и транспортными средствами;

– между пользователями/третьими лицами;

– между ЭБУ, датчиками и исполнительными механизмами в транспортных средствах.

Рекомендуется обеспечить конфиденциальность и аутентичность сообщений при связи, осуществляемой между облачной системой и транспортными средствами или пользователями/третьими лицами. Конфиденциальность и аутентичность могут быть обеспечены с помощью криптографических средств, таких как протокол безопасности транспортного уровня (TLS).

Также рекомендуется гарантировать готовность соединения между облачной системой и транспортным средством. Это означает, что огромное количество данных EDR и DSSAD,

поступающих от многочисленных транспортных средств, должно храниться в облачном хранилище данных надлежащим образом.

Рекомендуется обеспечить целостность сообщений и данных при обмене данными между ЭБУ, датчиками и исполнительными механизмами в транспортных средствах в целях генерирования правильных данных EDR/DSSAD, поскольку данные, поступающие от ЭБУ и датчиков, имеют отношение к авариям или действиям водителя.

9.4 Безопасный доступ

Рекомендуется отключить интерфейсы отладки, такие как JTAG в устройстве EDR/DSSAD, не обязательные для работы в полевых условиях, и соблюдать правила безопасной загрузки. Применяются следующие способы отключения интерфейсов отладки:

– постоянное удаление;

– условное отключение путем применения средств управления доступом.

В случае повторного подключения интерфейсов отладки для анализа при рекламационном возврате интерфейсы отладки должны быть доступны только для авторизованных и аутентифицированных лиц. Рекомендуется ограничить права доступа приложений, получающих данные через аппаратные и программные интерфейсы, по принципу наименьших привилегий.

Критически важные для безопасности функции и данные, передаваемые посредством диагностических команд и запросов, рекомендуется защитить с помощью криптографического механизма. Это означает, что лицо, желающее получить доступ к устройству EDR/DSSAD, прежде чем подавать команды, должно быть аутентифицировано.

9.5 Безопасное обновление

Рекомендуется, чтобы процедура обновления микропрограммного обеспечения и правил гарантировала подлинность и целостность, то есть чтобы разрешалось загружать только аутентифицированные и немодифицированные пакеты обновлений. Кроме того, не рекомендуется понижать версию микропрограммного обеспечения и правил до более ранней версии во избежание злонамеренного использования известных уязвимостей безопасности. Рекомендуется, чтобы OTA-пакеты передавались по безопасному каналу, защищенному криптографическими средствами.

9.6 Взаимосвязь между выявленными угрозами и требованиями безопасности

В приведенной ниже таблице 3 угрозы для безопасности, перечисленные в разделе 8, сопоставляются с требованиями безопасности.

Таблица 3 − Взаимосвязь между выявленными угрозами и требованиями безопасности

Требования безопасности	Угрозы	Цели по обеспечению безопасности
Безопасная загрузка	Манипулирование потоком команд: – манипулирование микропрограммным обеспечением – манипулирование правилами EDR/DSSAD	Целостность правил EDR/DSSAD, хранящихся в транспортных средствах Целостность микропрограммного обеспечения EDR/DSSAD
Безопасная регистрация в журнале событий	Манипулирование потоком команд: – манипулирование журналами событий Потеря отслеживаемости событий	Целостность данных EDR/DSSAD в транспортных средствах Целостность облачного журнала событий

Таблица 3 − Взаимосвязь между выявленными угрозами и требованиями безопасности

Требования безопасности	Угрозы	Цели по обеспечению безопасности
Безопасная связь	Подслушивание Перехват информации посредством подсоединения к проводной линии связи Манипулирование потоком команд Атака через посредника Атака путем подмены участника Атака с дублированием DoS-атака	Конфиденциальность и/или целостность трафика в шине передачи данных Конфиденциальность и аутентичность связи с серверными системами Готовность серверных систем
Безопасный доступ	Физический доступ	Конфиденциальность и/или аутентичность связи со средствами отладки/диагностики
Безопасное обновление	Подслушивание Манипулирование потоком команд: – манипулирование правилами EDR/DSSAD Атака путем подмены участника	Конфиденциальность и целостность OTA-пакетов

10 Руководящие указания по реализации облачных систем регистрации данных

При использовании данных EDR/DSSAD и управлении ими в облачных системах регистрации данных требуется надежная защита данных. Облачные системы регистрации данных дополнительно обеспечивают расширенные функциональные возможности для исследований и разработок в области создания более безопасных транспортных средств за счет использования сохраненных данных, которые невозможно получить от обычных регистраторов данных. В этом разделе содержатся руководящие указания по реализации облачной системы регистрации данных.

10.1 Разделение облачного хранилища данных

Вследствие важности информации VII в облачной системе EDR/DSSAD необходимо обеспечить надежную защиту такой информации. В облачных системах EDR/DSSAD требуется физическое разделение данных EDR/DSSAD и содержащейся в них информации VII. Это не только гарантирует безопасность, но и позволяет использовать дополнительные функции, такие как предоставление данных EDR/DSSAD третьих лиц без каких-либо нарушений конфиденциальности. Хранилище данных должно быть физически разделено на отдельные накопители, управляемые независимо друг от друга. Для хранилища данных VII (на рисунке 15 обозначенное как база данных VII) ввиду его относительной важности требуется более высокий уровень защиты, чем для других данных.

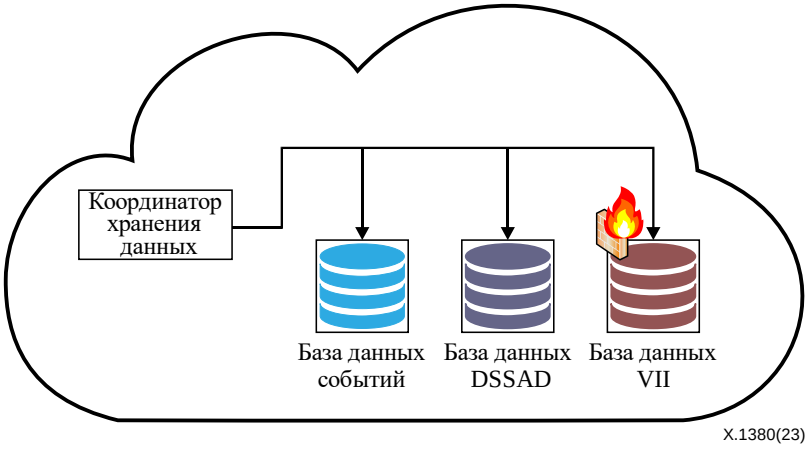

Рисунок 15°− Разделение хранилища данных

10.1.1 Процедура сохранения данных

Чтобы обеспечить конфиденциальность и подлинность данных, передаваемых в облачную систему, необходимо, прежде чем передавать данные EDR/DSSAD из бортовой системы в облачную, предварительно установить безопасный канал связи.

Когда данные из транспортного средства поступают через облачный интерфейс координатору хранения данных, тот производит разделение данных EDR/DSSAD и данных VII. После разделения координатор хранения данных создает связующую информацию, устанавливающую соответствие между данными EDR/DSSAD и данными VII. После этого два набора данных сохраняются в разных хранилищах (базах данных). Как показано на рисунке 16, данные VII и данные EDR/DSSAD вместе со связующей информацией хранятся соответственно в базе данных VII и в базе данных событий/DSSAD. По окончании процедуры сохранения данных записывается ее результат – успешное или неудачное завершение процедуры.

Одним из важнейших моментов в процессе сохранения данных является соблюдение соответствующих регуляторных документов, таких как Генеральный регламент ЕС о защите персональных данных (GDPR). Поэтому прежде чем собирать какие-либо данные от транспортных средств, рекомендуется получить согласие владельцев этих данных.

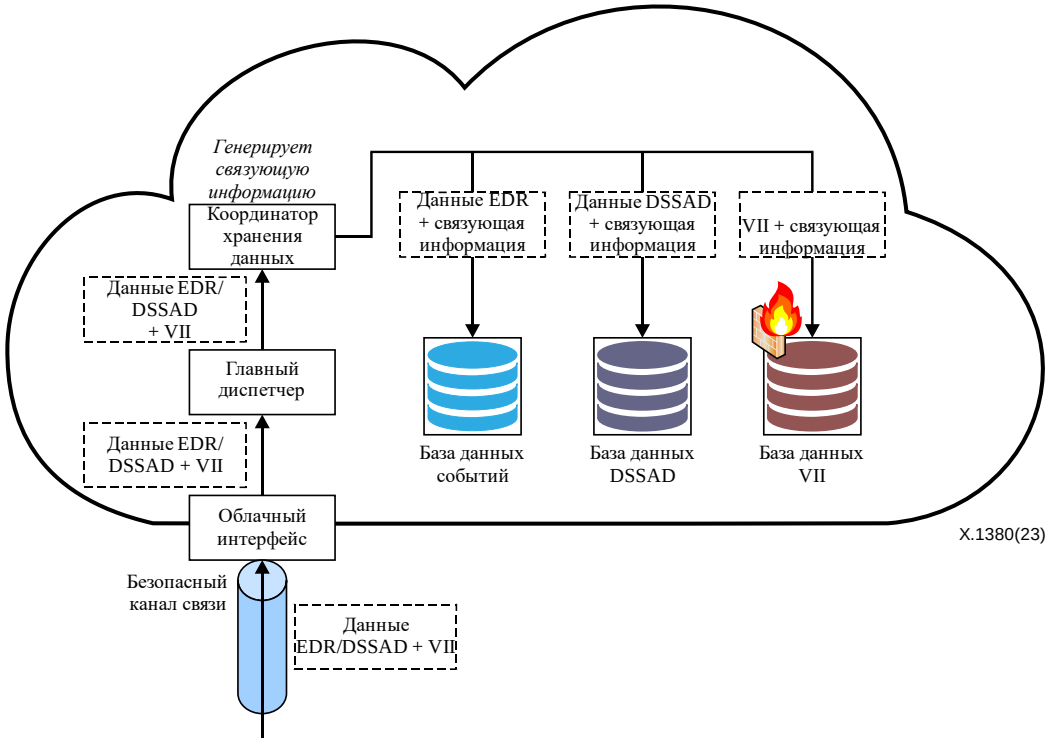

Рисунок 16 − Процедура сохранения данных в раздельных хранилищах

10.1.2 Процедура извлечения данных

Процедура извлечения данных EDR/DSSAD начинается с запроса пользователя/третьего лица на извлечение данных EDR/DSSAD. Когда пользователь/третье лицо обращается к облачной системе, облачный интерфейс аутентифицирует его, регистрируя все попытки получения доступа. Если аутентификация прошла успешно, координатор хранения данных использует предоставленную информацию VII для поиска связующей информации в базе данных VII (см. рисунок 17 (a)). По найденной связующей информации координатор хранения данных осуществляет поиск данных EDR/DSSAD. Когда данные EDR/DSSAD найдены, координатор хранения данных передает их запрашивающей стороне, причем процедура управления доступом главного диспетчера зависит от уровня полномочий запрашивающей стороны. Извлечение информации VII разрешено с ограничениями и требует высокоуровневых полномочий. В то же время данные EDR или данные DSSAD, не содержащие VII, могут быть получены третьим лицом. Когда данные VII удалены и переданы на отдельный нейтральный сервер, данные EDR или DSSAD могут извлекаться без процедуры поиска VII (см. рисунок 17 (b)).

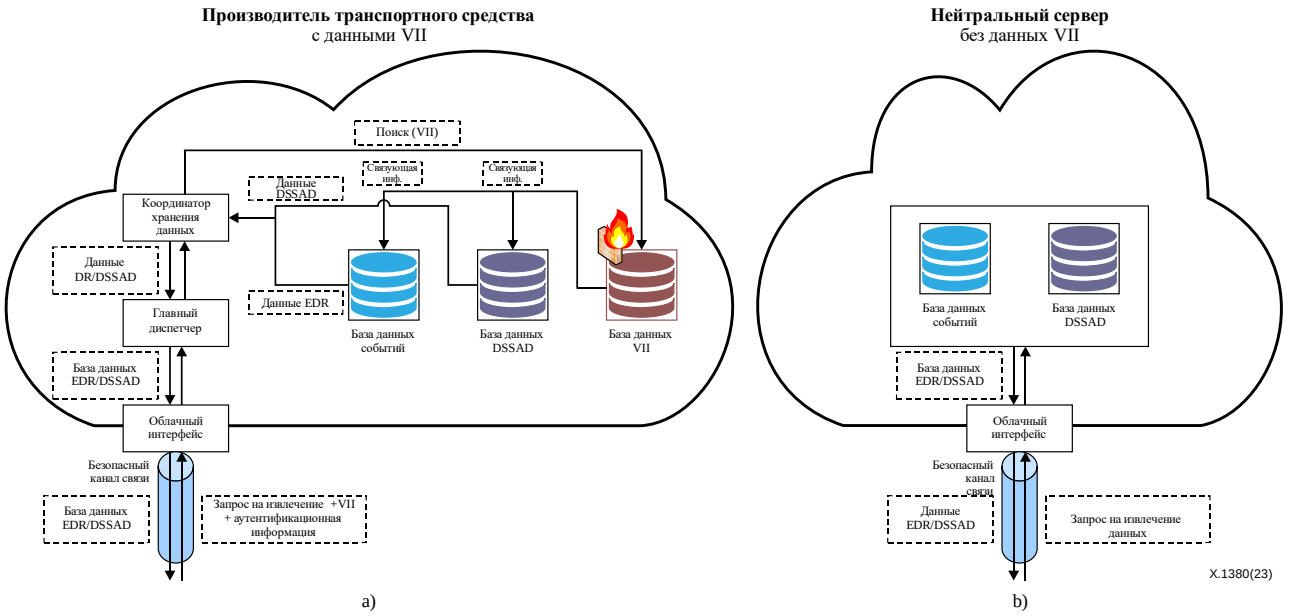

Рисунок 17 − Процедура извлечения данных из раздельного хранилища

10.1.3 Процедура удаления данных

Для сбора данных EDR/DSSAD облачная система должна получить согласие пользователя с указанием срока хранения собранных данных VII. По истечении срока хранения собранные данные должны автоматически удаляться из облачной системы.

Если пользователи просят удалить свои данные до истечения срока хранения, облачная система должна удалить данные в соответствии с запросом. Когда пользователь запрашивает удаление данных, облачный интерфейс должен аутентифицировать этого пользователя и зарегистрировать все попытки получения доступа. Если аутентификация прошла успешно, координатор хранения данных использует представленную информацию VII для поиска связующей информации, которая хранится в базе данных VII. По найденной связующей информации координатор хранения данных осуществляет поиск данных EDR/DSSAD и обнаружив, удаляет их. Затем координатор хранения данных сохраняет регистрационную запись, касающуюся результата процедуры удаления, и сообщает результат запрашивающей стороне.

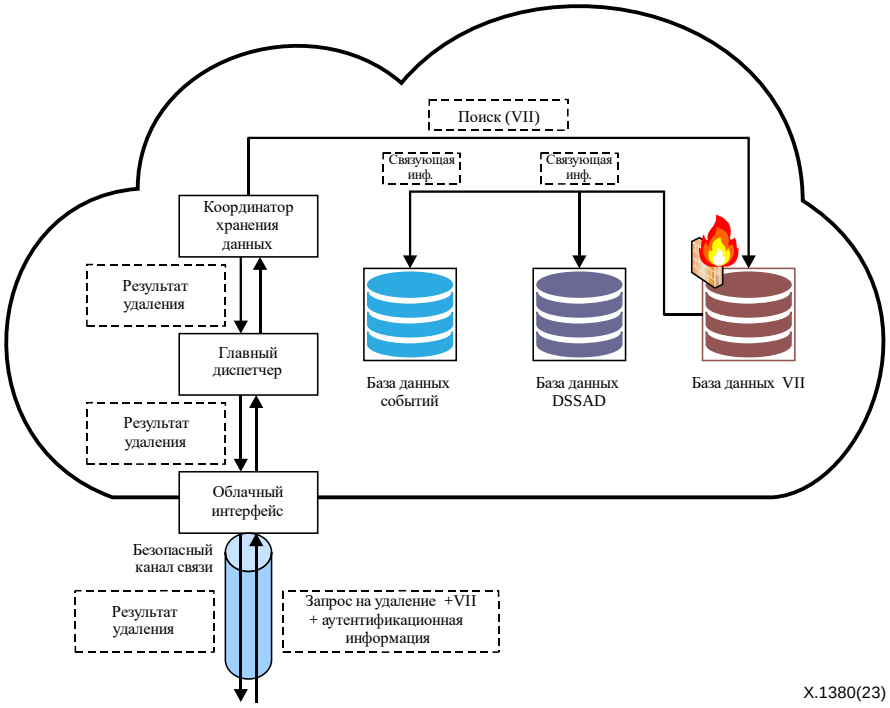

Рисунок 18 − Процедура удаления данных из раздельного хранилища

10.2 Регистрация транспортного средства в облачной системе

Процедура регистрации облачных регистраторов данных в автомобильной среде представлена на рисунке 19.

Как показано на рисунке 19, при поступлении от транспортного средства запроса аутентификации для его регистрации в облачной системе регистрации данных на этапе 1, на этапе 2 должна быть проведена проверка идентификатора этого транспортного средства, например, с использованием алгоритма цифровой подписи криптосистемы с открытым ключом. Запрос аутентификации транспортного средства может быть выполнен посредством передачи сообщения, подписанного личным ключом транспортного средства, в облачную систему регистрации данных. Если в результате проверки на этапе 2 идентификатор транспортного средства определен как недействительный, то на этапе 3 облачная система регистрации данных генерирует соответствующий ответ об ошибке аутентификации и передает его транспортному средству.

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

После получения ответа об аутентификации, то есть удачной аутентификации транспортного средства, пользователь создает информацию о регистрации в облачной системе регистрации данных, включая типы регистрируемых данных, периодичность сообщений и т. д., и на этапе 5 транспортное средство передает эту информацию в облачную систему регистрации данных, тем самым запрашивая регистрацию в облачной системе регистрации данных.

Затем в случае поступления от транспортного средства запроса на регистрацию в облачной системе регистрации данных, включающего информацию о регистрации в облачной системе регистрации данных, на этапе 6 облачная система регистрации данных формирует политику безопасности на основе информации о регистрации в облачной системе регистрации данных, такой как типы регистрируемых данных, периодичность сообщений и т. д., после чего сохраняет/регистрирует эту информацию.

После этого на этапе 7 облачная система регистрации данных назначает каждому транспортному средству псевдоним, генерирует запрос на получение сертификата псевдонима, назначенного каждому транспортному средству, и на этапе 8 передает запрос на сертификат в центр аутентификации.

На этапе 9 облачная система регистрации данных отслеживает получение сертификата псевдонима из центра аутентификации. Если сертификат псевдонима получен, облачная система регистрации данных

сохраняет его в базе данных облачной системы регистрации данных. Сертификат псевдонима может представлять собой сообщение из центра аутентификации с цифровой подписью. Обоснованность псевдонима удостоверяется его сертификатом.

Каждому транспортному средству может быть присвоено несколько псевдонимов. Поскольку псевдоним не содержит информации, связанной с идентификатором каждого транспортного средства, его PII может быть защищена.

При получении соответствующего уведомления облачная система регистрации данных на этапе 10 генерирует информацию о регистрации в облачной системе регистрации данных для каждого транспортного средства, сохраняет ее в базе данных облачной системы регистрации данных и передает каждому транспортному средству. Информация о регистрации в облачной системе регистрации данных может включать в себя псевдоним, назначенный каждому транспортному средству, сертификат псевдонима и т. п. Каждое транспортное средство, то есть пользователь транспортного средства, зарегистрированного в облачной системе регистрации данных, может выполнять регистрацию данных в облаке путем обмена сообщениями между облачным центром и транспортными средствами с использованием информации о регистрации в облачной системе регистрации, полученной из этой системы.

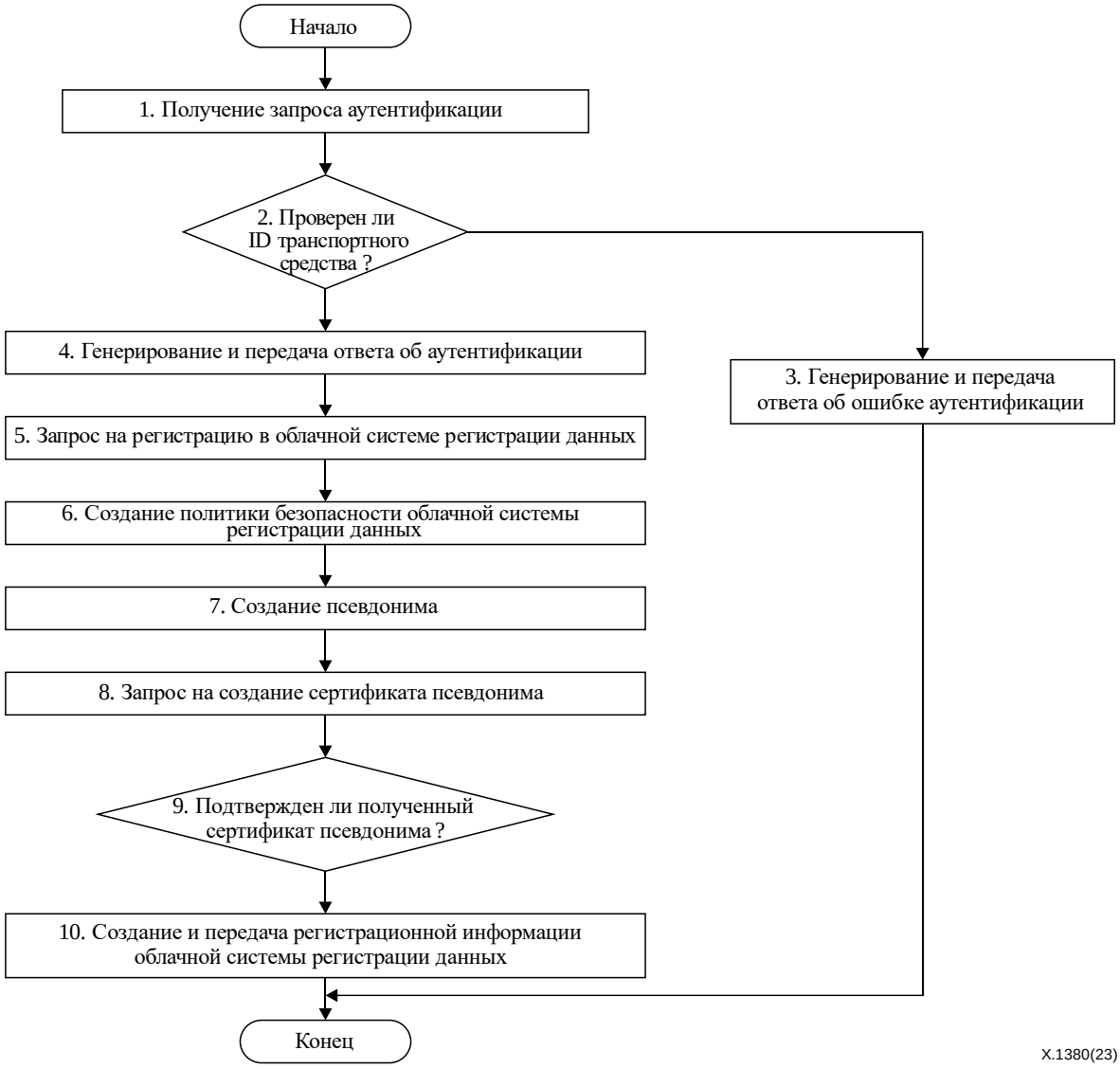

Рисунок 19 − Регистрация транспортного средства в облачной системе регистрации данных

В таких сценариях, как аренда транспортных средств, продажа бывших в употреблении транспортных средств и т. д., можно рассмотреть процедуру отмены регистрации транспортного средства в облачной системе регистрации данных, поскольку сменившиеся владельцы автомобиля не желают передавать данные EDR/DSSAD в облачную систему.

11 Сценарии использования облачных регистраторов данных в автомобильной среде

Когда происходит автомобильная авария, данные EDR/DSSAD можно реально использовать для анализа ее причин и определения того, являются ли автомобиль и водитель ответственными за нее. На рисунке 20 показан поток данных EDR/DSSAD. Данные EDR/DSSAD, сгенерированные в транспортном средстве, передаются в облако по линии беспроводной связи. Владелец, производитель, поставщик транспортного средства или уполномоченные третьи стороны (например, страховые компании) могут использовать данные EDR/DSSAD из облака.

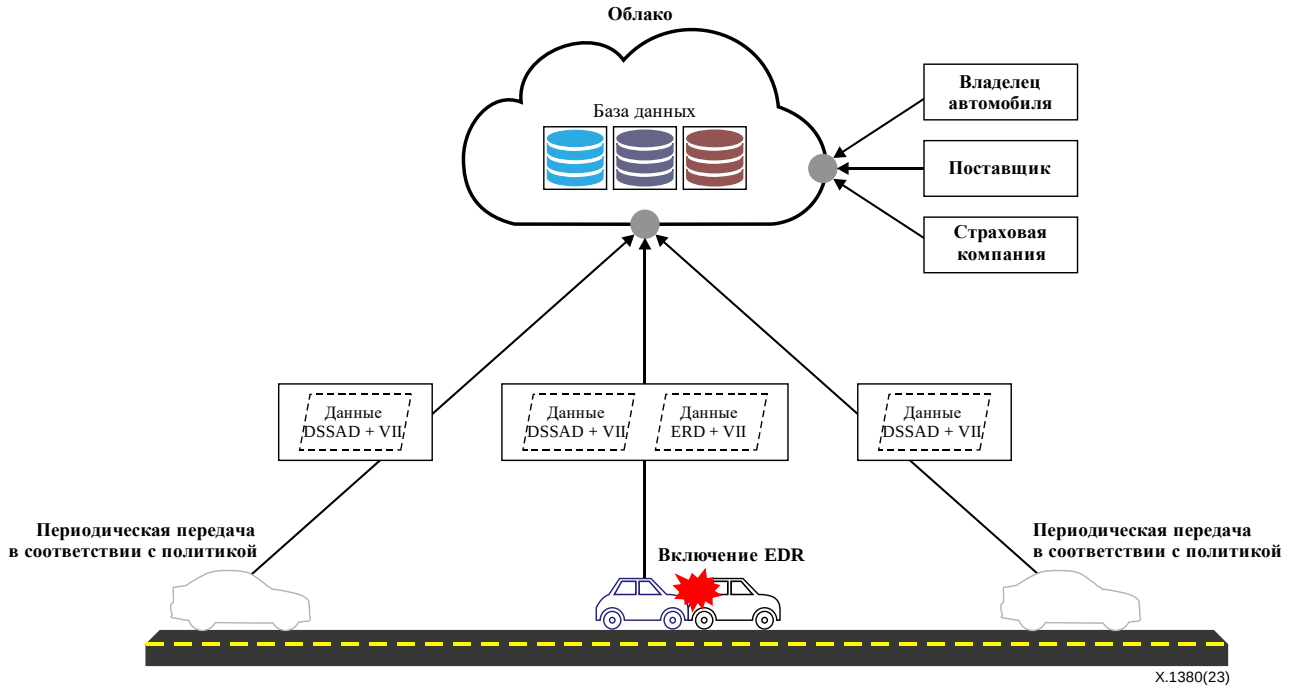

Рисунок 20 − Поток данных EDR/DSSAD

У облачной системы регистрации данных много преимуществ. Во-первых, данные EDR/DSSAD легко получить даже в потенциально рискованных ситуациях (например, при возгорании или затоплении транспортного средства). Во-вторых, авторизованным специалистам, осуществляющим анализ дорожно-транспортного происшествия, проще получить данные из облачной системы, чем непосредственно из ЭБУ транспортного средства.

11.1 Сценарий 1. Столкновение транспортных средств

На рисунке 21 в хронологическом порядке показан сценарий событий, происходящих во время движения по автодороге транспортного средства, оборудованного автоматизированной системой удержания полосы движения (ALKS). В точке *e)* происходит авария и включается EDR. Данные EDR/DSSAD о событиях с момента времени *a)*, когда включилась ALKS, до момента *e)*, когда произошла авария, сохраняются в облаке. Сохраненные данные EDR/DSSAD дают следующую информацию.

С 10:19:10, когда водитель включил ALKS, управление транспортным средством перешло к этой системе. Через 1 минуту 50 секунд погода испортилась и ALKS попросила водителя взять управление транспортным средством на себя, но водитель не отреагировал. В 10:22:00 ALKS автоматически выполнила минимально рискованный маневр (MRM). В 10:22:30 произошло столкновение.

Проанализировав данные EDR/DSSAD, можно установить время и обстоятельства аварии. Облачные системы регистрации данных хранят данные EDR/DSSAD в облачных хранилищах в соответствии с заданной политикой передачи данных. Это упрощает сбор информации об аварии по сравнению с прямым извлечением из ЗУ EDR в транспортном средстве.

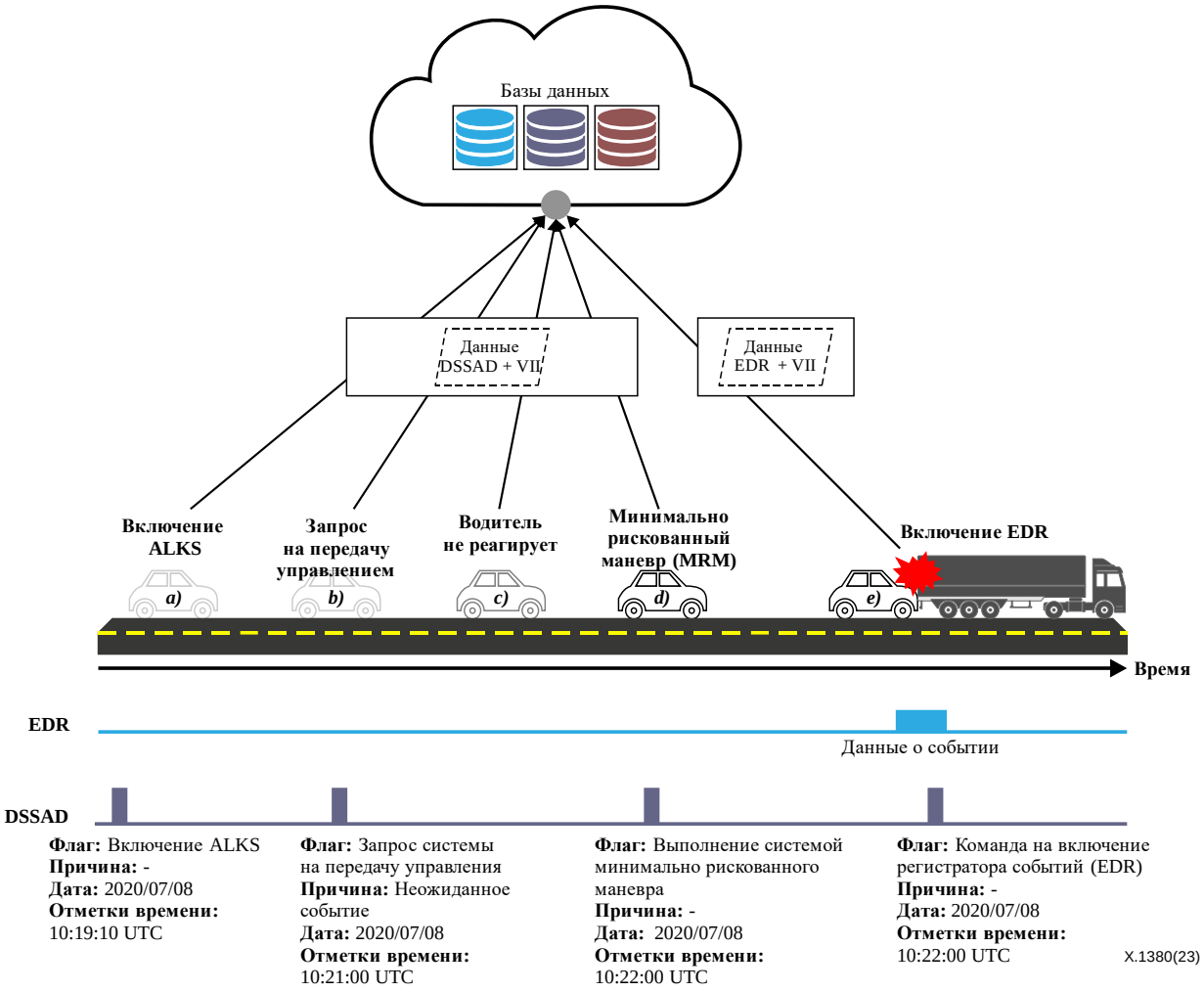

Рисунок 21 − Столкновение транспортных средств

11.2 Сценарий 2. Столкновение автомобиля с велосипедом

На рисунке 22 в хронологическом порядке показан сценарий событий во время движения по автодороге автомобиля, оснащенного ALKS. В точке *c)* происходит мягкое столкновение автомобиля с велосипедом, но поскольку удар довольно слабый, EDR не включается. Однако все недавние данные DSSAD загружены в облако. Сохраненные данные EDR/DSSAD дают следующую информацию.

> В 07:10:00 водитель включил ALKS. Через 15 секунд водитель управлял автомобилем непосредственно, и тогда ALKS выключилась. В 07:10:16 произошло столкновение автомобиля с велосипедом.

В данном случае воздействие на транспортное средство настолько незначительно, что условие включения EDR не выполнено, и данные EDR не собирались. Тем не менее аварийную ситуацию легко смоделировать и проанализировать во всех деталях, поскольку в облачной системе сохранены данные DSSAD.

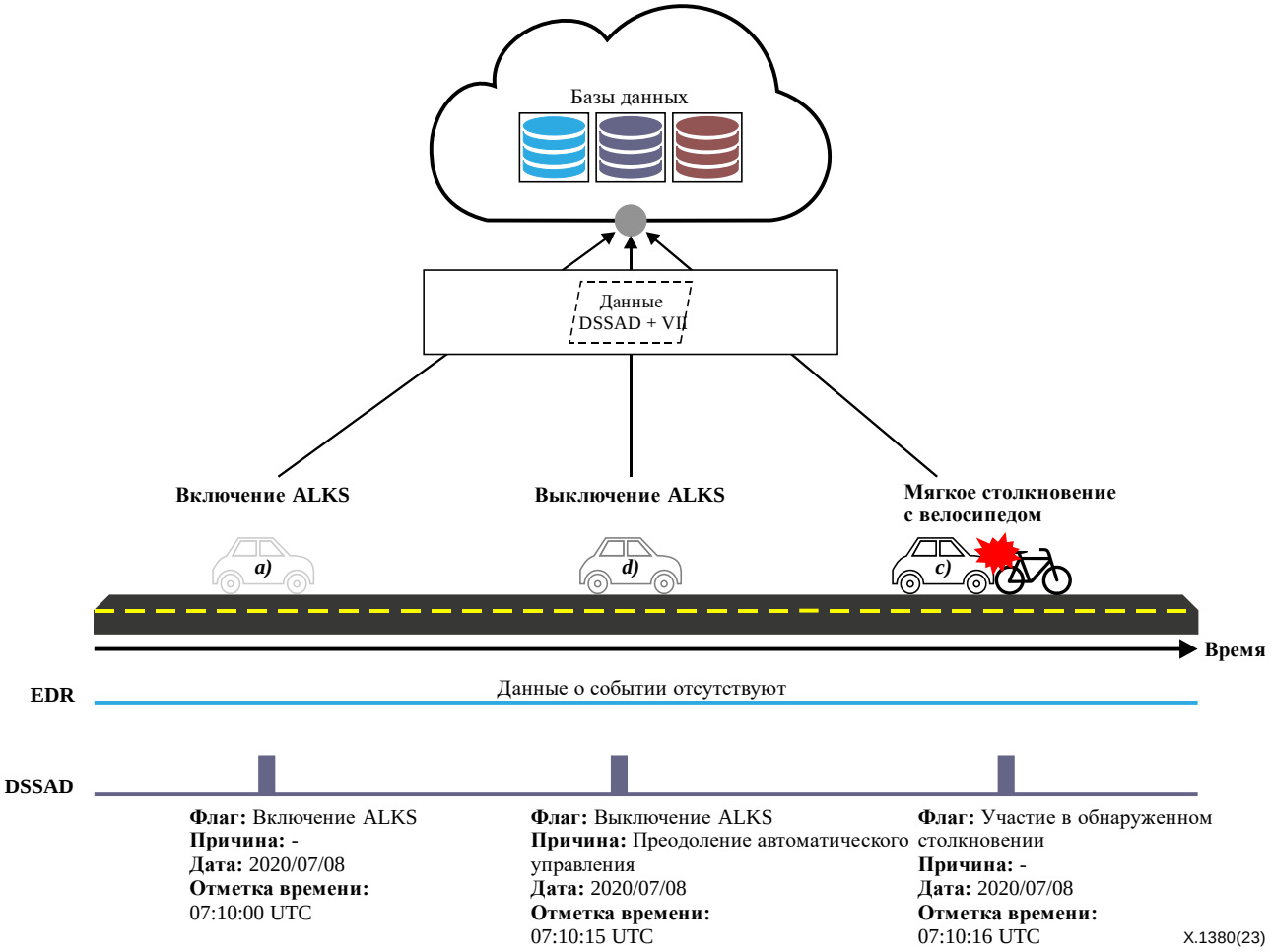

Рисунок 22 − Столкновение автомобиля с велосипедом

Дополнение I

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Пример набора данных обычного EDR

Этот пример набора данных представляет собой важный обязательный элемент данных обычных EDR, эксплуатация которых в Соединенных Штатах Америки (США) регулируется Национальным управлением безопасности дорожного движения (NHTSA).

Таблица I.1 − Важные обязательные элементы данных для обычного EDR [b-NHTSA EDR]

№ п/п	Элементы данных	Время записи*	Частота опроса	Диапазон значений	Точность	Разрешение
1	Характеристическая скорость в прямом направлении	От 0 до 250 мс или от 0 до конца события плюс 30 мс – в зависимости от того, что короче	100/с	От –100 до 100 км/ч	±10%	1 км/ч
2	Максимальная характеристическая скорость в прямом направлении	От 0 до 300 мс или от 0 до конца события плюс 30 мс – в зависимости от того, что короче	Н/П	От –100 до 100 км/ч	±10%	1 км/ч
3	Время максимальной характеристической скорости в прямом направлении	От 0 до 300 мс или от 0 до конца события плюс 30 мс – в зависимости от того, что короче	Н/П	От 0 до 300 мс или от 0 до конца события плюс 30 мс – в зависимости от того, что короче	±3 мс	2,5 мс
4	Приборная скорость транспортного средства	От –5,0 до 0 с	2/с	0–200 км/ч	±1 км/ч	1 км/ч
5	Открытие дроссельной заслонки двигателя, % от полного (ход педали акселератора, % от полного)	От –5,0 до 0 с	2/с	0–100%	± 5%	1%
6	Рабочий тормоз, вкл./выкл.	От –5,0 до 0 с	2/с	Вкл./выкл.	Н/П	Вкл./выкл.
7	Цикл включения/выключения зажигания на момент аварии	–1,0 с	Н/П	0–60 000	±1 цикл	1 цикл
8	Цикл включения/выключения зажигания на момент загрузки	В момент загрузки	Н/П	0–60 000	±1 цикл	1 цикл
9	Состояние ремня безопасности водителя	–1,0 с	Н/П	Вкл./выкл.	Н/П	Вкл./выкл.
10	Контрольная лампа фронтальной подушки безопасности	–1,0 с	Н/П	Вкл./выкл.	Н/П	Вкл./выкл.
11	Время срабатывания фронтальной подушки безопасности водителя (1-й этап для многоэтапных подушек безопасности)	Во время события	Н/П	0–250 мс	±2 мс	1 мс
12	Время срабатывания фронтальной подушки безопасности пассажира (1-й этап для многоэтапных подушек безопасности)	Во время события	Н/П	0–250 мс	±2 мс	1 мс
13	Количество событий (1 или 2)	Во время события	Н/П	1, 2	Н/П	1, 2
14	Время между событиями 1 и 2	По необходимости	Н/П	0–5,0 с	0,1 с	0,1 с
15	Файл записан полностью (да или нет)	После остальных данных	Н/П	Да/нет	Н/П	Да/нет

Н/П – неприменимо.

Библиография

[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 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.*

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2021 г.), *Базовые термины и определения в области управления определением идентичности.*

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

[b-UN R157] UN Regulation No. 157, *Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems.*

[b-UN R160] Addendum 159 – UN Regulation No. 160, *Uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder.*

[b-NHTSA EDR] NHTSA, *Final regulatory evaluation: Event data recorders (EDRs).*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие 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, энегоэффективность; 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.