Международный союз электросвязи

МСЭ-Т H.551

(01/2022)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ
И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Автомобильные шлюзы и интеллектуальные транспортные системы (ИТС) – Архитектура автомобильных шлюзов

Архитектура мультимедийных систем для транспортных средств

Рекомендация МСЭ-Т H.551

РЕКОМЕНДАЦИИ МСЭ-R СЕРИИ H

АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	H.100–H.199
ИНФРАСТРУКТУРА АУДИОВИЗУАЛЬНЫХ СЛУЖБ	
Общие положения	H.200–H.219
Мультиплексирование и синхронизация при передаче	H.220–H.229
Системные аспекты	H.230–H.239
Процедуры связи	H.240–H.259
Кодирование подвижных видеоизображений	H.260–H.279
Сопутствующие системные аспекты	H.280–H.299
Системы и оконечное оборудование для аудиовизуальных услуг	H.300–H.349
Архитектура услуг справочника для аудиовизуальных и мультимедийных услуг	H.350–H.359
Качество архитектуры обслуживания для аудиовизуальных и мультимедийных услуг	H.360–H.369
Телеприсутствие, среда с эффектом присутствия, виртуальная и расширенная реальность	H.420–H.439
Дополнительные услуги для мультимедиа	H.450–H.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	H.500–H.509
Мобильность для мультимедийных систем и услуг серии H	H.510–H.519
Приложения и услуги мобильной мультимедийной совместной работы	H.520–H.529
Защита мобильных мультимедийных систем и услуг	H.530–H.539
Защита приложений и услуг мобильной мультимедийной совместной работы	H.540–H.549
АВТОМОБИЛЬНЫЕ ШЛЮЗЫ И ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ (ИТС)	
Архитектура автомобильных шлюзов	**H.550–H.559**
Интерфейсы автомобильных шлюзов	H.560–H.569
ШИРОКОПОЛОСНЫЕ И МУЛЬТИМЕДИЙНЫЕ TRIPLE-PLAY УСЛУГИ	
Предоставление широкополосных мультимедийных услуг по VDSL	H.610–H.619
Усовершенствованные мультимедийные услуги и приложения	H.620–H.629
Доставка контента и приложения повсеместно распространенных сенсорных сетей	H.640–H.649
МУЛЬТИМЕДИЙНЫЕ УСЛУГИ IPTV И ПРИЛОЖЕНИЯ ДЛЯ IPTV	
Общие аспекты	H.700–H.719
Оконечные устройства IPTV	H.720–H.729
Промежуточное ПО для IPTV	H.730–H.739
Обработка событий приложений IPTV	H.740–H.749
Метаданные IPTV	H.750–H.759
Структуры мультимедийных приложений IPTV	H.760–H.769
Обнаружение услуги IPTV вплоть до ее использования	H.770–H.779
Цифровой информационный экран	H.780–H.789
МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ, УСЛУГИ И ПРИЛОЖЕНИЯ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ	
Системы персонального медицинского обслуживания	H.810–H.819
Проверка соответствия на функциональную совместимость систем персонального медицинского обслуживания (HRN, PAN, LAN, TAN и WAN)	H.820–H.859
Услуги обмена мультимедийными данными электронного здравоохранения	H.860–H.869
Безопасное прослушивание	H.870–H.879

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

Рекомендация МСЭ-Т H.551

Архитектура мультимедийных систем для транспортных средств

Резюме

В Рекомендации МСЭ-Т H.551 определена конфигурация мультимедийных систем для транспортных средств (VMS), эталонная модель архитектуры VMS и эталонное решение для мультимедийных приложений VMS. Наряду с этим рассматриваются вопросы безопасности VMS, а также вопросы защиты информации, позволяющей установить личность, и неприкосновенности частной жизни.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т H.551	28.01.2022 г.	16-я	11.1002/1000/14811

Ключевые слова

Архитектура, мультимедийные системы для транспортных средств.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение положений 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/авторскими правами на программное обеспечение, которые могут потребоваться для выполнения положений настоящей публикации. 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 соответствующим базам данных МСЭ-Т, имеющимся на веб-сайте МСЭ-Т по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т H.551

Архитектура мультимедийных систем для транспортных средств

1 Резюме

В настоящей Рекомендации определены функциональные возможности и конфигурации мультимедийных систем для транспортных средств (VMS), а также эталонная модель архитектуры VMS. Наряду с этим определены эталонная модель платформы мультимедийных услуг для транспортных средств, эталонный стек протоколов для конвергентной передачи и эталонная модель приемника бортовых устройств для мультимедийных приложений VMS. Рассматриваются вопросы безопасности VMS, а также вопросы защиты информации, позволяющей установить личность, и неприкосновенности частной жизни.

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 источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[ITU-T F.749.3] Рекомендация МСЭ-Т F.749.3 (2020 г.), *Сценарии использования и требования для мультимедийных сетей в транспортных средствах*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 мультимедийные сети для транспортных средств (vehicular multimedia networks) (VMN) [ITU-T F.749.3]: VMN состоит из платформы мультимедийных услуг для транспортных средств (VMSP), сетей радиовещания и связи, а также бортовой мультимедийной системы для транспортных средств (VMS).

3.1.2 платформа мультимедийных услуг для транспортных средств (vehicular multimedia service platform) (VMSP) [ITU-T F.749.3]: VMSP – это облачная платформа, которая позволяет предоставлять мультимедийные услуги конечному пользователю, находящемуся в транспортном средстве.

3.1.3 мультимедийная система для транспортного средства (vehicle multimedia system) (VMS) [ITU-T F.749.3]: VMS состоит из входов мультимедийной системы транспортного средства (VM I/P), мультимедийного блока транспортного средства (VMU) и выходов мультимедийной системы транспортного средства (VM O/P).

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 основная функция VMS (VMS core function): Функция мультимедийной системы транспортного средства (VMS), работающая с физическими, функциональными и логическими данными VMS.

3.2.2 сопряженная функция VMS (VMS associated function): Функция мультимедийной системы транспортного средства (VMS), которая только принимает и отображает функциональные и логические данные, поступающие от других систем или подсистем.

3.2.3 общая функция VMS (VMS shared function): Функция мультимедийной системы транспортного средства (VMS), используемая другими системами или подсистемами для обмена физическими, функциональными и логическими данными и управляющей информацией.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ADAS	Advanced Driver Assistance System		Усовершенствованная система помощи водителю
AM	Amplitude modulation	AM	Амплитудная модуляция
ANC	Active noise cancellation		Активное шумоподавление
APP	Application		Приложение
AR	Augmented reality		Дополненная реальность
AVM	Around view monitoring		Круговой обзор
bCall	Breakdown call		Аварийный вызов; вызов в случае неисправности
BGS	Background scan		Фоновое сканирование
CA	Conditional access		Условный доступ
CDN	Content Distribution Network		Сеть распределения контента
CDR	Convergent digital radio		Конвергированное цифровое радио
DAB	Digital audio broadcasting		Цифровое звуковое радиовещание
DASH	Dynamic Adaptive Streaming over HTTP		Динамическая адаптивная потоковая передача по протоколу HTTP
DMS	Driver monitoring system		Система контроля водителя
DNT	Do not track		Не отслеживать
DRM	Digital rights management		Управление цифровыми правами
DTTB	Digital Terrestrial Television Broadcasting	ЦНТВ	Цифровое наземное телевизионное вещание
eCall	Emergency call		Экстренный вызов
ECM	Entitlement control message		Сообщение контроля прав доступа
ECU	Electronic control unit	ЭБУ	Электронный блок управления
EMM	Entitlement management message		Сообщение управления правами доступа
FM	Frequency modulation	ЧМ	Частотная модуляция
GDPR	General Data Protection Regulation		Общий регламент по защите данных
HEO	High earth orbit	ВОО	Высокая околоземная орбита
HLS	HTTP Live Streaming		Потоковое вещание по протоколу HTTP
HMI	Human machine interface		Интерфейс человек–машина
HTTP	Hypertext Transfer Protocol		Протокол передачи гипертекста
HVAC	Heating, ventilation and air conditioning		Отопление, вентиляция и кондиционирование воздуха
IAM	Identity and Access Management		Управление определением идентичности и доступом
IBOC	In-band on-channel		Передача в общей полосе и по общему каналу
iCall	Information call		Информационный вызов

IP	Internet Protocol		Протокол Интернет
LCD	Liquid crystal display	ЖК	Жидкокристаллический дисплей
LED	Light emitting diode		Светоизлучающий диод
LEO	Low earth orbit	НОО	Низкая околоземная орбита
MR	Mixed reality		Смешанная реальность
NAT	Network Address Translation		Трансляция сетевых адресов
OBD	On-board diagnostics		Бортовая диагностика
OEM	Original equipment manufacturer		Производитель оригинального оборудования
OLED	Organic light emitting diode		Органический светодиод
OS	Operating system	ОС	Операционная система
OTA	Over the air		По каналам беспроводной связи
PD	Phase diversity	ФР	Фазовое разнесение
PII	Personally identifiable information		Информация, позволяющая установить личность
PUF	Physical unclonable function		Физическая неклонируемая функция
RDS	Radio data system		Система передачи данных по радио
RF	Radio frequency	РЧ	Радиочастота
RVC	Rear view camera		Камера заднего вида
TCP	Transfer Control Protocol		Протокол управления передачей
TMC	Traffic message channel		Канал сообщений о дорожном движении
UDP	User Datagram Protocol		Протокол пользовательских датаграмм
V2I	Vehicle-to-infrastructure		[Связь] транспортного средства с инфраструктурой
V2P	Vehicle-to-person		[Связь] транспортного средства с человеком
V2V	Vehicle-to-vehicle		[Связь] между транспортными средствами
V2X	Vehicle-to-everything		[Связь] транспортного средства с различными объектами
VM	Vehicular Multimedia		Мультимедиа для транспортных средств
VM I/P	Vehicle multimedia system inputs		Входы мультимедийной системы транспортного средства
VM O/P	Vehicle multimedia system outputs		Выходы мультимедийной системы транспортного средства
VMN	Vehicular multimedia network		Мультимедийная сеть транспортного средства
VMSP	Vehicular multimedia service platform		Платформа мультимедийных услуг для транспортных средств
VMS	Vehicle multimedia system		Мультимедийная система транспортного средства
VMU	Vehicle multimedia unit		Мультимедийный блок транспортного средства
VR	Virtual reality		Виртуальная реальность

5 Соглашения

В настоящей Рекомендации:

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

– ключевое слово "запрещается" означает 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 настоящей Рекомендации это требование не является обязательным;

– ключевое слово "не рекомендуется" означает требование, которое не является рекомендуемым, но при этом специально не запрещается, таким образом заявление о соответствии настоящей Рекомендации возможно даже при наличии данного требования.

6 Базовая информация

В настоящей Рекомендации определены функциональные возможности и конфигурации мультимедийных систем для транспортных средств (VMS) и эталонная модель архитектуры VMS в соответствии с требованиями, приведенными в [ITU-T F.749.3]. Наряду с этим определены эталонная модель платформы мультимедийных услуг для транспортных средств (VMSP), эталонный стек протоколов для конвергентной передачи и эталонная модель приемника бортовых устройств для мультимедийных приложений VMS. Рассматриваются вопросы безопасности VMS, а также вопросы защиты информации, позволяющей установить личность (PII), и неприкосновенности частной жизни.

Настоящая Рекомендация организована следующим образом:

В разделе 7 приведены определения функциональных возможностей и конфигураций VMS; в разделе 8 определена эталонная модель архитектуры VMS; в разделе 9 определена эталонная модель VMSP, эталонный стек протоколов для конвергентной передачи мультимедийного контента по разнородным сетям и эталонная модель приемника бортовых устройств. В разделе 10 рассматриваются вопросы безопасности VMS. В разделе 11 рассматриваются вопросы защиты PII и неприкосновенности частной жизни.

7 Функциональные возможности и конфигурации VMS

7.1 Функциональные возможности VMS

Функциональные возможности VMS определяются на основе следующих принципов:

– пользовательский интерфейс, развлекательные и информационные функции и приложения для водителя и пассажиров;

– требования, характерные для конкретных рынков, регионов и стран;

– требования законодательства и обязательные требования.

Однако функциональные возможности VMS не характеризуют ни общую сетевую архитектуру транспортных средств, ни интеграцию разных видов систем в транспортном средстве.

7.2 Конфигурации VMS

Конфигурации VMS основаны на следующих принципах:

– конфигурации VMS определяют отдельные требования к развлечениям и отображению информации для водителя и пассажиров;

– рекомендуется, чтобы конфигурации VMS были определены на уровне функциональных возможностей и функций;

– рекомендуется, чтобы в конфигурации VMS были включены аппаратные компоненты VMS;

– возможны несколько конфигураций VMS;

– рекомендуется, чтобы конфигурации VMS были высоконастраиваемыми. Рекомендуется рассматривать как оригинальные (заводские), так и подключаемые после приобретения транспортного средства компоненты VMS.

Однако конфигурации VMS не характеризуют ни общую сетевую архитектуру транспортных средств, ни интеграцию разных видов систем в транспортном средстве.

7.2.1 Решающие факторы

Конфигурации VMS определяются на основе следующих решающих факторов:

– требования к потребительским качествам;

– функциональные возможности, функциональные требования;

– требования к интерфейсу;

– требования к стоимости;

– сравнительные требования.

7.3 Перечень функциональных возможностей VMS

Эталонные функциональные возможности VMS приведены в таблице 1.

Таблица 1 – Эталонные функциональные возможности VMS

Функциональные возможности	Подфункции	Возможность настройки
Интерфейс человек–машина (HMI)	Технология отображения информации	Светодиодный дисплей (LED)/жидкокристаллический дисплей (ЖК)/дисплей на органических светодиодах (OLED) и т. д.
	Количество дисплеев	Несколько (передний, центральный, задний и т. д.)
	Управление	Традиционные средства управления: кнопки/ручки/ сенсорные элементы управления и т. д.
		Интеллектуальное управление: голосовое управление, распознавание лиц, голосовые биометрические данные, жесты, персонализация, управление посредством движения глаз, сенсорная тактильно-гибкая обратная связь и т. д.
	Многоэкранное взаимодействие	Вывод информации на разные экраны
		Синхронное или асинхронное воспроизведение видеофайлов
		Сдвоенный навигационный дисплей
		Свободное согласование интерфейса дисплеев
	Системный язык	Пользовательский интерфейс: различные требования к языку в соответствии с правилами
	Дисплей видеокамеры	Камера заднего вида (RVC)/круговой обзор (AVM)
	Управление и отображение информации	Дисплей и элементы управления отоплением, вентиляцией и кондиционированием воздуха (HVAC)
		Средства управления и дисплеи системы помощи водителю
Радиовещание	Наземное	Аналоговое: радиовещание с амплитудной модуляцией (АМ), радиовещание с частотной модуляцией (ЧМ), ЧМ-радиовещание с двойным тюнером и фазовым разнесением (ФР), ЧМ-радиовещание с фоновым сканированием (BGS), система передачи данных по радио (RDS) и т. д.
		Цифровое: цифровое звуковое радиовещание (DAB), цифровое наземное телевизионное вещание (ЦНТВ), технологии передачи в пределах той же полосы и по тому же каналу (IBOC), конвергированное цифровое радио (CDR) и т. д.
	Спутниковое	Услуги спутниковой системы передачи звука/видеоданных (например, услуги потоковой передачи звука/изображения по каналам спутниковой связи)

Таблица 1 – Эталонные функциональные возможности VMS

Функциональные возможности	Подфункции	Возможность настройки
Подключение к внешней сети	Сети сотовой связи	3G/4G/5G
	Двусторонняя спутниковая связь	Спутниковые сети двусторонней связи на низкой околоземной орбите (НОО)
		Спутниковые сети двусторонней связи на высокой околоземной орбите (ВОО)
	Связь транспортного средства с различными объектами (V2X)	Связь между транспортными средствами (V2V), связь транспортного средства с инфраструктурой (V2I), связь транспортного средства с человеком (V2P)
	Беспроводные локальные сети	Точки доступа IEEE 802.11
Подвижная связь в транспортных средствах		Вызовы по громкой связи и воспроизведение музыки с использованием персональной сети
		Веб-серфинг с использованием локальных сетей IEEE 802.11
		Совместное использование экрана через сети малого радиуса действия
		Сторонние приложения для интерфейса транспортных средств
Конфигурации телематики	Пульт ДУ	Дистанционный контроль, управление, передача данных о транспортном средстве
	Вызовы	Экстренный вызов (eCall), аварийный вызов (bCall), информационный вызов (iCall)
Онлайновые магазины/ пакеты приложений	Магазин приложений	Загрузка новых функций
	Магазин тем	Замена тематических скинов
Обновление по каналам беспроводной связи (OTA)		Программное обеспечение OTA
Средства передачи	Звук	Обычное и высокое качество воспроизведения
	Изображение	В разных форматах
	Видео	Обычное видео с различными значениями оптического разрешения, дополненная реальность (AR), виртуальная реальность (VR), смешанная реальность (MR)
Навигация	Локальная навигация	
	Облачная навигация	Данные от модема телематического блока (3G/4G/5G)/ мобильные данные пользователя
	Трафик в режиме реального времени	Канал сообщений о дорожном движении (TMC), Группа экспертов по транспортному протоколу (TPEG), центр сообщений о дорожном движении в реальном времени и т. д.
	Службы	Навигационные службы, службы прогноза погоды в режиме реального времени и т. д.
	Расширенные возможности	Интеллектуальные приложения для путешественников, такие как календарь, планировщики и т. д.

Таблица 1 – Эталонные функциональные возможности VMS

Функциональные возможности	Подфункции	Возможность настройки
Распознавание голоса (VR) и синтез речи	Локальное VR, облачное VR и синтез речи	Понимание естественного языка
		Автоматическое распознавание речи
		Преобразование текста в речь
Звук	Качество звука	Функция регулирования громкости и скорости воспроизведения
		Алгоритмы обработки звука
		Активное шумоподавление (ANC)
		Настройки персонализации (звуковые шаблоны и распознавание лиц)
		Регулировка оптимального положения прослушивания
		Технология снижения качества звука
	Конфигурации усилителя	Многоканальные встроенные усилители
		Усилители с громкоговорителями
	Конфигурация звука	Несколько конфигураций громкоговорителей твитер (высокочастотный громкоговоритель)/вуфер (низкочастотный громкоговоритель)/широкополосные громкоговорители
Безопасность		Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций
		Сетевая безопасность
		Операционная безопасность
		Безопасность приложений
		OTA-безопасность программного обеспечения
		Безопасность оборудования
		Криптографическая безопасность
Конфиденциальность		Общие вопросы защиты данных
		Защита персональных данных
		Защита видимости данных
		Конфиденциальность, целостность и доступность
Интеллектуальные функции	Система контроля водителя (DMS)	Распознавание усталости, выражения лица и эмоций
	Охрана здоровья	Кардиомонитор и монитор артериального давления
	Офисная среда	Электронная почта, видео-конференц-связь, голографическая проекция, распознавание жестов, управление посредством движения глаз, рукописные заметки
	Игры	Голосовые интерактивные викторины, интерактивные голографические игры, приключенческие игры
	Общение	Социальные приложения в транспортных средствах

ПРИМЕЧАНИЕ. – Функциональные возможности, обеспечивающие безопасность и неприкосновенность частной жизни, необходимы для VMS в конфигурациях M1–M5, но их можно настроить для VMS в конфигурации M0. Примеры VMS в конфигурациях M0–M5 приведены в Дополнении I к [ITU-T F.749.3].

8 Архитектура VMS

В данном разделе приведены классификация функций VMS, решающие факторы и эталонная модель архитектуры VMS.

8.1 Функции VMS

В общем случае функции VMS можно разделить на три категории: основные функции VMS, сопряженные функции VMS и общие функции VMS.

Основные функции VMS – это функции VMS, работающие с физическими, функциональными и логическими данными VMS. В качестве примеров основных функций VMS можно назвать функции тюнера, обработки мультимедиа, отображения информации и т. д.

Сопряженные функции VMS – это функции, которые только принимают и отображают функциональные и логические данные из других систем или подсистем. К примерам сопряженных функций VMS относятся передача данных с камеры заднего вида транспортного средства, отображение информации eCall в случае аварии и т. д.

Общие функции VMS – это функции, используемые другими системами или подсистемами для обмена физическими, функциональными и логическими данными и управляющей информацией. Примерами общих функций VMS могут служить функции управления HVAC через мультимедийный блок транспортного средства (VMU).

8.2 Решающие факторы при выборе архитектуры VMS

На выбор архитектуры VMS влияют следующие факторы:

– технические требования;
– требования к операционной системе, памяти и оборудованию;
– функциональные возможности, подсистемы, логические и физические требования;
– требования к интерфейсу;
– требования к стоимости;
– требования к потребительским качествам;
– сравнительные требования;
– требование соответствия стандартам.

8.3 Эталонная модель архитектуры VMS

Архитектура VMS определяется на уровне интерфейса, подсистем и систем. Эталонная модель архитектуры VMS представлена на рисунке 1.

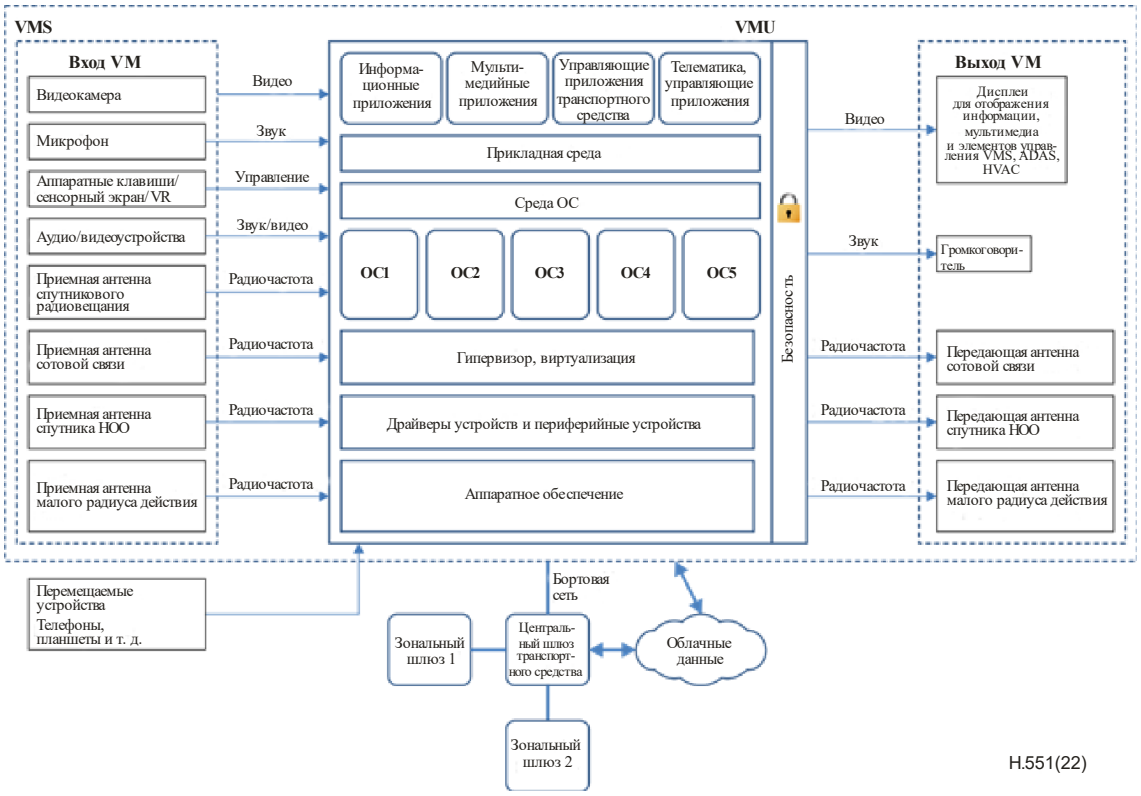

Рисунок 1 – Эталонная модель архитектуры VMS

8.3.1 Приложения

К приложениям VMS относятся:

– информационные приложения, например приборная панель, верхние дисплеи, навигация и прогноз погоды;

– мультимедийные приложения, например медиаплеер, навигация, виртуальная реальность и интерфейс человек–машина и др.;

– приложения для управления транспортным средством, например HVAC и соединенные автомобили;

– телематические приложения, например дистанционное управление, диагностика и доступ к данным;

– приложения для отображения информации, например передний и задний дисплеи.

8.3.2 Прикладная среда

Доступ к функциям и функциональным возможностям VMS осуществляется с помощью инструментов пользовательского интерфейса, соответствующих прикладной среде.

8.3.3 Среда операционной системы (ОС)

Среда ОС управляет системными службами. Это может быть проприетарная среда производителей оригинального оборудования (OEM) и разработчиков VMS.

8.3.4 Операционная система

В зависимости от требований к нагрузке, скорости и точности обработки используются различные встроенные операционные системы (ОС) и ядра.

8.3.5 Гипервизор и виртуализация

Для поддержки нескольких операционных систем и обработки задач одним мощным процессором посредством совместного использования вычислительных ресурсов используются методы гипервизора и виртуализации.

8.3.6 Драйверы устройств и периферийные устройства

К драйверам устройств относятся драйвер сетевого интерфейса транспортного средства, драйверы аудио- и видеоустройств, драйверы дисплеев, драйверы протоколов межпроцессорной связи и драйверы протоколов внутрипроцессорной связи.

8.3.7 Аппаратное обеспечение

Аппаратное обеспечение включает в себя процессоры, память и другие компоненты.

8.3.8 Облачные данные

К облачным данным относятся:

– данные мультимедийных служб;

– данные телематических служб, то есть служб дистанционной диагностики, служб OTA обновления программного обеспечения, служб eCall/bCall/iCall и служб навигации.

9 Мультимедийные приложения VMS

На рисунке 2 представлена система для мультимедийных приложений VMS, которая состоит из платформы облачных мультимедийных услуг для транспортных средств (VMSP), разнородных сетей и бортовых устройств. Для повышения эффективности передачи мультимедийного контента по разнородным сетям, то есть сетям спутникового радиовещания и сетям подвижной связи, используется схема конвергентной передачи. В данном разделе приведено описание эталонной модели VMSP (пункт 9.1), эталонного стека протоколов для конвергентной передачи мультимедийного контента по разнородным сетям (пункт 9.2) и эталонной модели приемника бортовых устройств (пункт 9.3).

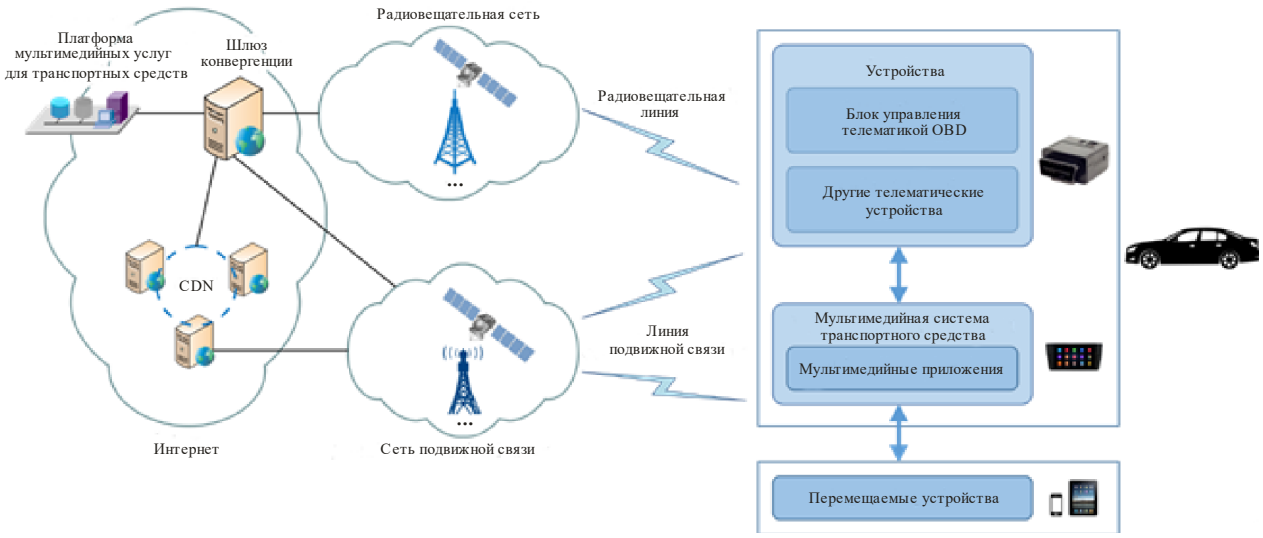

Рисунок 2 – Диаграмма системы для мультимедийных приложений VMS

9.1 Эталонная модель VMSP

VMSP состоит из сервера контента, сервера лицензий (необязательно) и сервера условного доступа (CA) (необязательно). Эталонная модель VMSP показана на рисунке 3.

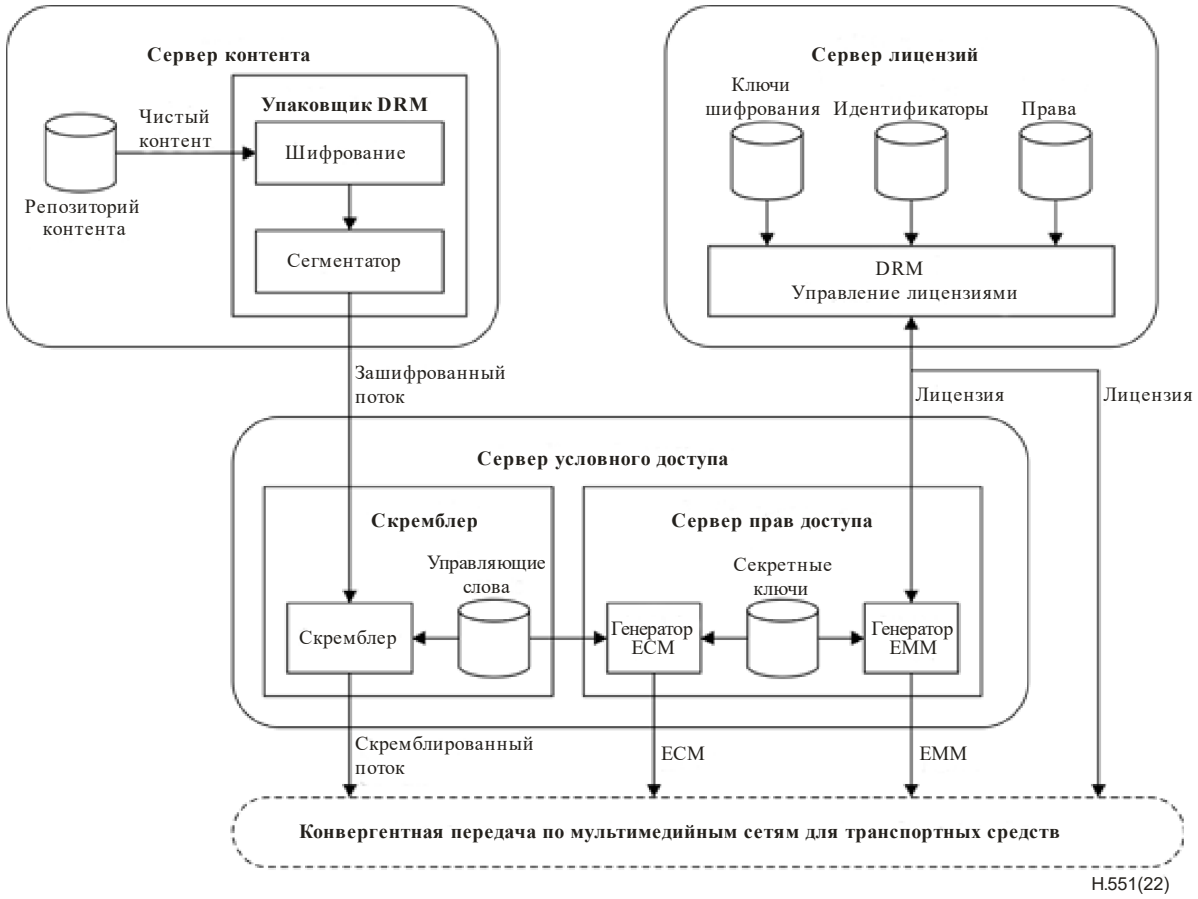

Рисунок 3 – Эталонная модель VMSP

Сервер контента состоит из репозитория контента и упаковщика системы управления цифровыми правами (DRM). Репозиторий контента используется для хранения чистого контента, который хочет распространять поставщик контента (CP). Следует отметить, что репозиторий контента нередко бывает встроен в решение DRM, а иногда интегрируется в систему управления контентом, которая взаимодействует с сервером DRM. Упаковщик DRM шифрует и упаковывает мультимедийный контент для потоковой передачи по VMN. Сервер лицензий используется для управления созданием, изменением и отзывом лицензий DRM. Лицензия DRM содержит идентификаторы, спецификацию прав и ключи шифрования. Обычно клиенты DRM могут приобрести свои лицензии DRM на сервере лицензий, используя соединения по сети подвижной связи. В качестве схем упаковки для потоковой передачи в VMN могут использоваться MPEG-DASH [b-ISO/IEC 23009-1] и HLS [b-IETF RFC 8216].

Сервер условного доступа (CA) состоит из скремблера и сервера прав доступа. Скремблер используется для скремблирования входящих потоков с помощью управляющих слов. Сервер прав доступа используется для генерирования сообщений контроля прав доступа (ECM) и сообщений управления правами доступа (EMM). Исходящие скремблированные потоки сообщений ECM и EMM, как правило, доставляются по сетям спутникового радиовещания. Однако имеются следующие два исключения.

1) Когда транспортное средство оказывается в месте, где отсутствует покрытие сетей сотовой связи, лицензии DRM не могут быть получены по какой-либо сети подвижной связи. В этом случае лицензии DRM могут встраиваться в EMM и доставляться пользователю по спутниковым сетям. Таким образом может обеспечиваться непрерывность обслуживания.

2) Когда оператор услуг связи начинает свое дело, тысячи новых клиентов могут попытаться активировать свои устройства в течение короткого периода времени. Однако в сетях спутникового радиовещания может недоставать полосы пропускания для доставки сообщений EMM на их устройства. В этом случае сообщения EMM могут быть временно перенесены из сетей спутникового радиовещания в сети подвижной связи. Таким образом можно обеспечить успешное начало работы оператора.

9.2 Эталонный стек протоколов для конвергентной передачи

Широковещательная передача обычно считается наиболее экономичным способом доставки линейных программ широкому кругу населения на обширных географических территориях. Несмотря на успехи фиксированного цифрового телевизионного вещания в Ka- и Ku-диапазонах во всем мире, предоставление услуг для транспортных средств посредством радиовещания оказалось сложной задачей. Например, в городских условиях надежность широковещательной связи является довольно проблематичной из-за движущихся приемников и частой блокировки сигнала высокими зданиями. Проблема радиовещания в городах может быть решена с помощью наземных ретрансляционных сетей, которые заполняют пробелы в охвате, однако создание ретрансляционной инфраструктуры является дорогостоящим делом и требует очень много времени. Еще одно ограничение широковещательной связи заключается в однонаправленном характере ее услуг и, следовательно, ее неспособности обеспечить предоставление персонализированных услуг или взаимодействие с пользователем.

Для решения этих проблем предлагается схема конвергентной передачи мультимедийного контента через VMN, когда большая часть мультимедийного контента доставляется массовому пользователю по радиовещательным сетям, а сети подвижной связи применяются лишь для восстановления пакетов, отброшенных радиовещательными сетями. Скремблированные потоки от VMSP поступают в шлюзы конвергенции, где сегменты медиаданных оформляются в виде последовательных пакетов и передаются всем пользователям по спутниковой радиовещательной сети. Недостающие или ошибочные пакеты таких потоков легко обнаруживаются в терминале. Эти отброшенные пакеты восстанавливаются путем их повторной передачи по сети подвижной связи. Когда мультимедийные потоки будут беспрепятственно восстановлены, терминал может не только воспроизводить их на дисплеях и в динамиках в кабине транспортного средства, но и служить в качестве локального информационно-развлекательного центра для передачи этих мультимедийных потоков всем пассажирам на их персональные устройства, такие как смартфоны и планшеты, через Wi-Fi. Схема конвергентной передачи приведена на рисунке 4.

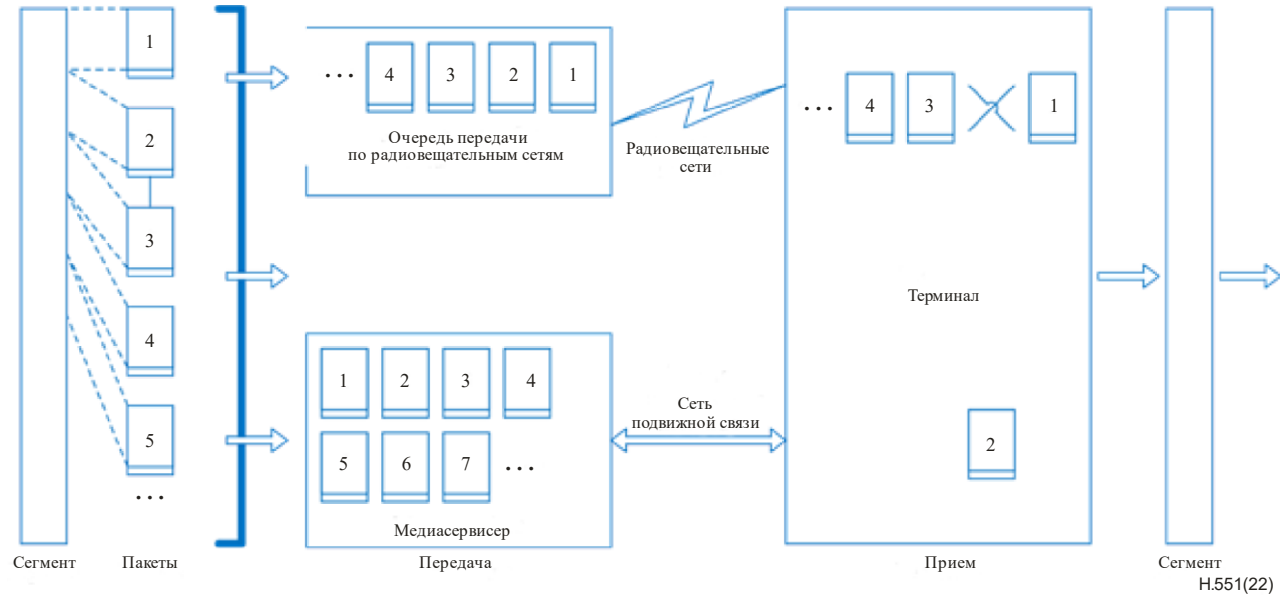

Рисунок 4 – Обработка данных при конвергентной передаче

Схема конвергентной передачи в полной мере использует взаимодополняющие преимущества радиовещательных сетей и сетей подвижной связи. Следовательно, системы услуг потоковой передачи мультимедиа через VMN обеспечивают оптимальную эффективность.

На рисунке 5 показан эталонный стек протоколов для конвергентной передачи мультимедийного контента по VMN. Следует отметить, что протоколы конвергентной передачи не зависят от базовых стандартов физического уровня и прозрачны для стандартов верхних уровней. Таким образом можно гарантировать, что потребуется лишь минимальная модификация существующей инфраструктуры радиовещания или подвижной связи.

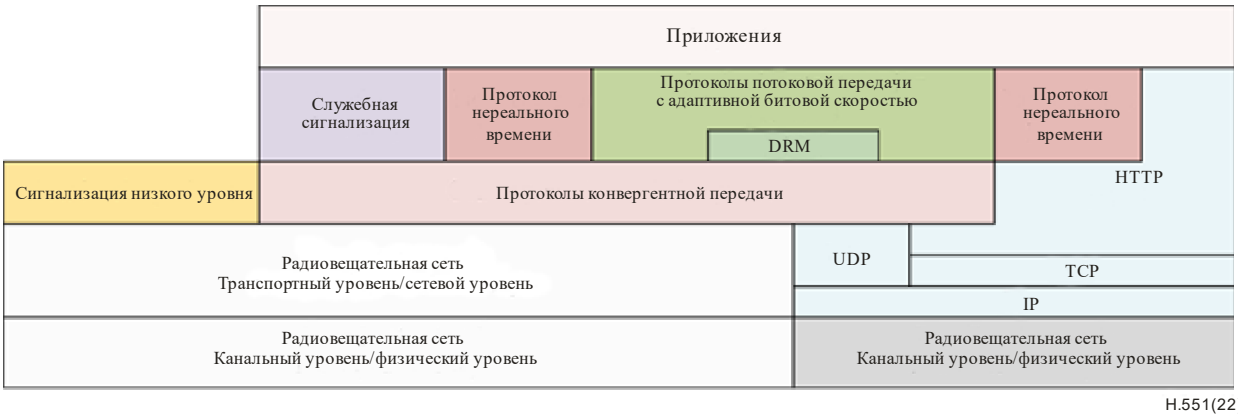

Рисунок 5 – Эталонный стек протоколов для конвергентной передачи

Общее предположение состоит в том, что протокол сетевого уровня может быть основан на обеих версиях протокола IP (IPv4 и IPv6). Для прямого и безопасного соединения между VMS и облачными платформами целесообразно выбирать IPv6 [b-IETF RFC 8200] по следующим причинам.

– IETF четко рекомендует другим организациям по разработке стандартов (OPC) отдавать предпочтение IPv6 [b-IAB]. В результате в работе по стандартизации рекомендуется предполагать использование IPv6.

– Адресное пространство IPv4 было формально исчерпано в январе 2011 года, когда Орган присвоения номеров интернета (IANA) присвоил последнее адресное пространство IPv4 верхнего уровня (то есть /8). Таким образом, принятие IPv6 в качестве единственного сетевого протокола является единственным жизнеспособным решением, гарантирующим развитие сетевых служб и приложений.

– Переход исключительно на IPv6 считается стратегической инициативой ряда государственных ведомств. Одним из примеров может служить документ [b-USG OMB], в котором Федеральным правительством США устанавливаются конкретные сроки и цели для перевода сетей его национальных управлений на IPv6.

– Пользовательским устройствам, расположенным в транспортном средстве, может потребоваться сквозная доступность, например, для подключения к любым приложениям и платформам. В этом случае нельзя использовать трансляцию сетевых адресов (NAT) [b-IETF RFC 2663] в сочетании с частной адресацией IPv4. И наоборот, IPv6 обеспечивает полную поддержку международной схемы адресации, при которой пользовательские устройства всегда доступны.

Хотя люди лучше знакомы с IPv4, а развертывание IPv6 связано с определенными новыми проблемами, рост числа пользователей и объемов трафика IPv6 происходит намного быстрее, чем IPv4. Это означает, что с учетом всех обстоятельств коллективный разум отрасли выбрал на будущее IPv6 [b-ETSI WP35].

9.3 Эталонная модель приемника

Эталонная модель приемника бортовых устройств представлена на рисунке 6, где обозначены следующие функции:

– радиовещательные соединения и широкополосные соединения, обеспечивающие возможность подключения приемника для приема сигналов и данных;

– стек протоколов конвергентной передачи/UDP/HTTP/TCP/IP и стек протоколов HTTP/TCP/IP – объектно ориентированных транспортных протоколов приемника для приема ресурсов потоковой передачи с адаптивной битовой скоростью (например, DASH или HLS) для услуг потоковой передачи мультимедийного контента;

– низкоуровневая сигнализация – передача сигналов по радиовещательным сетям, позволяющая приемнику создать список основных услуг и инициировать обнаружение служебных сигналов для каждой мультимедийной услуги;

– служебная сигнализация – сигнализация, относящаяся к службам, которая позволяет приемнику обнаруживать услуги потоковой передачи мультимедийного контента и получать доступ к ним и к компонентам их контента;

– кэш – временное хранение и обработка манифестов, сегментов инициализации и сегментов медиаданных, прием которых облегчается служебной сигнализацией;

– сервер потоковой передачи с адаптивной битовой скоростью (то есть DASH/HLS) – локальный сервер потоковой передачи с адаптивной битовой скоростью, используемый для абстрагирования нижележащих уровней по отношению к клиенту потоковой передачи с адаптивной битовой скоростью. Манифесты, сегменты инициализации и сегменты медиаданных для клиента потоковой передачи с адаптивной битовой скоростью передаются через сервер потоковой передачи с адаптивной битовой скоростью;

– клиент потоковой передачи с адаптивной битовой скоростью – функция, использующая манифесты и сегменты и взаимодействующая с другими компонентами в приемнике для персонализации работы с мультимедиа в зависимости от функциональных возможностей платформы, а также предпочтений и действий пользователя;

– приложение – встроенное или загружаемое приложение, которое использует данные, доставляемые по радиовещательной или широкополосной сети, чтобы предоставлять конечному пользователю разнообразные и интерактивные услуги.

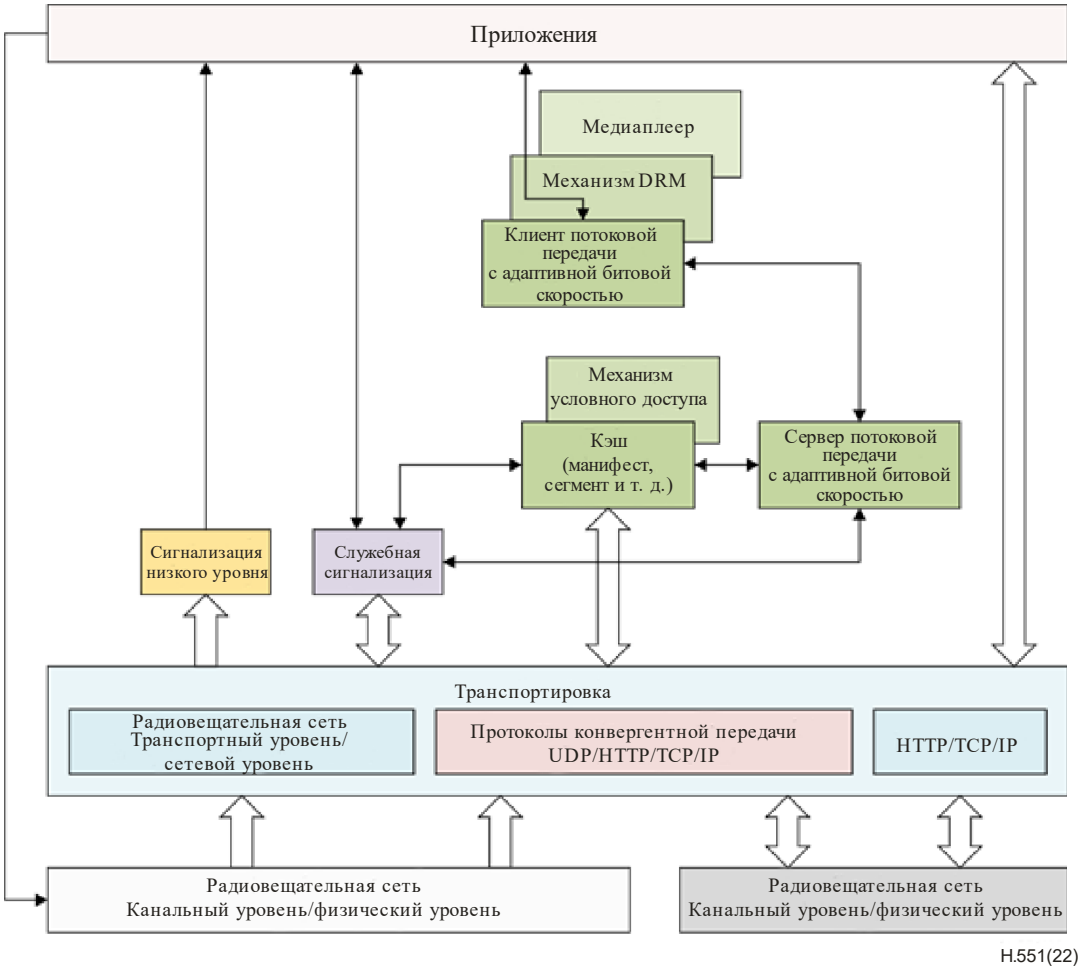

Рисунок 6 – Эталонная модель приемника бортовых устройств

Ниже представлена типичная последовательность начальной загрузки эталонного приемника.

– Приложение запрашивает предварительно составленный список услуг в системе сигнализации низкого уровня. Список услуг доставляется в это приложение, которое затем обеспечивает пользовательский интерфейс для выбора услуг потоковой передачи мультимедийного контента. Пользователь выбирает услугу потоковой передачи мультимедийного контента.
– Приложение с помощью информации о точке входа служебной сигнализации, содержащейся в списке услуг для выбранной услуги, предоставляет информацию для доступа к стеку протоколов конвергентной передачи/UDP/HTTP/TCP/IP в целях получения сигналов служебной сигнализации. Сигналы служебной сигнализации доставляются в это приложение.
– С помощью служебной сигнализации приложение предоставляет информацию для доступа к стеку протоколов конвергентной передачи/UDP/HTTP/TCP/IP в целях загрузки медиакомпонентов выбранной услуги в формате потоковой передачи с адаптивной битовой скоростью, которые направляются в кэш для сохранения, дескремблируются и впоследствии пересылаются на сервер потоковой передачи с адаптивной битовой скоростью.
– После выбора услуги приложение активирует клиента потоковой передачи с адаптивной битовой скоростью, в результате чего клиент DASH/HLS запрашивает и принимает сегменты медиаданных от сервера потоковой передачи с адаптивной битовой скоростью, как только они становятся доступными.
– После приема сегментов медиаданных комбинированная функция, состоящая из клиента потоковой передачи с адаптивной битовой скоростью, механизма DRM и медиаплеера, декодирует принятые сегменты и декодированные медиаданные возвращаются в приложение для воспроизведения.

10 Безопасность VMS

Взаимодействие между VMS и другими компонентами, участвующими в обеспечении безопасности автомобиля (обычно электронным блоком управления (ЭБУ)), рекомендуется ограничить общими функциями, указанными в пункте 8.1.

Подробная информация приведена в Приложении A.

11 Защита информации, позволяющей установить личность (PII), и неприкосновенность частной жизни

Так как транспортные средства становятся соединенными и предоставляют все больше интерактивных услуг, рекомендуется, чтобы VMS обеспечивала сквозную защиту. Для обеспечения конфиденциальности и целостности пользовательских данных, хранящихся в VMS, в транспортном средстве и в облаке VMS или на внутренних серверах, необходимо защищать все больше пользовательских данных и информации, связанной с неприкосновенностью частной жизни.

Подробная информация приведена в Приложении B.

Приложение A

Безопасность VMS

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

A.1 Обзор

Взаимодействие между VMS и другими компонентами, участвующими в обеспечении безопасности автомобиля (обычно ЭБУ), рекомендуется ограничить общими функциями, указанными в пункте 8.1. Рекомендуется, чтобы VMS не оказывала негативного воздействия на функции других компонентов, обеспечивающие требуемую безопасность автомобиля, особенно в случае автономных транспортных средств.

Что касается безопасности самой VMS, то предполагаемые угрозы для VMS и ее экосистемы кратко изложены в пункте A.2, а возможности защиты от этих угроз представлены в качестве справочной информации в пункте A.3.

A.2 Предполагаемые угрозы для VMS и ее экосистемы

A.2.1 Угрозы для платформы мультимедийных услуг для транспортных средств (VMSP)

В последние годы значительно увеличилось разнообразие возможностей установления соединений в транспортных средствах, и, в частности, настоятельно требуется возможность установления соединений с различными серверами, расположенными в VMSP. В контексте VMS к удаленным серверам, называемым VMSP, относятся серверы, предоставляемые OEM, поставщиками оборудования и поставщиками услуг для поддержки экосистемы транспортных средств из удаленного центра обработки данных. Можно выделить следующие виды угроз, связанных с VMSP:

– использование серверов, расположенных в VMSP, для осуществления атак на транспортные средства или извлечения данных;

– предоставление услуг поврежденными VMSP;

– потеря или компрометация данных, хранящихся на серверах в VMSP.

A.2.2 Угрозы для транспортных средств, связанные с каналами связи

К услугам связи для транспортного средства относятся услуги внешней связи по сотовым сетям, через спутник НОО, радиовещательные сети и сети малого радиуса действия. Каналы, используемые для этих видов связи, могут быть объектами атак, таких как спуфинг, прослушивание, манипуляция с сообщениями и др. Можно выделить следующие виды угроз, связанных с каналами связи:

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

  Интерфейсы VM могут использоваться для получения доступа к другой (интеллектуальной) инфраструктуре транспортного средства (например, к ЭБУ, не имеющему отношения к VMS).

– Использование недостоверных/ненадежных сообщений и перехват сеанса/атака повторного воспроизведения

  Поскольку приложения VM можно обновлять по каналам беспроводной связи, такие атаки могут применяться и по отношению к VM.

– Раскрытие информации

  См. пункт 9 [ITU-T F.749.3].

– Атаки типа "отказ в обслуживании"

  Сами VM могут не иметь доступа к критически важной инфраструктуре транспортного средства, но служить шлюзом для таких атак.

– Привилегированный доступ со стороны непривилегированного пользователя

  Поскольку персонализированные учетные записи пользователей могут быть связаны с приложениями VM, возможен непривилегированный доступ. Непривилегированный доступ через VM может не обеспечивать прямого доступа к критически важной инфраструктуре (например, корневой доступ, доступ к тормозной системе), но опять же может служить шлюзом для доступа к инфраструктуре транспортного средства.

– Внедрение вирусов в среду передачи

  Интеллектуальные VM используют передачу данных между VMS и VMSP в облаке. Проникнув в этот канал связи, злоумышленники могут использовать сообщения/данные, передаваемые от VMSP к VMS, для установки вредоносного ПО.

– Сообщения с вредоносным контентом

  Интеллектуальные VM используют передачу данных между VMS и, например, VMSP в облаке. Проникнув в этот канал связи, злоумышленники могут изменить сообщения/данные, передаваемые от VMSP к VMS, для получения доступа к VMS и/или ЭБУ атакуемого интеллектуального транспортного средства.

А.2.3 Угрозы, связанные с процедурами обновления ПО на транспортных средствах

Существует два способа обновления систем транспортного средства, а именно обновление по каналам проводной связи через порт бортовой диагностики (OBD) и портативные устройства, такие как защищенная цифровая (SD) карта или флеш-накопитель USB, и обновление по каналам беспроводной связи (OTA). Обновляться может прошивка или данные конфигурации транспортного средства. Большинство неисправностей электроники и ошибок ПО могут быть скорректированы и исправлены электронным образом без физического доступа, например с помощью тестера OBD. Кроме того, обновление по каналам беспроводной связи помогает сократить цикл обновления и минимизировать подверженность известных уязвимостей ПО атакам. Можно выделить следующие виды угроз, связанных с процедурами обновления:

– Злоупотребление процедурами обновления или их компрометация

  Вне зависимости от способа обновления – по каналам беспроводной связи или на месте/при наличии физического доступа – процедура обновления может содержать угрозы при использовании поддельных программ обновления систем или скомпрометированной прошивки.

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

  Криптографические материалы, такие как криптографические ключи и сертификаты, используемые при обновлении ПО, могут быть скомпрометированы прежде всего в ходе процедуры обновления, следствием чего может стать неверное обновление ПО.

– Отказ в обслуживании и отказ в легальном обновлении

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

А.2.4 Угрозы для транспортных средств, связанные с возможностями взаимодействия и соединениями с внешними объектами

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

– Манипулирование функциями установления соединений для транспортных средств

  VMS не обеспечивает прямого доступа к критически важным функциям транспортного средства, но может использоваться в качестве шлюза для доступа к критически важным компонентам, например к специализированным ЭБУ.

– Размещение стороннего ПО

  Приложения VMS можно отнести к классу "размещенное стороннее программное обеспечение".

– Устройства, подключенные к внешним интерфейсам

  Как указано в [ITU-T F.749.3], возможность установления соединений может базироваться на принесенных устройствах, таких как смартфоны.

A.3 Возможности по обеспечению безопасности на основе выявленных угроз

A.3.1 Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций

С предоставлением услуг VMS связано много администраторов и пользователей, при этом доступ к этим услугам и их использование осуществляются внутренним и внешним образом. Управление определением идентичности необходимо не только для защиты идентичностей, но и для упрощения процессов управления доступом, аутентификации, авторизации и аудита транзакций в такой динамичной и открытой инфраструктуре VMS.

Одна или несколько общих моделей доверия необходимы IAM для аутентификации идентичностей, а также разработчикам, гипервизорам и другим компонентам системы для аутентификации компонентов системы, например загруженных программных модулей, приложений и наборов данных.

Процесс IAM способствует обеспечению конфиденциальности, целостности и готовности услуг и ресурсов, и поэтому имеет важнейшее значение в VMS. Кроме того, IAM обеспечивает возможность осуществления однократной регистрации и реализации федерации идентичности в VMS с помощью различных механизмов аутентификации или механизмов, распределенных по различным доменам безопасности.

Аудит транзакций обеспечивает защиту от непризнания участия, позволяет осуществлять экспертно-технических анализ после инцидентов безопасности и является средством предотвращения атак (как внешних, так и внутренних вторжений). Аудит транзакций подразумевает не просто ведение журнала, а включает и активный мониторинг в целях привлечения внимания к подозрительным действиям.

A.3.2 Безопасность интерфейса

Данная возможность обеспечивает безопасность интерфейсов, открытых для разработчиков VMS и/или других сторонних поставщиков VMSP, которые поставляют VMS различных типов, а также безопасность связи через эти интерфейсы. Доступные механизмы обеспечения безопасности интерфейсов включают, в частности, одностороннюю/взаимную аутентификацию, контрольную сумму для проверки целостности, сквозное шифрование и цифровую подпись.

A.3.3 Безопасность сети

В среде VMS безопасность сети позволяет изолировать физическую и виртуальную сети и обеспечить безопасную связь между всеми участниками. Эта возможность делает доступным разбиение домена безопасности, средства управления доступом на границе сети (например, брандмауэр), обнаружение и предотвращение вторжения, разделение сетевого трафика на основе политики безопасности. Кроме того, она обеспечивает защиту сети от атак в средах физической и виртуальной сетей.

A.3.4 Эксплуатационная безопасность

Данная возможность обеспечивает безопасность повседневной эксплуатации и технического обслуживания VMS и инфраструктуры VMSP.

Данная возможность обеспечения эксплуатационной безопасности включает:

– определение набора принципов политики безопасности и деятельности по обеспечению безопасности, например управление конфигурацией, совершенствование корректировки, оценку безопасности, реагирование на инциденты;

– контроль выполнения VMSP мер безопасности и их эффективности и предоставление надлежащих отчетов затронутым VMS.

В случае изменения мер безопасности VMSP или их эффективности все нижестоящие VMS оповещаются о таких изменениях.

Эти отчеты и оповещения позволяют авторизованным VMS просматривать информацию о соответствующих инцидентах, данные аудита, а также данные конфигурации, относящиеся к их VMS.

А.3.5 Обновления программного и микропрограммного обеспечения

Безопасные обновления OTA должны соответствовать базовым стандартам безопасности. Рекомендуется, чтобы процесс обновления осуществлялся с учетом операционных факторов (таких как время обновлений и процессы шифрования/дешифрования). Наличие нескольких OEM и сторонних поставщиков способствует появлению разных интерфейсов подсистем транспортных средств. Таким образом, любая уязвимость или риск кибербезопасности, относящиеся к этим OEM или поставщикам, могут оказать реальное воздействие на легальное обновление программного обеспечения OTA, которое затем передается в виде облачных данных для установки на транспортных средствах.

Рекомендуется разработать, внедрить и использовать механизм обновления программного и микропрограммного обеспечения VMS (ЭБУ и связанных с ним систем).

При разработке службы VMS рекомендуется разработать и внедрить в качестве базовой функции механизм обновления программного и микропрограммного обеспечения VMS. Также рекомендуется предусмотреть механизм отката программного и микропрограммного обеспечения, который будет использоваться в случае сбоя при обновлении.

При эксплуатации и поддержке службы VMS перед началом процесса обновления устройство проверяет цифровую подпись, сертификаты подписи и цепочку сертификатов подписи пакета обновлений программного/микропрограммного обеспечения.

Рекомендуется осуществлять безопасное управление криптографическими ключами, используемыми для защиты целостности и конфиденциальности обновления, и применять их надлежащим образом. Когда обновления выполняются по каналам беспроводной связи (OTA), рекомендуется делать это по шифрованным каналам связи.

Рекомендуется, чтобы обновления с использованием OTA либо успешно завершались, либо процесс прерывался с возможностью восстановления. Рекомендуется, чтобы в случае неудачной попытки обновления выполнялся откат до последней работающей конфигурации устройства, и рекомендуется обеспечить, чтобы не было возможности прервать соединение устройства с сервером обновлений.

А.3.6 Безопасность приложений

Данные возможности обеспечения безопасности часто используют для повышения безопасности "приложения VMS" путем обнаружения, исправления и предотвращения уязвимостей VMS и ее экосистемы. Применяются различные методы выявления таких уязвимостей на разных этапах жизненного цикла приложений, таких как проектирование, разработка, развертывание, обновление, обслуживание.

А.3.7 Управление инцидентами

Управление инцидентами предусматривает мониторинг и прогнозирование инцидентов, оповещение об инцидентах и реагирование на них. Для того чтобы знать, работает ли услуга VMS в штатном режиме в пределах всей инфраструктуры, необходим непрерывный мониторинг (например, мониторинг показателей работы серверов, используемых в VMSP). Это дает возможность системе собирать информацию о состоянии безопасности услуги, выявлять нештатные условия и обеспечивать раннее предупреждение о перегрузках системы безопасности, нарушениях работы, перебоях в обслуживании и т. д. После наступления событий инцидента безопасности обеспечивается выявление проблемы и быстрое реагирование на инцидент, осуществляемое либо автоматически, либо с вмешательством администратора-человека. Обработанные инциденты заносятся в журнал и проводится их анализ в целях создания на их основе шаблонов, с помощью которых в дальнейшем обеспечивается упреждающая обработка.

А.3.8 Криптография

Эта возможность обеспечивает конфиденциальность и целостность данных, используемых и передаваемых в VMS и ее экосистемах. Это основной метод хранения и передачи данных в определенной форме, так что прочитать и обработать их могут только те, для кого они предназначены. Эта возможность не только обеспечивает защиту данных VMS от кражи или изменения, но и может использоваться для аутентификации пользователей и т. д.

В качестве хорошего примера реализации криптографии в [b-ITU-T X.1197 Amd1] приведены руководящие указания по выбору криптографических примитивов для систем IPTV, которые могут применяться к мультимедийным потокам в системах для транспортных средств с тем же уровнем важности/критичности, что и у мультимедийных потоков в любых других системах IPTV. Аналогично для транспортных средств с возможностью подключения к сети 5G в [b-ITU-T X.1811] содержатся дополнительные руководящие указания по реализации базовых уровней безопасности [b-ITU-T X.1197 Amd1], включая, помимо прочего, мультимедийные потоки.

Кроме того, благодаря решению DRM на основе надежного аутентификационного шифрования, призванному обеспечить возможность использования информационно-развлекательной системы только легального контента, защищенного авторским правом, информационно-развлекательная система и система ассистированного вождения будут учитывать только легальные внешние мультимедийные потоки в зоне прямой видимости, позволяя продолжать движение без всяких затруднений.

А.3.9 Безопасность оборудования

Данная возможность направлена на устранение слабых мест и уязвимостей безопасности, присущих оборудованию VMS, и обеспечивает безопасную среду реализации на аппаратном уровне. В частности, появилась необходимость в аппаратной реализации многих фундаментальных криптографических функций, таких как управление криптографическими ключами, шифрование/дешифрование, а также цифровые подписи и строгая аутентификация, которые важны для обеспечения безопасности в VMS. Для этого необходимо безопасно спроектировать соответствующее оборудование и проверить его функционирование на этапе проектирования с учетом возможных угроз и атак.

Например, для обеспечения безопасности на уровне ЭБУ в архитектуре VMS рекомендуется, чтобы каждый установленный ЭБУ был защищен модулями HSM и PUF, которые представляют собой типичные компоненты аппаратных модулей безопасности.

А.3.10 Общие возможности обеспечения безопасности

ПРИМЕЧАНИЕ. – В рамках настоящей Рекомендации следующие возможности обеспечения безопасности являются факультативными. Однако их можно эффективно использовать для повышения безопасности VMS.

– Оценка и аудит безопасности услуги

  Данная возможность позволяет осуществлять оценку безопасности VMS. Она позволяет авторизованной стороне производить проверку соответствия VMS применимым требованиям обеспечения безопасности. Оценка безопасности или аудит безопасности могут осуществляться VMS, VMSP или третьей стороной, а сертификация системы безопасности может выполняться авторизованной третьей стороной.

  Для обеспечения взаимного понимания в отношении уровня безопасности между VMS и VMSP вводятся надлежащие критерии безопасности.

– Модель доверия

  Для любой системы, в которой несколько поставщиков сотрудничают в целях оказания заслуживающей доверия услуги, необходима общая модель доверия.

  В связи с предполагающим наличие нескольких участников характером VMS необходимо, чтобы среда VMS включала общую модель доверия. Эта модель доверия позволит создавать острова и/или федерации доверенных объектов, так чтобы разрозненные элементы системы могли аутентифицировать идентичность и санкционированные права других объектов и компонентов. Каждый остров федерации доверия будет основан на одном или нескольких доверенных органах выдачи сертификатов инфраструктуры открытых ключей (PKI).

– Изолирование и защита данных

a) Изолирование данных

Изолирование данных может быть реализовано логически или физически, в зависимости от требуемого объема изолированных данных и конкретного развертывания программного и аппаратного обеспечения VMS.

b) Защита данных

Защита данных обеспечивает надлежащую защиту данных VMS и производных данных, хранящихся в VMSP, так чтобы доступ к ним и их изменение могли осуществляться только с разрешения VMS. Такая защита может включать некоторую комбинацию списков контроля доступа, проверку целостности, исправление ошибок/восстановление данных, шифрование и другие надлежащие механизмы.

В том случае когда VMSP обеспечивает для VMS шифрование данных на запоминающем устройстве, данная функция может быть шифрованием на стороне клиента (например, в приложении VMS) или шифрованием на стороне сервера.

– Координация обеспечения безопасности

В связи с тем что в разных VMS подразумеваются разные способы реализации средств управления безопасностью, с помощью данной возможности обеспечения безопасности координируются действия разнородных механизмов обеспечения безопасности, чтобы не допустить конфликтов механизмов защиты.

Стороны, выполняющие разные роли в экосистеме VMS, имеют разные степени контроля над физическими или виртуальными ресурсами и услугами, включая контроль безопасности.

Для каждой стороны существуют различные механизмы обеспечения безопасности, в том числе изолирование гипервизора, IAM, защита сети и т. д.

Координация обеспечения безопасности зависит от функциональной совместимости и согласования разнообразных механизмов обеспечения безопасности.

– Безопасность цепи поставок

VMSP использует ряд поставщиков для создания своих услуг. Некоторые из этих поставщиков являются участниками отрасли VMS, в то время как другие являются традиционными поставщиками оборудования или услуг информационных технологий (ИТ), например производителями аппаратного обеспечения, не имеющими прямого отношения к VMS. Данная возможность позволяет создавать отношения доверия между VMSP и всеми участниками цепи поставок с помощью деятельности в области безопасности. Такая деятельность в области безопасности цепи поставок предусматривает определение и сбор информации о приобретенных VMSP компонентах и услугах, которые используются для предоставления услуг VMS, и обеспечение соблюдения политики безопасности цепи поставок.

Например, типовая деятельность в области безопасности цепи поставок в VMSP может включать:

a) подтверждение справочной информации об участниках цепи поставок;

b) валидацию аппаратного и программного обеспечения и услуг, применяемых VMSP;

c) проверку аппаратного и программного обеспечения, приобретаемого VMSP с целью удостовериться в том, что оно не было подделано при транспортировке (передаче);

d) предоставление механизмов проверки происхождения программного обеспечения VMS, например кода, предоставленного поставщиком ПО.

Данная возможность является непрерывной и охватывает постоянное развитие и обновление системы.

– Безопасная среда и процедуры разработки

Данная возможность имеет целью исключить появление уязвимостей безопасности в VMS и ее экосистемах в процессе разработки. К среде разработки относятся люди, процессы, технологии и средства, связанные с разработкой системы. Разработчикам услуг VMS рекомендуется оценивать риски в каждом процессе разработки VMS и создать безопасную среду разработки с учетом:

a) персонала, работающего в этой среде;

b) применяемых методов разработки, программного обеспечения и процессов обработки данных;

c) используемых сторонних продуктов и услуг;

d) физической и сетевой среды;

e) согласования с другими конструкторскими и технологическими процессами.

Разработчикам услуг VMS также необходимо определить среду разработки и соответствующие процедуры для снижения рисков. Эти процедуры рекомендуется распространить среди лиц, участвующих в разработке.

Приложение B

Защита информации, позволяющей установить личность (PII), и неприкосновенность частной жизни

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Поскольку транспортные средства становятся соединенными и предоставляют все больше интерактивных услуг, рекомендуется, чтобы VMS обеспечивала сквозную защиту. Для обеспечения конфиденциальности и целостности пользовательских данных, хранящихся в VMS, в транспортном средстве и в облаке VMS или на внутренних серверах, необходимо защищать все больше пользовательских данных и информации, связанной с неприкосновенностью частной жизни.

Согласно определению Национального института стандартов и технологий (NIST) США, PII – это "любое представление информации, позволяющее прямым или косвенным способом обоснованно установить личность человека, к которому относится эта информация" [b-NIST SP 800-79-2].

Единого определения английского термина "privacy" [и его эквивалентов на русском языке, одним из которых является "неприкосновенность частной жизни"] не существует. Его значение зависит от правового, политического, социального, культурного и социотехнического контекста.

Как правило, "неприкосновенность частной жизни в отношении информации", то есть "конфиденциальность информации" можно определить следующим образом:

1) конфиденциальность информации и какого-либо лица обеспечена, если его данные защищены от проникновения, вмешательства или доступа со стороны несанкционированных лиц.

Защита PII – один из аспектов обеспечения неприкосновенности частной жизни.

VMS может хранить PII или функционировать как шлюз для доступа к PII владельца транспортного средства, водителя и/или пользователей.

B.1 Источники информации

VMS включает в себя несколько источников информации, таких как:

– датчики (движения, местоположения и т. д.);

– видеокамеры (персонализации, распознавания характерных признаков и т. д.);

– микрофон – ввод звука (также может использоваться для записи и распознавания голоса, голосовой биометрии и т. д.);

– идентификаторы сетевых протоколов связи, такие как IP-адрес, MAC-адрес и т. д.;

– источники медиаданных, такие как карта памяти USB, защищенная цифровая (SD) карта, внешний жесткий диск и т. д.;

– сторонние приложения, платежные шлюзы, услуги, устройства, принадлежности и т. д.

VMS хранит информацию и обменивается ею с другими бортовыми системами или с облаком в зависимости от архитектуры транспортного средства, региональных, законодательных и сертификационных требований.

B.2 Реализация защиты PII: общие соображения

Должна быть обеспечена защита персональных данных (например, в данных, тексте, звуковых данных и изображениях), а также всякой информации, которую могут запрашивать пользователи, помимо предполагаемого клиента и любых конечных пользователей VMS (удаленное облако, магазины, процессы и т. д.).

Для доступа к персональным данным, относящимся к каждому клиенту, конечным пользователям и третьим сторонам, необходимо соглашение об обмене данными. Любое такое клиентское соглашение или любое другое соответствующее соглашение, регулирующее использование служб VMS, должно основываться на следующих критериях:

– персонализированный доступ на основе выбора услуг и предпочтений пользователя;

– VMS, предназначенная для использования в соответствии с нормативными требованиями неприкосновенности частной жизни;

– программное обеспечение, оборудование и сеть VMS, которые по своей конструкции обеспечивают только аутентифицированный доступ;

– защита PII и неприкосновенности частной жизни в VMS должны быть предназначены как для частных транспортных средств только с одним пользователем, так и для транспортных средств с несколькими пользователями.

B.3 Видимость и прозрачность данных

Рекомендуется применять хорошо известные и тщательно проверенные стандарты безопасности. Рекомендуется избегать использования проприетарных алгоритмов шифрования.

Рекомендуется применять хорошо известные процессы.

Рекомендуется уведомлять пользователей о данных, хранящихся в VMS/доступных через VMS. Поскольку прозрачность повышает приемлемость для пользователей, рекомендуется, чтобы уведомление пользователя содержало информацию о типе данных, цели их сбора, названии организаций, обрабатывающих данные, и сроках хранения данных.

B.3.1 Неприкосновенность частной жизни по умолчанию

Рекомендуется, чтобы пользователи могли контролировать предельный объем загрузки данных, а также разрешать/запрещать загрузку и хранение данных. Стратегии, предполагающие возможность отказа, в большей степени способствуют сохранению неприкосновенности частной жизни и лучше соответствуют принципу обеспечения неприкосновенности частной жизни по умолчанию. Поэтому рекомендуется использовать стратегии, предполагающие возможность отказа.

Рекомендуется, чтобы для VMS был определен список сценариев использования, соответствующий требованиям к конфиденциальности данных и соответствующим настройкам.

Для каждого конкретного сценария приложения могут использовать несколько ресурсов. Например, в случае службы определения местоположения для определения приблизительного местоположения пользователя могут использоваться технологии Bluetooth, GPS, общественные точки доступа Wi-Fi или местоположение вышек сотовой связи. Рекомендуется, чтобы VMS предоставляла пользователям возможность отключения определенных функций отслеживания. Для этого можно использовать управление общими настройками, определив общую для всех приложений политику неприкосновенности частной жизни. В качестве альтернативы пользователям может быть разрешено управлять доступом к данным на уровне каждого приложения. Можно использовать и такие способы обеспечения неприкосновенности частной жизни, как профили PRICON, сочетающие оба подхода. Еще одним вариантом для VMS может быть сигнал "Не отслеживать" (DNT), который уже используется в веб-браузерах. Сигнал DNT – это поле заголовка HTTP, указывающее предпочтение пользователя в отношении отслеживания его действий в рамках службы или при межсайтовом отслеживании пользователей.

Например, приложения или элементы управления могут запрашивать данные о местоположении только во время использования приложения или разрешать его в любое время. Пользователи могут отказаться от такого доступа, и рекомендуется, чтобы они имели возможность в любое время изменить свой выбор в настройках. Общий регламент по защите данных (GDPR) применительно к службе, которая работает и в Европейском союзе, требует обеспечить возможность для принятия пользователем обоснованных решений в отношении неприкосновенности частной жизни. Это возможно, если человек осведомлен о последствиях раскрытия данных (кто, с какой целью и при каких условиях получает те или иные данные) или отказа от него (какие конкретные функции будут ограничены).

Если приложению был предоставлен доступ к определенным данным, то для того чтобы использовать их в фоновом режиме, необходимо напомнить пользователю о его разрешении и предоставить возможность изменить права доступа для приложения.

Рекомендуется, чтобы архитектура VMS надежно предотвращала доступ приложений к информации, если пользователь не дал явного на то разрешения.

B.4 Точность и целостность данных

Рекомендуется, чтобы VMS поддерживала определенным образом все операции с данными, такие как передача данных, загрузка данных, обмен данными и удаление данных.

Сквозная безопасность – защита всего жизненного цикла. Рекомендуется регулярно проводить проверку кода и тщательное тестирование его безопасности. Кроме того, рекомендуется реализовать стратегии защиты на уровнях радиовещания, базы данных и приемника.

Рекомендуется, чтобы были обеспечены гарантии безопасности программного обеспечения для предотвращения потери, неточности, изменения, недоступности или неправомерного использования применяемых, контролируемых и защищаемых данных и ресурсов.

Рекомендуется, чтобы пользователям было разрешено проверять точность PII и законность ее обработки.

Целостность означает поддержание согласованности, точности и достоверности данных с течением времени.Следовательно, рекомендуется установить защиту от неправомерного изменения или уничтожения информации. Рекомендуется принять надлежащие меры для обеспечения аутентичности информации и невозможности отказа.

Рекомендуется, чтобы в настройках пользователям было видно, каким приложениям они разрешили доступ к той или иной информации, и чтобы они могли разрешать или запрещать любые способы доступа на будущее.

Кроме того, рекомендуется, чтобы ОС VMS обеспечивала ограничения, предотвращающие перемещение данных между приложениями и учетными записями, установленными надежным решением для управления данными и самим пользователем.

Пользователи могут потребовать исправления, изменения или удаления своей информации, позволяющей установить личность, если она неточна или если они считают, что обработка такой информации нарушает действующее законодательство.

Должны быть реализованы системы, приложения и процедуры для обеспечения защиты информации, позволяющей установить личность пользователя, чтобы минимизировать риск кражи, повреждения или потери информации, а также несанкционированного доступа к ней или ее неправомерного использования.

Рекомендуется, чтобы любые несанкционированные изменения PII в VMS или облаке обнаруживались и чтобы пользователь уведомлялся об этом.

B.5 Конфиденциальность

Конфиденциальность заключается в сохранении санкционированных ограничений на доступ и раскрытие информации, включая средства защиты неприкосновенности частной жизни и личной информации.

B.5.1 Уровни необходимой конфиденциальности

Рекомендуется оценивать PII для определения уровня необходимой конфиденциальности, чтобы применить надлежащие меры защиты. Рекомендуется, чтобы не все хранящиеся или создаваемые данные PII обрабатывались одинаково.

Рекомендуется оценивать необходимый уровень конфиденциальности как низкий, средний или высокий в зависимости от идентифицируемости, секретности данных и от требований к защите данных в соответствии с действующим законодательством.

B.5.2 Защита конфиденциальности

Рекомендуется, чтобы была реализована защита конфиденциальности с применением следующих мер:

– реализация механизма управления доступом с использованием пароля для доступа к данным VMS;

– многоуровневый доступ к высококонфиденциальной PII;

– многоуровневое управление доступом с мобильных телефонов, ноутбуков и персональных цифровых устройств;

– шифрование PII перед передачей. Подробные меры описаны в пункте A.3.8 (Криптография).

Кроме того, перед внедрением новых требований рекомендуется провести оценку рисков. Рекомендуется реализовать механизм непрерывного контроля рисков для оценки изменений в VMS и выявления новых рисков, связанных с VMS.

B.6 Анонимизация данных

Анонимизация данных – это процесс необратимого изменения секретных данных для защиты субъектов PII.

Анонимизируя данные, обрабатываемые в среде VMS, можно реализовать широкий спектр процессов анализа данных и обмена данными.

B.7 Доступность данных

Доступность требует обеспечения своевременного и надежного доступа к информации и ее использования.

Рекомендуется, чтобы авторизованным пользователям была предоставлена возможность детального контроля над использованием информации о местоположении системными службами. Это означает возможность отключения внесения информации о местоположении в данные, собираемые внутренними приложениями, в историю навигационного поиска и в сведения о доступе к сетям Bluetooth и Wi-Fi. Если пользователь входит в облако OEM, функционально необходимым приложениям по умолчанию предоставляется доступ к облаку OEM. Рекомендуется, чтобы пользователи могли управлять доступом каждого приложения к облаку в настройках.

Если доступ к PII осуществляется удаленно с помощью телематики, рекомендуется, чтобы подключенные службы работали с многоуровневой аутентификацией.

Поскольку данные получаются путем выполнения различных операций по обработке данных (вычисление, статистическая обработка и т. д.) в зашифрованном формате (например, с использованием гомоморфного шифрования), подобная обработка данных может выполняться и с данными в VMS.

Библиография

[b-ITU-T X.1197 Amd1] ITU-T X.1197 Amd.1 (2019), *Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection, Amendment 1.*

[b-ITU-T X.1811] МСЭ-Т X.1811 (2020 г.), *Руководящие указания по безопасности для применения в системах 5G алгоритмов, обеспечивающих квантовую безопасность.*

[b-ETSI WP35] ETSI White Paper 35 (2020), *IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward*. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf

[b-IEEE 802.11] IEEE 802.11-2020, *Стандарт IEEE для информационных технологий – Электросвязь и обмен информацией между системами – Локальная и городская сети – Специальные требования – Часть 11. Спецификации уровня управления доступом к среде (MAC) и физического уровня (PHY) в беспроводной локальной сети.*

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations.*

[b-IETF RFC 8200] IETF RFC 8200 (July 2017), *Internet Protocol, Version 6 (IPv6) Specification.*

[b-IETF RFC 8216] IETF RFC 8216 (2017), *HTTP Live Streaming.*

[b-ISO/IEC 23009-1] ISO/IEC 23009-1:2019, *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats.*

[b-IAB] Internet Architecture Board (IAB) statement on IPv6 address exhaustion (November 2016). https://www.iab.org/2016/11/07/iab-statement-on-ipv6/ [Online]

[b-NIST SP 800-79-2] NIST Special Publication 800-79-2 (2015), *Guidelines for the Authorization of Personal Identity Verification Card Issues (PCI) and Derived PIV Credential Issuers (DPCI).*

[b-USG OMB] US Office of Management and Budget (November 2020), *Memorandum for heads of executive departments and agencies*. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf [Online]

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, 2022 г.