ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1381 (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 бортовых автомобильных сетей на базе Ethernet

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

Сети передачи данных, взаимосвязь открытых систем и безопасность

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1-X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200-X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300-X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400-X.499
СПРАВОЧНИК	X.500-X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600-X.699
УПРАВЛЕНИЕ В ВОС	X.700-X.799
БЕЗОПАСНОСТЬ	X.800-X.849
ПРИЛОЖЕНИЯ ВОС	X.850-X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900-X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	X.1000-X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	X.1100-X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200-X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	X.1300-X.1499
Связь в чрезвычайных ситуациях	X.1300-X.1309
Безопасность повсеместных сенсорных сетей	X.1310-X.1319
Безопасность умных электросетей	X.1330-X.1339
Сертифицированная электронная почта	X.1340-X.1349
Безопасность интернета вещей (IoT)	X.1350-X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	**X.1370-X.1399**
Безопасность технологии распределенного реестра (DLT)	X.1400-X.1429
Безопасность приложений (2)	X.1450-X.1459
Безопасность веб-среды (2)	X.1470-X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500-X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600-X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700-X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750-X.1799
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800-X.1819

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

Рекомендация МСЭ-Т X.1381

Руководящие указания по обеспечению безопасности бортовых автомобильных сетей на базе Ethernet

Резюме

В Рекомендации МСЭ-Т X.1381 представлены руководящие указания по обеспечению безопасности бортовых автомобильных сетей (IVN) на базе Ethernet. Текущая тенденция в построении электрической и электронной (E/E) архитектуры заключается в интеграции Ethernet с традиционными IVN, такими как локальная сеть контроллеров (CAN), локальная соединительная сеть (LIN), передача данных мультимедийных систем (MOST) и FlexRay. В прошлом Ethernet рассматривался только как соединение между транспортными средствами и внешней средой. Для связи между внешней средой и транспортными средствами использовались стандартные протоколы, обеспечивающие соединения на основе протокола Интернет через Ethernet (диагностическая связь по протоколу Интернет, универсальный протокол для измерения и калибровки и т. д.). Эти сценарии использования, как правило, не обязательно соответствуют строгим ограничениям режима реального времени. Однако от бортовых автомобильных приложений, использующих связь на базе Ethernet, требуется обеспечение таких характеристик, как высокая чувствительность ко времени и надежность.

Текущие разработки в области технологий бортовой автомобильной связи требуют увеличения пропускной способности сети. По сравнению с Ethernet характеристики традиционных сетей IVN недостаточны для удовлетворения требований, предъявляемых к пропускной способности современных автомобильных приложений. Поэтому в будущем, как и сегодня, основной частью электрической/электронной архитектуры будут оставаться IVN на базе Ethernet.

Однако меры по обеспечению безопасности, применяемые в обычных компьютерных сетях, не подходят для автомобильных приложений, поскольку они разработаны без учета соответствующих требований и возможностей.

Для того чтобы удовлетворить этим требованиям, в настоящей Рекомендации представлены руководящие указания по обеспечению безопасности технологии автомобильного Ethernet. В данной Рекомендации содержатся эталонная модель автомобильного Ethernet и анализ угроз и уязвимостей для IVN на базе Ethernet. Кроме того, в ней представлены требования безопасности и примеры использования IVN на базе Ethernet.

Хронологическая справка *

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1381	03.03.2023 г.	17-я	11.1002/1000/15107

Ключевые слова

Безопасность автомобильного Ethernet, безопасность ИТС.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т X.1381

Руководящие указания по обеспечению безопасности бортовых автомобильных сетей на базе Ethernet

1 Сфера применения

В настоящей Рекомендации представлены руководящие указания по обеспечению безопасности бортовых автомобильных сетей (IVN) на базе Ethernet. В ней в аспекте кибербезопасности рассматриваются следующие вопросы:

1) анализ угроз безопасности,

2) требования безопасности,

3) сценарии использования.

Кибербезопасность означает, что соответствующая техническая архитектура связи является или может быть неотъемлемой частью киберфизических систем (таких как стеки протоколов связи Ethernet, интегрированные во встроенные системы).

1.1 Заявления о применимости

Сети в целом и сети Ethernet в частности используются для предоставления услуг связи. Следовательно, контекст безопасности в настоящей Рекомендации относится к безопасности связи, но не обязательно к информационной безопасности как таковой для вычислительных узлов с Ethernet-соединением.

Таким образом, руководящие указания по обеспечению безопасности в настоящей Рекомендации охватывают проектирование сетей на базе Ethernet, используемых в автомобильных приложениях, с точки зрения технических аспектов безопасности. Важнейшей частью таких аспектов безопасности является соответствующая многоуровневая архитектура связи с ее многоуровневыми стеками протоколов.

1.2 Подтверждение руководящих указаний по обеспечению безопасности с течением времени

Безопасность архитектуры связи, необходимая для бортовых автомобильных сетей Ethernet, стремительно развивается в первую очередь благодаря:

1) возможным изменениям в топологии сети (вызванным развитием архитектуры распределенных вычислений, использующих эти сети связи, например, в направлении автоматизации транспортных средств);

2) многоуровневой архитектуре протоколов – современные стеки протоколов Ethernet и не-Ethernet могут изменяться, дополняться и т. д.;

3) эволюции протоколов – современные протоколы информационно-коммуникационных технологий (ИКТ) (регламентируемые организациями по разработке стандартов, такими как IEEE, IETF, МСЭ-Т, ETCИ, 3GPP) продолжают совершенствоваться и расширяться, что отражается в профилировании этих протоколов (например для чувствительных ко времени сетей (TSN) IEEE в автомобильных приложениях) [b-IEEE 1722-2016] или в появлении их новых версий;

ПРИМЕЧАНИЕ. – Кроме того, обновлению также могут подлежать и аспекты безопасности, относящиеся к спецификации протокола.

1) развитию средств и решений по обеспечению безопасности в контексте безопасности связи.

Поэтому ожидается, что в будущем настоящая Рекомендация будет пересматриваться.

Настоящая Рекомендация посвящена в частности первоначальным руководящим указаниям по обеспечению безопасности, определяемым первой группой сценариев использования. Основной сферой ее применения являются IVN на базе Ethernet первого поколения, что соответствует

современному передовому опыту и руководящим указаниям по обеспечению безопасности на момент публикации настоящей Рекомендации.

2 Справочные документы

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

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

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

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

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

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

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

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

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

3.1.8 брандмауэр (firewall) [b-ITU-T X.1039]: Вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий локальной политике безопасности.

3.1.9 шлюз безопасности (security gateway) [b-ITU-T X.1039]: Точка соединения между сетями, или подгруппами внутри сетей, или программными приложениями различных доменов безопасности, которая предназначена для защиты сети в среде интернета вещей в соответствии с заданной политикой безопасности.

3.1.10 автомобильный шлюз (**vehicle gateway (VG))** [b-ITU-T F.749.1]: Устройство, обеспечивающее связь между устройством, установленным в автомобиле и другим устройством, которое может физически находиться как внутри, так и снаружи автомобиля, (таким как придорожная станция, облачный сервер и т. д.). VG обеспечивает стандартизированные интерфейсы и протоколы, передачу данных в разнородных сетях, оптимизированный выбор сети на основе потребностей

приложений и качества обслуживания сети, арбитраж и интеграцию сетевых соединений, безопасность и коммутацию сетевых соединений для обеспечения непрерывности обслуживания.

ПРИМЕЧАНИЕ 1. – Термин "центральный шлюз" (введенный в настоящей Рекомендации) обычно является синонимом термина "автомобильный шлюз" в абстрактных бортовых автомобильных сетях (IVN) или термина "автомобильный пограничный шлюз" в более детальной архитектуре IVN.

ПРИМЕЧАНИЕ 2. – Термин "шлюз интеллектуальной транспортной системы" (ИТС), как правило, является синонимом термина "автомобильный шлюз".

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 электрическая и электронная архитектура (electrical and electronic architecture (E/E architecture)): Связанная двухплоскостная архитектура бортовой автомобильной сети, состоящая из: 1) плоскости сети распределения электроэнергии или мощности; и 2) архитектурной плоскости сети обработки информации и передачи данных.

ПРИМЕЧАНИЕ. – Иногда к E/E добавляется третий символ для обозначения технологии движения автомобиля, например E^3; третий символ E указывает на электромобиль.

3.2.2 автомобильный пограничный шлюз (vehicle border gateway): Автомобильный шлюз, расположенный на границе и внутри домена (доменов) внутренней бортовой автомобильной сети и домена (доменов) сети, внешней по отношению к автомобилю. Следовательно, весь трафик между автомобилем и различными объектами (V2X) направляется через автомобильный шлюз такого типа.

ПРИМЕЧАНИЕ 1. – Термин "автомобильный шлюз" охватывает и это значение и, следовательно, может считаться достаточным для архитектуры бортовой автомобильной сети (IVN) только с одним автомобильным шлюзом. Однако в IVN также могут использоваться автомобильные шлюзы, предназначенные только для внутренних соединений и целей взаимодействия. В таких сетевых контекстах может потребоваться более детальное разграничение типов шлюзов.

ПРИМЕЧАНИЕ 2. – Конкретные функции взаимодействия, поддерживаемые *шлюзом* определенного типа, часто выражаются расширенным наименованием шлюза, указывающим, например, положение в сетевой иерархии (например, на уровне доступа или в базовой сети), границу или тип межсоединения при межсетевом взаимодействии (например, домены безопасности), определенные сетевые интерфейсы или технологии связи.

ПРИМЕЧАНИЕ 3. – Под блоком управления связью понимается технический компонент, относящийся (функционально) к категории автомобильного пограничного шлюза.

ПРИМЕЧАНИЕ 4. – Связь V2X охватывает все типы трафика, например от телематических служб, ИТС или диагностических служб.

3.2.3 зонально ориентированная электрическая и электронная архитектура (zone-oriented electrical and electronic architecture): Электрическая и электронная (E/E) архитектура, объединяющая компоненты автомобиля (примечание 1), такие как датчики, приводы и вычислительные узлы, по их расположению (примечание 2) в субдоменах сети. В каждом субдомене, так называемой зоне (примечание 3), имеется относящийся к этой зоне выделенный автомобильный вычислительный узел (в автомобильных приложениях называемый зональным контроллером), подключенный ко всем компонентам внутри субдомена. Зональные контроллеры каждой зоны связаны с высокопроизводительным автомобильным вычислительным узлом более высокого уровня. Таким образом, с точки зрения архитектуры распределенных вычислений существует иерархия обработки данных между отдельными зонами и общим доменом бортовой автомобильной сети (IVN).

ПРИМЕЧАНИЕ 1. – Имеются в виду вычислительные и сетевые компоненты в контексте IVN.

ПРИМЕЧАНИЕ 2. – Под "положением" понимается положение в сети на физическом или виртуальном топологическом уровне IVN.

ПРИМЕЧАНИЕ 3. – Понятие зоны здесь в первую очередь связано с концепцией сетевых доменов в контексте электрической/электронной архитектуры. Такая зона не обязательно включает концепцию зоны безопасности, доверенной зоны или демилитаризованной зоны, которая используется в других Рекомендациях МСЭ-Т, относящихся к безопасности (например [b-ITU-T Y.2770]).

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ADAS	Advanced Driver Assistance System		Усовершенствованная система помощи водителю
ARP	Address Resolution Protocol		Протокол разрешения адресов
AUTOSAR	Automotive Open System Architecture		Открытая автомобильная системная архитектура
AVB	Audio Video Bridging		Аудио-видео мост
CAN	Controller Area Network		Локальная сеть контроллеров
CGW	Central Gateway		Центральный шлюз
CPU	Central Processing Unit	ЦП	Центральный процессор
CRC	Cyclic Redundancy Check		Контроль циклическим избыточным кодом
DHCP	Dynamic Host Configuration Protocol		Протокол динамической конфигурации хост-компьютера
DoIP	Diagnostic communication over Internet Protocol		Диагностическая связь по протоколу Интернет
DoS	Denial of Service		Отказ в обслуживании
DTLS	Datagram Transport Layer Security		Протокол датаграмм безопасности транспортного уровня
ECU	Electronic Control Unit	ЭБУ	Электронный блок управления
E/E	Electrical and Electronic		Электрическая/электронная [архитектура]
FDB	Forwarding Database		База данных переадресации
FIB	Forwarding Information Base		Информационная база переадресации
HSM	Hardware Security Module		Аппаратный модуль безопасности
ICMP	Internet Control Message Protocol		Протокол управляющих сообщений в интернете
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
ID	Identifier		Идентификатор
IDS	Intrusion Detection System		Система обнаружения вторжений
IP	Internet Protocol		Протокол Интернет
IPsec	Internet Protocol Security		Безопасность протокола Интернет
IPv4	Internet Protocol version 4		Протокол Интернет версии 4
IPv6	Internet Protocol version 6		Протокол Интернет версии 6
ITS	Intelligent Transport System	ИТС	Интеллектуальная транспортная система
IVN	In-Vehicle Network		Бортовая автомобильная сеть
LIN	Local Interconnect Network		Локальная соединительная сеть
MAC	Media Access Control		Управление доступом к среде передачи

MACsec	Media Access Control security	Безопасное управление доступом к среде передачи
MCU	Microcontroller Unit	Блок микроконтроллера
MOST	Media Oriented Systems Transport	Передача данных мультимедийных систем
MPU	Multipoint Control Unit	Блок многоточечного контроля
OBD	On-Board Diagnostic	Бортовая диагностическая система
OEM	Original Equipment Manufacturer	Производитель оригинального оборудования
PDU	Protocol Data Unit	Блок данных протокола
PVID	Port VLAN ID	Идентификатор порта VLAN
QoS	Quality of Service	Качество обслуживания
SecOC	Secure Onboard Communication	Безопасная бортовая связь
SR	Security Recommendation	Рекомендация по безопасности
TARA	Threat Analysis and Risk Assessment	Анализ угроз и оценка рисков
TCP	Transmission Control Protocol	Протокол управления передачей
TLS	Transport Layer Security	Безопасность транспортного уровня
TP	Transport Protocol	Транспортный протокол
TSN	Time-Sensitive Networking	Чувствительная ко времени сеть
UDP	User Datagram Protocol	Протокол датаграмм пользователя
UDS	Unified Diagnostic Service	Единая диагностическая служба
V2X	Vehicle to Everything	Связь транспортных средств с различными объектами
VG	Vehicle Gateway	Автомобильный шлюз
VID	VLAN Identifier	Идентификатор VLAN
VLAN	Virtual Local Area Network	Виртуальная локальная сеть

5 Соглашения

В настоящей Рекомендации представлен перечень требований безопасности, обозначаемых [SR-*x*], где *x* – число. Для таких SR используются следующие формулировки с указанными здесь значениями.

Формулировки "**рекомендуется**" или "**следует**" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом для заявления о соответствии настоящей Рекомендации это требование не является обязательным.

Формулировка "**может факультативно**" означает необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и что функция может быть активирована по желанию оператора сети или поставщика услуг дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии спецификациям.

6 Обзор архитектуры бортовых автомобильных сетей на базе Ethernet и новых бортовых автомобильных сетей

Автомобильный Ethernet – это физическая сеть, которая используется для соединения компонентов внутри автомобиля по проводной сети. Термин "автомобильный Ethernet" также применяется как название всей бортовой автомобильной сети Ethernet как таковой, включая все уровни протоколов и протоколы, используемые в этом сетевом домене. Эта сеть предназначена для удовлетворения потребностей авторынка, включая соответствие требованиям, предъявляемым к электрооборудованию (по излучению электромагнитных/радиочастотных помех и восприимчивости к ним), к пропускной способности, задержке, синхронизации и управлению сетью. Поскольку большое внимание уделяется технологиям автономных транспортных средств и усовершенствованным системам помощи водителю (ADAS), современные автомобили обычно оснащают несколькими видеокамерами, бортовыми диагностическими системами (OBD) и информационно-развлекательными системами, для которых требуется сеть с высокой пропускной способностью. Кроме того, по мере увеличения количества функций увеличивается и количество взаимосвязанных бортовых вычислительных узлов (таких как электронные блоки управления (ЭБУ)) в автомобиле. Это приводит к увеличению количества жгутов проводов и массы автомобиля, что ухудшает его ходовые характеристики и эффективность использования топлива. Зонально ориентированная электрическая и электронная архитектура является ярким примером конкретной бортовой автомобильной вычислительной и сетевой архитектуры, в которой Ethernet также используется на верхнем уровне иерархии сети для соединения всех зон (так называемая магистральная сеть) в общую архитектуру. Если традиционную IVN, включая локальную сеть контроллеров (CAN), локальную соединительную сеть (LIN), сеть передачи данных мультимедийных систем (MOST) или FlexRay, объединить с сетью Ethernet, то можно использовать стандартные кабели Ethernet, что значительно уменьшит массу и стоимость автомобиля. Кроме того, благодаря высокой пропускной способности можно будет уменьшить количество и сложность систем управления.

Однако не все домены IVN, такие как домены трансмиссии, салона или шасси, будут переводиться на автомобильный Ethernet. Это означает, что для таких доменов, как домен салона, которым не требуется большое количество данных и высокая пропускная способность, не нужно изменять сетевые протоколы, расходуя на это дополнительные ресурсы и усилия.

На рисунке 1 показана смешанная IVN с применением традиционных протоколов IVN, таких как CAN, и автомобильного Ethernet. Для соединений, не требующих высокой пропускной способности, можно по-прежнему использовать традиционные протоколы IVN, а там, где необходима высокая пропускная способность, например для функций автоматического вождения или ADAS, можно заменить их на IVN на базе Ethernet.

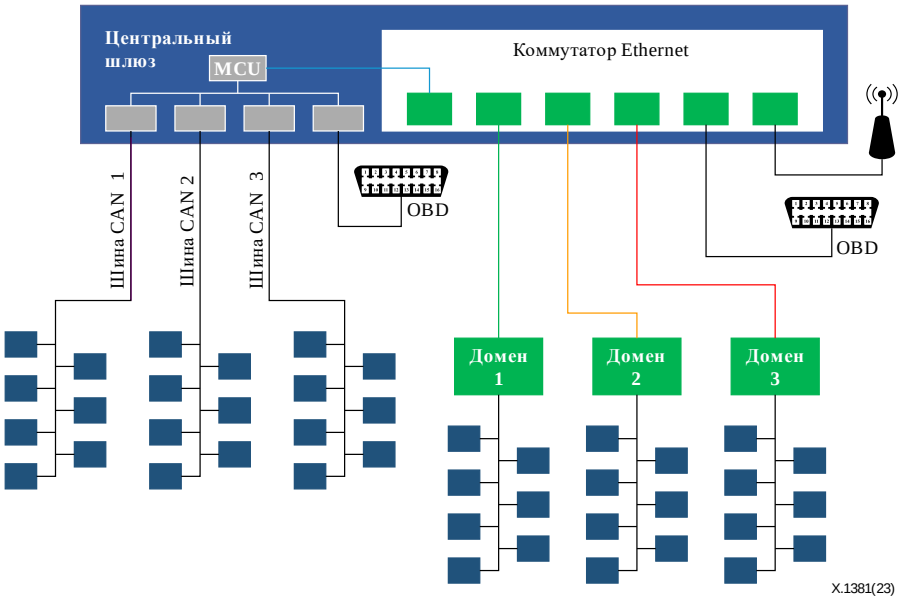

Рисунок 1 − Неоднородность типичной современной бортовой автомобильной сети на основе традиционных протоколов и автомобильного Ethernet

Ожидается, что IVN на базе Ethernet будут развиваться со временем. Такое эволюционное развитие сетей обычно сопровождается изменениями в коммуникационной архитектуре связи (определяемой топологиями связи, многоуровневыми стеками протоколов и т. д.), которые в свою очередь, скорее всего, повлияют на соответствующую архитектуру обеспечения безопасности связи.

Концепции безопасности для классической электрической и электронной архитектуры, то есть архитектуры, основанной на технологиях CAN/FlexRay/LIN и иногда MOST, уже обсуждались в прошлом, и некоторые предложенные механизмы уже прошли стандартизацию. Ethernet и связанные с ним протоколы верхнего уровня станут не только простой, но и более быстродействующей заменой традиционным системам автомобильных шин передачи данных, а также, вероятно, изменят фундаментальные концепции современной электрической и электронной архитектуры.

Внедрение Ethernet – это огромный шанс повысить безопасность автомобиля, поскольку для Ethernet многие серьезные проблемы безопасности, возникающие в автомобильных приложениях, уже решены – например, в сфере так называемых ИКТ операторского класса (городские сети на базе Ethernet, наземные сети радиодоступа на базе Ethernet и т. д.), а также в сфере классических информационных технологий (Ethernet как базовая возможность установления соединений в частных сетях, корпоративные локальные сети). Однако это создает и огромные проблемы, в том числе вызванные ограничениями бортовых автомобильных или встроенных систем, для обеспечения по крайней мере того же уровня безопасности, который в настоящее время ожидается от существующей электрической и электронной архитектуры повышенной безопасности.

6.1 Электрическая и электронная архитектура бортовой автомобильной вычислительной сети

В прежней электрической и электронной архитектуре предполагалось наличие центрального шлюза (CGW, известного также как VG или автомобильный ИТС-шлюз в IVN этого типа) для бортовой автомобильной связи и взаимосвязи между различными субдоменами. Таким образом, существуют сквозные соединения, маршрутизируемые через такие VG.

ПРИМЕЧАНИЕ 1. – "Маршрутизация" в данном контексте означает функцию общей маршрутизации трафика, а не иную маршрутизацию, например для IP. В современных IVN на базе Ethernet IP-маршрутизаторы не используются – только шлюзы IP-типа. При таком использовании IP и Ethernet создается нечто вроде коммутируемой IP-сети (для услуг связи на базе IP).

Этот аспект имеет решающее значение с точки зрения безопасности связи, поскольку он упрощает задачи обеспечения безопасности, связанные с IP (например, отсутствуют угрозы безопасности, связанные с протоколами IP-маршрутизации).

Ожидается, что целевая система связи на базе Ethernet будет удовлетворять требованиям по высокой производительности в режиме реального времени и надежной связи, а также выиграет от применения зрелой, широко используемой и проверенной технологии и техники связи.

ПРИМЕЧАНИЕ 2. – Стандарт [b-IEEE 802.1], особенно [b-IEEE 802.1CB], обеспечивает надежную сеть передачи данных с кольцевой архитектурой и характеристикой избыточности уровня 2 (R-Tag).

В частности, в бортовых автомобильных сетях стандартно используются шины CAN, FlexRay, LIN и MOST; наиболее популярной является шина CAN. Важными элементами сети и системы безопасности в бортовых автомобильных сетях и архитектуре связи являются CGW, VG в целом и автомобильные пограничные шлюзы в частности. В Дополнениях II и III представлена дополнительная информация, которая может оказаться полезной с точки зрения обеспечения безопасности связи.

В прошлом не было возможности получить удаленный доступ к транспортному средству (например, с использованием соединения с цеховой сетью связи для целей диагностики или различных вариантов связи V2X). Бортовые ЭБУ соединялись друг с другом через одну или несколько оптимизированных автомобильных полевых шин.

Законный постпроизводственный доступ был возможен только посредством прямого физического кабельного соединения. Таким образом прямое соединение на небольшом расстоянии используется исключительно для диагностических целей и требует подключения к OBD-порту по протоколу CAN. Производители оригинального оборудования (OEM) знали о повышенном риске безопасности, связанном с диагностическими функциями и стандартным протоколом CAN, который не обеспечивает никаких мер безопасности. В документе [b-Autosar 654] основное внимание уделено аутентичности и

целостности сообщений CAN, и соответствующие концепции безопасности в основном используют коды аутентификации сообщений.

Текущие разработки делают возможной связь внешних устройств с транспортным средством по сети Ethernet. Обычно точкой доступа для внешней линии связи того или иного типа в автомобиле служит специальный ЭБУ. При необходимости ЭБУ передает соответствующую информацию другим ЭБУ по общей бортовой автомобильной сети или перенаправляет трафик через Ethernet-соединение в CGW для маршрутизации к другим ЭБУ, подключенным обычным способом.

6.2 Сравнение будущей и текущей электрической и электронной архитектуры с точки зрения безопасности

Из-за многочисленных случаев ненадлежащей эксплуатации компонентов бортовой автомобильной сети в текущей электрической и электронной архитектуре применяются специальные механизмы обеспечения безопасности. Что касается систем связи, то механизмы аутентификации для преобладающей сети CAN уже опубликованы, стандартизированы и будут частично применяться в автомобилях будущих поколений. В открытой автомобильной системной архитектуре (AUTOSAR) определен модуль безопасной бортовой связи, который гарантирует аутентичность и целостность сообщений, передаваемых в автомобиле. Следует отметить, что механизм аутентификации относится не только к аутентичности передаваемых сообщений, он также гарантирует подлинность участников связи.

Кроме того, CAN как технология шины физического уровня передает сообщения только в вещательном режиме.

ПРИМЕЧАНИЕ 1. – Таким образом, фундаментальная природа технологии обмена данными через общую физическую среду передачи, такую как топология шины, в корне отличается от технологии коммутируемых сетей Ethernet.

Каждый участник может считывать весь трафик, передаваемый по шине CAN. Различные сетевые домены на основе шины, а также дополнительные субдомены отделяют трафик, требующий защиты, от других типов трафика, таких как трафик информационно-развлекательных систем или систем обеспечения комфортных условий. Связь между сетевыми доменами возможна только через CGW, который обычно реализует механизмы применения правил политики (например правил, связанных с фильтрами) для предотвращения лавинных атак и обеспечения готовности сети.

ПРИМЕЧАНИЕ 2. – Автомобильные шлюзы (такие как CGW) обеспечивают набор сетевых функций, конкретный поднабор которых относится к обеспечению безопасности связи. Следовательно, применяются не только правила политики безопасности, но и другие специальные правила политики, не связанные с безопасностью (например, для передачи данных VLAN, IP-переадресации или настройки действий QoS, управляемых TSN).

Ethernet представляет собой установившийся стандарт сетевой связи с широким спектром применений. Он используется для обычных сетей связи машинного типа (например, компьютерных), охватывающих локальные сети разного размера (малые, локальные, городские и т. д.), а также для наземных сетей радиодоступа в системах подвижной связи. С учетом этих исторических и технологических предпосылок могут найтись готовые системы обеспечения безопасности сети, пригодные для использования в качестве шаблона.

Ввиду распространенности этой технологии возможны несколько видов атак на сети Ethernet (включая протоколы верхнего уровня), но существуют и контрмеры для различных сценариев использования. Например, для транспортных служб в интернете, основанных (только) на протоколе управления передачей (TCP), настоятельно рекомендуется использовать протокол безопасности транспортного уровня (TLS), чтобы обеспечить подлинность, целостность и конфиденциальность связи. А для транспортных служб, основанных на протоколе датаграмм пользователя (UDP), рекомендуется дополнительно использовать протокол датаграмм безопасности транспортного уровня (DTLS). При использовании Ethernet в качестве установившегося и распространенного стандарта бортовой автомобильной сети можно применять готовые механизмы безопасности, связанные со стеком протоколов Интернет (IP). Однако меры безопасности, применяемые в обычных компьютерных сетях, не подходят для автомобильных приложений, поскольку они разработаны без учета соответствующих требований и возможностей таких приложений. Например, они могут не обеспечивать гарантии в отношении реального времени и требовать улучшенных рабочих характеристик, недостижимых для

встроенных устройств с ограниченными ресурсами. Поэтому на момент публикации настоящей Рекомендации вопрос интеграции механизмов безопасности для чувствительных ко времени протоколов передачи данных на базе Ethernet не рассматривается.

Решающее значение имеет разделение бортовой автомобильной сети по соображениям безопасности. В настоящее время производители OEM рассматривают возможность логической изоляции трафика Ethernet с использованием виртуализации сети, которая в случае Ethernet относится к виртуальной локальной сети (VLAN) как виртуальной частной сети уровня 2. Следует отметить, что разделение трафика в бортовой автомобильной сети может быть достигнуто и другими средствами, такими как применение VPN уровня 1 (посредством физического разделения сетей Ethernet) или уровня 3 (с использованием известного решения VPN для услуг связи IP поверх Ethernet).

VLAN – это хорошо зарекомендовавший себя способ логической изоляции на канальном уровне в обычных компьютерных сетях. VLAN обычно используются для разделения физических сетей на отдельные логические сети. Возможность применения VLAN в бортовой автомобильной сети главным образом основана на том факте, что VLAN обеспечивает приоритизацию трафика (например, путем преобразования кодов приоритета VLAN непосредственно в классы трафика TSN).

ПРИМЕЧАНИЕ 3. – Вопросы обеспечения безопасности иерархических сетей VLAN, которые могут применяться в будущих IVN для конкретных моделей связи V2X, выходят за рамки данного издания настоящей Рекомендации. Таким образом, здесь предполагается только применение однотеговых сетей VLAN или сетей на основе портов.

Применение широко распространенного стандарта Ethernet для бортовых автомобильных сетей, с одной стороны, открывает некоторые новые возможности, а с другой – требует особого внимания. Помимо отсутствия готового механизма безопасности, подключение внешних устройств к автомобилю по сети Ethernet рекомендуется осуществлять без какого-либо специального оборудования.

Пользователи даже могут попытаться подключить свои ноутбуки или воспользоваться смартфоном для расширения доступа к IVN. Использование коммутатора Ethernet в качестве дополнительного компонента может предоставить неавторизованным "умельцам" интересный вектор атак. Злоумышленники могут осуществлять известные атаки из интернета или использовать опубликованные эксплойты для обычных коммутаторов Ethernet. Как и в области безопасности связи, существуют контрмеры для обычных коммутаторов Ethernet. Однако в отношении автомобильной среды необходимы дальнейшие исследования.

В таблице 1 на абстрактном уровне показаны различия между традиционными протоколами IVN, ориентированными на полевые шины, и протоколами на базе Ethernet. В первом столбце для каждой цели сравнения указан уровень зрелости критериев, обозначенный соответствующим символом: низкий (–), средний (0), высокий (+), наивысший (++). Следует отметить, что таблица 1 намеренно упрощена; для более серьезной оценки протоколов потребуется сравнение Ethernet с каждой отдельной технологией полевой или автомобильной шины передачи данных.

Таблица 1 − Сравнение традиционной архитектуры бортовой автомобильной сети с архитектурой на базе Ethernet

Критерии	**Протоколы IVN, ориентированные на полевые шины (Примечание 1)**		**IVN на базе Ethernet**	
Простота	–	Сложный неоднородный многопротокольный шлюз	++	Очень однородная с коммутаторами (в основном) уровня 2
Гибкость	–	Трудно расширить/ адаптировать новую подсеть (существующие – легко)	++	Легко расширять/адаптировать как новые, так и существующие подсети
Пропускная способность	+	Зависит от типа шины	++	До нескольких гигабит в секунду
Работа в режиме реального времени	++	Хорошо зарекомендовали себя за десятилетия	–	Возможна, но сеть не рассчитана на это

Таблица 1 − Сравнение традиционной архитектуры бортовой автомобильной сети с архитектурой на базе Ethernet

Критерии	**Протоколы IVN, ориентированные на полевые шины (Примечание 1)**		**IVN на базе Ethernet**	
Количество необходимого физического материала	–	Индивидуальная проводка на каждую шину	+	Одна витая пара на всю сеть
Стоимость (инвестиции, не эксплуатация)	–	Мелкосерийное производство для автомобильной промышленности	+	Глобальное массовое производство не только для автомобильной промышленности
Степень стандартизации	–	Большое разнообразие стандартов	+	Малое количество стандартов
Модели установления соединений на физическом уровне и уровне канала передачи данных (ПРИМЕЧАНИЕ 2)	–	Только модели соединений точка – много точек ввиду использования общей физической среды передачи (шины).	+	Ethernet поддерживает обе модели связи – точка–точка и точка – много точек (ПРИМЕЧАНИЕ 3)
Целостность сообщений (ПРИМЕЧАНИЕ 4)	+	Контроль циклическим избыточным кодом (CRC) + специальные меры защиты шины	+	CRC, блочные коды
Меры безопасности (ПРИМЕЧАНИЕ 5)	–	Практически отсутствуют	0	Надстройки (протокол Интернет версии 4 (IPv4)), безопасность протокола Интернет (IPsec) (протокол Интернет версии 6 (IPv6))

ПРИМЕЧАНИЕ 1. – Оценки по перечисленным критериям отражают типичную структуру протокола, но действительны не для всех видов технологий связи, ориентированных на полевые шины, например CAN не предоставляет собственных протокольных средств для поддержки связи в режиме реального времени.

ПРИМЕЧАНИЕ 2. – Здесь принято следующее допущение: в автомобильных приложениях обычно требуются услуги передачи данных с топологией соединений точка–точка или точка – много точек. Такие топологии должны обслуживаться топологиями логических соединений, что в данном случае подразумевает рассмотрение топологии соединений канального уровня в качестве общего знаменателя уровня протокола обсуждаемых технологий связи.

ПРИМЕЧАНИЕ 3. – Автомобильные сети Ethernet будут развертываться и эксплуатироваться только в коммутируемом режиме (главным образом в соответствии с целями качества обслуживания (QoS)), что подразумевает поддержку моделей соединения точка–точка только на уровне физической среды передачи Ethernet. Физическая среда передачи не является совместно используемой, а каждая конечная точка Ethernet уровня 1 имеет монопольный доступ к ресурсам физического уровня. Тем не менее топологии связи точка – много точек также поддерживаются либо напрямую с помощью собственных встроенных возможностей многоадресной и широковещательной передачи сети Ethernet с использованием функций переадресации на канальном уровне, либо косвенно с помощью протоколов верхнего уровня (таких как IP и его типы сетевых адресов многоадресной, произвольной и широковещательной передачи).

ПРИМЕЧАНИЕ 4. – Целостность, относящаяся к безопасности, здесь охватывает: a) целостность битов; b) целостность данных, то есть либо целостность отдельных битов блока данных протокола (PDU), либо целостность всего PDU как такового (на определенных протокольных уровнях).

ПРИМЕЧАНИЕ 5. – Меры безопасности оцениваются независимо от того, имеет ли соответствующая спецификация протокола неотъемлемые функции безопасности или нет.

Изложенные критерии сравнения охватывают базовую разработку сетей и служб передачи данных, а также аспекты, связанные с безопасностью.

6.3 Службы передачи данных с использованием Ethernet в автомобильных приложениях

В настоящее время автомобильный Ethernet используется главным образом для диагностики и передачи мультимедийных потоков, таких как видеоданные от видеокамер для ADAS. Кроме того, в середине 2010-х годов возможность обмениваться данными через Ethernet появилась у вычислительных узлов в транспортных средствах (таких как ЭБУ).

6.3.1 Диагностика

Обычный метод диагностики транспортных средств заключается в подключении диагностического инструмента к порту OBD-II для обмена данными с целевым ЭБУ по протоколу единой диагностической службы (UDS). UDS – это специально разработанный для автомобильной промышленности протокол прикладного уровня, который позволяет диагностическим системам обмениваться данными с ЭБУ для диагностики неисправностей и соответствующего перепрограммирования ЭБУ (см. [b-ISO 14229-5]).

Диагностическая связь по протоколу Интернет (DoIP) основана на IP (см. [b-ISO 13400-2]). DoIP позволяет передавать сообщения UDS между транспортным средством и внешним испытательным оборудованием через Ethernet, и становится возможным удаленно получать диагностические данные от автомобиля без необходимости физического подключения к нему. DoIP обеспечивает инкапсуляцию сообщений UDS в пакеты TCP или датаграммы UDP, как показано на рисунке 2.

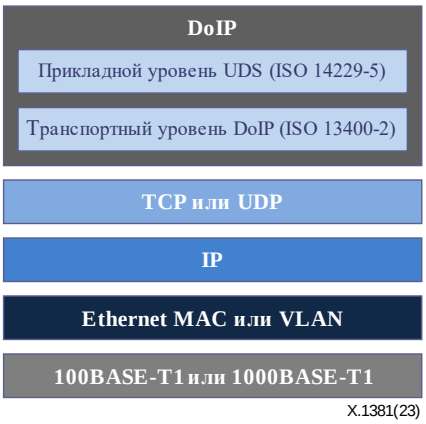

Рисунок 2 − Стек протоколов для передачи диагностических данных посредством приложения на базе протокола Интернет

Сам протокол DoIP не содержит никаких механизмов обеспечения безопасности передачи данных. Сообщения, как правило, не аутентифицируются и никаким образом не шифруются. DoIP допускает аутентификацию на верхнем уровне (уровнях), но она не обязательна.

6.3.2 Медиапотоки в контексте мультимедийных услуг

Для ADAS в высокоавтоматизированных и полностью автономных транспортных средствах требуется множество датчиков, таких как видеокамеры высокого разрешения и средства связи, которые позволяют получить достаточную информацию для восприятия транспортным средством окружающей среды. Кроме того, многие автомобили оснащены устройствами, которые используют или передают медиапотоки на уровне приложений (не путать с (под)уровнями физической среды передачи в случае Ethernet) для информационно-развлекательных систем, системы кругового обзора, системы помощи при парковке, системы удержания в пределах полосы движения, системы ночного видения и т. д. Видеокамеры генерируют относительно большие медиапотоки (с точки зрения объема трафика) с целевыми значениями QoS, зависящими от приложения, при короткой задержке и высококачественной передаче. Если используется протокол CAN, то вышеуказанные требования выполнить невозможно из-за присущих этому протоколу ограничений, например диапазона размера полезной нагрузки.

Автомобильный Ethernet позволяет выполнить эти требования с использованием структуры аудио-видео моста (AVB) IEEE.

ПРИМЕЧАНИЕ. – Термин AVB относится к набору стандартов [b-IEEE 802.1], включая [b-IEEE 802.1Qav], [b-IEEE 802.1AS] и [b-IEEE 802.1Qat]. Поэтому в 2012 году рабочая группа IEEE AVB изменила свое название на Целевую группу TSN, которая теперь охватывает и стандарты AVB.

AVB может удовлетворить более общие требования TSN, открывая возможности для единой сети, управляющей информационно-развлекательной системой, оборудованием салона, системами помощи водителю и даже критически важными функциями безопасности.

В случае системы кругового обзора группа видеокамер обеспечивает синхронизированный круговой обзор на 360° вокруг автомобиля. Этот поток видеоданных можно передавать в систему информирования водителя, такую как система отображения информации на лобовом стекле или навигационная видеосистема. Через сеть AVB также можно синхронизировать дополнительные данные датчиков с соответствующими ЭБУ.

6.3.3 Магистраль бортовой автомобильной сети

Современные автомобили могут иметь более 100 ЭБУ. ЭБУ, или вычислительный узел автомобиля, относится к сетевым узлам в топологии IVN Ethernet с одним или несколькими конечными узлами (в зависимости от количества физических, логических или виртуальных интерфейсов подключения Ethernet на вычислительный узел). Более того, количество ЭБУ может еще больше возрасти, в результате чего для ADAS и автономных транспортных средств потребуется большая пропускная способность IVN.

Кроме того, для традиционных протоколов IVN используется тяжелая и дорогостоящая система жгутов проводов. Если в качестве магистрали IVN используется Ethernet, то можно исключить до 80% затрат на внутренние соединения и 30% массы электропроводки в автомобиле.

Как показано на рисунке 1, IVN на базе Ethernet состоит из нескольких доменов. В каждом домене используются традиционные протоколы IVN, а Ethernet применяется для междоменной связи, то есть на уровне базовой сети (если сравнивать их с сетями ИКТ), которую часто называют магистральной сетью.

Автомобильный Ethernet отличается от топологии шинной системы. Здесь отсутствует проводник шины, подключенный к многочисленным ЭБУ, датчикам и исполнительным устройствам. Вместо этого все они подключаются к коммутатору Ethernet с использованием соединения точка–точка. Если информационные сообщения должны передаваться из одного домена в другой, это легко делается с помощью функций межсетевого взаимодействия, которые в IVN на базе Ethernet предоставляются коммутаторами Ethernet, шлюзами VLAN, а возможно и IP-маршрутизаторами и IP-шлюзами. Для традиционных протоколов на базе автомобильной полевой шины, напротив, требуется поддержка сети, а для обмена данными с конечными точками, расположенными в сети Ethernet, возможно, также поддержка службы межсетевого взаимодействия, обычно обеспечиваемая шлюзами.

7 Анализ угроз

7.1 Методика подхода к анализу угроз

В данном пункте анализируются сценарии угроз безопасности в контексте бортовых автомобильных сетей Ethernet. Общие выявленные угрозы для соединенных транспортных средств описаны в [ITU-T X.1371].

Чтобы вывести концепцию безопасности, необходимо определить ее цели. Для определения метода управления рисками на этапе определения цели безопасности выполняется анализ угроз и оценка рисков (TARA). Для того чтобы выполнить TARA, необходимо определить активы безопасности и цели по обеспечению безопасности, а также связанные с ними угрозы. Концепцию безопасности можно установить, если определить метод управления соответствующими рисками с помощью оценки воздействия и оценки возможности атак на основе выявленных активов безопасности, целей по обеспечению безопасности и угроз; дополнительную информацию см. в [b-ISO/SAE 21434]. В данном пункте определяются активы безопасности и связанные с ними цели по обеспечению безопасности, а затем рассматриваются угрозы безопасности в соответствии с подходом к анализу угроз, изложенным в [b-ISO/SAE 21434].

Процесс оценки воздействия, оценки возможности атак и принятия решения о риске выходит за рамки настоящей Рекомендации и подлежит дальнейшему изучению.

7.2 Активы безопасности

Актив безопасности (защищаемый актив) – это любой информационный объект, функция или ресурс, которые должны быть защищены. Активы безопасности, выявленные при рассмотрении IVN на базе Ethernet, перечислены в таблице 2.

Таблица 2 − Активы безопасности

Актив	Описание
Данные управления	Данные управления подразделяются на две категории (Примечание 1): 1) данные о конфигурации, которые характеризуют функциональное поведение сетевых элементов или сетевых функций, связанных с Ethernet-соединениями, таких как шлюз, коммутатор Ethernet, система обнаружения вторжений (IDS) и брандмауэр; 2) данные о рабочем состоянии, описывающие не только фактическое поведение этих сетевых объектов, но и все услуги управления, использующие уведомления [b-ITU-T M.3702], такие как аварийные сообщения [b-ITU T M.3703], в рамках управления отказами. Потоки данных управления обеих категорий между управляющим и управляемым объектами, как правило, подлежат защите. Однако влияние на безопасность, например, манипулирования данными конфигурации обычно бывает намного выше, чем на данные о рабочем состоянии. С другой стороны, например, намеренное подавление аварийного сигнала, переданного сетевым элементом Ethernet, может усугубить текущую ситуацию отказа
Блоки данных протокола уровня 2, относящиеся к связи на базе Ethernet	Трафик Ethernet состоит из трафика канального уровня, то есть кадров управления доступом к среде передачи Ethernet (MAC) (как PDU уровня 2), передаваемых в автомобильную IVN на базе Ethernet
Данные управления, создаваемые при регистрации событий (Примечание 2)	Успешное обнаружение событий безопасности и соответствующая информация о них могут быть проверены
Криптографический материал	Ключи и сертификаты для симметричных и асимметричных схем шифрования, включая другие данные, подтверждающие полномочия, такие как пароли
Образы микропрограммного или программного обеспечения	Скомпилированный код для исполнения на вычислительных узлах автомобиля, таких как ЭБУ
ПРИМЕЧАНИЕ 1. – См. применимую структуру управления сетью Ethernet, например описанную в [b-ITU-T M.3010, b-ITU-T X.703, b-ITU-T G.8013, b-ITU-T Y.1730]. Данные управления для сетевых объектов Ethernet основаны на языке моделирования спецификаций и данных управления YANG [b-IETF RFC 6020]. Модели данных управления на языке YANG для всевозможных объектов Ethernet, то есть основную справочную информацию по данным управления для настоящей Рекомендации, предлагает группа IEEE 802 (как ответственная за технологию Ethernet). ПРИМЕЧАНИЕ 2. – Управление функциями регистрации событий [b-ITU-T M.3705] в этой таблице не рассматривается. Здесь имеется в виду регистрация системных событий, вызванных потоками информации управления, которые записываются функциями регистрации событий (о внутренних потоках данных управления сетевого оборудования см. в [b-ITU-T G.7710]). ПРИМЕЧАНИЕ 3. – Такая функция обнаружения относится к категории проверки статистической гипотезы, в первую очередь из-за неопределенностей в описании событий или условий правила политики для однозначной идентификации таких событий. Таким образом, успешное обнаружение дает лишь вероятностные результаты, в том числе ложные помимо истинных. Следовательно, должна быть квалифицирована и количественно определена степень качества обнаружения, например, путем оценки ожидаемой доли ложных результатов.	

7.3 Цели по обеспечению безопасности

В таблице 3 активы безопасности (см. пункт 7.1) анализируются по отношению к перечню целей по обеспечению безопасности.

Таблица 3 − Цели по обеспечению безопасности

Актив безопасности	Цель по обеспечению безопасности	Пояснения
Данные управления	Целостность, конфиденциальность	Не следует подвергать манипуляциям данные, определяющие функциональное поведение сетевых элементов Ethernet, таких как автомобильный шлюз, коммутатор Ethernet, IDS и брандмауэр автомобиля.
Блоки данных протокола уровня 2, относящиеся к связи на базе Ethernet	Конфиденциальность	Предотвращение раскрытия блоков данных протокола определенного уровня ((Lx)-PDU), передаваемых в автомобильную IVN на базе Ethernet.
	Готовность	Следует, чтобы услуги передачи данных через автомобильную IVN на базе Ethernet были доступны всякий раз, когда это необходимо, при условии соблюдения связанных с ними четко определенных ограничений.
	Аутентичность	Следует, чтобы система связи по автомобильной IVN на базе Ethernet обнаруживала и отклоняла несанкционированные запросы других компонентов.
	Целостность	Предотвращение манипулирования данными связи, обмен которыми осуществляется по автомобильной IVN на базе Ethernet.
Данные управления, создаваемые при регистрации событий	Целостность	Предотвращение манипулирования доказательствами и сведениями о зарегистрированных событиях безопасности, которые могут быть проверены, без обнаружения. Имеется в виду целостность битов и данных, относящихся к регистрируемой информации.
Криптографический материал	Конфиденциальность	Предотвращение раскрытия секретных и личных ключей, а также учетных данных пользователей, таких как пароли.
	Целостность	Предотвращение манипулирования ключами и сертификатами без обнаружения.
Образы микропрограммного или программного обеспечения	Конфиденциальность	Предотвращение раскрытия неавторизованным объектам содержания микропрограммного и программного обеспечения, например скомпилированный код и калибровочные данные, относящиеся к интеллектуальной собственности.
	Целостность	Предотвращение манипулирования образами микропрограммного и программного обеспечения, например объектом процедур изменения функциональных возможностей (например, с помощью управления встроенным ПО по беспроводной сети, управления ПО по беспроводной сети, общего управления программным обеспечением).

7.4 Выявленные угрозы

7.4.1 Угрозы для конфиденциальности

– Несанкционированное раскрытие трафика Ethernet (по утверждению PDU физического уровня (L1) или уровня канала передачи данных (L2) Ethernet)

Злоумышленник может прослушивать трафик Ethernet, подключившись к компоненту, отвечающему за внешнюю связь с коммутатором Ethernet. Он сможет анализировать информацию трафика, прослушивая PDU, относящиеся к Ethernet.

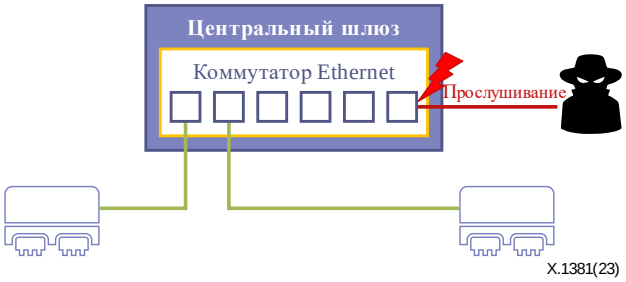

Рисунок 3 – Угрозы для конфиденциальности – прослушивание

– Несанкционированное раскрытие криптографических материалов

Злоумышленник может перехватить криптографические материалы следующими способами:

- путем физического вскрытия корпуса накопителя;
- путем считывания криптографических материалов из памяти каждого компонента, где они используются;
- путем изменения микропрограммного обеспечения и изменения потока управления для раскрытия криптографических материалов.

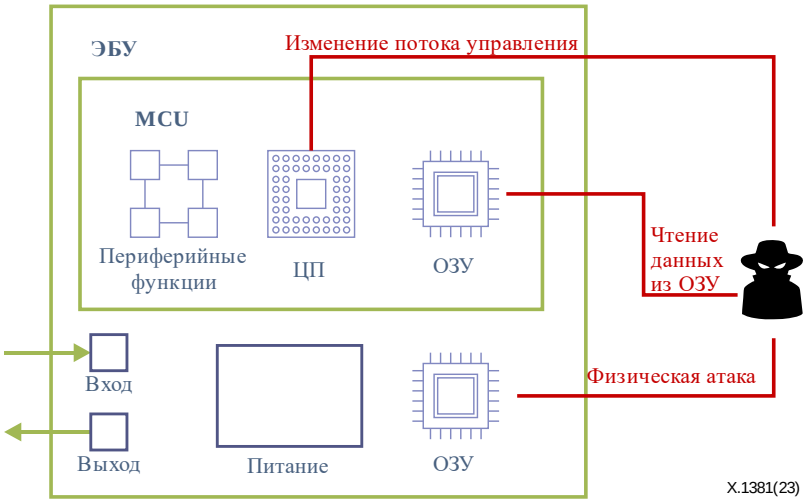

Рисунок 4 – Угрозы для конфиденциальности криптографических материалов

7.4.2 Угрозы для целостности данных

Контекст целостности ограничен объектами данных в целом, определяемыми здесь конкретными сценариями обеспечения безопасности.

– Манипулирование данными конфигурации

Злоумышленник может манипулировать данными конфигурации коммутатора Ethernet.

– Манипулирование данными журнала регистрации событий

Злоумышленник может удалить или изменить данные журнала регистрации событий и особенно контрольного журнала регистрации событий безопасности через IDS, брандмауэр и систему беспроводной связи.

– Манипулирование криптографическими материалами

Злоумышленник может самостоятельно изменить действительные криптографические материалы.

– Манипулирование микропрограммным обеспечением

Злоумышленник может заменить микропрограммное обеспечение вредоносным.

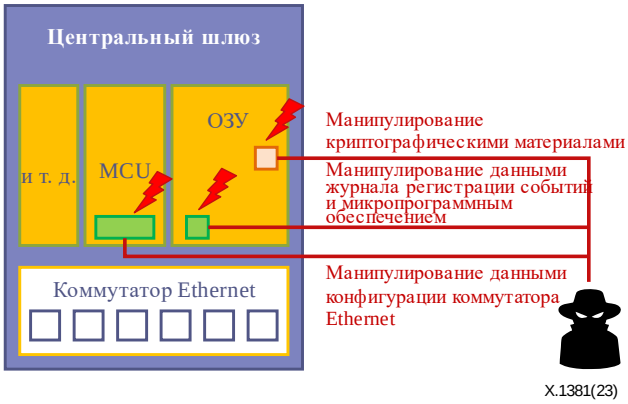

Рисунок 5 – Угрозы для целостности передаваемых блоков данных

7.4.3 Угрозы для готовности

Атрибут качества "готовность" в данном случае относится к готовности услуг связи на базе Ethernet, которая трансформируется в требования к готовности соединений на отдельных уровнях и в сети в целом, что в свою очередь может приводить, например, к готовности тракта Ethernet в случае IVN с избыточными трактами Ethernet.

– Угрозы для готовности – атака типа отказ в обслуживании (DoS) на IVN на базе Ethernet

Злоумышленник может осуществить DoS-атаку, чтобы помешать работе определенного ЭБУ, включая CGW, автомобильный пограничный шлюз или блок управления соединениями.

Как показано на рисунке 6, злоумышленник может сделать определенные ЭБУ и CGW недоступными для соответствующих ЭБУ-партнеров, используя хорошо известные методы DoS-атак, такие как атаки через транспортный протокол IP, например SYN flood или teardrop для TCP. Злоумышленник также может истощить ресурсы IVN, используя такие атаки, как лавины широковещательных пакетов уровня 2, так что обмен обычными MAC-кадрами Ethernet (как PDU уровня 2) становится невозможным.

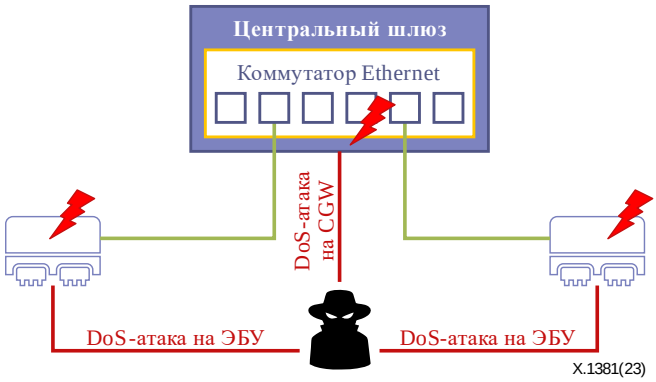

Рисунок 6 – Угрозы для готовности

7.4.4 Угрозы для аутентичности

– Подмена вычислительных узлов автомобиля (например, ЭБУ)

Злоумышленник может подменить компонент, такой как ЭБУ, и передавать вредоносные сообщения другим компонентам. Он может притвориться действительной конечной точкой связи (например, находящейся в ЭБУ) и отправлять вредоносные сообщения или получать сетевой трафик. В примере, показанном на рисунке 7, нормальная ситуация представлена соединениями верхнего уровня между ЭБУ A и B (например, двухточечными IP-соединениями транспортного уровня), так что ЭБУ A передает трафик Ethernet в ЭБУ B (и, возможно, наоборот). Злоумышленник подменяет ЭБУ A, используя такие методы атаки, как спуфинг протокола разрешения адресов (ARP) или спуфинг IP (см., например, [b-IETF RFC 2827], [b-IETF RFC 4953], [b-IETF RFC 6575], [b-IETF RFC 6959]), а затем передает вредоносное сообщение в ЭБУ B.

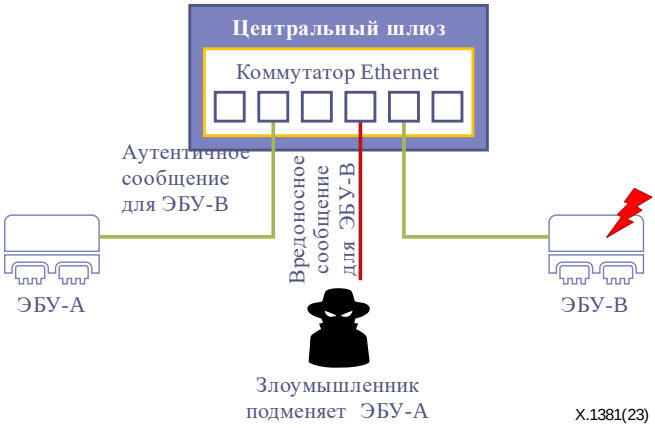

Рисунок 7 – Угрозы для аутентичности

8 Требования безопасности

В данном разделе представлены требования безопасности для устранения выявленных угроз в среде IVN на базе Ethernet.

8.1 Конфиденциальность

– [SR-01] ЭБУ, в котором хранятся и используются криптографические материалы, рекомендуется использовать для безопасного хранения криптографических материалов безопасный накопитель, такой как аппаратный модуль безопасности (HSM).

– [SR-02] Рекомендуется использовать известные алгоритмы и протоколы, например алгоритмы и протоколы, определенные международными организациями по разработке стандартов.

– [SR-03] Для обеспечения безопасности при передаче сообщений по сети Ethernet рекомендуется использовать механизмы предотвращения прослушивания.

  В составе трафика автомобильной сети на базе Ethernet в дополнение к соответствующему уровню протокола для его шифрования и шифрования PDU для конкретных протоколов (полного или частичного) могут факультативно применяться различные протоколы безопасности, зависящие от уровня. Примерами таких протоколов безопасности связи могут служить протокол безопасного управления доступом к среде передачи (MACsec), IPsec, TLS и DTLS.

– [SR-04] Предотвращается раскрытие конфиденциальных криптографических материалов неавторизованным объектам.

  Когда криптографические материалы становятся доступными для неавторизованных объектов, механизм безопасности, применяемый в транспортном средстве, перестает быть безопасным.

– [SR-05] Для работы с криптографическими материалами на этапе производства рекомендуется использовать только уполномоченный персонал и разрешенное оборудование в соответствии с политикой управления доступом в транспортном средстве.

– [SR-06] Рекомендуется статическая настройка таблицы MAC-адресов коммутатора Ethernet.

  Если таблица MAC-адресов в коммутаторе Ethernet настроена статически, то доступ к автомобильной сети Ethernet смогут получать только заранее определенные ЭБУ.

  Использование динамических MAC-адресов может привести к проблемам безопасности, таким как спуфинг и флуд-атака на MAC-адреса. Если в таблице хранится большое количество MAC-адресов, коммутатор может производить широковещательную передачу кадров данных на все сетевые порты. В случае автомобиля во избежание этих проблем безопасности можно настроить таблицу MAC-адресов статически, поскольку ЭБУ, устанавливающий связь с коммутатором, уже известен.

– [SR-07] Рекомендуется отключить функцию динамического обучения таблицы MAC-адресов в коммутаторе Ethernet.

  Отключение функции динамического обучения таблицы MAC-адресов может предотвратить MAC-флудинг (MAC-flooding), который может привести к передаче сообщений Ethernet в непредусмотренные пункты назначения.

  Тем не менее, если это все же необходимо для эксплуатации или технического обслуживания автомобиля, то коммутатор должен хранить изученные MAC-адреса лишь в течение ограниченного времени.

– [SR-08] Рекомендуется, чтобы сетевые IP-интерфейсы функций IP-хоста (например, реализованные в ЭБУ), использующие Ethernet, получали фиксированные IP-адреса, присваиваемые ответственной функцией управления сетью.

ПРИМЕЧАНИЕ. – Здесь конкретные функции управления сетью – это функции управления определением идентичности, включая управление сетевыми адресами. Такие функции управления могут выполняться на разных этапах жизненного цикла и эксплуатации IVN на базе Ethernet, например полностью статическое предварительное определение или сочетание статического и динамического управления конфигурацией, которое также может зависеть или не зависеть от использования операционных сетевых протоколов для уровней Ethernet и интернета.

Это требование безопасности относится не только к отдельным ЭБУ в целом, но и к каждому сегменту или узлу в сети Ethernet (например, к каждой виртуальной машине).

8.2 Целостность

– [SR-09] Рекомендуется, чтобы данные регистрации событий и конфигурации коммутатора Ethernet были защищены от несанкционированного изменения и удаления.

– [SR-10] Рекомендуется, чтобы обновление данных конфигурации осуществлялось только авторизованными объектами.

– [SR-11] Рекомендуется, чтобы в ЭБУ использовались функции безопасной загрузки наряду с проверкой целостности микропрограммного обеспечения.

Микропрограммное обеспечение ЭБУ и данные коммутатора Ethernet, хранящиеся в памяти ЭБУ, должны проверяться на целостность до или во время исполнения. Для безопасной загрузки можно использовать проверку целостности конфигурации и входных параметров микропрограммного обеспечения.

8.3 Готовность

Понятие готовности в данном контексте относится к готовности доменов сети Ethernet, то есть готовности услуг связи. На достижение этих целей готовности могут повлиять атаки, направленные на подрыв безопасности, а также другие события, не связанные с безопасностью (например, отказ компонента или нарушение связи).

Таким образом, требования готовности (указанные в этом пункте) на самом деле представляют собой требования безопасности, потенциально влияющие на целевые показатели готовности.

– [SR-12] Рекомендуется, чтобы DoS-атаки на IVN на базе Ethernet учитывались на этапе проектирования автомобиля.

– [SR-13] Рекомендуется, чтобы коммутатор обнаруживал DoS-атаки и обеспечивал защиту от них с применением информационных сообщений Ethernet.

  Контроль потоков трафика между ЭБУ и управление ими имеют решающее значение для минимизации рисков, создаваемых DoS-атаками в IVN.

– [SR-14] Критически важные для безопасности функции рекомендуется изолировать от других бортовых автомобильных сетей.

8.4 Аутентичность

Аутентичность – это возможность удостовериться в том, что данная информация не содержит изменений или подлога и что она действительно была создана тем объектом, который представляется источником данной информации.

– [SR-15] Рекомендуется предусмотреть меры противодействия, гарантирующие защиту информационных сообщений Ethernet от атак подмены.

– [SR-16] Рекомендуется, чтобы физические сетевые интерфейсы Ethernet сетевых элементов IVN, не предназначенные для использования в серийных транспортных средствах, допускали временное изменение административного состояния (включение, отключение) со значением параметра конфигурации по умолчанию "отключено".

  ПРИМЕЧАНИЕ. – Такое требование, связанное с управлением сетью, очевидно подразумевает поддержку соответствующей детальной модели данных управления для Ethernet.

  Соблюдение этого требования ограничивает поверхность атаки за счет уменьшения количества доступных точек входа.

– [SR-17] Рекомендуется, чтобы доступ к интерфейсу связи, реализованному в аппаратной или программной области, был ограничен в соответствии с принципом наименьших привилегий.

– [SR-18] Рекомендуется, чтобы интерфейс отладки в ЭБУ был настроен для защиты от несанкционированного доступа. Это требование распространяется на интерфейсы локальной отладки вычислительных узлов автомобиля, а также интерфейсы удаленной отладки с доступом к таким сетевым узлам через IVN.

В таблице 4 показано соответствие между выявленными угрозами, рассмотренными в разделе 7, и требованиями безопасности раздела 8.

Таблица 4 − Сопоставление угроз и требований безопасности

Угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Несанкционированное раскрытие сообщений Ethernet	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
Несанкционированное раскрытие криптографических материалов	Y	Y	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	Y
Манипулирование данными конфигурации	Y	Y	–	–	–	Y	Y	–	Y	Y	Y	–	–	–	–	–	–	Y
Манипулирование данными журнала регистрации событий	Y	Y	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	Y
Манипулирование криптографическими материалами	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
DoS-атака на IVN на базе Ethernet	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–
Подмена ЭБУ	–	Y	–	–	–	Y	Y	Y	–	–	–	–	–	Y	Y	Y	Y	Y

Каждая из выявленных угроз может быть устранена путем выполнения соответствующих требований безопасности, помеченных символом Y. Например, для первой угрозы – несанкционированного доступа к информационным сообщениям Ethernet – требованиями безопасности являются [SR-2], [SR-3] и [CP-18].

9 Реализация безопасных автомобильных сетей на базе Ethernet

9.1 Предварительные соображения, связанные с реализацией

В настоящей Рекомендации представлены соображения, связанные с реализацией, в целях:

- рассмотрения аспектов безопасности, обусловленных техническими ограничениями;
- иллюстрации проблем безопасности, характерных для реализации типичной технической архитектуры IVN.

Ценность такой информации по безопасности, по существу, тесно связана лишь с конкретным техническим представлением, поэтому в будущем эта информация может устареть, например если изменится техническая архитектура системы IVN.

Однако еще не существует никаких применимых нетехнических эталонных моделей и эталонной архитектуры IVN, которые можно было бы использовать в качестве основы для обсуждения аспектов безопасности, связанных с реализацией. Поэтому в настоящей Рекомендации рассматриваются по крайней мере некоторые аспекты безопасности на примере технических систем IVN (как представленных в разделе 6).

9.2 Функции шлюза безопасности, относящиеся к автомобильному Ethernet

Важное значение для минимизации риска несанкционированного доступа и DoS-атак в IVN на базе Ethernet имеют контроль и управление потоками данных между различными логическими сетевыми доменами (например, VLAN, подсеть IPv4, подсеть, определяемая префиксом IPv6; каждый логический сетевой домен представляет определенный домен безопасности со своими параметрами безопасности). Для разрешения или запрета передачи данных в соответствии с заранее определенными правилами в IVN или на стыке бортовой автомобильной и внешней сетей в целях повышения уровня безопасности используются шлюзы безопасности и, в частности, брандмауэры.

Для реализации таких функций шлюза безопасности (например, брандмауэра) рекомендуются следующие известные технические компоненты современной типовой технической электрической и электронной архитектуры бортовой автомобильной сети, способные контролировать сообщения, поступающие извне или через IVN.

– Коммутатор Ethernet.

  ПРИМЕЧАНИЕ 1. – Компонент логического коммутатора Ethernet представляет собой тип сетевого, а не конечного узла. Существуют два варианта реализации IVN: с коммутатором Ethernet как самостоятельным техническим компонентом и с коммутатором Ethernet, монолитно интегрированным в вычислительный узел автомобиля в качестве периферийного или центрального узла.

– Автомобильный пограничный шлюз.

  ПРИМЕЧАНИЕ 2. – Естественный выбор, поскольку этот технический компонент представляет собой единую точку наблюдения за регулярным трафиком V2X.

– ЭБУ – когда у ЭБУ имеется прямая внешняя связь.

  ПРИМЕЧАНИЕ 3. – Вычислительный узел автомобиля может предоставлять дополнительные интерфейсы для прямой связи с другим транспортным средством (то есть в обход автомобильного пограничного шлюза), например для целей диагностики.

Брандмауэр использует несколько механизмов фильтрации пакетов, включая статическую фильтрацию пакетов, проверку пакетов без учета состояния или с отслеживанием состояния, поверхностную, углубленную и даже глубокую проверку пакетов.

ПРИМЕЧАНИЕ 4. – Для однозначности метафорические термины "поверхностный", "углубленный" и т. д. следует относить: a) к уровню протокола; и b) к информации о контексте PDU (см., например, [b-ITU-T Y.2770], [b-ITU-T Y.2771]), например, "поверхностная проверка пакетов" в случае интернет-трафика – это, как правило, проверка заголовков L3,4.

В частности, механизм статической фильтрации пакетов основан на предопределенных правилах политики. Следовательно, рекомендуется установка определенного правила политики в соответствии с электрической и электронной архитектурой автомобиля и применяемым протоколом передачи

данных. Кроме того, согласно политике брандмауэра по умолчанию применяется метод белого списка, когда, как правило, блокируются все соединения, которые не разрешены явно.

Одной из основных функций брандмауэра является защита от DoS-атак. Брандмауэры могут защитить сеть от DoS-атак, устанавливая заданные пороговые значения параметров, таких как счетчики, или применяя частотные фильтры.

Другой дополнительной функцией брандмауэра является ведение журнала событий (то есть сетевой элемент брандмауэра как управляемый объект обеспечивает встроенную функцию управления журналом событий в соответствии с [b-ITU-T M.3705]). Ожидается, что предметом регистрации будут события, связанные с безопасностью. Таким образом брандмауэры, IDS или шлюзы безопасности в целом регистрируют информацию при возникновении события безопасности, что не только помогает экспертам анализировать ситуацию, связанную с событием, но и повышает точность политики брандмауэра за счет таких исследований, как изучение заблокированных записей. Поэтому при хранении журнала регистрации событий необходимо использовать криптографический механизм, гарантирующий целостность записей.

9.3 Безопасная конфигурация VLAN

Настройка безопасной VLAN чрезвычайно важна для обеспечения безопасности связи IVN в целях соблюдения требований [SR-14] и [SR-17]. Предполагается, что ответственность за спецификацию этой VLAN несут OEM, поскольку конфигурация VLAN зависит от электрической и электронной архитектуры автомобиля, выбранной такими производителями.

У каждой VLAN имеется уникальный числовой идентификатор (ID). В соответствии со спецификацией VLAN можно использовать значения VLAN ID (VID) от 0 до 4094, но предопределенные идентификаторы VLAN, указанные в таблице 5, использовать не следует. VLAN ID 1 также может использоваться для атак с двойным тегированием, поэтому коммутатор должен заменять VLAN ID 1 другим значением VLAN ID.

Таблица 5 − Зарезервированные идентификаторы VLAN

Значение VID (шестнадцатеричное)	Смысловое наполнение/назначение
0	Нулевой VID указывает, что заголовок тега содержит только информацию о приоритете; в кадре VID отсутствует. Это значение VID не следует использовать в качестве идентификатора порта VLAN (PVID) или члена набора VID, а также в любой записи базы данных переадресации (FDB) или в каких-либо операциях управления
1	Значение PVID по умолчанию, используемое для классификации кадров при входе через мостовой порт. Значение PVID для порта может быть изменено администратором
FFF	Зарезервировано для использования в реализации. Это значение VID не следует использовать в качестве PVID или члена VID или передавать в заголовке тега. Это значение VID можно использовать для указания совпадения с подстановочным символом для VID в операциях управления или в записях FDB

Злоумышленник может отслеживать трафик Ethernet, получив несанкционированный доступ из другой VLAN с помощью атаки перехода в сетях VLAN (VLAN hopping). Для смягчения такой атаки производится настройка на отбрасывание кадров, не помеченных какой-либо виртуальной локальной сетью. Однако возможны следующие исключения. В целях синхронизации сообщения передаются по протоколу точного времени, который требует передачи кадров без тегов VLAN в соответствии с [b-IEEE 802.1AS].

Злоумышленник, внедрившийся в оригинальную VLAN автомобиля, может осуществить атаку с двойным тегированием, используя идентификатор по умолчанию оригинальной VLAN. Злоумышленник добавляет к кадру два тега: первый содержит идентификатор по умолчанию оригинальной VLAN, а второй – идентификатор целевой VLAN злоумышленника. Когда кадр с добавленными тегами проходит через первый коммутатор, первый тег удаляется, а кадр со вторым пересылается в следующий коммутатор. Затем этот коммутатор, используя оставшийся второй тег,

пересылает кадр в целевую VLAN. Таким образом злоумышленник может отправить сообщение в целевую VLAN. Чтобы предотвратить такую атаку, нужно изменить идентификатор по умолчанию оригинальной VLAN.

9.4 Безопасность коммутаторов Ethernet в автомобильном контексте

Мост Ethernet IEEE, широко известный как коммутатор Ethernet, первоначально использует в качестве стандартного средства для процесса пересылки и коммутации информационную базу переадресации (FIB). Такая FIB включает в себя таблицу MAC-адресов.

ПРИМЕЧАНИЕ 1. – В настоящей Рекомендации используется весьма абстрактная модель коммутатора Ethernet, основное внимание в которой уделяется только сетевым функциям, потенциально подверженным угрозам безопасности. Полный обзор всех основных функций коммутатора Ethernet содержится в [b-IEEE Std 802.1Q].

ПРИМЕЧАНИЕ 2. – Например, в [b-IEEE 802.1Q] определена модель обработки кадра MAC правила (политики) Ethernet, которая делится на правила входа, переадресации и выхода. Это представляет особый интерес, например, в контексте VLAN.

В сетях, от которых требуется гибкость, типичные коммутаторы Ethernet обеспечивают механизмы динамического обучения таблицы адресов. Когда к порту коммутатора подключается новый ЭБУ, в таблицу MAC-адресов автоматически добавляется запись с MAC-адресом конечного узла Ethernet, чтобы он мог взаимодействовать с другими ЭБУ во всем домене сети Ethernet через эту ступень коммутации.

ПРИМЕЧАНИЕ 3. – На сквозном тракте передачи данных может находиться несколько коммутаторов Ethernet.

Функция динамического обучения таблицы MAC-адресов облегчает несанкционированный доступ к сети и должна быть отключена. Эта функция может потребоваться, если для обслуживания или диагностики необходимы внешние диагностические устройства. В этом случае коммутатор должен поддерживать возможность ограничения времени действия динамически изученных MAC-адресов. Очевидно, что эти две рекомендации противоречат друг другу, но на самом деле все зависит от конкретного эксплуатационного контекста бортовой автомобильной сети Ethernet: имеется ли внешнее подключение, например, к DoIP-домену сети Ethernet или нет. Такая зависимость от эксплуатационного контекста сети может привести к условным рекомендациям по безопасности, например в данном случае применять ограниченное временно́е окно, в котором разрешено динамическое обучение таблицы адресов, и т. д.

Спуфинг MAC-адресов – это хорошо известный тип атак на компьютерные сети, которые могут быть реализованы в сценариях атак против транспортных средств. Для защиты IVN, если используется вариант с доступом извне, необходимо гарантировать аутентификацию и надежность подключенных устройств с помощью управления доступом к сети посредством портов. При таком управлении компонент аутентифицируется, прежде чем ему будет предоставлен доступ к сети. Коммутатор Ethernet устанавливает связь с сетью только в случае успешной аутентификации.

Для смягчения DoS-атак коммутатор должен предотвращать лавину широковещательных пакетов и поддерживать ограничения скорости приема пакетов через порты (об управлении параметрами трафика Ethernet см. в [b-ITU-T Y.1222]).

Для безопасности коммутатора должна быть обеспечена целостность данных управления конфигурацией коммутатора, и это должно быть возможно только посредством механизма безопасного программирования или безопасного протокола управления обновлениями при установке обновлений.

– Как правило, для эксплуатации коммутаторов Ethernet и управления ими в автомобильных приложениях со встроенным собственным процессором необходимы следующие функции безопасности – безопасное хранилище данных.

  Безопасное хранилище обеспечивает конфиденциальность и целостность хранимых данных. Такие данные, как ключи и MAC-адреса, должны быть защищены с помощью безопасного хранилища, например HSM.

– Безопасная загрузка

Безопасная загрузка предполагает проверку целостности программного обеспечения при каждом цикле загрузки. При начальной загрузке создается код аутентификации сообщения с образом программного обеспечения, который сохраняется в безопасном хранилище данных. При следующей загрузке целостность программного обеспечения будет гарантирована, если вновь сгенерированный код аутентификации сообщения совпадет с сохраненным.

– Безопасный интерфейс отладки

Безопасный интерфейс отладки предотвращает несанкционированный доступ к интерфейсу отладки. Интерфейсы отладки обычно рекомендуется удалять, чтобы невозможно было подключить никакие отладочные средства. Тем не менее, если в целях обеспечения качества изделия или его обслуживания такие интерфейсы необходимы, то доступ должен быть разрешен только авторизованным объектам.

– Безопасное обновление программного обеспечения

Безопасное обновление программного обеспечения позволяет перепрограммировать систему только в том случае, если гарантирована подлинность программного обеспечения. Поставщик программного обеспечения создает цифровую подпись, используя свой секретный ключ, и передает ее вместе с образом программного обеспечения. Подлинность программного обеспечения считается гарантированной, если получатель с помощью открытого ключа поставщика убедился, что цифровая подпись сгенерирована поставщиком.

Дополнение I

Описание некоторых протоколов бортовой автомобильной сети на базе Ethernet, конечные точки связи которой расположены в вычислительных узлах AUTOSAR или не-AUTOSAR

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Для сети на базе Ethernet существует несколько протоколов передачи данных, и во многих сценариях использования бортовой автомобильной связи на базе Ethernet применяется один из них или их комбинация. Кроме того, вычислительные узлы IVN могут работать не только с системой, соответствующей программной архитектуре на основе AUTOSAR (AUTOSAR Classic Platform, AUTOSAR Adaptive Platform и т. д.), но и использовать программную архитектуру систем передачи данных, отличную от AUTOSAR.

Поэтому в общем случае предположим, что IVN состоит из сочетания вычислительных узлов AUTOSAR и не-AUTOSAR в контексте проектирования IVN на базе Ethernet и интернета.

I.1 Обзор и сфера применения

В данном Дополнении кратко рассматриваются протоколы, предназначенные для использования в бортовой автомобильной сети передачи данных на базе Ethernet, как показано на рисунке I.1.

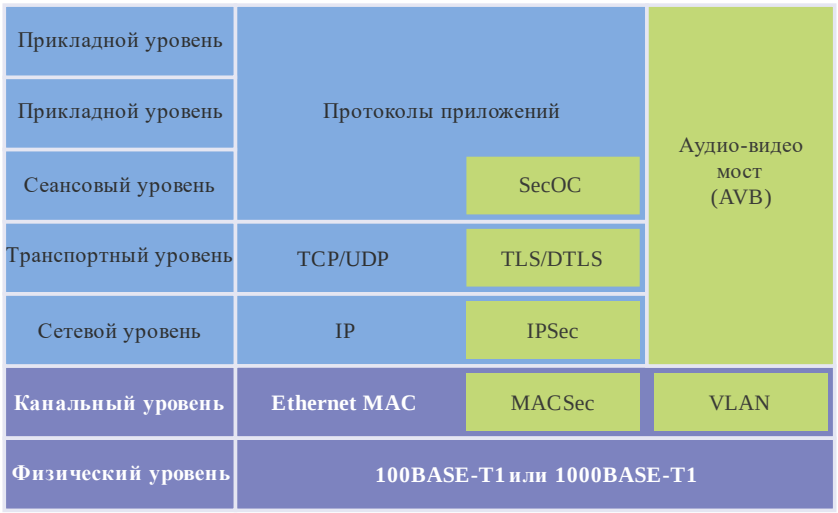

Рисунок I.1 − Предназначенные для бортовых автомобильных сетей услуги передачи данных по сети Ethernet на основе протокола Интернет и без использования протокола Интернет с соответствующими протоколами безопасности для конкретных уровней

Следует отметить, что на рисунке I.1 основное внимание уделяется транспортным услугам передачи данных, а не протоколам сеансового и прикладного уровней. Например, масштабируемое сервис-ориентированное промежуточное программное обеспечение на базе AUTOSAR поверх IP – протокол сеансового уровня и уровня представления для сервис-услуг передачи данных на основе IP – выходит за рамки настоящей Рекомендации.

I.2 Безопасная бортовая система связи AUTOSAR с протоколами безопасности нижнего протокольного уровня

Следует напомнить, что стандарт AUTOSAR определяет только архитектуру программного обеспечения, а следовательно, архитектура развертывания сетей не рассматривается. Таким образом, существует множество способов размещения описанной ниже программной системы на процессорах (с использованием многозадачности, параллелизма, замены стандартного стека протоколов передачи данных AUTOSAR готовым коммерческим стеком и т. д.).

Ethernet стал составной частью этого стандарта начиная с классической версии AUTOSAR 4.0 [b-Autosar 654]. В архитектуре AUTOSAR стек протоколов передачи данных Ethernet расположен (в программной архитектуре) параллельно с экземплярами стеков CAN, LIN и FlexRay.

Маршрутизатор PDU AUTOSAR отвечает за внутреннюю маршрутизацию PDU AUTOSAR в вычислительных узлах между приложениями AUTOSAR и сетевыми интерфейсами, связанными с конечными точками.

ПРИМЕЧАНИЕ 1. – Таким образом, функция маршрутизатора PDU AUTOSAR перекрывается с традиционными функциями маршрутизации трафика в конечных точках не-AUTOSAR, но их не следует путать.

Сообщение, генерированное приложением, передается в маршрутизатор PDU, который направляет это сообщение в соответствующий модуль интерфейса или транспортного протокола (TP). Каждый интерфейс/TP передает сообщение в сетевой интерфейс через соответствующий драйвер. В случае Ethernet маршрутизатор PDU направляет сообщение в адаптер сокета (то есть в точку доступа к услуге уровня 4 для передачи данных по протоколу TCP или UDP), и оно передается в интерфейс Ethernet через модуль TCP/IP. На рисунке I.2 показаны потоки пакетов управления и данных в расширенном стеке протоколов передачи данных AUTOSAR.

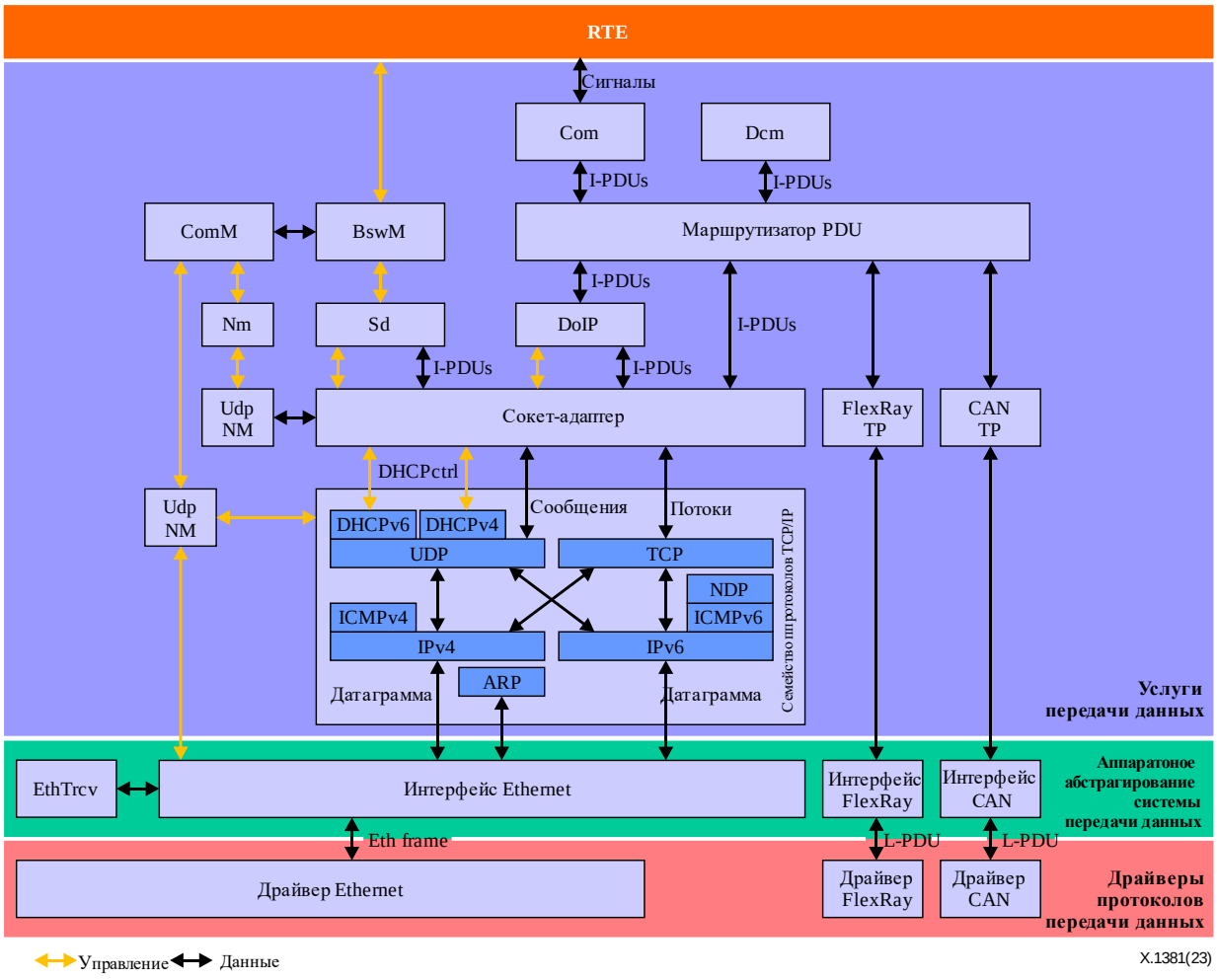

Рисунок I.2 – Расширенный стек протоколов передачи данных AUTOSAR (только программная архитектура) (Источник [b-AUTOSAR 617])

ПРИМЕЧАНИЕ 2. – В AUTOSAR введена нотация PDU, которая отличается от традиционной семантики PDU, используемой в ИКТ (как описано в [b-ITU-T X.200]). Внутренние I-PDU, N-PDU или L-PDU системы программного обеспечения AUTOSAR отображаются в используемых сетевых интерфейсах передачи данных как PDU уровня *x*, обычно (L*x*)-PDU, в зависимости от конкретного используемого стека протоколов.

I.2.1 Безопасная бортовая связь

Криптографические услуги AUTOSAR предоставляются посредством криптографической службы, аппаратного модуля безопасности и криптографического драйвера, которые в совокупности называются криптографическим стеком. Криптографический драйвер зависит от микроконтроллера и предоставляет интерфейс для доступа к оборудованию. Аппаратный модуль безопасности обеспечивает общий интерфейс, действующий как промежуточное программное обеспечение между криптографической службой и аппаратным модулем безопасности. Общий интерфейс гарантирует независимость криптографического драйвера, зависящего от аппаратного модуля безопасности, от криптографической службы как службы верхнего уровня. Единственным модулем, который должен входить в состав криптографической службы, является диспетчер криптографической службы (CSM).

Безопасная бортовая связь (SecOC) представляет собой услугу CSM и обеспечивает целостность сообщений.

Цель SecOC – предоставление практичных и экономичных механизмов аутентификации для уровня программного обеспечения (или протокольного уровня) PDU. Такого рода механизм аутентификации использует код аутентификации сообщений, основанный на симметричном криптографическом алгоритме, поскольку он должен минимизировать потребление ресурсов для работы в традиционных системах.

Для генерирования и проверки кода аутентификации сообщения SecOC использует CSM. CSM может ускорить вычисление кода аутентификации сообщения с помощью HSM.

Функциональная схема SecOC представлена на рисунке I.3.

Отправитель создает безопасный PDU, добавляя к PDU тег аутентификации, содержащий код аутентификации сообщения и признак новизны. Признаком новизны может служить значение счетчика или отметка времени.

Получатель проверяет тег аутентификации в полученном безопасном PDU, то есть генерирует код аутентификации сообщения на основе данных полученного безопасного PDU и сравнивает его с полученным кодом аутентификации сообщения.

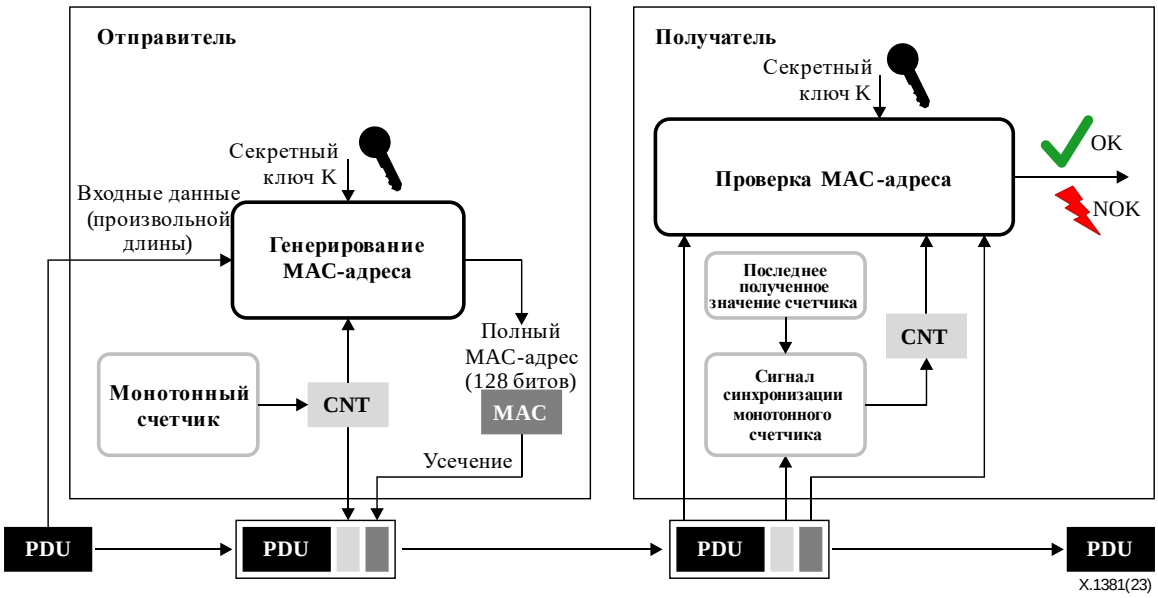

Рисунок I.3 − Аутентификация и проверка новизны сообщения [b-Autosar 654]

I.2.2 Безопасность транспортного уровня

TLS предоставляет услуги сквозной безопасной передачи данных по надежным TP, таким как TCP.

AUTOSAR не поддерживает версии TLS ниже TLS 1.2.

ПРИМЕЧАНИЕ. – См. также [b-IETF RFC 8996] об устаревании версий TLS 1.0 и TLS 1.1.

Для того чтобы использовать TLS в AUTOSAR, диспетчер криптографической службы позволяет решать задачи шифрования и производить операции с ключами, используемые подмодулем TLS и IPsec. Подробные требования и спецификации содержатся в [b-AUTOSAR 617].

I.2.3 Протокол датаграмм безопасности транспортного уровня

Данная тема подлежит дальнейшему изучению для следующего издания настоящей Рекомендации.

I.2.4 Безопасность протокола Интернет

IPsec – это в основном оригинальный протокол безопасности сетевого уровня для сетей на базе IP, поддерживающий аутентификацию и шифрование. IPsec необязателен для IPv4, но обязателен для IPv6. Внедрение IPsec в ИКТ, как правило, если и происходит, то ограничивается малыми IP-сетями, но в крупных IP-сетях он не используется из-за ограниченного, чрезвычайно чувствительного сквозного IP-соединения (которое, например, может прерываться из-за IP-шлюзов со скрытой топологией или IP-шлюзов безопасности).

Однако бортовые автомобильные IP-сети относятся скорее к категории (очень) небольших локальных сетей и подчиняются единому органу управления сетью, что не должно препятствовать использованию IPsec, ограниченному доменом (доменами) бортовой автомобильной IP-сети.

Согласно [b-AUTOSAR 617] туннельный режим IPsec в AUTOSAR в настоящее время недоступен. Можно использовать только транспортный режим. Также не поддерживаются IPv6 и многоадресная рассылка. Подробные требования и спецификации содержатся в [b-AUTOSAR 970].

ПРИМЕЧАНИЕ. – Вопросы безопасности протокола IPsec, относящиеся к конкретной версии IP, в данном издании настоящей Рекомендации не рассматриваются.

I.3 Диагностическая связь по протоколу Интернет

DoIP предназначена для диагностических целей и не содержит никаких встроенных средств безопасности.

DoIP – это TP на основе IP, как указано в [b-ISO 13400-2]. DoIP позволяет передавать сообщения между UDS автомобиля и внешним тестовым оборудованием по сети Ethernet. DoIP зависит от следующих протоколов:

– DHCP;

– ICMP;

– поиск MAC-адресов по IP-адресу (IPv4: ARP, IPv6: протокол обнаружения соседей).

В UDP каждая датаграмма содержит только одно сообщение DoIP. В случае данных на основе TCP отдельные сообщения DoIP в потоке данных разделяются заголовком.

Для DoIP-связи (диагностические запросы и ответы) между внешним диагностическим оборудованием и бортовым ЭБУ автомобиля следует использовать зарегистрированный в IANA общеизвестный TCP-порт 13400.

Протокол DoIP не содержит никаких механизмов обеспечения безопасной передачи данных. Сообщения не аутентифицируются и никак не шифруются. Поэтому при проектировании услуг DoIP разработчики архитектуры системы безопасности должны рассмотреть возможность использования протоколов безопасности различных уровней.

I.4 Безопасность управления доступом к среде передачи

MACsec – это стандартный протокол безопасности [b-IEEE 802.1AE], который обеспечивает безопасную передачу всего трафика на канальном уровне. MACsec поддерживает сквозную защиту или защиту от участка к участку на уровне Ethernet-соединения уровня 2 (то есть сквозные каналы или локальные каналы) между конечными узлами или узлами коммутаторов Ethernet. MACsec обеспечивает аутентификацию и шифрование или дешифрование, что позволяет выявлять и предотвращать большинство угроз безопасности, включая атаки типа отказ в обслуживании (DOS), вторжение, атаки через посредника, маскарадные атаки, пассивное прослушивание и атаки повторной передачи.

Дополнение II

Автомобильные шлюзы с подключением к сети Ethernet, IP-сети или интернету

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Назначение

CGW, автомобильный пограничный шлюз или VG в целом играют решающую роль в архитектуре безопасности автомобильной связи, особенно для сетевых доменов и служб передачи данных на базе Ethernet и IP. Расположение CGW в топологии сети как автомобильного пограничного шлюза подразумевает и определяет роль шлюза безопасности между внутренним и внешним доменами бортовой автомобильной сети.

Спецификация и стандартизация сетевых элементов такого типа обычно связана с явными соображениями безопасности или даже с руководящими указаниями и спецификациями по безопасности.

II.2 Цель данного Дополнения

В данном Дополнении приведен неполный список стандартов VG, относящихся к безопасности, которые в рамках сферы применения настоящей Рекомендации могут быть полезны, например, благодаря дополнительной информации о безопасности связи. В последующих изданиях настоящей Рекомендации данное Дополнение может быть пересмотрено.

II.3 Избранные Рекомендации по автомобильным шлюзам с информацией по безопасности

В данном разделе перечислены Рекомендации, относящиеся к безопасности, без какой-либо оценки их содержания:

– [b-ITU-T F.749.1] – содержит функциональные требования безопасности;

– [b-ITU-T F.749.2] – содержит отдельные пункты с требованиями безопасности связи и общими требованиями безопасности;

– [b-ITU-T H.550] – аспекты безопасности, в первую очередь связанные с управлением безопасностью VG;

– [b-ITU-T H.560] – аспекты безопасности, в первую очередь связанные с интерфейсом передачи данных VG, используемым для внешней связи.

Дополнение III

Безопасность бортовой интеллектуальной транспортной системы автомобиля

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

III.1 Базовая информация

Понятие ИТС включает в себя архитектуру автомобильной сети связи, которая охватывает внутреннюю систему передачи данных, а также соединение с внешними автомобильными системами и службами передачи данных. Наиболее важным сетевым и коммуникационным элементом в общей архитектуре является так называемая бортовая станция ИТС автомобиля, см., например, [b-ETSI EN 302 665], [b-ETSI TR 101 607].

Станция ИТС представляет собой бортовую автомобильную сеть передачи данных, которая может быть основана на Ethernet, обеспечивающую IP- и не-IP услуги передачи данных. Такое техническое решение ИТС соответствовало бы сфере применения настоящей Рекомендации.

III.2 Бортовые сети ИТС

Архитектура IVN, квалифицируемой как ИТС, состоит из тех же сетевых элементов, какие описаны в основной части настоящей Рекомендации: бортового шлюза ИТС; бортового хост-компьютера ИТС; бортового маршрутизатора ИТС; пограничного маршрутизатора или шлюза ИТС и т. д. Следовательно, руководящие указания по обеспечению безопасности ИТС также в значительной степени применимы к настоящей Рекомендации, особенно в тех случаях, когда технологии связи (то есть протоколы и стеки протоколов) и архитектура связи одинаковы.

III.3 Безопасность ИТС

Оценка безопасности, относящаяся к ИТС, не является целью настоящей Рекомендации. Однако анализ угроз, уязвимостей и рисков, проводимый для ИТС, руководящие указания по обеспечению безопасности, службам безопасности или архитектуре безопасности ИТС будут полезны в качестве дополнительного материала, особенно если они относятся к безопасности системы передачи данных. Дополнительную информацию и дополнительные справочные документы по безопасности см. в [b-ETSI TS 102 731].

Библиография

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

[b-ITU-T F.749.2] Recommendation ITU-T F.749.2 (2017), *Service requirements for vehicle gateway platforms.*

[b-ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2020), *Common equipment management function requirements.*

[b-ITU-T G.8013] Рекомендация МСЭ-Т G.8013/Y.1731 (2015 год), *Функции и механизмы эксплуатации, управления и технического обслуживания (OAM) для сетей на базе Ethernet.*

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

[b-ITU-T H.560] Recommendation ITU-T H.560 (2017), *Communications interface between external applications and a vehicle gateway platform.*

[b-ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network.*

[b-ITU-T M.3702] Recommendation ITU-T M.3702 (2010), *Common management services – Notification management – Protocol neutral requirement and analysis.*

[b-ITU-T M.3703] Recommendation ITU-T M.3703 (2010), *Common management services – Alarm management – Protocol neutral requirement and analysis.*

[b-ITU-T M.3705] Recommendation ITU-T M.3705 (2013), *Common management services – Log management – Protocol neutral requirements and analysis.*

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open systems interconnection – Basic reference model: The basic model.*

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

[b-ITU-T X.703] Recommendation ITU-T X.703 (1997), *Information technology – Open distributed management architecture.*

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

[b-ITU-T X.1039] Recommendation ITU-T X.1039 (2016), *Technical security measures for implementation of ITU-T X.805 security dimensions.*

[b-ITU-T Y.1222] Recommendation ITU-T Y.1222 (2007), *Traffic control and congestion control in Ethernet-based networks.*

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

[b-ITU-T Y.1730] Recommendation ITU-T Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services.*

[b-ITU-T Y.2770] Рекомендация МСЭ-Т Y.2770 (2012 год), *Требования к углубленной проверке пакетов в сетях последующих поколений.*

[b-ITU-T Y.2771] Рекомендация МСЭ-Т Y.2771 (2014 год), *Структура углубленной проверки пакетов.*

[b-Autosar 617] AUTOSAR 617 (2021), *Specification of TCP/IP stack*, AUTOSAR CP R21-11.

[b-Autosar 654] AUTOSAR 654 (2017), *Specification of secure onboard communication*, AUTOSAR CP Release 4.3.1.

[b-Autosar 970] AUTOSAR 970 (2019), *Requirements on IPsec Protocol*, AUTOSAR FO R19-11.

[b-ETSI EN 302 665] European Standard ETSI EN 302 665 V1.1.1 (2010), *Intelligent transport systems (ITS); Communications architecture.*

[b-ETSI TR 101 607] Technical Report ETSI TR 101 607 V1.2.1 (2020), *Intelligent transport systems (ITS); Cooperative ITS (C-ITS); Release 1.*

[b-ETSI TS 102 731] Technical Specification ETSI TS 102 731 V1.1.1 (2010), *Intelligent transport systems (ITS); Security; Security services and architecture.*

[b-IEEE 802.1] IEEE 802.1 (Internet). *Welcome to the IEEE 802.1 Working Group*. Available [viewed 2022-06-30]. https://1.ieee802.org/

[b-IEEE 802.1AE] IEEE 802.1AE-2018, *IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) security.*

[b-IEEE 802.1AS] IEEE 802.1AS (Internet), *Standard for Local and metropolitan area networks – Timing and synchronization for time-sensitive applications in bridged local area networks.* Available [viewed 2022-06-30]. https://www.ieee802.org/1/pages/802.1as.html

[b-IEEE 802.1CB] IEEE 802.1CB-2017, *IEEE Standard for local and metropolitan area networks – Frame replication and elimination for reliability.*

[b-IEEE 802.1Q] IEEE 802.1Q-2018, *IEEE Standard for local and metropolitan area network – Bridges and bridged networks.*

[b-IEEE 802.1Qat] IEEE 802.1Qat (Internet), *Standard for Local and metropolitan area networks – Virtual bridged local area networks – Amendment 9: Stream reservation protocol (SRP).* Available [viewed 2022-06-30]. https://www.ieee802.org/1/pages/802.1at.html

[b-IEEE 802.1Qav] IEEE 802.1Qav-2009, *IEEE Standard for Local and metropolitan area networks – Virtual bridged local area networks amendment 12: Forwarding and queuing enhancements for time-sensitive streams.*

[b-IEEE 1722-2016] IEEE 1722-2016, *Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks.*

[b-IETF RFC 2827] IETF RFC 2827 (1997), *Network ingress filtering: Defeating IP source address spoofing denial of service attacks.*

[b-IETF RFC 4953] IETF RFC 4953 (2007), *Defending TCP against spoofing attacks.*

[b-IETF RFC 6020] IETF RFC 6020 (2010), *YANG – A data modeling language for the network configuration protocol (NETCONF).*

[b-IETF RFC 6575] IETF RFC 6575 (2012), *Address resolution protocol (ARP) mediation for IP interworking of layer 2 VPNs.*

[b-IETF RFC 6959] IETF RFC 6959 (2013), *Source address validation improvement (SAVI) threat scope.*

[b-IETF RFC 8996] IETF RFC 8996 (2021), *Deprecating TLS 1.0 and TLS 1.1.*

[b-ISO 13400-2] International Standard ISO 13400-2:2019, *Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 2: Transport protocol and network layer services.*

[b-ISO 14229-5] International Standard ISO 14229-5:2022, *Road vehicles – Unified diagnostic services (UDS) – Part 5: Unified diagnostic services on Internet Protocol implementation (UDSonIP).*

[b-ISO/SAE 21434] International Standard ISO/SAE 21434:2021, *Road vehicles – Cybersecurity engineering.*

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, 2013 г.