Международный союз электросвязи

МСЭ-Т X.1812

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(05/2022)

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

Безопасность сетей IMT-2020

Структура безопасности на основе доверительных отношений для экосистемы IMT-2020

Рекомендация МСЭ-Т X.1812

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределения 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	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
Киберзащита	X.1590–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	**X.1800–X.1819**

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

Рекомендация МСЭ-Т X.1812

Структура безопасности на основе доверительных отношений для экосистемы IMT-2020

Резюме

В Рекомендации МСЭ-Т X.1812 определены заинтересованные стороны в экосистеме Международной подвижной электросвязи 2020 (IMT-2020, или сетей пятого поколения), проведен анализ доверительных отношений между ними, выявлены угрозы и разъяснены обязанности по обеспечению безопасности каждой из заинтересованных сторон, а также определены границы безопасности между заинтересованными сторонами и описана структура безопасности на основе этих доверительных отношений.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1812	20.05.2022 г.	17-я	11.1002/1000/14808

Ключевые слова

Экосистема, структура, IMT-2020, доверие.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами/авторскими правами на программное обеспечение, которые могут потребоваться для выполнения 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 соответствующим базам данных МСЭ-Т, доступным на веб-сайте МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

В системе Международной подвижной электросвязи 2020 (IMT-2020, или сетей пятого поколения (5G)) группа заинтересованных сторон шире и разнообразнее, чем в предыдущих системах связи. В системах второго, третьего и четвертого поколений (2G, 3G и 4G) основные заинтересованные стороны можно кратко охарактеризовать как поставщиков услуг, операторов сетей, поставщиков/продавцов оборудования и абонентов. В экосистеме IMT-2020 задействованы еще и участники вертикальных отраслей, такие как промышленные и коммерческие предприятия. Кроме того, поставщиков услуг можно подразделить на операторов облачных платформ, компании по анализу данных, поставщиков приложений и т. д. Более того, на стороне терминалов абоненты – это не только конечные пользователи, как раньше. К абонентам могут относиться заинтересованные стороны разного типа, особенно в отношении коммерческих терминалов, например в случае совместно используемого оборудования связи автомобиля. Эти изменения приводят к сложным отношениям между заинтересованными сторонами разного типа и поднимают ряд новых проблем безопасности в экосистемах IMT-2020.

В сети IMT-2020 также вводятся новые функции. Например, появление в IMT-2020 виртуализации сети разрывает фиксированные соединения между объектами сети и позволяет создавать сети с программируемыми параметрами. Еще одним примером может служить архитектура на основе услуг. Благодаря такой архитектуре в сеть IMT-2020 можно встроить больше облачных функций. Кроме того, нарезка сети может способствовать более эффективному взаимодействию между сетью IMT-2020 и услугами.

Со временем к системам IMT-2020 будет применяться все больше методов информационных технологий (ИТ), причем не только к услугам, но и к сети. Сеть IMT-2020 целиком основана на протоколе Интернет. Спецификация ее архитектуры базируется на услугах, а не на эталонных точках, как в архитектуре предшествующих сетей. Сигналы все чаще поступают не из выделенных сетей, а из интернета. Менее популярный транспортный протокол Diameter [b-IETF RFC 6733] в сетях IMT-2020 заменен протоколом передачи гипертекста, который широко используется во всем мире. Все эти изменения благоприятно скажутся на развертывании и эксплуатации сетей и услуг IMT-2020.

Однако использование популярных протоколов и открытой среды соединений также может сыграть на руку злоумышленникам. Им не придется тратить много времени на изучение сложных протоколов электросвязи и в принципе будет проще найти точку вторжения в сеть. Поэтому неразумно предполагать, что внутренняя связь в сетях IMT-2020 все еще является надежной и заслуживает доверия. Таким образом, переход с систем 4G на системы IMT-2020 нарушает доверительные отношения между операторами сетей.

Кроме того, сеть IMT-2020 призвана быть более гибкой, чтобы удовлетворять различные требования, предъявляемые к услугам. В частности, в сети IMT-2020 введена нарезка. Сети IMT-2020 также могут предоставлять некоторые возможности службам. Такое предоставление возможностей позволит службе IMT-2020 управлять некоторыми сетевыми функциями. Эти новые функции сделают границу безопасности между сетью IMT-2020 и услугами более размытой.

В настоящей Рекомендации определены заинтересованные стороны в экосистеме IMT-2020, проведен анализ доверительных отношений между ними, выявлены угрозы и разъяснены обязанности по обеспечению безопасности каждой из заинтересованных сторон, а также указаны границы безопасности между заинтересованными сторонами и описана структура безопасности на основе этих доверительных отношений.

Рекомендация МСЭ-Т X.1812

Структура безопасности на основе доверительных отношений для экосистемы IMT-2020

1 Сфера применения

В настоящей Рекомендации определена структура безопасности на основе доверительных отношений для экосистемы Международной подвижной электросвязи 2020 (IMT-2020). В данной Рекомендации описан общий подход:

– к определению сценариев предоставления услуг IMT-2020;

– выявлению заинтересованных сторон в экосистеме IMT-2020;

– анализу доверительных отношений между заинтересованными сторонами;

– выявлению угроз для каждой заинтересованной стороны;

– разъяснению обязанностей по обеспечению безопасности каждой из заинтересованных сторон;

– описанию границ безопасности между заинтересованными сторонами;

– описанию требований безопасности на основе модели доверия; и

– созданию структуры безопасности, основанной на доверительных отношениях между заинтересованными сторонами.

2 Справочные документы

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

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 бизнес-единица (business unit) [b-ISO/TS 21089]: Отдельная и поддающаяся учету функция или подфункция в организации.

ПРИМЕЧАНИЕ. – Бизнес-единицей может быть отдел, служба или специальность в организации, предоставляющей медицинские услуги.

3.1.2 развертывание (deployment) [b-ISO/IEC/IEEE 24765]: Этап проекта, на котором система вводится в эксплуатацию и решаются проблемы перехода.

3.1.3 разработчик (developer) [b-NIST SP 800-53]: Организация, которая включает: i) разработчиков или производителей информационных систем, компонентов систем или услуг информационных систем; ii) системных интеграторов; iii) поставщиков/продавцов; и iv) торговых посредников.

3.1.4 домен (domain) [b-ISO/IEC 14888-1]: Группа предприятий, действующих в рамках единой политики безопасности.

ПРИМЕР. – Сертификаты открытых ключей, созданные одним или рядом органов, придерживающихся одной и той же политики безопасности.

3.1.5 информационная система (information system) [b-ISO/IEC 27000]: Набор приложений, услуг, информационно-технологических ресурсов или других средств обработки информации.

3.1.6 жизненный цикл (lifecycle) [b-ISO/IEC/IEEE 15288]: Развитие системы, продукта, услуги, проекта или другого рукотворного объекта, начиная от замысла и заканчивая выводом из эксплуатации.

3.1.7 сетевая функция (network function) [b-ITU-T Y.3100]: В контексте IMT-2020 – функция обработки в сети.

ПРИМЕЧАНИЕ 1. – К сетевым функциям, в частности, относятся функциональные возможности узла сети, такие как управление сеансом, управление мобильностью и функции транспортировки, с определенными интерфейсами и функциональным поведением.

ПРИМЕЧАНИЕ 2. – Сетевые функции могут быть реализованы на специализированном оборудовании или в виде виртуализированных программных функций.

ПРИМЕЧАНИЕ 3. – Сетевые функции не считаются ресурсами; скорее любые сетевые функции могут быть созданы с использованием ресурсов.

3.1.8 заинтересованная сторона (stakeholder) [b-ISO/PAS 19450]: Отдельное лицо, организация или группа лиц, которые заинтересованы в планируемой, разрабатываемой или развертываемой системе или могут быть затронуты такой системой.

3.1.9 поставщик (supplier) [b-ISO 10393]: Организация или лицо, которые поставляют продукты или услуги.

3.1.10 разработка систем (system development) [b-ISO/IEC 2382]: Процесс, который обычно включает в себя анализ требований, проектирование системы, внедрение, оформление документации и обеспечение качества.

3.1.11 доверие (trust) [b-ISO/IEC 25010]: Степень уверенности пользователя или другой заинтересованной стороны в том, что продукт или система будут выполнять свои функции, как это предполагалось.

3.1.12 уровень доверия (trust level) [b-ISO 28598-1]: Оценка потребителем весомости предварительных, дополнительных и косвенных свидетельств способности поставщика выполнить установленные требования к качеству.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 внешний поставщик услуг (external service provider): Группа объектов, в которую входят: a) объекты внутри организации, но за пределами границ авторизации безопасности, установленных для информационных систем организации; b) объекты вне организации, относящиеся либо к государственному сектору (например, федеральные агентства), либо к частному сектору (например, поставщики коммерческих услуг); или c) некоторая комбинация вариантов государственного и частного секторов.

ПРИМЕЧАНИЕ. – Основано на [b-NIST SP 800-53].

3.2.2 цепочка поставок (supply chain): Сеть организаций, которые через восходящие и нисходящие связи участвуют в процессах и деятельности, приводящих к созданию стоимости в виде продуктов и услуг в руках конечного потребителя.

3.2.3 жизненный цикл разработки системы (system development lifecycle): Структурированный подход к планированию, созданию, тестированию, развертыванию и обслуживанию информационной системы.

3.2.4 модель доверия (trust model): Модель, состоящая из компонентов, которые описывают доверительные отношения и цепочки между заинтересованными сторонами.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

2G	Second Generation		Второе поколение
3G	Third Generation		Третье поколение
4G	Fourth Generation		Четвертое поколение
5G	Fifth Generation		Пятое поколение
5GC	Fifth Generation Core		Базовая сеть пятого поколения
BS	Base Station	БС	Базовая станция
CAB	Conformity Assessment Body		Орган по оценке соответствия
E2E	End to End		Сквозной
HO	Home Operator		Оператор домашней сети
ICP	Internet Content Provider		Поставщик интернет-контента
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
IMT-2020	International Mobile Telecommunications-2020		Международная подвижная электросвязь 2020
IoT	Internet of Things		Интернет вещей
IoV	Internet of Vehicles		Интернет транспортных средств
IPX	Internetwork Packet Exchange		Межсетевой обмен пакетами
ISP	Internet Service Provider		Поставщик интернет-услуг
IT	Information Technology	ИТ	Информационные технологии
NE	Network Element		Сетевой элемент
NESAS	Network Equipment Security Assurance Scheme		Схема обеспечения безопасности сетевого оборудования
NF	Network Function		Сетевая функция
NFV	Network Functions Virtualization		Виртуализация сетевых функций
NPN	Non-Public Network		Закрытая сеть
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PLMN	Public Land Mobile Network		Сеть сухопутной подвижной связи общего пользования
SCAS	Security Assurance Specification		Спецификация обеспечения безопасности
SDL	Security Development Lifecycle		Жизненный цикл разработки системы безопасности
UICC	Universal Integrated Circuit Card		Универсальная карта с интегральной схемой
VNF	Virtualized Network Function		Виртуализированная сетевая функция
VO	Visited Operator		Оператор гостевой сети

5 Соглашения

В настоящей Рекомендации:

выражение "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом, для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

выражение "**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 настоящей Рекомендации.

6 Обзор

До эпохи 5G системы электросвязи использовались главным образом для предоставления услуг телефонной связи, доступа в интернет и соответствующих услуг. Из-за ограниченных возможностей и скорости этих систем сценарии их использования в целом были простыми. В частности, в системе связи было задействовано лишь небольшое количество ролей. Так, в услугах вызова участвуют только вызывающий абонент, вызываемый абонент и подвижная сеть. В услугах передачи данных задействованы терминал, подвижная сеть и поставщики услуг или приложений. Кроме того, в процессе создания сетей и прикладных систем участвуют поставщики/продавцы. На уровне терминалов задействованы производители терминалов и поставщики универсальных карт с интегральной схемой (UICC). Это основные роли, задействованные в системах электросвязи 2G, 3G и 4G.

Однако в экосистеме IMT-2020 все обстоит иначе. В эту экосистему входят не только все заинтересованные стороны, имеющие отношение к системе электросвязи, терминалам, сети и услугам, но и другие заинтересованные стороны. На стороне оконечных устройств абоненты – это не только конечные пользователи, как было раньше, поскольку мобильное устройство может быть не только телефоном, но и одним из многих разных типов оборудования, которое может совместно использоваться несколькими сторонами. В сети IMT-2020 вводится ряд новых функций. Например, виртуализация сети в IMT-2020 разрывает фиксированное соединение между сетевыми объектами и позволяет создавать сети с программируемыми параметрами, нарушая границы безопасности развернутой сети. В сетях IMT-2020 применяется все больше и больше информационных технологий (ИТ), которые могут использоваться и злоумышленниками. Служба представления возможностей сети открывает перед злоумышленником интерфейсы не в плоскости пользователя, а в плоскости управления. В предоставлении услуг задействованы участники вертикальных отраслей (вертикальные участники), такие как промышленные и коммерческие предприятия. Это ведет к делению поставщиков услуг на операторов облачных платформ, компании по анализу данных, поставщиков приложений и т. д., как показано на рисунке 1.

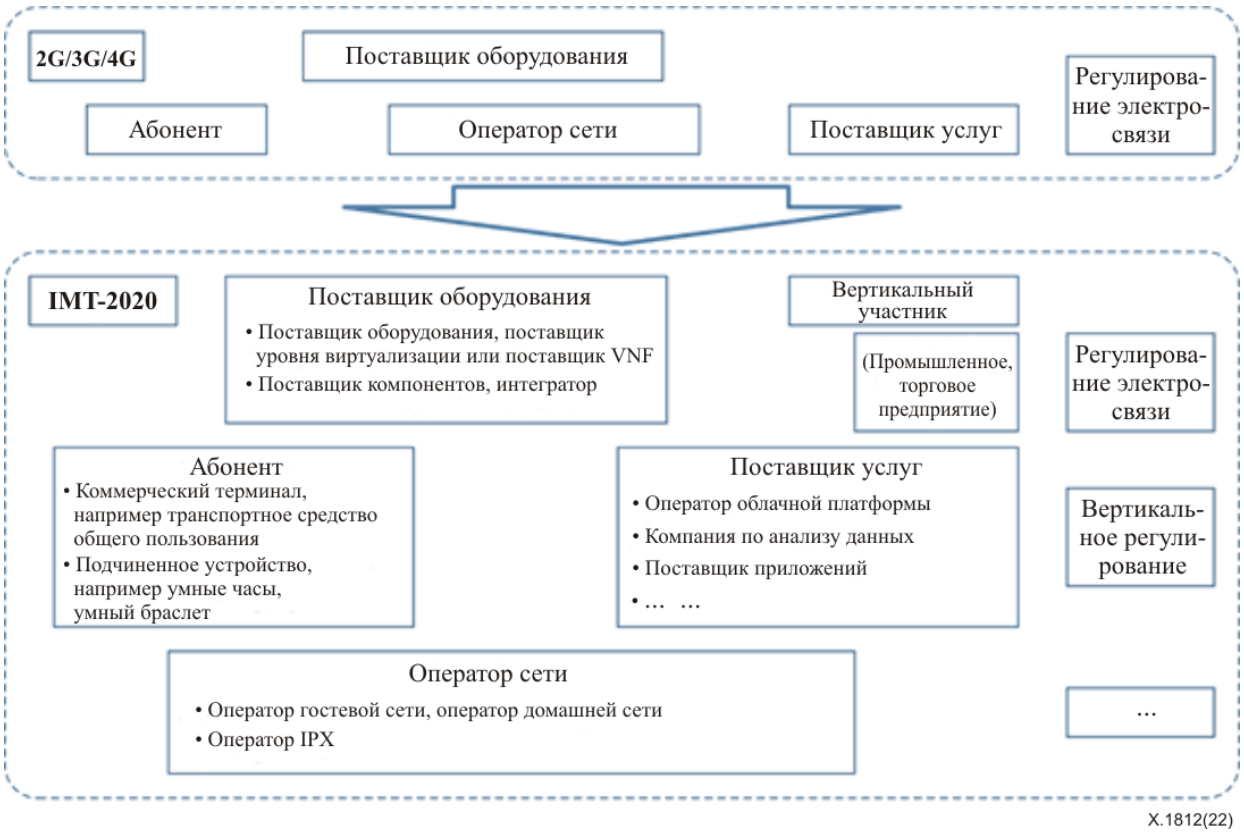


Рисунок 1 – Развитие экосистемы от 2G, 3G и 4G до IMT-2020

В данном случае доверительные отношения системы IMT-2020 имеют другой характер. Пользователи или абоненты и сети или системы обслуживания стали гораздо ближе, чем раньше. Сложная и длинная цепочка поставок заставляет операторов уделять больше внимания оценке поставщиков. Тесная связь между услугами и сетью заставляет вертикальные отрасли в значительной мере полагаться на сеть и требует более полного доверия и безопасности. Необходимо рассмотреть вопрос о создании новой модели доверия для экосистемы IMT-2020 с определением четких требований безопасности и установлением границ безопасности между заинтересованными сторонами. Таким образом может быть обеспечено максимальное повышение эффективности связи и гарантирована безопасность данных.

Надежность системы IMT-2020 зависит от пяти характеристик, а именно устойчивости, безопасности связи, управления определением идентичности, защиты информации, позволяющей установить личность (PII), и гарантии безопасности.

- Устойчивость. Устойчивость – это способность организации противостоять влиянию различных сбоев. Множество дополнительных и частично перекрывающихся функций в IMT-2020 может способствовать достижению устойчивости системы IMT-2020 к кибератакам и непредвиденным инцидентам.
- Безопасность связи. Безопасность связи в IMT-2020 относится к передаче данных. В системе IMT-2020 безопасная связь с устройствами и собственной инфраструктурой имеет исключительно важное значение.
- Управление определением идентичности. Система управления определением идентичности состоит из процессов и правил, участвующих в управлении жизненным циклом, ценностью, типом и дополнительными метаданными атрибутов, составляющих идентичность объектов в системе IMT-2020. Рекомендуется обеспечить безопасное управление определением идентичности для идентификации и аутентификации абонентов как находящихся, так и не находящихся в роуминге, а также для гарантии того, что только подлинные абоненты могут получить доступ к услугам сети. Такие системы строятся на сильных криптографических примитивах и характеристиках безопасности.

- Защита PII. Конфиденциальность данных определяется в [b-ISO/TS 21719-2] как права и обязанности физических лиц и организаций в отношении сбора, использования, хранения, раскрытия и удаления персональной информации. Защита PII включает в себя процедуры защиты информации PII, которая может использоваться неавторизованными сторонами для установления личности абонентов.
- Гарантия безопасности. Гарантия безопасности дает основания для обоснованной уверенности в том, что заявление о достижении целей в области безопасности было или будет выполнено. Гарантия безопасности – это средство обеспечения соответствия сетевого оборудования требованиям безопасности, которое достигается за счет внедрения безопасных процессов разработки и управления жизненным циклом продуктов.

7 Структура безопасности, поддерживаемая моделью доверия

В настоящей Рекомендации анализируются и определяются роли заинтересованных сторон в экосистеме IMT-2020, а также доверительные отношения между ролями посредством анализа нескольких типичных сценариев. Затем предпринимается попытка определить уровень доверия с учетом ключевых факторов. На этой основе даются рекомендации по определению требований безопасности в зависимости от уровня доверия и формированию структуры безопасности на основе доверительных отношениях, как показано на рисунке 2.

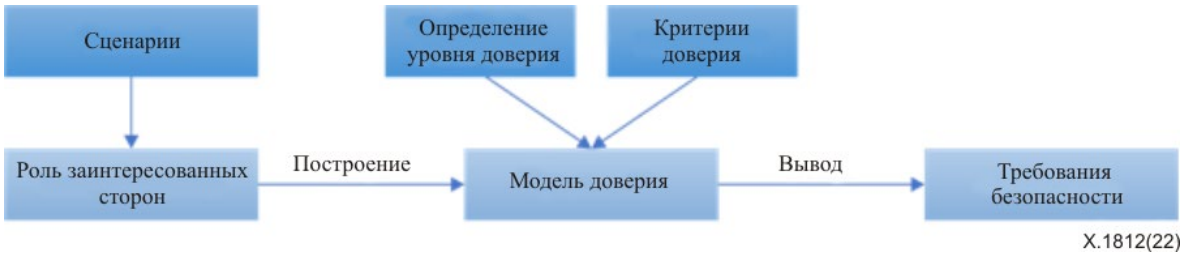
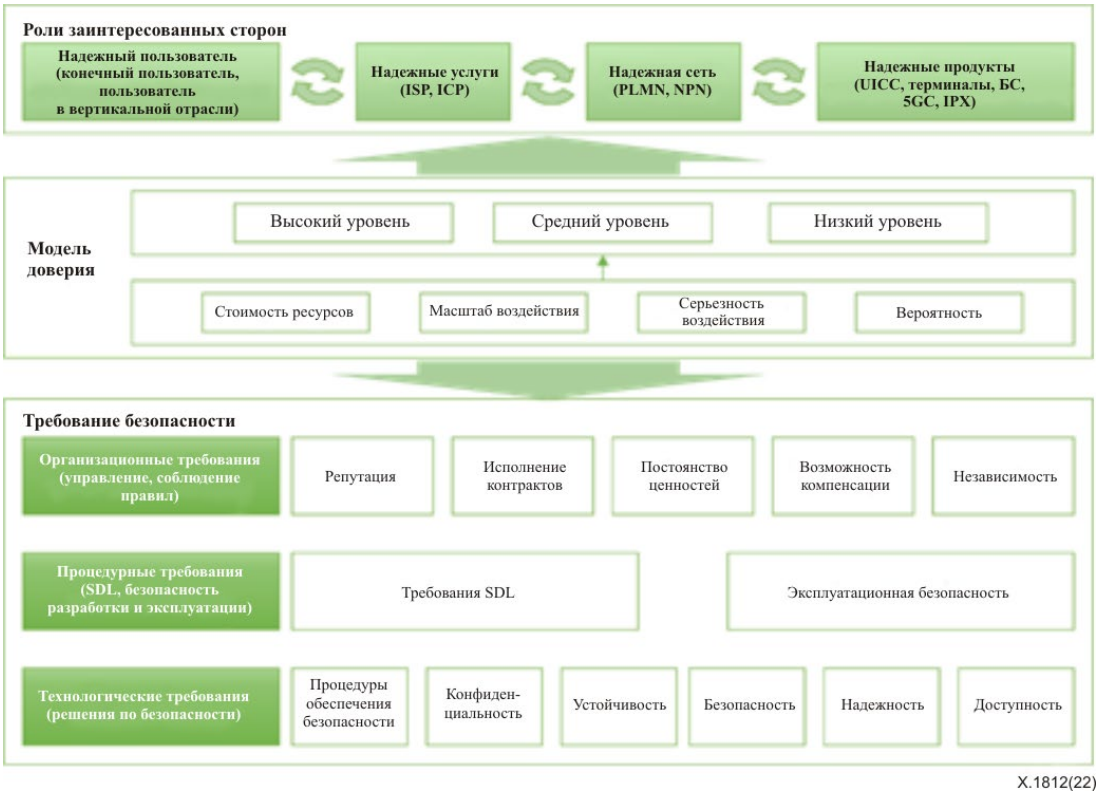


Рисунок 2 – Направление движения к построению структуры безопасности на основе доверительных отношений для экосистемы IMT-2020

На рисунке 3 показана структура безопасности, основанная на роли и отношениях, модели доверия и требованиях безопасности всех заинтересованных сторон и поддерживаемая моделью доверия, представленной в настоящей Рекомендации. Все компоненты структуры, а именно роли заинтересованных сторон, модель доверия и требования безопасности, описаны соответственно в пунктах 8, 9 и 10.



5GC – базовая сеть пятого поколения; БС – базовая станция; ICP – поставщик интернет-контента; ISP – поставщик интернет-услуг; NPN – закрытая сеть; SDL – жизненный цикл разработки системы безопасности

Рисунок 3 – Структура безопасности, поддерживаемая моделью доверия, основанной на доверительных отношениях между заинтересованными сторонами

8 Роль заинтересованных сторон в сценариях для экосистемы IMT-2020

8.1 Общие положения

Существующая система электросвязи подразделяется на три подсистемы – терминалы, сети и услуги. Необходимо учитывать возможные отношения как между этими подсистемами, так и внутри них. Поскольку отношения терминал – сеть уже изучены другими организациями по стандартизации, такими как Проект партнерства третьего поколения (3GPP), они в данном разделе не рассматриваются.

Набор из пяти сценариев, рассматриваемых в данном разделе, в совокупности охватывает все возможные межсистемные отношения, за исключением отношения терминал – сеть.

8.2 Сценарий 1. Развертывание сети виртуализации в домене оператора сети

8.2.1 Общие положения

В данном сценарии основное внимание уделяется отношениям внутри сети.

В современных сетях электросвязи сетевые элементы (NE), развернутые в сети, обычно реализуются как выделенные физические устройства. Каждый NE реализован как один или несколько физических серверов в зависимости от их возможностей. Для подключения таких сетевых устройств через физические интерфейсы используются кабель, оптическое волокно, коммутаторы и маршрутизаторы. В данном сценарии основными заинтересованными сторонами являются пользователи или абоненты, производители мобильных терминалов, поставщики UICC, поставщики/продавцы сетевых устройств и операторы. Это показано на рисунке 4.

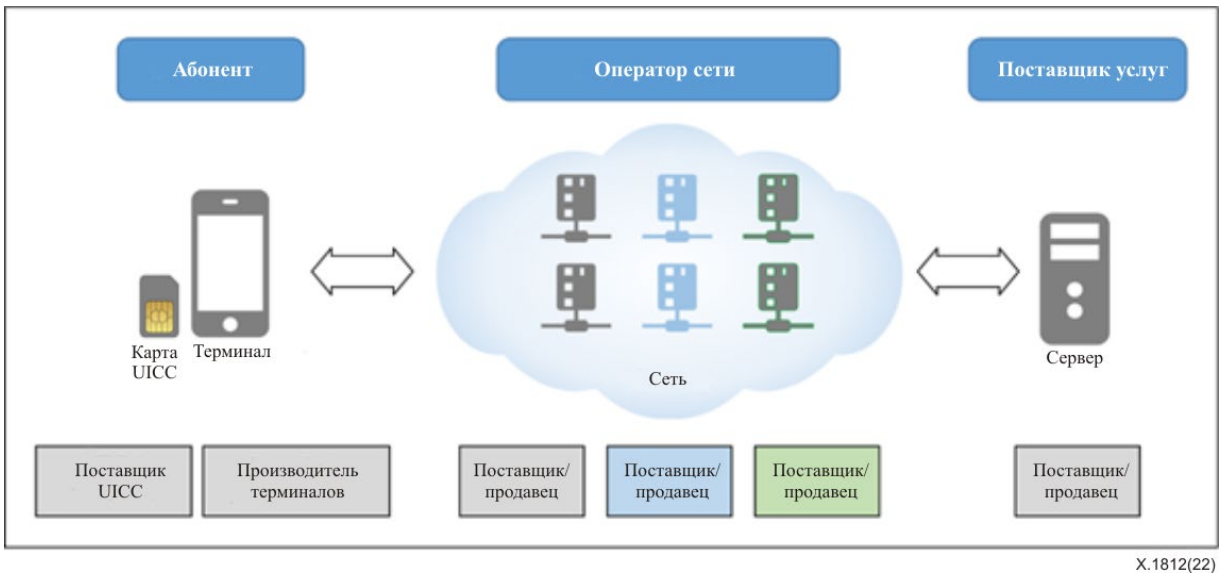


Рисунок 4 – Основные заинтересованные стороны в домене оператора сети

В IMT-2020 значительное развитие получила технология сетей с программируемыми параметрами/виртуализации сетевых функций, которая постепенно начала внедряться в сети. С расширением использования ИТ развиваются и сети электросвязи. При разработке сетевой архитектуры IMT-2020 была предложена новая архитектура на основе услуг, чтобы лучше использовать ИТ для целей развертывания и сопровождения. NE заменен более гибкой в эксплуатации и обслуживании сетевой функцией (NF). NF может быть реализована как виртуализированная сетевая функция (VNF) и даже в виде программных приложений, работающих на виртуальной машине. Это говорит о том, что при развертывании сетей IMT-2020 будет широко использоваться виртуализация сети. Таким образом, вместо программно-аппаратных интегрированных устройств теперь реализуется трехуровневая комбинация оборудования уровня виртуализации и VNF. В результате основными заинтересованными сторонами, участвующими в этом сценарии, становятся пользователи или абоненты, производители мобильных терминалов, поставщики UICC, поставщики/продавцы NE (поставщики оборудования, средств виртуализации, VNF) и операторы сети. Это показано на рисунке 5.

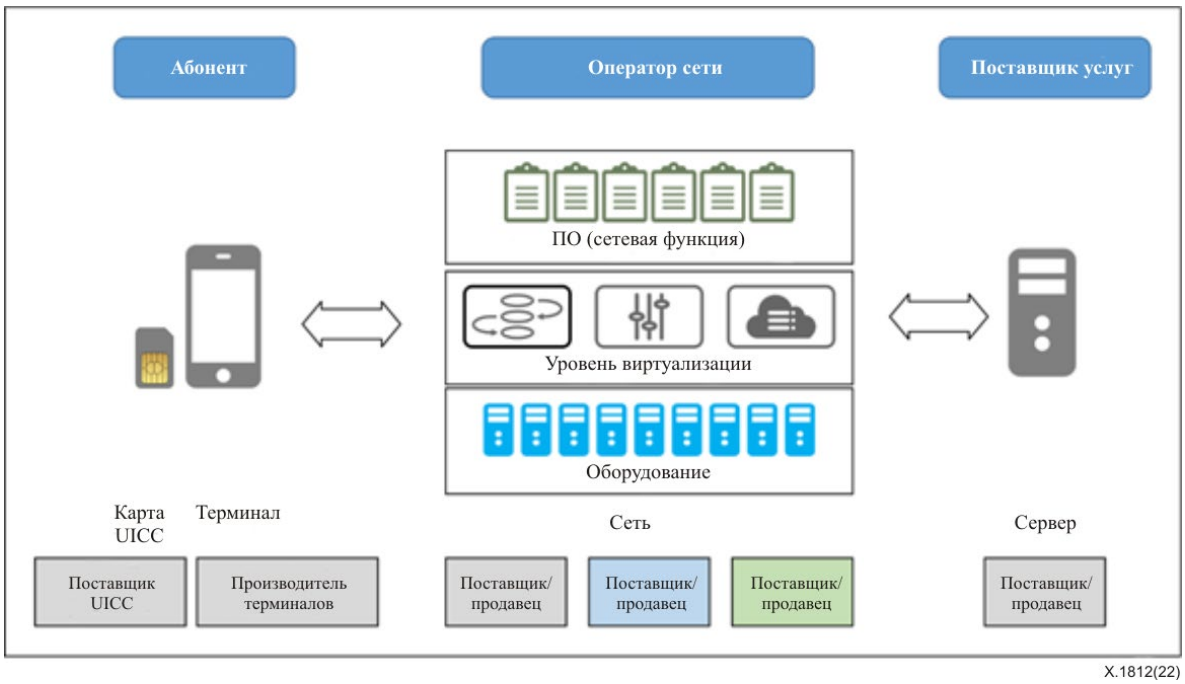


Рисунок 5 – Основные заинтересованные стороны при развертывании сети виртуализации в домене оператора сети

8.2.2 Роли заинтересованных сторон в данном сценарии

В данном сценарии заинтересованные стороны играют следующие роли.

- Пользователи или абоненты. Это конечные пользователи, то есть потребители услуг электросвязи. Абонентское оборудование состоит из мобильного терминала, предоставляемого производителем, и UICC, предоставляемой поставщиком/продавцом карт.
- Производитель мобильных терминалов. Это предприятие предоставляет терминалы, которые могут использоваться пользователями или абонентами, обменивающимися данными с сетью.
- Поставщик UICC. Это предприятие предоставляет карты UICC, которые могут использоваться для идентификации абонентов.
- Поставщик/продавец NE. Это предприятие предлагает устройства или компоненты устройств, из которых можно построить систему электросвязи или платформу/систему услуг.

  ПРИМЕЧАНИЕ. – Если поставщик/продавец предоставляет компоненты, его можно дополнительно классифицировать как поставщика оборудования, поставщика уровня виртуализации или поставщика VNF.
- Оператор сети. Эта организация владеет всеми элементами, необходимыми для продажи и предоставления услуг электросвязи абонентам и поставщикам услуг, или контролирует эти элементы.

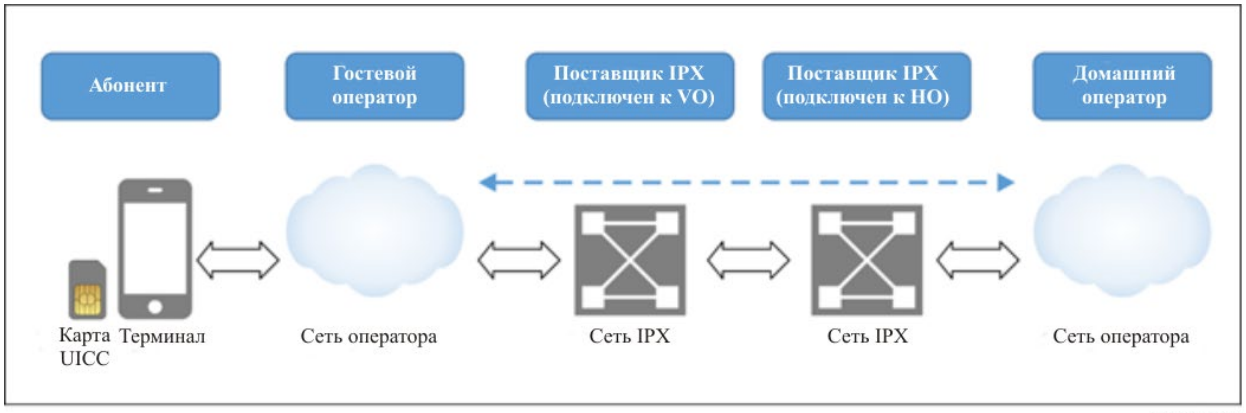
8.3 Сценарий 2. Межсетевое взаимодействие и роуминг

8.3.1 Общие положения

В данном сценарии основное внимание уделяется отношениям внутри сети.

Сеть подвижной связи может предоставлять услуги пользователям во всем мире на основе межсетевого взаимодействия и координации между глобальными операторами. Такое межсетевое взаимодействие и координация между операторами предполагают координацию и сотрудничество на уровне услуг и на транспортном уровне.

До сих пор принцип межсетевого взаимодействия между операторами сетей сухопутной подвижной связи общего пользования (PLMN) предполагал, что операторы (на уровне услуг) могут полностью доверять друг другу и что можно быть уверенным в надежности передачи сигналов и пользовательских данных. Чтобы обеспечить надлежащую пересылку сообщений сигнализации определенному оператору, был добавлен поставщик услуг межсетевого обмена пакетами (IPX). Однако с развитием сети и использованием интернета IPX-соединения становятся все более сложными, и также могут подвергаться атакам через интернет. В результате операторы могут гарантировать безопасность лишь IPX-соединений, подключенных к ним напрямую, но не линий между операторами и всех других линий операторов. Это показано на рисунке 6.



HO – оператор домашней сети; VO – оператор гостевой сети

Рисунок 6 – Основные заинтересованные стороны в сценарии межсетевого взаимодействия и роуминга

Кроме того, у операторов обнаружились и используются многочисленные уязвимости, позволяющие злоумышленникам организовывать атаки на других операторов, используя взломанные устройства в качестве трамплина. В результате операторы больше не доверяют сообщениям на уровне услуг [b-3GPP TS 33.501].

В таком сценарии основными участниками являются пользователи или абоненты, операторы гостевой сети (гостевые операторы), операторы домашней сети (домашние операторы) и операторы IPX (в том числе IPX, подсоединяющих операторов гостевой сети, и IPX, подсоединяющих операторов домашней сети).

8.3.2 Роли заинтересованных сторон в данном сценарии

В этом сценарии заинтересованные стороны играют следующие роли.

- Пользователь или абонент. Это конечный пользователь, то есть потребитель услуг электросвязи.
- Операторы гостевой сети. Такие операторы предоставляют абонентам услуги доступа, когда абонент находится за пределами зоны охвата оператора своей домашней сети.
- Оператор домашней сети. Это оператор, с которым абоненты заключили контракт и который предоставляет им услуги связи.
- Оператор IPX (IPX, подсоединяющих операторов гостевой сети, или IPX, подсоединяющих оператора домашней сети). Это предприятие предоставляет услуги межсетевого обмена пакетами между операторами.

8.4 Сценарий 3. Аренда автомобиля с дистанционным управлением

8.4.1 Общие положения

В данном сценарии основное внимание уделяется отношениям внутри терминала и отношениям терминал – услуга.

Появляется все больше и больше транспортных средств, которые поддерживают связь с удаленной платформой с помощью встроенного или установленного модуля связи. Такие транспортные средства могут передавать удаленной платформе данные о своем состоянии или получать от нее инструкции. В этой ситуации транспортное средство состоит из двух частей: одна относится к средствам электросвязи, которые предоставляет производитель терминалов, а другая – это само транспортное средство, изготовленное автопроизводителем.

Традиционная сеть подвижной связи главным образом предоставляет абонентам услуги доступа к сети передачи голоса, коротких сообщений или данных. Абонент является конечным пользователем терминала. В случае услуг аренды автомобилей водители, использующие арендованные транспортные средства, оборудованные терминалами связи, не являются абонентами. С другой стороны, арендатору автомобиля, как правило, необходимо использовать специальное приложение на своем мобильном терминале для взаимодействия с платформой через сеть связи, чтобы дистанционно получать информацию об автомобиле или дистанционно управлять им, например определять его местонахождение, отпирать и запирать двери без ключей или включать и выключать кондиционер.

Следовательно, в случае, показанном на рисунке 7, основными заинтересованными сторонами являются арендаторы автомобилей, автомобили (которые представляют собой мобильный терминал), производители мобильных терминалов, поставщики UICC, автопроизводители, поставщики/продавцы NE, операторы сетей и поставщики приложений.

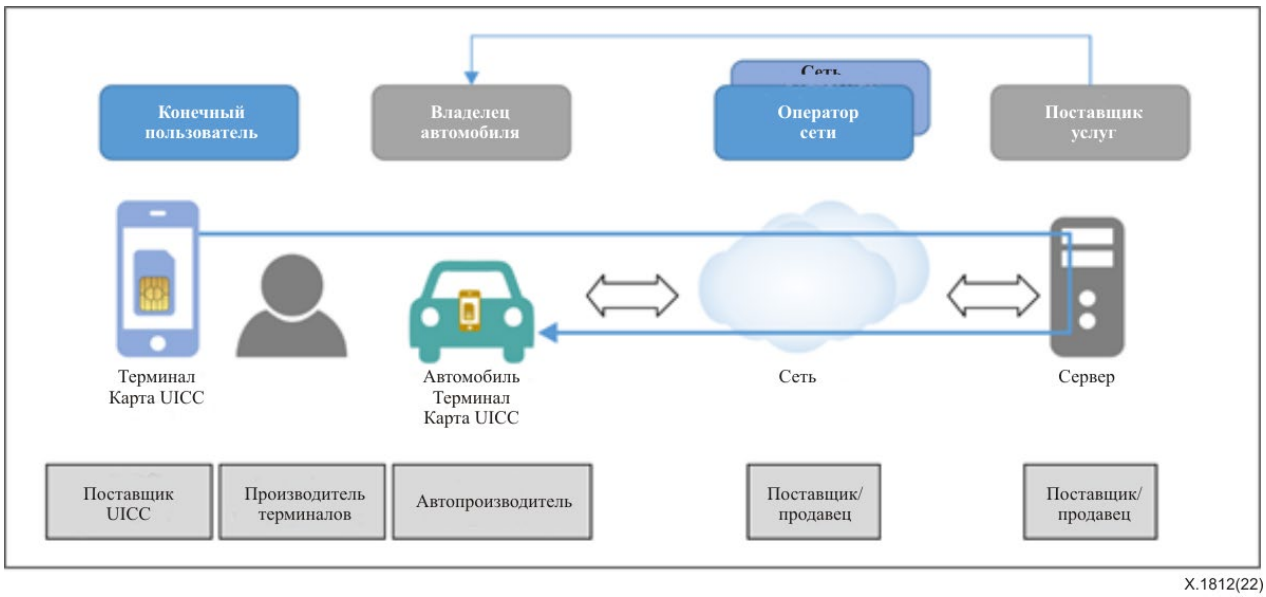


Рисунок 7 – Основные заинтересованные стороны в сценарии аренды автомобиля с дистанционным управлением

8.4.2 Роли заинтересованных сторон в данном сценарии

В данном сценарии перечисленные заинтересованные стороны играют следующие роли.

- Арендатор автомобиля. Определенный пользователь арендует автомобиль в компании по прокату автомобилей. Этот человек также является абонентом подвижной сети и имеет мобильный терминал.
- Автомобиль. Автомобиль принадлежит компании по прокату автомобилей и снабжен специальным встроенным мобильным терминалом, который можно считать абонентом сети.
- Производитель мобильных терминалов. Это предприятие поставляет терминалы, которые могут использоваться абонентами, обменивающимися данными с сетью.
- Поставщик UICC. Это предприятие предоставляет карты UICC, которые могут использоваться для идентификации абонентов.
- Автопроизводитель. Это предприятие производит автомобили, которые могут содержать или не содержать встроенный мобильный терминал.
- Поставщик/продавец NE. Это предприятие предлагает устройства или компоненты устройств, из которых можно построить систему электросвязи или платформу или систему услуг.
- Оператор сети. Эта организация владеет всеми элементами, необходимыми для продажи и предоставления услуг электросвязи абонентам и поставщикам услуг, или контролирует эти элементы.
- Поставщик приложений. Это предприятие предоставляет приложение для пользователей услуг аренды автомобилей.

8.5 Сценарий 4. Представление возможностей сети для промышленности

8.5.1 Общие положения

В данном сценарии основное внимание уделяется отношениям сеть – услуги и отношениям между услугами.

IMT-2020 обладает новыми функциями, такими например, как усовершенствованная подвижная широкополосная связь, подключение к массовому интернету вещей (IoT) и сверхнадежная связь с короткой задержкой. Благодаря этим функциям сеть IMT-2020 может обеспечить лучшую поддержку сетевых соединений для вертикальных областей, таких как промышленность.

По сравнению с персональной связью, у связи вертикальной отрасли другие потребности, такие как необходимость в разнообразии услуг, дифференциации функций и неоднородности технологий. К связи вертикальной отрасли на уровне приложений обычно предъявляются строгие требования безопасности, например изоляция связи от других отраслевых пользователей, более широкие возможности управления, сотрудничество с операторами сетей со специальными функциями, такими как представление возможностей сети.

По сравнению с традиционными службами службы связи вертикальной отрасли могут сотрудничать с операторами сетей, поэтому подключаются поставщики приложений, а также привлекаются поставщики соответствующих серверов приложений или облачных платформ.

На стороне терминала, как в сценарии 3, оконечное устройство также может состоять из двух частей – одна из них относится к средству связи, предоставляемому производителем терминалов, а другая – к специальным вертикальным приложениям, предоставляемым другими производителями промышленных терминалов.

В случае, показанном на рисунке 8, основными заинтересованными сторонами являются пользователи в вертикальной отрасли, производители терминалов связи, поставщики UICC, производители промышленных терминалов, поставщики/продавцы NE, поставщики услуг серверов приложений или облачной платформы, поставщики приложений и операторы сети.

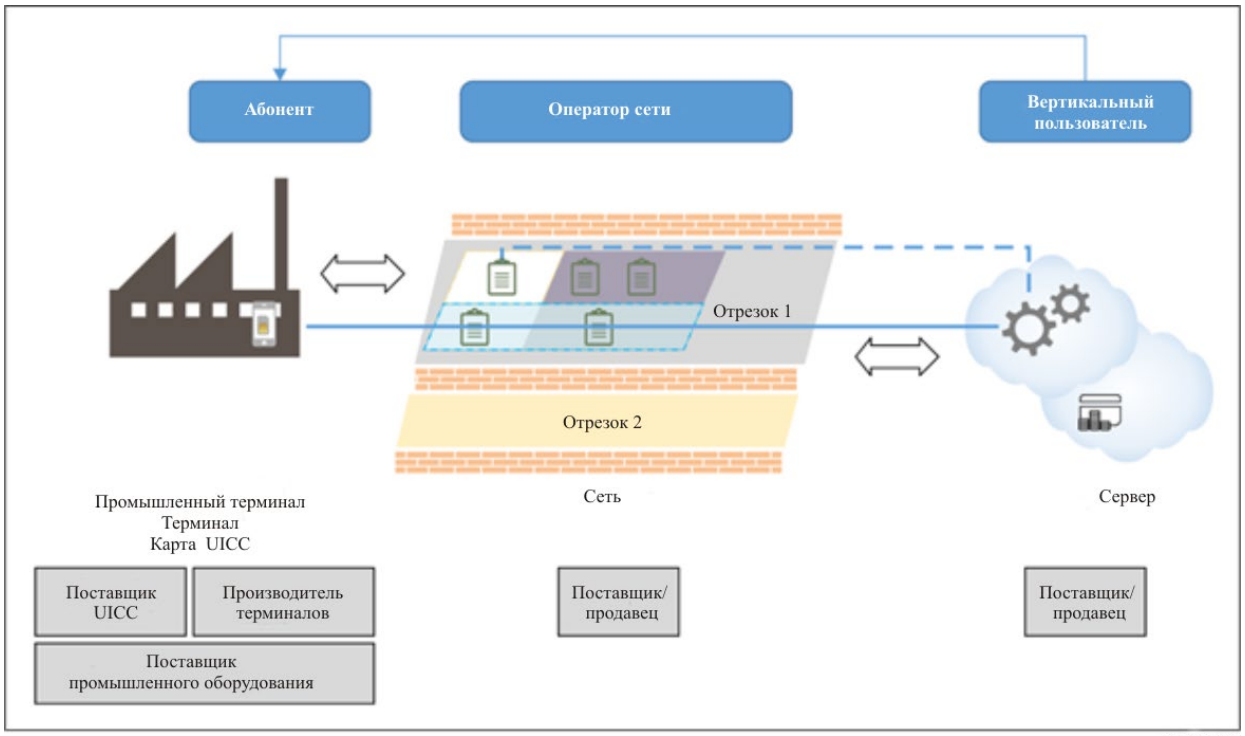


Рисунок 8 – Основные заинтересованные стороны в сценарии представления возможностей сети

8.5.2 Роли заинтересованных сторон в данном сценарии

В данном сценарии основные заинтересованные стороны играют следующие роли.

- Пользователь в вертикальной отрасли. Пользователь в вертикальной отрасли дистанционно управляет промышленным терминалом через сеть электросвязи, используя специальные приложения, работающие на серверах приложений или на открытых или частных облачных платформах.
- Производитель терминалов связи. Это предприятие поставляет терминалы, которыми могут пользоваться абоненты, обменивающиеся данными с сетью.
- Поставщик UICC. Это предприятие предоставляет карты UICC, которые могут использоваться для идентификации абонентов.

- Производитель промышленных терминалов. Это предприятие поставляет промышленные машины, сети или системы для заводов или предприятий.
- Поставщик/продавец NE. Это предприятие предлагает устройства или компоненты устройств, из которых можно построить систему электросвязи или платформу/систему услуг.
- Поставщик услуг сервера приложений или облачной платформы. Этому предприятию принадлежит инфраструктура и платформа, которая предлагает услуги по предоставлению ресурсов хранения данных и вычислительных ресурсов для приложений верхнего уровня.
- Поставщик приложений. Завод или предприятия собирают информацию или обеспечивают управляющую сигнализацию для промышленных терминалов.
- Оператор сети. Эта организация владеет всеми элементами, необходимыми для продажи и предоставления услуг электросвязи абонентам и поставщикам услуг, или контролирует эти элементы.

8.6 Сценарий 5. Цепочки поставок

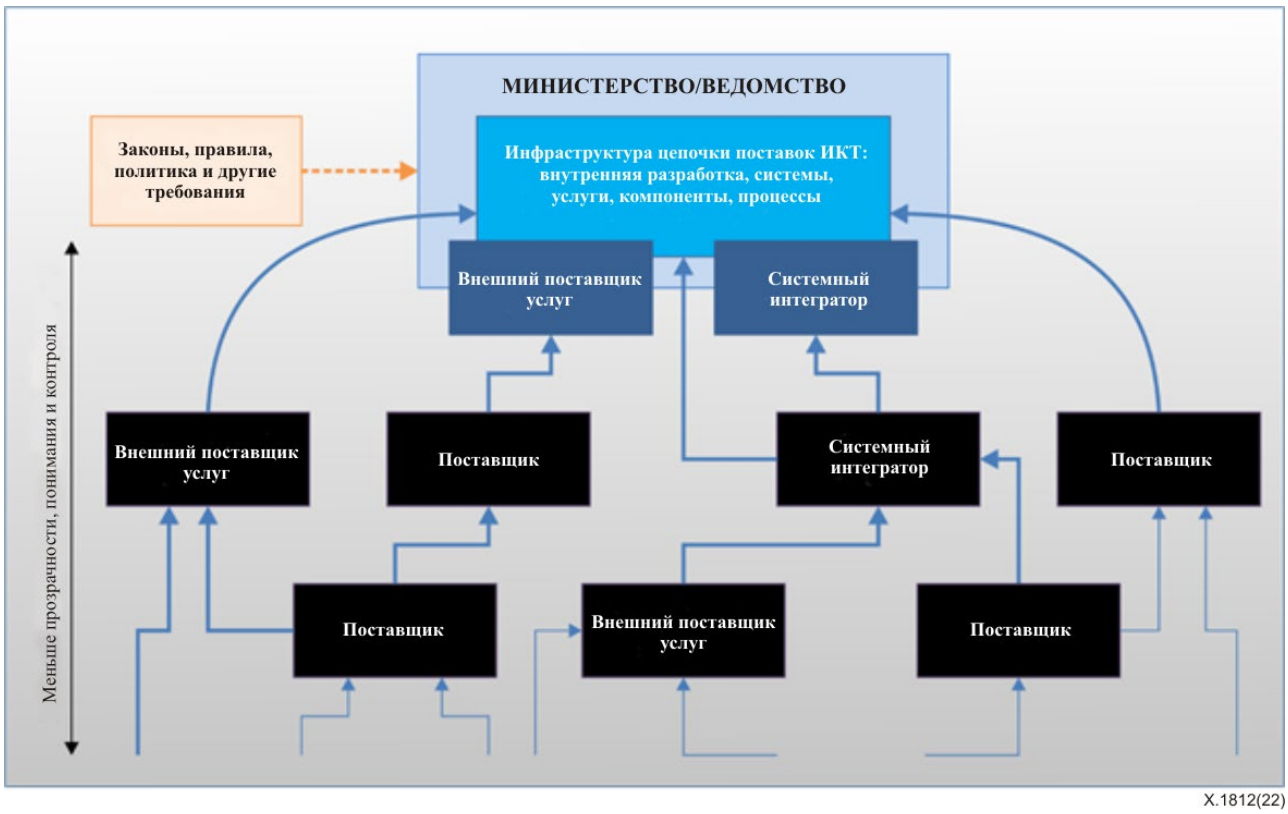
8.6.1 Общие положения

Под экосистемой IMT-2020 понимается сообщество, состоящее из множества организаций, которые вносят огромный вклад в виде различных технологий и знаний, чтобы обеспечить функционирование услуг и приложений IMT-2020.

Цепочка поставок – это система организаций, людей, видов деятельности, информации и ресурсов, участвующих в процессе перемещения продукта или услуги от поставщика к потребителю. Управление рисками цепочки поставок – это скоординированные усилия организации по выявлению, мониторингу, обнаружению и смягчению угроз для непрерывности и рентабельности цепочки поставок. Управление рисками цепочки поставок для экосистемы IMT-2020 опирается на четыре основных аспекта безопасности, как описано ниже.

- Защита. Этот аспект относится к конфиденциальности, целостности и доступности информации, которая (a) описывает цепочку поставок (например, информация о поперечных путях продуктов и услуг IMT-2020, как логических, так и физических) или (b) пересекает цепочку поставок (например, интеллектуальная собственность, содержащаяся в продуктах и услугах IMT-2020), а также к информации о заинтересованных сторонах, участвующих в цепочке поставок (всех, кто имеет дело с продуктами или услугами IMT-2020 на протяжении всего их жизненного цикла).
- Целостность. Этот аспект гарантирует, что продукты или услуги IMT-2020 в цепочке поставок являются подлинными и неизмененными и что эти продукты и услуги будут работать в соответствии со спецификациями приобретателя и не будут иметь нежелательных дополнительных функций.
- Устойчивость. Этот аспект гарантирует, что цепочка поставок обеспечивает необходимые продукты и услуги в случае перегрузки или отказа.
- Качество. Этот аспект уменьшает уязвимость, которая может ограничивать предполагаемую функцию компонента, приводить к отказу компонента или предоставлять возможности для взлома.

В данном сценарии основное внимание уделяется цепочке поставок и взаимоотношениям. Основные участники сценариев цепочки поставок показаны на рисунке 9.



ИКТ – информационно-коммуникационные технологии

Рисунок 9. Основные заинтересованные стороны в сценариях цепочки поставок

8.6.2 Роли заинтересованных сторон в данном сценарии

В цепочке поставок участвуют несколько заинтересованных сторон: разработчик или производитель, системный интегратор, поставщик/продавец, торговые посредники, поставщик и внешний поставщик услуг.

Под разработчиком или производителем понимаются: i) разработчики или производители информационных систем, системных компонентов или услуг информационных систем; ii) системные интеграторы; iii) поставщики/продавцы; или iv) торговые посредники.

Системный интегратор – это частное лицо или компания, задачей которых является объединение компонентов подсистем в единое целое и обеспечение совместного функционирования этих подсистем – так называемая системная интеграция.

Поставщик/продавец – это тот, кто предоставляет товары или услуги компании или частным лицам. Нередко поставщик/продавец производит товары, а затем продает их покупателю. Предприятие – это отдельное от компании-подрядчика юридическое лицо, которое предоставляет такие услуги, как консультирование или разработка программного обеспечения.

Торговый посредник – это компания или частное лицо, которые покупают товары или услуги в целях их перепродажи, а не потребления или использования.

Поставщик – это организация, которая поставляет товары и услуги другим.

К внешним поставщикам услуг относятся: i) структуры внутри организации, но за границами области авторизации безопасности, установленными для информационных систем организации; ii) объекты за пределами организации либо в государственном секторе (например, федеральные агентства), либо в частном секторе (например, поставщики коммерческих услуг); или iii) некоторая комбинация из вариантов, относящихся к государственному и частному секторам.

8.7 Заинтересованные стороны в экосистеме IMT-2020

На основе сценариев использования, описанных в пунктах 8.2–8.6, в экосистеме IMT-2020 можно выделить четыре вида заинтересованных сторон: производители, операторы сетей, поставщики услуг и конечные пользователи, как показано на рисунке 10.

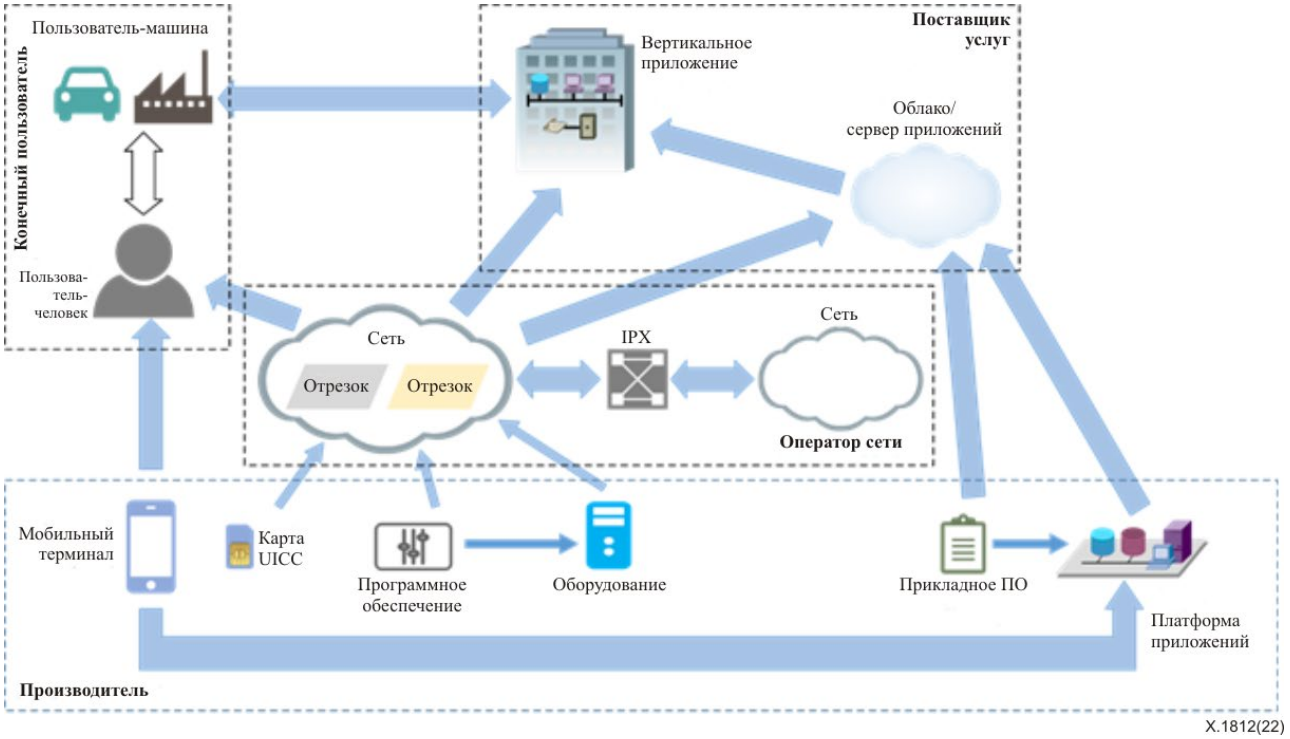


Рисунок 10 – Заинтересованные стороны в экосистеме IMT-2020

Одна заинтересованная сторона может поддерживать прямые отношения с другой стороной и косвенные отношения с другими сторонами через третью заинтересованную сторону, то есть вести себя как звено цепочки поставок.

В экосистеме IMT-2020 производителей можно рассматривать как группу разработчиков или изготовителей, системных интеграторов и поставщиков/продавцов. Операторов сетей можно рассматривать как торговых посредников и поставщиков сетевых услуг. Поставщиков услуг можно рассматривать как внешних поставщиков услуг.

Производители компонентов предоставляют технологические структурные блоки производителям беспроводных устройств и сетевого оборудования. Эти производители компонентов также могут предоставлять такие структурные блоки напрямую операторам сетей. Производители беспроводных устройств предоставляют оборудование для конечных пользователей или в качестве компонентов промышленных машин, а производители сетевого оборудования выпускают оборудование для поддержки сетевой инфраструктуры (включая беспроводную и проводную). Операторы сетей объединяют эти устройства, сетевые компоненты, сетевое оборудование и сети других операторов через IPX во всемирную операционную сеть для обслуживания конечных пользователей. Конечные пользователи совершают голосовые вызовы, отправляют текстовые сообщения и запускают приложения в сети. Операторы сетей также предоставляют услуги связи и сопутствующие услуги внешним поставщикам услуг через свою службу представления возможностей сети или другие специальные службы.

9 Уровень, критерии и модель доверия

9.1 Общие положения

Как определено в пункте 3.1.11, доверие – это степень уверенности пользователя или другой заинтересованной стороны в том, что продукт или система будут выполнять свои функции, как это предполагалось. Доверие также играет важную роль в экосистеме IMT-2020. В настоящей Рекомендации определяется модель доверия в экосистеме IMT-2020, позволяющая заинтересованным сторонам принимать обоснованные решения в отношении доверия и безопасности.

Данная модель доверия в экосистеме IMT-2020 подразделяется на три уровня.

- Первый уровень доверия охватывает требования, предъявляемые к доверию государственными и регуляторными органами. К ключевым факторам, определяющим доверие, относятся принятие международных стандартов, а также открытый и прозрачный процесс сертификации.
- Второй уровень доверия – это удовлетворение требований к доверию отраслевых организаций. К ключевым факторам для таких организаций относятся определение заинтересованных сторон, владельца сквозного (E2E) решения, конечного коммерческого пользователя, бизнес-модели, уровней доверия и доверительных отношений.
- Третий уровень доверия – это обеспечение доверия путем предоставления технических решений, основанных на ключевых факторах первого и второго уровней.

В настоящей Рекомендации основное внимание уделяется второму и третьему уровням, то есть отраслевым организациям и техническим решениям.

Оператору сети IMT-2020 для создания своей сетевой системы необходимо полагаться на устройства или оборудование, предоставляемые производителями. Таким образом, ему необходимо полагаться на то, что производители предоставят устройства, которые могут удовлетворять требованиям оператора сети.

Поставщик услуг для передачи информации полагается на сеть, поэтому он должен доверять оператору сети в том, что тот обеспечит правильную и своевременную передачу данных. Для создания своих услуг поставщик услуг также должен полагаться на устройства, предоставляемые производителями, и следовательно, он тоже должен доверять производителям в вопросе предоставления устройств, которые смогут соответствовать требованиям поставщика услуг.

Конечным пользователям необходимо полагаться на передачу по сети и обслуживающие приложения, поэтому они должны быть уверены, что доступ к сети, предоставляемый оператором сети, будет законным и эффективным. Аналогичные требования доверия они предъявляют к поставщику услуг.

9.2 Уровни доверия

Доверию трудно дать значимую количественную оценку. В модели доверия, представленной в настоящей Рекомендации, вводится качественное понятие уровня доверия, чтобы можно было судить о последствиях различных степеней доверия.

Услуги с поддержкой IMT-2020 работают в разных контекстах и, следовательно, предъявляют разные требования к доверию. Например, в разных вертикальных отраслях оказываются разные услуги и применяются разные сценарии и, следовательно, им присуще разное доверительное позиционирование. Кроме того, одни отрасли классифицируются как часть национальной критически важной инфраструктуры, например умные электросети, а другие работают только в менее критических повседневных сценариях, таких как аренда автомобилей.

Если определенная вертикальная отрасль считается частью критически важной инфраструктуры, то очевидно, что в этой отрасли требуется более высокий уровень уверенности в том, что система IMT-2020 будет функционировать так, как это предполагалось. Другими словами, в этой отрасли необходимо установить более высокий уровень доверия, поскольку любой ущерб скажется на стабильности государства. А вот в тех отраслях, где последствия сбоя относительно незначительны, требуется более низкий уровень доверия.

Например, для услуг узкополосного IoT, таких как интернет транспортных средств (IoV), промышленный интернет, умная электросеть и полив цветов, требуются разные уровни доверия, поскольку ущерб, нанесенный этим отраслям, оказывает разное воздействие на общество или пользователей.

Уровень доверия в конкретном сценарии использования в основном зависит от уровня воздействия, которое оказывает на общество и государство ущерб, нанесенный определенной вертикальной отрасли. Это, вероятно, лучше всего определяется вертикальной организацией, поскольку в ней присутствуют представители разных областей и носители разных профессиональных знаний и опыта, необходимых для выполнения анализа; к тому же определение уровня доверия входит в их обязанности в рамках процедуры должного исполнения. Таким образом для сценариев использования, в которых требуется более высокий уровень доверия, ответственность вовлеченных заинтересованных сторон должна быть выше; другими словами, для этих заинтересованных сторон также необходимо установить более высокий уровень доверия.

В рамках представленной здесь модели доверия предполагается, что для различных сторон может быть установлен один из трех качественных уровней доверия – высокий, средний или низкий. Это предположение сделано по двум основным причинам:

- во-первых, присвоение уровням доверия количественных значений, вероятно, будет весьма проблематичным из-за отсутствия очевидной меры измерения доверия (в отличие, например, от анализа риска, где мера может быть основана на сочетании вероятности возникновения и оценке среднегодовой стоимости воздействия);
- во-вторых, эта трехуровневая шкала достаточно широка, чтобы охватить многие существующие сценарии использования, и принята для измерения требований к доверию в других областях, например в схеме обеспечения безопасности сетевого оборудования (NESAS) [b-GSMA FS.13], [b-GSMA FS.14], [b-GSMA FS.15], [b-GSMA FS.16].

Для последовательного использования модели, представленной в настоящей Рекомендации, остается решить проблему определения значения этих трех уровней доверия. Критерии доверия, разработанные для определения уровней доверия, приведены в пункте 9.3.

Учитывая разнообразие ресурсов и широкий спектр сценариев развертывания в конкретных вертикальных отраслях, на практике общий уровень доверия требует дальнейшего уточнения в зависимости от контекста. Например, уровень доверия, необходимый для автономного вождения, очевидно, зависит от конкретного IoV, территории или макросети.

Необходимость комплексного определения уровня доверия, зависящего от контекста, дополнительно иллюстрирует следующий пример. Предположим, что оператор выбирает производителей сетевого оборудования в соответствии с определенным уровнем доверия. Если определен только один уровень, то все производители сетевого оборудования должны быть выбраны в соответствии с этим единственным уровнем доверия. Однако базовая сеть имеет большую чувствительность, ценность и влияние, чем, например, антенны, поэтому в типичном сценарии уровень доверия в отношении производителя базовой сети должен быть выше, чем в отношении производителя антенн.

В качестве дальнейшего уточнения отдельно определяется уровень доверия для бизнес-единицы и бизнес-сценария. В случае вертикальной отрасли это означает отдельные определения уровня доверия для всей вертикальной отрасли и для конкретного сценария в рамках вертикальной отрасли. Возможные комбинации уровней доверия для двух случаев приведены в таблице 1.

Таблица 1 – Уровень доверия для бизнес-единицы и бизнес-сценариев и соотношение между ними

Уровень доверия для бизнес-единицы	Уровень доверия для бизнес-сценариев
Высокий	Высокий
	Средний
	Низкий
Средний	Средний
	Низкий
Низкий	Низкий

Чтобы сделать определение уровня более практичным и универсальным, рекомендуется гибко определять уровень доверия для компонентов. Например, уровень доверия для компонентов можно определить в зависимости от стоимости ресурса или зоны развертывания.

Рассмотрим конкретный пример. Уровень доверия для всей умной электросети высок, но внутри сети кабели и опоры не так ценны, как инфраструктура датчиков и передача сигналов сети IMT-2020. Но даже в отношении инфраструктуры датчиков и передачи сигналов умная электросеть, развернутая в небольшом городе, не так чувствительна, как электросеть в мегаполисе.

В таблице 2 приведены возможные уровни доверия для отношений между вертикальной отраслью и заинтересованной стороной.

Таблица 2 – Возможные уровни доверия между вертикальной отраслью и заинтересованной стороной

Уровень доверия для системы	**Уровень доверия для компонента**	**Уровень доверия для заинтересованной стороны**
Высокий	Высокий	Высокий
	Средний	Средний
	Низкий	Низкий
Средний	Средний	Средний
	Низкий	Низкий
Низкий	Низкий	Низкий

9.3 Критерии доверия

Для оценки уровня доверия как высокого, среднего или низкого требуется оценка доверительных отношений между заинтересованными сторонами. На доверительные отношения между любыми двумя заинтересованными сторонами влияет множество факторов, и степень доверия между разными заинтересованными сторонами в одной категории и разными заинтересованными сторонами в другой категории также будет различаться. Следовательно, критерии оценки необходимо определять индивидуально.

Поскольку уровень доверия выбирается в целях минимизации вреда от потенциальных угроз и связанных с ними рисков, в число критериев могут входить стоимость ресурсов, масштаб воздействия, серьезность воздействия и вероятность возникновения риска, рассчитанная на основе стандартов управления рисками, таких как [b-NIST SP800-30], [b-ISO 31000] и [b-ISO/IEC 27005].

- Ресурсы. Важность этого фактора очевидна. Чем важнее ресурс, тем значительнее необходимость держать его под полным контролем заинтересованной стороны и тем выше необходимый уровень доверия.
- Масштаб воздействия. Для крупной заинтересованной стороны чем больше область ее влияния, тем более разрушительны последствия любого отказа. Следовательно, если область влияния велика, требуется высокий уровень доверия. Например, оператору требуется меньший уровень доверия к поставщику/продавцу небольших сот, покрывающих крошечные области, чем к поставщику/продавцу NE базовой сети, покрывающих обширную территорию.
- Серьезность воздействия. Для заинтересованной стороны, являющейся частью ключевой инфраструктуры, последствия ущерба более серьезны и, следовательно, требуются большие усилия для предотвращения такого ущерба. Это приводит к большей потребности в тщательной оценке при взаимодействии с другими сторонами. Таким образом, чем серьезнее последствия отказа при взаимодействии, тем выше необходимый уровень доверия.
- Вероятность возникновения риска. Чем выше вероятность возникновения риска, тем более вероятно, что он возникнет.

Экосистема IMT-2020 очень сложна. Для различных классов заинтересованных сторон, например конечных пользователей, производителей оборудования, операторов сетей и поставщиков услуг, в каждой категории содержится множество частных случаев. Поскольку доверие – субъективное

понятие, его трудно измерить и стандартизировать, и уровень доверия между двумя случаями также различен. Однако чтобы предоставить руководство для каждого объекта в экосистеме IMT-2020, необходимо определить набор общих уровней доверия, охватывающий большинство ситуаций, а именно низкий, средний и высокий уровни.

Пример того, как можно определить общий уровень доверия на основе различных критериев, приведен в таблице 3.

Таблица 3 – Критерии для уровней доверия

Общий уровень доверия	**Критерии для уровня доверия**			
	Стоимость ресурсов	**Масштаб воздействия**	**Серьезность воздействия (степень)**	**Вероятность возникновения риска**
Высокий	Высокая	Высокий	Высокая	Высокая
Средний	Средняя	Средний	Средняя	Средняя
Низкий	Низкая	Низкий	Низкая	Низкая

При использовании соотношений из таблицы 3 важно, чтобы уровень риска критериев доверия учитывал меры по снижению риска, которые либо уже приняты, либо будут реализованы. Например, если для высокоэффективной электронной коммерции используется существующий интернет, то стоимость ресурсов, масштаб воздействия и серьезность воздействия можно оценить как очень высокие; более того, на первый взгляд может показаться, что вероятность атаки также будет очень высокой, учитывая, что интернет-протоколы связи не содержат надежных функций безопасности. Используя таблицу 3, можно предположить, что для удовлетворения потребностей электронной коммерции уровень доверия в интернете должен быть высоким. Однако несмотря на то что реальный уровень доверия в интернете является низким с учетом того, что интернет не дает гарантий конфиденциальности, целостности или доступности каналов связи, электронная коммерция очень широко и успешно используется для огромных объемов сделок.

На самом деле причина, по которой этот сценарий работает, заключается в том, что риски для конфиденциальности и целостности данных при их передаче устраняются путем стандартного использования средств обеспечения безопасности транспортного уровня [b-IETF RFC 5246] для защиты линий связи между конечными точками, что можно рассматривать как часть требований безопасности, приведенных в пункте 10.2.

В заключение следует отметить, что при расчете требуемого уровня доверия фактический уровень угрозы необходимо учитывать после того, как были применены меры по снижению рисков для конкретных приложений. В противном случае могут быть предъявлены нереалистичные требования в отношении уровня доверия к поставщикам оборудования и услуг, что приведет к значительному увеличению затрат.

9.4 Модель доверия на основе сопоставления доверительных отношений

Для установления границ безопасности IMT-2020 и мер безопасности совместимым стандартизированным способом необходимо надлежащим образом разработать и использовать модель доверия. Чтобы обеспечить эффективность такой модели, необходимо провести анализ доверительных отношений.

С учетом факторов, определенных в пункте 9.2, общие доверительные отношения между двумя сторонами также являются однонаправленными, а не двунаправленными. Пример анализа доверительных отношений между различными классами заинтересованных сторон приведен в таблице 4.

Таблица 4 – Уровень доверительных отношений между заинтересованными сторонами

Субъект	Объект			
	Конечный пользователь	**Производитель**	**Оператор сети**	**Поставщик услуг**
Конечный пользователь		Средний/низкий	Высокий/средний/ низкий	Высокий/средний/ низкий
Производитель	–		Высокий	Высокий
Оператор сети	Низкий	Высокий/средний/ низкий		Высокий/средний/ низкий
Поставщик услуг	Высокий/средний/ низкий	Высокий/средний/ низкий	Высокий/средний/ низкий	

Доверительные отношения между различными партнерами в экосистеме IMT-2020 обычно очень сложны. Следовательно, необходимо создать модель доверия, способную отражать эту сложность. То есть можно уточнить общие доверительные отношения, чтобы получить доверительные значения на уровне подсистем. Пример анализа доверительных отношений на уровне подсистем приведен в таблице 5.

Таблица 5 – Доверительные отношения между производителями на уровне подсистем

Субъект	Объект			
	Чипсет/модем	**Модуль**	**Поставщик устройств**	**Поставщик программного обеспечения**
Чипсет/модем		–	–	–
Модуль	Высокий/средний		–	–
Поставщик устройств	Высокий/средний	Высокий/средний		–
Поставщик программного обеспечения	Высокий/средний	Высокий/средний	Высокий/средний	

В качестве сквозного примера с использованием модели, приведенной в таблице 6, представлен сценарий аренды автомобиля.

Таблица 6 – Модель доверия на основе доверительных отношений в сценарии аренды автомобиля

Объект		Объект						
		Поставщик услуг (автомо-биль)	**Арендатор**	**Производитель**			**Оператор сети**	**Постав-щик услуг**
				Терминал/ UICC	**Автомобиль (исключая терминал и UICC)**	**Сетевое оборудо-вание**		
Автомобиль			Средний/ низкий	Средний	Высокий/ средний	–	Высокий/ средний/ низкий	Высокий
Арендатор		Высокий/ средний		Средний/ низкий	Средний/ низкий	–	Высокий/ средний/ низкий	Высокий/ средний/ низкий
Производитель	**терминалов/ UICC**	–	–		–	–	Высокий	Высокий
	автомобилей	–	–	–		–	–	Высокий
	сетевого оборудования	–	–	–	–		Высокий	–
Оператор сети		Низкий	Низкий	Высокий/ средний/ низкий	–	Высокий/ средний/ низкий		Высокий/ средний/ низкий
Поставщик услуг		Высокий	Средний/ низкий	Высокий/ средний/ низкий	Высокий/ средний	–	Высокий/ средний/ низкий	

10 Требования безопасности, поддерживаемые моделью доверия на основе доверительных отношений

10.1 Общие положения

В конкретном сценарии система создается рядом заинтересованных сторон, предоставляющих различные услуги и функции для обеспечения того, чтобы система вела себя и работала так, как предполагалось – принося пользу заинтересованным сторонам. Эти заинтересованные стороны, вместе взятые, образуют экосистему.

В процессе функционирования экосистемы могут возникнуть потенциальные угрозы и опасности, мешающие работе предприятия. Чтобы предотвратить причинение вреда этими угрозами, все заинтересованные стороны должны гарантировать непрерывную работу экосистемы, соблюдая законодательные нормы и предоставляя безопасные продукты, услуги и решения с использованием безопасной процедуры разработки.

В целях содействия определению требований безопасности, основанных на доверии, для заинтересованных сторон может использоваться модель доверия, представленная в пункте 9.

10.2 Требования безопасности на основе уровня доверия

10.2.1 Обзор

Для оценки того, способна ли заинтересованная сторона обеспечить соответствующую возможность защиты от ущерба, можно использовать уровень доверия к этой заинтересованной стороне. Для уменьшения такого ущерба могут быть разработаны требования безопасности. В итоге требования безопасности могут быть основаны на возможностях организации, включая профессиональный уровень персонала, на использовании безопасных процессов разработки, таких как жизненный цикл безопасной разработки системы, или на возможностях безопасной эксплуатации, а также на технологических возможностях, связанных с надежными решениями. Дополнительную информацию см. в стандартах и практических рекомендациях, таких как [b-NIST FICIC] и [b-BSIMM]. См. таблицу 7.

Таблица 7 – Уровень доверия и категории требований безопасности

Уровень доверия	**Категории требований безопасности**		
Субъект	**Объект**		
	Возможности организации (хорошая репутация)	Безопасность разработки системы и жизненного цикла продукта или возможности безопасной эксплуатации (хорошая процедура)	Технологические возможности, связанные с надежными решениями (хорошее решение)
Высокий	✓	✓	✓
Средний	✓	✓	–
Низкий	✓	–	–

10.2.2 Организационные требования

10.2.2.1 Введение

Возможности организации по обеспечению безопасности, связанные с доверием, можно подразделить следующим образом: репутация организации, способность выполнять контракты, постоянство ценностей, возможность компенсации за нарушения контракта и независимость.

10.2.2.2 Исполнение контрактов

Репутация отражает степень исторической приверженности определенным целям в отношении продукта или системы. Репутация – это показатель, который можно получить на основе прямого или косвенного знания о предыдущих взаимодействиях заинтересованных сторон и который используется

для оценки уровня доверия к заинтересованной стороне. Как выражение уверенности, доверие обычно основывается на исторической информации для определения вероятности надежности в будущем. Следовательно, если конкретная заинтересованная сторона ранее успешно работала в соответствии с соглашением, ее репутация в отрасли также будет более высокой, и таким образом она может пользоваться большим доверием у другой стороны. Данные для управления репутацией можно получить из различных надежных и широко распространенных источников, основанных на фактических данных, таких как сертификаты или официальные годовые и финансовые отчеты. Однако конкретная заинтересованная сторона может иметь разную репутацию в разных областях. Например, отношения между производителем устройств и оператором сети или поставщиком услуг представляют собой отношения поставщик – клиент, в то время как отношения между разными производителями могут быть отношениями конкуренции. Следовательно, производитель устройств может иметь хорошую репутацию у оператора сети или поставщика услуг, но плохую у конкурента. В результате при анализе полученной извне информации о репутации операторы сети или поставщики услуг не могут использовать в качестве основного источника информацию о репутации, полученную от конкурирующего производителя.

10.2.2.3 Исполнение контрактов

В случае непрерывного совместного или многократного периодического исполнения контрактов качество исполнения влияет на доверие обеих сторон. Оно также оказывает влияние на доверительные отношения между сторонами. При качественном исполнении контракта взаимное доверие возрастает и доверительные отношения крепнут. Напротив, когда исполнение контракта оставляет желать лучшего, взаимное доверие понижается и доверительные отношения ослабевают. При непрерывном многократном сотрудничестве, например когда пользователи много раз посещают поставщика услуг, оценка пользователем качества предоставленных в предыдущие годы услуг напрямую влияет на его доверие к системе обслуживания. В этом случае информацию о таком предыдущем опыте пользователя рекомендуется классифицировать как проблему, связанную с исполнением пользовательского контракта, а не как проблему репутации.

10.2.2.4 Постоянство ценностей

Когда заинтересованные стороны разделяют одни и те же ценности, отношения между ними становятся более тесными, а их ожидания в отношении далекого будущего – более устойчивыми. В результате достигается более высокое взаимное доверие и между ними возникают более доверительные отношения.

10.2.2.5 Компенсация

Возможность компенсации относится к ожиданию компенсации в случае невыполнения обязательств. Ожидание компенсации можно рассматривать как еще одну гарантию того, что заинтересованная сторона будет стремиться выполнить контракт даже в аномальных обстоятельствах. В целом чем больше компенсация, тем меньше потери для партнера. Такая возможность повысит уверенность и доверие к другой стороне. Например, уровень и строгость наказания или компенсации для различных заинтересованных сторон в целях повышения надежности могут определяться региональными законами о кибербезопасности.

10.2.2.6 Независимость

Независимость заинтересованной стороны отражает ее автономию при исполнении контракта. Независимость включает способность материнской компании контролировать дочернюю компанию, а также влияние на коммерческое предприятие органов власти. Чем больше заинтересованных сторон в нем участвует, тем большее влияние они на него оказывают и тем больше страдают его доверительные отношения.

10.2.2.7 Выводы

Пример того, как уровни доверия могут быть связаны с возможностями организации, приведен в таблице 8. На практике точный выбор аспектов, которые требуются для достижения среднего и низкого уровней доверия, зависит от сферы применения. Например, в одних случаях для низкого уровня доверия может оказаться достаточной соответствующая репутация поставщика, а в других случаях этот аспект может не иметь значения, даже когда требуется средний уровень доверия.

Таблица 8 – Уровни доверия и требования безопасности, связанные с возможностями организации

Уровень доверия	Требования безопасности в аспекте возможностей организации				
	Репутация	**Исполнение контрактов**	**Постоянство ценностей**	**Возможность компенсации**	**Независимость**
Высокий	✓	✓	✓	✓	✓
Средний	(✓)	✓	–	✓	(✓)
Низкий	–	✓	–	(✓)	–

10.2.3 Процедурные требования

10.2.3.1 Введение

Возможность безопасной эксплуатации может достигаться с помощью следующих средств: обеспечения безопасности процесса разработки и жизненного цикла продукта, а также возможности безопасной эксплуатации.

10.2.3.2 Безопасность процесса разработки и жизненного цикла продукта

В рамках NESAS процесс разработки и жизненный цикл продукта охватывают все аспекты, потенциально влияющие на срок службы сетевого оборудования (продукта), включая планирование, проектирование, внедрение, доставку, модернизацию и, в конечном счете, утилизацию этого оборудования. В настоящее время для сети IMT-2020 схема NESAS, совместно разработанная Ассоциацией глобальной системы подвижной связи (GSMA) и 3GPP, определяет безопасность процесса разработки и жизненного цикла продуктов для сетевого оборудования IMT-2020, охватывающего этапы, через которые сетевое оборудование проходит на протяжении всего процесса разработки (включая планирование, проектирование, внедрение, тестирование, выпуск, производство и доставку), и жизненный цикл продукта (охватывающий этапы, через которые проходит разрабатываемое сетевое оборудование до конца срока службы, включая техническое обслуживание и выпуски обновлений). Рекомендуется учитывать это при оценке процесса разработки и жизненного цикла продуктов поставщика.

10.2.3.3 Возможность безопасной эксплуатации

Возможность безопасной эксплуатации означает, что при коммерческом использовании продукта или сети ими необходимо надлежащим образом управлять, обеспечивая безопасное развертывание, усиленную защиту и контроль ограниченного доступа.

10.2.3.4 Выводы

Таким образом, что касается возможности безопасной эксплуатации, рекомендуются требования, указанные в таблице 9.

Таблица 9 – Уровень доверия и требования безопасности в отношении возможности безопасной эксплуатации

Уровень доверия	Требования безопасности в отношении возможности безопасной эксплуатации	
	Безопасность процесса разработки системы и жизненного цикла продукта	**Безопасная эксплуатация**
Высокий	✓	✓
Средний	(✓)	✓
Низкий	–	✓

10.2.4 Технические требования

Возможность надежности может обеспечиваться путем соблюдения соответствующих уровней в следующих отношениях: безопасные процедуры, конфиденциальность, устойчивость, безопасность, безотказность и доступность. Это ключевые свойства, рекомендуемые для обеспечения надежности продуктов и решений в области безопасности, предоставляемых заинтересованной стороной, как описано в ряде документов, таких как [b-BSI 10754-1] и [b-NIST SP800-160v1].

Пример того, как уровни доверия могут быть связаны с надежностью организации, приведен в таблице 10. Как и прежде на практике точный выбор аспектов, которые требуются для достижения среднего и низкого уровней доверия, зависит от сферы применения. Например, в одних случаях для достижения низкого уровня доверия может потребоваться надлежащий уровень защиты конфиденциальности данных, а в других этот аспект может не иметь значения, даже когда требуется средний уровень доверия.

Таблица 10 – Уровень доверия и требования безопасности для обеспечения надежности

Уровень доверия	Требования безопасности для обеспечения надежности					
	Безопасные процедуры	Конфи-денциаль-ность	Устойчивость	Безопасность	Безотказ-ность	Доступность
Высокий	√	√	√	√	√	√
Средний	√	(√)	(√)	(√)	(√)	√
Низкий	√	–	–	(√)	(√)	–

В реальных реализациях точные требования зависят от сценариев обслуживания и должна обеспечиваться гибкость. Как отмечалось выше, в случае низкого уровня доверия, хотя требования безопасности могут быть относительно низкими, может возникнуть необходимость в более строгом соблюдении других требований, таких как конфиденциальность.

10.3 Интерпретация доверия для определения детальных требований гарантии безопасности

Когда для конкретного сценария использования определен требуемый уровень доверия, необходимо интерпретировать этот уровень в целях принятия решений по внедрению и эксплуатации.

Это может быть достигнуто путем сопоставления требуемого уровня доверия с конкретными требованиями, перечисленными в пункте 10.2, и эти требования могут быть выполнены посредством гарантии безопасности продукта и системы. Существует ряд давно установленных и стандартизованных методов гарантирования надежности продуктов и систем путем испытаний и оценок, например проводимых третьими сторонами. Их можно использовать в качестве основы для сопоставления требуемого уровня доверия, полученного в результате анализа, описанного в пункте 9.4, с конкретными требованиями гарантии безопасности при приобретении и использовании оборудования и услуг.

Пример, приведенный в таблице 11, позволяет сопоставить требуемые уровни доверия с основанными на уровне доверия коммерческими и эксплуатационными решениями в зависимости от оценок продуктов и систем.

Таблица 11 – Пример сопоставления требуемого уровня доверия с требованиями гарантии безопасности

Требуемый уровень доверия	Тип гарантирующей организации	Примеры схем гарантирования безопасности
Высокий	Оценка признанным государственным органом	Общие критерии [b-ISO/IEC 15408 (все части)] Национальный регуляторный орган [b-ISO/IEC 27001] NESAS Спецификация гарантии безопасности (SCAS) [b-3GPP TS33.511], [b-3GPP TS33.512], [b-3GPP TS33.513], [b-3GPP TS33.514], [b-3GPP TS33.515], [b-3GPP TS33.516], [b-3GPP TS33.517], [b-3GPP TS33.518], [b-3GPP TS33.519]
Средний	Оценка аккредитованным органом по оценке соответствия (CAB)	Общие критерии [b-ISA/IEC 62443 (все части)] [b-ISO/IEC 27001] NESAS/SCAS
Низкий	Оценка CAB или самооценка	Общие критерии NESAS/SCAS

Даже в рамках конкретной схемы гарантирования безопасности для разных уровней доверия могут подходить разные степени или типы гарантий.

- Некоторые методы, в частности определенные в [b-ISO/IEC 15408 (все части)], позволяют указывать несколько уровней гарантии, так что для разных уровней доверия могут факультативно потребоваться разные уровни оценки по [b-ISO/IEC 15408 (все части)]. Однако другие схемы, такие как [b-ISO/IEC 27001], допускают только один уровень оценки.
- Степень гарантии, которую можно получить в результате оценки, может факультативно варьироваться в зависимости от выполняющего ее органа (как указано в среднем столбце таблицы 11). Например, для низкого уровня доверия может подойти самооценка соответствия требованиям [b-ISO/IEC 27001].

Кроме того, вес, придаваемый оценке, может быть усилен другими факторами, например:

- критично ли оборудование или услуга для выполнения миссии или это всего лишь один из множества способов обеспечения конкретной функции (например, путем резервирования);
- имеется ли нескольких оценок гарантий, относящихся к разным аспектам конкретного продукта, системы или услуги.

Библиография

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers.*

[b-ISO 28598-1] ISO 28598-1:2017, *Acceptance sampling procedures based on the allocation of priorities principle (APP) – Part 1: Guidelines for the APP approach.*

[b-ISO 31000] ISO 31000:2018, *Risk management – Guidelines*. Available [viewed 2022-07-18] at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary.*

[b-ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General.*

[b-ISO/IEC/IEEE 15288] ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes.*

[b-ISO/IEC 15408(all parts)] ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security.*

[b-ISO/IEC/IEEE 24765] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary.*

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models.*

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

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements.*

[b-ISO/IEC 27005] ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management.*

[b-ISO/PAS 19450] Publicly Available Specification ISO/PAS 19450:2015, *Automation systems and integration – Object-process methodology.*

[b-ISO/TS 21089] Technical Specification ISO/TS 21089:2018, *Health informatics – Trusted end-to-end information flows.*

[b-ISO/TS 21719-2] Technical Specification ISO/TS 21719-2:2018, *Electronic fee collection – Personalization of on-board equipment (OBE) Part 2: Using dedicated short-range communication.*

[b-ISO/TS 22318] Technical Specification ISO/TS 22318:2021, *Security and resilience – Business continuity management systems – Guidelines for supply chain continuity management.*

[b-ISA/IEC 62443] ISA/IEC 62443 (all parts) [series of automation and control systems cybersecurity standards].

[b-GSMA FS.13] GSM Association (2022). *Network equipment security assurance scheme – Overview,* Official Document FS.13, version 2.1. London: GSM Association. 29 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf

[b-GSMA FS.14] GSM Association (2022). *Network equipment security assurance scheme – Security test laboratory accreditation,* Official Document FS.14, version 2.1. London: GSM Association. 15 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.14-v2.1.pdf

[b-GSMA FS.15] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle assessment methodology,* Official Document FS.15, version 2.1. London: GSM Association. 33 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.15-v2.1.pdf

[b-GSMA FS.16] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle security requirements,* Official Document FS.16, version 2.1. London: GSM Association. 22 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol – Version 1.2.*

[b-IETF RFC 6733] IETF RFC 6733 (2012), *Diameter base protocol.*

[b-3GPP TS 33.501] Technical Specification 3GPP TS 33.501 V17.6.0 (2022), *Security architecture and procedures for 5G system.*

[b-3GPP TS 33.511] Technical Specification 3GPP TS 33.511 V17.1.0 (2022), *Security assurance specification (SCAS) for the next generation node B (gNodeB) network product class.*

[b-3GPP TS 33.512] Technical Specification 3GPP TS 33.512 V17.3.0 (2022), *5G security assurance specification (SCAS); Access and mobility management function (AMF).*

[b-3GPP TS 33.513] Technical Specification 3GPP TS 33.513 V17.0.0 (2022), *5G security assurance specification (SCAS); User plane function (UPF).*

[b-3GPP TS 33.514] Technical Specification 3GPP TS 33.514 V17.0.0 (2022), *5G security assurance specification (SCAS) for the unified data management (UDM) network product class.*

[b-3GPP TS 33.515] Technical Specification 3GPP TS 33.515 V17.0.0 (2022), *5G security assurance specification (SCAS) for the session management function (SMF) network product class.*

[b-3GPP TS 33.516] Technical Specification 3PGP TS 33.516 V17.0.0 (2022), *5G security assurance specification (SCAS) for the authentication server function (AUSF) network product class*.

[b-3GPP TS 33.517] Technical Specification 3GPP TS 33.517 V17.0.0 (2022), *5G security assurance specification (SCAS) for the security edge protection proxy (SEPP) network product class.*

[b-3GPP TS 33.518] Technical Specification 3GPP TS 33.518 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network repository function (NRF) network product class.*

[b-3GPP TS 33.519] Technical Specification 3GPP TS 33.519 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network exposure function (NEF) network product class.*

[b-BSI 10754-1] BS 10754-1:2018, *Information technology. Systems trustworthiness – Governance and management specification.*

[b-BSIMM] British Standards Institution (2021). *Building security in maturity model,* BSIMM 12. London: British Standards Institution.

[b-NIST FICIC] NIST (2018). *Framework for improving critical infrastructure cybersecurity,* Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. 48 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[b-NIST SP800-30] Joint Task Force Transformation Initiative (2012). *Guide for conducting risk assessments,* NIST Special Publication, NIST SP800-30 Rev.1. Gaithersburg, MD: National Institute of Standards and Technology. 95 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[b-NIST SP 800-53] NIST SP 800-53 Rev 5 2020, *Security and privacy controls for information systems and organizations.*

[b-NIST SP800-160v1] Ross, R., McEvilley, M., Carrier Oren, J. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems – Volume 1,* NIST Special Publication, NIST SP800-160v1. Gaithersburg, MD: National Institute of Standards and Technology. 243 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.