Международный союз электросвязи

МСЭ-Т X.1814

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2022)

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

Безопасность сетей IMT-2020

Руководящие указания по безопасности для систем связи IMT-2020

Рекомендация МСЭ-Т X.1814

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.1814

Руководящие указания по безопасности для систем связи IMT-2020

Резюме

Для подключенных устройств интернета вещей (IoT) и мобильных приложений необходим беспроводной доступ к сети, который должен быть надежным, безопасным и способным обеспечить неприкосновенность частной жизни пользователей. Эти требования высокого уровня следует учитывать при проектировании систем связи IMT-2020. Необходимо определить структуру безопасности систем связи IMT-2020, которая могла бы служить основой для разработки дальнейших подробных технических Рекомендаций по вопросам безопасности IMT-2020.

В Рекомендации МСЭ-Т X.1814 определены все компоненты, относящиеся к безопасности систем связи IMT-2020, а также определены руководящие указания по безопасности для системы связи IMT-2020. Описана общая архитектура IMT-2020 и ее домены. Также определены угрозы и указаны требования к средствам безопасности для каждого компонента с учетом уникальных сетевых функций. Основой настоящей Рекомендации является архитектура безопасности 3GPP 5G.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1814	02.09.2022 г.	17-я	11.1002/1000/14992

Ключевые слова

Возможность, система связи IMT-2020, периферийные вычисления с множественным доступом, нарезка сети, виртуализация сети, руководящие указания по безопасности, угрозы.

* 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

Рекомендация МСЭ-Т X.1814

Руководящие указания по безопасности для систем связи IMT-2020

1 Сфера применения

В настоящей Рекомендации представлены руководящие указания по безопасности для разработки систем связи IMT-2020. В ней определены все компоненты, относящиеся к безопасности системы связи IMT-2020: абонентское оборудование, сеть доступа и базовая сеть. Описана общая архитектура IMT-2020 и ее домены. Также определены угрозы и указаны требования к средствам безопасности для каждого компонента с учетом уникальных сетевых функций, таких как периферийные вычисления с множественным доступом, сети с программируемыми параметрами, динамическая виртуализация сетевых функций и нарезка сети. Основой настоящей Рекомендацией является архитектура безопасности 3GPP 5G.

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.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*

[ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*

3 Определения

3.1 Термины, определенные в других документах

3.1.1 В настоящей Рекомендации используются следующие термины из [ITU-T X.800]:

– управление доступом (access control);

– аутентификация (authentication);

– готовность (availability);

– конфиденциальность (confidentiality);

– целостность данных (data integrity);

– неприкосновенность частной жизни (privacy);

– непризнание участия (repudiation);

– услуга безопасности (security service).

Кроме того, в настоящей Рекомендации используются следующие дополнительные термины, определенные в других документах.

3.1.2 управление (control) [b-ITU-T X.1408]: Мера, изменяющая риск.

ПРИМЕЧАНИЕ 1. – Средства управления включают любой процесс, политику, устройство, практику или иные действия, изменяющие риск.

ПРИМЕЧАНИЕ 2. – Возможно, что средства управления не всегда оказывают желаемое или предполагаемое изменяющее воздействие.

3.1.3 атака типа распределенный отказ в обслуживании (distributed denial-of-service (DDoS) attack) [b-ITU-T Y.4807]: Несанкционированный доступ к системным ресурсам или задержка системных операций и функций в целях взлома нескольких систем, чтобы занять полосу пропускания или ресурсы целевой системы, что приведет к потере доступности для авторизованных пользователей.

3.1.4 руководящие указания (guideline) [b-ITU-T X.1401]: Описание, разъясняющее, что и как следует делать для достижения целей, установленных политикой.

3.1.5 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, интерфейсы и функциональное поведение которых определены.

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.

3.1.6 виртуализация сетевых функций (network function virtualization) [b-ITU-T X.1811]: Технология, которая позволяет создавать логически изолированные участки сети в общих физических сетях так, чтобы в них могли одновременно сосуществовать разнородные группы из нескольких виртуальных сетей.

3.1.7 отрезок сети (network slice) [b-ITU-T Y.3100]: Логическая сеть с определенными сетевыми возможностями и сетевыми характеристиками.

ПРИМЕЧАНИЕ 1. – Отрезки сети позволяют создавать настраиваемые сети, обеспечивающие гибкие решения для различных коммерческих сценариев, которые предъявляют различные требования в отношении функциональности, производительности и распределения ресурсов.

ПРИМЕЧАНИЕ 2. – Отрезок сети может обладать способностью раскрывать свои возможности.

ПРИМЕЧАНИЕ 3. – Поведение отрезка сети реализуется посредством экземпляра(ов) отрезка сети.

3.1.8 оркестровка (orchestration) [b-ITU-T Y.3100]: В контексте IMT-2020 процессы, направленные на автоматизированное размещение, координацию, реализацию и использование сетевых функций и ресурсов как для физических, так и для виртуальных инфраструктур по заданным критериям оптимизации.

3.1.9 средства безопасности (security capability) [b-ISO 81001-1]: Широкая категория технических, административных или организационных средств управления рисками для конфиденциальности, целостности, готовности и подотчетности данных и систем.

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

3.1.11 система (system) [b-ISO/IEC 27000]: Приложения, услуги, информационно-технологические ресурсы или другие средства обработки информации.

3.1.12 угроза (threat) [b-ITU-T X.1406]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.1.13 виртуализированная сетевая функция (virtualized network function) [b-ITU-T Y.3150]: Сетевая функция, функциональное программное обеспечение которой отделено от аппаратного обеспечения и выполняется на виртуальной машине (машинах).

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 домен (domain): Группа имеющих отношение к сети IMT-2020 сетевых объектов, объединенных по физическим или логическим признакам.

3.2.2 система связи IMT-2020 (IMT-2020 communication system): Система управления процессами связи IMT-2020 для услуг IMT-2020.

ПРИМЕЧАНИЕ 1. – В контексте МСЭ-Т термин "5G" относится к IMT-2020.

ПРИМЕЧАНИЕ 2. – В настоящей Рекомендации термин "система связи IMT-2020" идентичен термину "система IMT-2020".

3.2.3 экосистема IMT-2020 (IMT-2020 ecosystem): Ряд заинтересованных сторон, которые взаимодействуют в целях создания стабильно функционирующей системы IMT-2020.

ПРИМЕЧАНИЕ. – Это относится главным образом к технологии связи IMT-2020, в рамках которой сообщество, включающее производителей, потребителей и поставщиков, вкладывает огромное количество продуктов, технологий и опыта для обеспечения работы системы IMT-2020 на разных уровнях, таких как уровни инфраструктуры, сети, платформы, услуг и приложений.

3.2.4 услуга IMT-2020 (IMT-2020 service): Преимущество, предоставляемое экосистемой IMT-2020.

3.2.5 атака переполнения таблицы потоков (flow table overflow attacks): Атака, при которой используются таблицы потоков, инициирующие передачу и обработку пакетов потоков, что приводит к тому, что другим потокам не остается места для установки правил потоков, вследствие чего возникает отказ в обслуживании (DoS) сети.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

4G	Fourth Generation of Mobile Communication Technology	Четвертое поколение технологий подвижной связи
AMF	Access and Mobility management Function	Функция управления доступом и мобильностью
API	Application Programming Interface	Интерфейс прикладных программ
AUSF	Authentication Server Function	Функция сервера аутентификации
C-PDU	Control Protocol Data Unit	Блок данных протокола управления
CU/DU	Central Unit/Distributed Unit	Центральный блок/распределенный блок
DCI	Data Centres Interconnect	Соединение центров обработки данных
DDoS	Distributed Denial-of-Service	Распределенный отказ в обслуживании
DoS	Denial-of-Service	Отказ в обслуживании
eMBB	enhanced Mobile Broadband	Усовершенствованная подвижная широкополосная связь
FAT	File Allocation Table	Таблица размещения файлов
IMSI	International Mobile Subscriber Identity	Международный идентификатор абонента подвижной связи
IMT-2020	International Mobile Telecommunications-2020	Стандарт "Международная подвижная электросвязь-2020"
IoT	Internet of Things	Интернет вещей
LTE	Long-Term Evolution	Стандарт "долгосрочное развитие"
MAC	Message Authentication Code	Код аутентификации сообщений
MEC	Multiaccess Edge Computing	Периферийные вычисления с множественным доступом
MEHW	Mobile Equipment Hardware	Оборудование подвижной связи
mIoT	massive Internet of Things	Массовый интернет вещей
mMTC	massive Machine-Type Communications	Массовая связь машинного типа
MNO	Mobile Network Operator	Оператор сети подвижной связи

NAS	Non-Access Stratum	Уровень "без доступа"
NF	Network Function	Сетевая функция
NFV	Network Function Virtualization	Виртуализация сетевых функций
NFVI	Network Functions Virtualization Infrastructure	Инфраструктура виртуализации сетевых функций
NRF	Network Function Repository Function	Функция хранилища сетевых функций
OAM	Operation, Administration, and Management	Эксплуатация, администрирование и управление
O&M	Operations And Management	Эксплуатация и управление
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PSK	Pre-Shared Key	Предварительно переданный ключ
RA/CA	Registration Authority and Certification Authority	Орган регистрации и орган сертификации
RRC	Radio Resource Control	Управление радиоресурсами
SBA	Service-Based Architecture	Архитектура на основе услуг
SBI	Service-Based Interface	Интерфейс на основе услуг
SDN	Software-Defined Networking	Сеть с программируемыми параметрами
SMF	Session Management Function	Функция управления сеансом
SQL	Structured Query Language	Структурированный язык запросов
SSL	Secure Sockets Layer	Протокол защищенных сокетов
TA	Trust Anchor	Точка доверия
TLS	Transport Layer Security	Безопасность транспортного уровня
TMSI	Temporary Mobile Subscriber's Identity	Временный идентификатор абонента подвижной связи
TPM	Trusted Platform Module	Модуль доверенной платформы
UDM	Unified Data Management	Единое управление данными
UE	User Equipment	Абонентское оборудование
UICC	Universal Integrated Circuit Card	Универсальная карта с интегральной схемой
URLLC	Ultra-Reliable and Low-Latency Communications	Сверхнадежная связь с короткой задержкой
USIM	Universal Subscriber Identity Module	Универсальный модуль идентификации абонента
VM	Virtual Machine	ВМ Виртуальная машина
VNF	Virtual Network Function	Функция виртуальной сети
VoIP	Voice over Internet Protocol	Передача голоса по протоколу Интернет

5 Соглашения

В настоящей Рекомендации ключевое слово "следует" ("рекомендуется") обозначает спецификацию, которая рекомендована, но не является абсолютно необходимой. Поэтому для заявления о соответствии эта спецификация не обязательна.

6 Обзор вопросов безопасности для системы связи IMT-2020

6.1 Упрощенная архитектура IMT-2020

В этом пункте дается обзор элементов безопасности системы связи IMT-2020. Для подключенных устройств IoT и мобильных приложений необходим беспроводной доступ к сети, который должен быть устойчивым, безопасным и надежным. Эти требования высокого уровня рекомендуется учитывать при проектировании системы связи IMT-2020.

Система связи IMT-2020 состоит из устройств, подключенных к сети доступа IMT-2020, которая, в свою очередь, подключена к остальной части системы, называемой базовой сетью IMT-2020.

На рисунке 1 показана упрощенная архитектура системы 5G 3GPP. Сеть доступа IMT-2020 включает в себя базовые радиостанции 3GPP и/или сеть доступа не-3GPP. Архитектура базовой сети IMT-2020 значительно превосходит архитектуру 4G с точки зрения возможности поддержки облачной реализации и интернета вещей (IoT) при существенных усовершенствованиях, таких как возможность нарезки сети и архитектура на основе услуг (SBA).

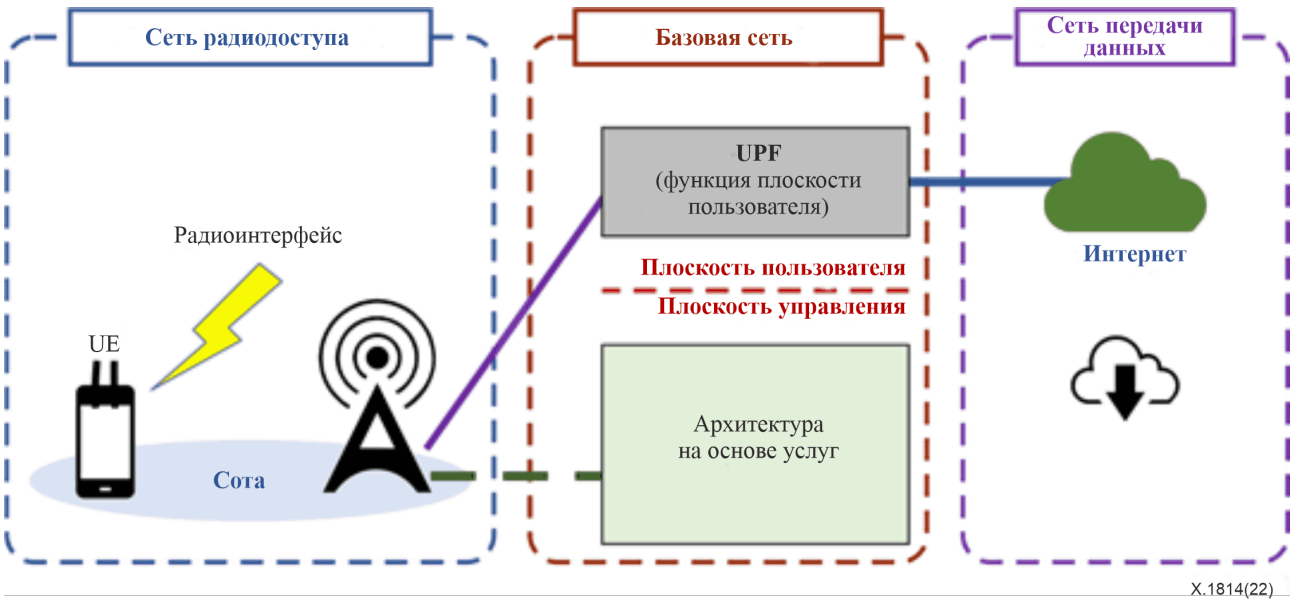

Рисунок 1 – Упрощенная архитектура IMT-2020

6.2 Общая архитектура системы IMT-2020

Система IMT-2020 предназначена для предоставления широкого спектра услуг с различными требованиями к их характеристикам. В соответствии со спецификациями 3GPP услуги, предоставляемые в сетях IMT-2020, можно разделить на три категории: 1) услуги усовершенствованной подвижной широкополосной связи (eMBB) – поддерживают более высокие скорости передачи данных и большую мобильность пользователей, чем технология подвижной связи четвертого поколения/сеть на основе стандарта "долгосрочное развитие" (4G/LTE); 2) услуги массового интернета вещей (mIoT) – обеспечивают массовую связь машинного типа; 3) услуги сверхнадежной связи с короткой задержкой (URLLC) – поддерживают критически важные услуги, для которых требуются повышенная надежность и короткая задержка. Система IMT-2020 должна стать гибкой платформой, позволяющей создавать новые бизнес-модели и интегрировать вертикальные отрасли, такие как автомобилестроение, промышленное производство, энергетика, электронное здравоохранение и развлечения. Кроме того, должны упроститься развертывание и обслуживание системы IMT-2020 по сравнению с сетями подвижной связи предыдущих поколений.

Для удовлетворения этих сложных требований в системе IMT-2020 представлен ряд инновационных технологий, таких как нарезка сети, виртуализация сетевых функций (NFV), сети с программируемыми параметрами (SDN), SBA и разделение на центральный и распределенный блоки (CU/DU).

Общая архитектура системы IMT-2020 [b-ITU-T X.1811] показана на рисунке 2 и включает в себя, исходя из требуемых функциональных возможностей, следующие уровни: транспортный уровень, сетевой уровень, уровень обслуживания и плоскость управления.

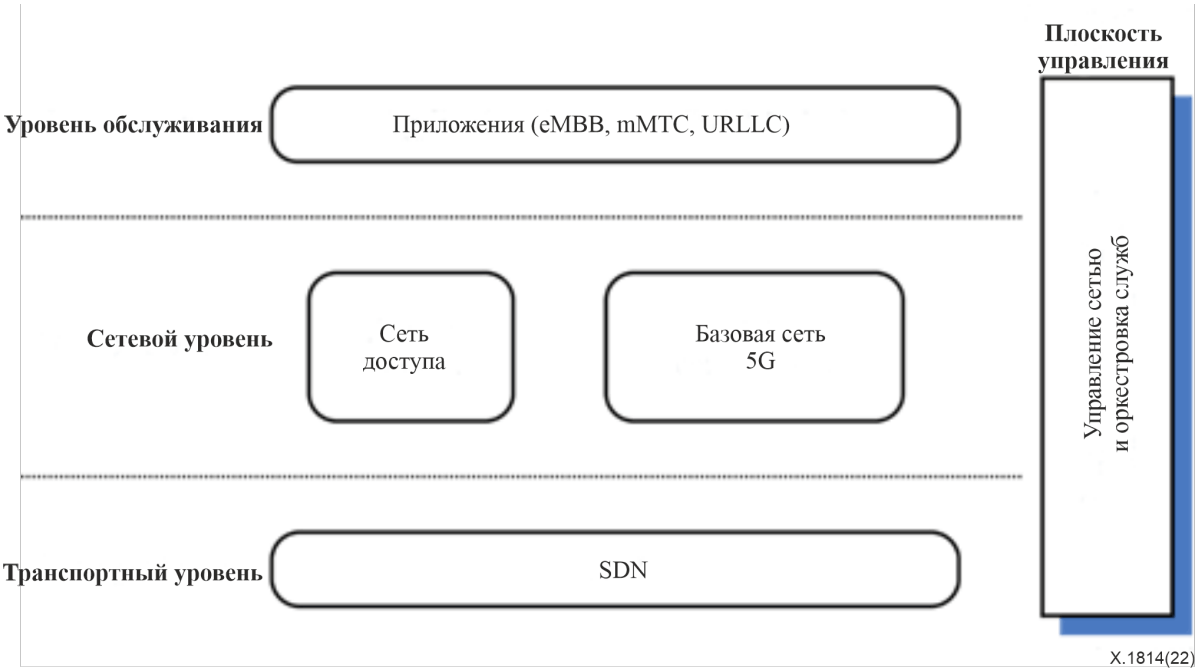

Рисунок 2 – Общая архитектура системы IMT-2020 [b-ITU-T X.1811], [b-TS 33.501]

- Транспортный уровень используется для транспортировки пакетов между источником и пунктом назначения. К традиционным технологиям транспортировки (например, многопротокольная коммутация с использованием меток) в системе IMT-2020 добавлена технология SDN для повышения скорости транспортировки и упрощения адаптации к требованиям к обслуживанию.
- Сетевой уровень состоит из сети доступа и базовой сети. Первая позволяет UE получить доступ к сети IMT-2020. Вторая разработана с учетом SBA для обеспечения расширяемости и простоты. Она состоит из ряда сетевых функций для поддержки передачи данных и развертывания служб. Примерами сетевых функций могут служить функция сервера аутентификации (AUSF), функция управления доступом и мобильностью (AMF) и функция управления сеансом (SMF).
- Уровень обслуживания состоит из приложений, работающих поверх системы IMT-2020, которые могут быть приложениями eMBB, mMTC или URLLC.
- Плоскость управления отвечает за управление сетью и оркестровку служб.

6.3 Домены системы IMT-2020

Безопасность IMT-2020 следует определять в соответствии с доменами, уровнями, требованиями безопасности и средствами обеспечения безопасности.

Домен – это группа имеющих отношение к сети IMT-2020 сетевых объектов, объединенных по физическим или логическим признакам. Для описания аспектов нарезки сети используется концепция домена нарезки. Домен может представлять собой различные функциональные возможности, службы и участников сетей IMT-2020. На рисунке 3 приведена блок-схема типичного домена IMT-2020.

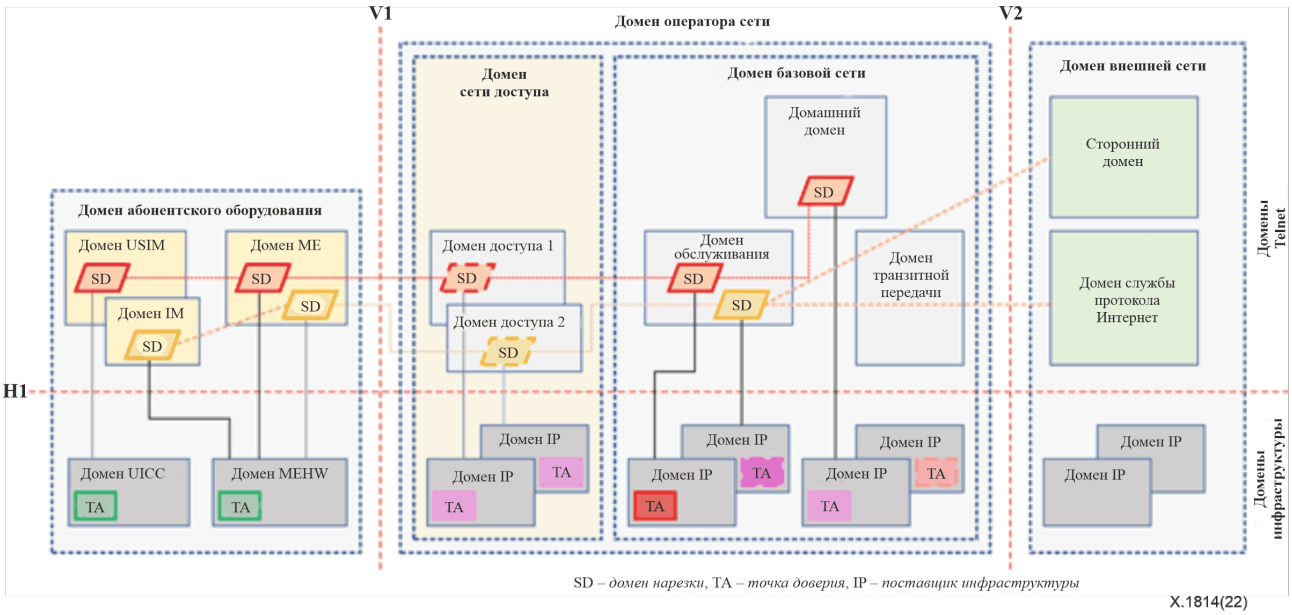

Рисунок 3 – Типичные домены IMT-2020

Элементы сети, расположенные выше линии H1 на рисунке 3, представляют собой аспекты логической сети, называемые доменами арендаторов, а элементы, расположенные ниже линии H1, – аспекты физической сети, называемые доменами инфраструктуры. Линия V1 отделяет домен абонентского оборудования (UE) от домена сети доступа, а линия V2 дополнительно отделяет домен базовой сети от домена внешней сети, например службы протокола Интернет, используемой сетью оператора.

Домены инфраструктуры содержат элементы сети, реализованные аппаратным и программным обеспечением, и выступают в качестве поставщика инфраструктуры. Сюда относятся как гипервизоры (программное обеспечение, которое создает и запускает виртуальные машины), так и точки доверия (авторитетные объекты, которые считаются заслуживающими доверие и не являются производными чего бы то ни было) [b-ITU-T X.509].

На стороне UE ниже линии H1 домены UE состоят из универсальной карты с интегральной схемой (UICC), которая представляет собой модуль, защищенный от несанкционированного доступа, и домена оборудования подвижной связи (MEHW), который осуществляет аппаратную поддержку, включая доверенную среду исполнения.

На стороне сети ниже линии H1 имеется домен поставщика инфраструктуры (IP), который состоит как из аппаратных средств (радио) доступа, так и из аппаратных средств для вычислений, хранения данных и сетевых ресурсов, необходимых для реализации базовых функциональных возможностей.

Точки доверия (TA) используются для обеспечения доверия виртуализированным системам. Сюда относится обеспечение целостности домена арендатора и того, что домен арендатора работает в предназначенной для него надежной инфраструктуре. TA также можно использовать для проверки целостности домена инфраструктуры и для привязки доменов арендаторов к доменам инфраструктуры.

Домены арендаторов содержат несколько логических доменов, использующих домены инфраструктуры, например для выполнения своих функций. Со стороны UE они состоят из оборудования подвижной связи, универсального модуля идентификации абонента (USIM), одного из нескольких программных приложений, которые находятся в аппаратной части, называемой UICC, хранящей информацию, относящуюся к абоненту, и обеспечивающей функции безопасности, относящиеся к аутентификации и шифрованию на стороне пользователя и в домене управления идентификацией. К доменам арендатора на стороне сети относятся домен доступа (A), домен обслуживания (S), домашний домен (H), домен транзитной передачи (T), сторонний домен (3P), служба протокола Интернет и домен управления (M).

6.4 Общие требования и средства безопасности

В данном разделе содержится краткое описание общих параметров (требований) безопасности, определенных в [b-ITU-T X.805]. Его целью является обеспечение основы для средств безопасности системы IMT-2020. В Дополнении I представлена общая архитектура безопасности сети для обеспечения сквозной безопасности сети.

Уровень безопасности относится к иерархии сетевого оборудования и совокупностям средств [b-ITU-T X.805]. Уровень безопасности состоит из совокупности протоколов, данных и функций, связанных с одним аспектом услуг, предоставляемых одним или несколькими доменами. Уровень архитектуры безопасности IMT-2020 обеспечивает общее представление протоколов, данных и функций, связанных между собой в том смысле, что они подвергаются воздействию общей среды угроз и предъявляют схожие требования безопасности. Распространенными угрозами для связи между UE и сетью радиодоступа являются радиопомехи, атаки подложных базовых станций, ввод данных в плоскость пользователя через радиоинтерфейс и поддельные сообщения управления радиоресурсами (RRC). С другой стороны, распространенными угрозами для связи между UE и базовой сетью являются отслеживание идентификаторов подписки, подделка сообщений плоскости управления, подделка функций безопасности и т. д. Примерами распространенных угроз для служб управления в сетях IMT-2020 являются несанкционированное изменение конфигурации, взлом сетевых ключей и сертификатов и динамическое добавление вредоносных сетевых функций. Уровень управления включает аспекты, связанные с обычным управлением сетью (настройка конфигурации, обновление программного обеспечения, управление учетными записями пользователей, ведение/анализ журналов регистрации событий и т. д.) и, в частности, аспекты управления безопасностью (контроль безопасности, управление ключами и сертификатами и т. д.). Кроме того, к этому уровню относятся аспекты, связанные с управлением виртуализацией и созданием/составлением услуг (оркестровка, управление нарезкой сети, изоляция и управление виртуальными машинами (ВМ) и т. д.).

Область безопасности шире доменов безопасности, к ней относятся требования безопасности одного или нескольких уровней или доменов.

Средства обеспечения безопасности в целом определяются как широкая категория технических, административных или организационных средств управления рисками для конфиденциальности, целостности, готовности и возможности учета данных и систем [b-ISO 81001-1]. Это набор функций и механизмов безопасности (включая защитные меры и контрмеры), относящихся к одному и тому же аспекту безопасности, например обеспечению целостности. Они содержат функции и механизмы безопасности для предотвращения, обнаружения, сдерживания, противодействия и минимизации рисков безопасности для сетей IMT-2020, в частности рисков для физической и логической инфраструктуры сети, ее служб, UE, сигнализации и данных. В таблице 1 представлены требования безопасности для доменов безопасности.

Таблица 1 – Требования безопасности для каждой области безопасности

Область безопасности	Требования безопасности
Сеть доступа	Требования безопасности, относящиеся к уровню и домену доступа, направлены на устранение угроз, связанных с этим доменом. Примерами таких требований могут служить защита конфиденциальности и целостности данных плоскости пользователя и плоскости управления, так же как и обеспечение безопасной подвижной связи
Приложения и услуги	Требования безопасности для уровня приложений, предоставляющего приложения и услуги для конечных пользователей (например, VoIP, VoLTE), направлены на устранение угроз, относящихся к этому домену. Примерами таких требований могут служить аутентификация и авторизация пользователей приложений и безопасный поиск услуг
Управление	Требования безопасности для уровня управления и домена управления направлены на устранение угроз, связанных с этим доменом, включая управление для обеспечения безопасности (например, безопасные обновления, безопасная оркестровка) и управление средствами безопасности (мониторинг, управление ключами и доступом)

Таблица 1 – Требования безопасности для каждой области безопасности

Область безопасности	Требования безопасности
UE	Требования безопасности, относящиеся к домену UE, включая управление доступом к устройствам, направлены на устранение угроз, связанных с этим доменом. Примерами таких требований могут служить взаимная аутентификация в сети и безопасное хранение контекста безопасности
Сеть	Определены требования безопасности, относящиеся к базовой сети и связи между сетью оператора и внешними сетями, включая аспекты, связанные с безопасным обменом данными сигнализации и конечных пользователей между узлами в доменах оператора и внешних сетей. Примерами могут служить обеспечение безопасности сети, конфиденциальности абонентов и аутентификации абонентов
Инфраструктура и виртуализация	Определены требования безопасности домена IP, например для аттестации, безопасной нарезки/изоляции и обеспечения доверия между доменами арендаторов, а также между доменами арендаторов и доменами инфраструктуры

В таблице 2 описаны средства безопасности для каждого параметра безопасности [b-ITU-T X.805]. Семь из них, а именно управление идентификацией и доступом, аутентификация, предотвращение непризнания участия, конфиденциальность, целостность, готовность и неприкосновенность частной жизни, были заимствованы из [b-ITU-T X.805]. Остальные три, а именно аудит [b-ITU-T X.800], достоверность и надежность и соответствие представляют собой параметры безопасности в архитектуре безопасности IMT-2020.

Таблица 2 – Средства обеспечения безопасности

Параметры безопасности	Средства обеспечения безопасности
Управление идентификацией и доступом	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры) для управления доступом и управления учетными данными и ролями
Аутентификация	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры) при аутентификации, которые служат для проверки достоверности атрибутов аутентификации пользователя, таких как заявленная идентичность
Предотвращение непризнания участия	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для службы предотвращения непризнания участия, которая защищает от ложного отказа от причастности к конкретному действию
Конфиденциальность	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для службы обеспечения конфиденциальности, которая защищает данные от несанкционированного раскрытия
Целостность	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для службы целостности, которая препятствует созданию или изменению данных
Готовность	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для обеспечения готовности ресурсов даже в случае атак. Сюда же относятся механизмы аварийного восстановления

Таблица 2 – Средства обеспечения безопасности

Параметры безопасности	Средства обеспечения безопасности
Неприкосновенность частной жизни	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для службы обеспечения неприкосновенности частной жизни, которые служат для предоставления объектам права определять, в какой мере они будут взаимодействовать и обмениваться информацией, позволяющей установить личность
Аудит	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для службы аудита, которая обеспечивает анализ и изучение записей и действий системы в целях определения адекватности ее функциональных возможностей и выявления нарушений. Сюда же относится аудит в целях сбора данных
Достоверность и надежность	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для службы гарантии достоверности и надежности, которая осуществляет передачу информации о надежности системы
Соответствие	Эти средства обеспечения безопасности относятся к набору функций и механизмов обеспечения безопасности (включая защитные меры и контрмеры), предназначенных для службы обеспечения соответствия, которая позволяет объекту или системе выполнять договорные или нормативные требования

7 Компоненты и надежность системы связи IMT-2020

7.1 Компоненты системы IMT-2020

Для подключенных устройств IoT и мобильных приложений необходим беспроводной доступ к сети, который должен быть устойчивым, безопасным и способным обеспечить защиту конфиденциальности отдельных пользователей. Систему связи IMT-2020 следует проектировать так, чтобы она соответствовала требованиям, описанным в пунктах 7.8 и 7.9 [b-ITU-T Y.3101]. Сеть IMT-2020 состоит из четырех компонентов: UE, сети радиодоступа, транспортной сети и базовой сети, которые показаны на рисунке 4.

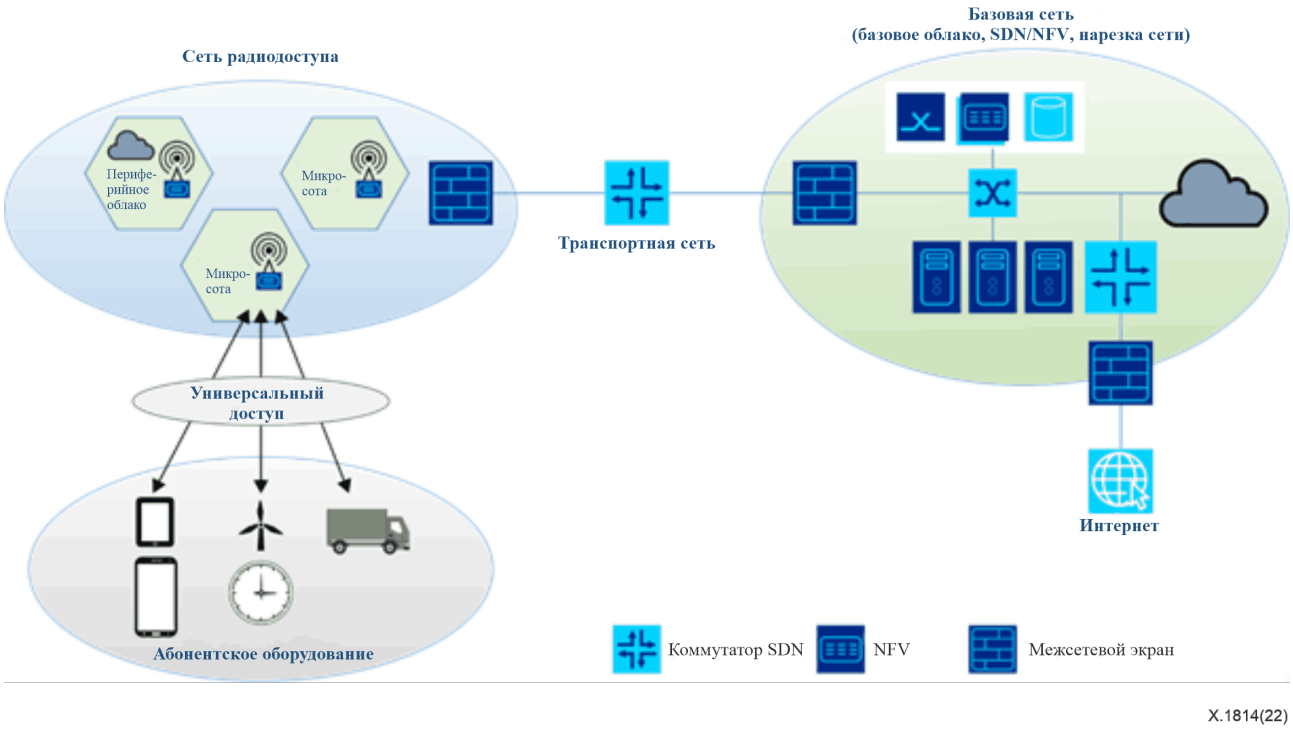

Рисунок 4 – Сеть связи IMT-2020 (по материалам [b-ITU workshop])

Система IMT-2020 строится на принципах мобильных облаков, SDN, NFV и нарезки сети для решения задач, связанных с массовым подключением, обеспечением гибкости и минимизацией затрат. Следовательно, необходимо определить меры безопасности для NFV, нарезки сети и периферийных облачных вычислений.

NFV изолирует сетевые функции от проприетарных устройств и выполняет их с помощью программного обеспечения на виртуальных машинах.

Функция виртуальной сети (VNF) представляет собой логический результат NFV, которая является сетевой функцией, программное обеспечение которой изолировано от оборудования и выполняется на виртуальной машине (машинах) (VM) [b-ITU-T Y.3100]. VNF выполняют определенные сетевые функции, такие как межсетевые экраны, коммутаторы, системы обнаружения вторжений и системы предотвращения вторжений.

Нарезка сети – это форма архитектуры виртуальной сети, использующая принципы, на которых основаны SDN и NFV в сетях фиксированной связи. Сети IMT-2020 подразделяются на отдельные виртуальные сети, называемые отрезками сети, каждая из которых оптимизирована для одного проекта. Они могут охватывать несколько доменов сети, включая домены сети доступа и базовой и транспортной сетей, и развертываться несколькими операторами, как показано на рисунке 5.

SDN – это архитектура, призванная сделать сети динамичными и гибкими. Задача SDN – улучшить контроль над сетью, позволяя компаниям и поставщикам сетевых услуг быстро реагировать на изменяющиеся требования.

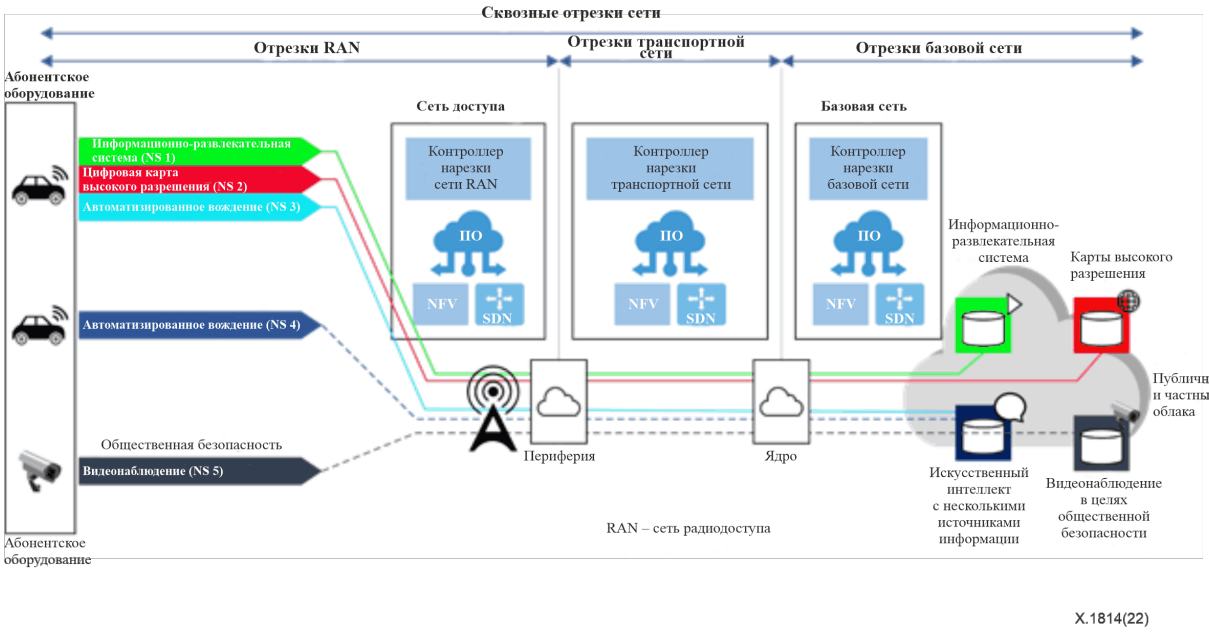

Рисунок 5 – Отрезки сети IMT-2020

Транспортная сеть IMT-2020 представляет собой инфраструктуру транспортной IP-сети, обеспечивающую подвижную связь IMT-2020.

Периферийные вычисления позволяют использовать возможности облачных вычислений на периферии сети IMT-2020. Периферийные вычисления – это парадигма распределенных вычислений, в которой вычисления в значительной степени или полностью выполняются в распределенных аппаратных узлах, называемых интеллектуальными устройствами или периферийными устройствами, в отличие от тех, которые выполняются главным образом в централизованной облачной среде. Периферийные вычисления приближают процессы обработки и хранения данных к оборудованию. Это позволяет устройствам IoT предоставлять свои услуги с короткой задержкой.

7.2 Надежность системы связи IMT-2020

Надежность системы связи IMT-2020 является следствием пяти характеристик, а именно устойчивости, безопасности связи, управления определением идентичности, обеспечения конфиденциальности и гарантии безопасности.

- Устойчивость – это способность организации противостоять влиянию различных сбоев. Множество дополнительных и частично перекрывающихся функций в IMT-2020 могут способствовать достижению устойчивости системы связи IMT-2020 к кибератакам и непредвиденным инцидентам.
- Безопасность связи относится к передаче данных в IMT-2020. В системе связи IMT-2020 безопасная связь с устройствами и собственной инфраструктурой имеет исключительно важное значение.
- Управление определением идентичности – это процессы и правила, участвующие в управлении жизненным циклом, а также ценность, типы и дополнительные метаданные атрибутов идентичности объектов, известных как домены IMT-2020. Должно быть обеспечено безопасное управление определением идентичности для идентификации и аутентификации абонентов, как находящихся, так и не находящихся в роуминге, для гарантии того, что только подлинные абоненты могут получить доступ к услугам сети. Оно должно опираться на сильные криптографические примитивы и характеристики безопасности.
- Обеспечение конфиденциальности – 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. Обеспечение конфиденциальности направлено на защиту информации, позволяющей установить личность (PII), которая может использоваться неавторизованными сторонами для установления личности абонентов.

- Гарантия безопасности. Гарантия безопасности – это 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, полученное в результате безопасных процессов разработки и управления жизненным циклом продуктов.

8 Угрозы компонентам и функциям

На рисунке 6 показаны типовые угрозы для систем IMT-2020. Они подразделяются на три категории: общеизвестные угрозы, связанные с уязвимостями программного обеспечения, ошибками конфигурации и лавинными атаками; угрозы из-за совместного использования инфраструктуры и угрозы на сетевом уровне, такие как угрозы, связанные с SDN, NFV, нарезкой сети и облачными вычислениями.

X.1814(22)

Рисунок 6 – Примеры угроз в системе IMT-2020 [b-ITU workshop]

8.1 Общие угрозы

В [b-ENISA] определены следующие общие угрозы.

- **Отказ в обслуживании (denial-of-service (DoS))** [b-ENISA] – эта атака направлена на то, чтобы сделать сетевой ресурс недоступным для предполагаемых пользователей, временно или постоянно вмешиваясь в работу сетевой службы или нарушая ее посредством переполнения огромным количеством запросов. К отказу в обслуживании могут привести такие угрозы самых разнообразных типов, как, например, лавинные атаки, штурм сигнализации и атаки насыщения. К популярным DoS-атакам относятся: 1) атаки с переполнением буфера – наиболее распространенная DoS-атака. Идея состоит в том, чтобы направить на сетевой адрес больший трафик, чем тот, на который рассчитана система. Сюда входят атаки, перечисленные ниже, а также другие атаки, использующие ошибки, характерные для определенных приложений или сетей; 2) лавина ICMP-пакетов – использует неправильно сконфигурированные сетевые устройства, направляя поддельные пакеты, пингующие не одну конкретную машину, а каждый компьютер в целевой сети. В этом случае сеть начинает усиливать трафик. Эту атаку еще называют смурф-атакой или атакой ping of death; 3) синхронная атака направляет запрос на подключение к серверу, но не завершает установление соединения. Так продолжается до тех пор, пока все открытые порты не будут заполнены запросами и доступных портов для подключения легитимных пользователей не останется.

- **Распределенный отказ в обслуживании (distributed-denial-of-service (DDoS))** [b-ENISA]. При DDoS-атаке множество систем атакуют одну с помощью DoS-атак, организуя синхронизированную DoS-атаку на одну и ту же цель. Существенное отличие состоит в том, что цель атакуется не из одного, а из многих мест одновременно.
- **Искажение, утечка, кража, уничтожение данных и манипулирование информацией** [b-ENISA]. Сюда относятся кража PII посредством несанкционированного доступа к системам и/или сети, несанкционированный доступ и, возможно, публикация личных/биометрических/медицинских данных, конфиденциальной информации организации или секретной государственной информации. Кража, взлом или утечка данных других типов, таких как учетные данные пользователей, ключи шифрования, журналы безопасности сетей, конфигурация программного обеспечения и т. д., также могут помочь злоумышленникам в проведении различных атак.
- **Подслушивание** [b-ENISA] – это термин, используемый для описания несанкционированного перехвата информации. Злоумышленник пытается проникнуть в различные элементы сети IMT-2020 (контроллер SDN, сетевую функцию, периферийный узел, оркестратор виртуализации) на уровне приложений или на уровне системы связи. Сюда относится перехват абонентских данных, конфиденциальной информации, системного времени, местонахождения абонента, электронных сообщений и информационных сигналов, передаваемых по сети. Злоумышленник следит, шпионит и/или подслушивает, чтобы определить местоположение организаций или получить доступ к конфиденциальной информации.
- **Эксплуатация уязвимостей программного и аппаратного обеспечения** [b-ENISA]. Угрозы этого типа позволяют злоумышленнику воспользоваться для организации атаки неизвестными (поставщику и пользователю) или известными, но неисправленными дефектами программного или аппаратного обеспечения. Примерами может служить использование известных дефектов аппаратного и программного обеспечения, таких как перегрузка сети и переполнение буфера. Сюда также относится использование других известных уязвимостей, связанных с системами подвижной связи предыдущих поколений.
- **Вредоносный код или вредоносное ПО** [b-ENISA]. Вредоносный код – это термин, используемый для описания любого кода в любой части системы программного обеспечения или сценария, предназначенного для создания нежелательных эффектов, нарушения безопасности или повреждения системы. К угрозам этого типа относятся установка и распространение вредоносного программного обеспечения или внедрение определенного кода или ПО в программный продукт или обновление. Примерами могут служить вредоносное ПО, программы-вымогатели, вирусы, черви, трояны, внедрение кода на языке SQL (язык структурированных запросов) [b-SQL], мошенническое ПО безопасности, а также ложное и филантропическое ПО. Примером вредоносного ПО в контексте IMT-2020 является использование неавторизованной VNF, способной незаконно устанавливаться и регистрироваться в базовой сети в целях предоставления API злоумышленникам.
- **Взлом сети системы снабжения, продавца или поставщика услуг** [b-ENISA]. Взлом сети системы снабжения, продавца или поставщика услуг позволяет внедрить в поставляемое изделие скрытое оборудование, вредоносное ПО или ПО с дефектами. Он также позволяет осуществлять неконтролируемые обновления ПО, манипулировать функциональными возможностями и внедрять функции для обхода механизмов контроля и лазейки.

  Если в процессах тестирования, технического обслуживания, настройки и эксплуатации изделия участвует ненадежный сторонний персонал, он сможет получить доступ к средствам управления сетью (локально или через удаленный интерфейс) для выполнения работ по техническому обслуживанию и оказанию технической поддержки. Привилегированный доступ к системе эксплуатации, администрирования и управления (OAM) сети предоставляет такому персоналу возможность получать различные данные, такие как данные об абонентах, конфигурации системы и сети, а также данные телеметрии.
- **Целенаправленные угрозы** [b-ENISA]. Целенаправленные угрозы исходят от вредоносных программ, нацеленных на конкретную организацию или отрасль. Они опасны, поскольку направлены на перехват конфиденциальной информации. Целью изощренных атак или высокоэффективных продолжительных угроз могут быть кража конфиденциальной информации или нарушение готовности конфиденциальных и критически важных служб.

- **Использование дефектов процедур безопасности, управления и эксплуатации** [b-ENISA]. Хотя эта угроза не имеет прямого отношения к IMT-2020, она становится актуальной, когда речь идет о сложности технологии и необходимости введения эксплуатационных процедур в процесс управления сетью. К угрозам этого типа, помимо прочего, относится использование недостатков в управлении эксплуатацией и безопасностью сети, управлении конфигурацией, обновлениями и исправлениями программного обеспечения. Ошибки из-за отсутствия эксплуатационных процедур и процедур безопасности или их неправильного проектирования могут иметь пагубные последствия для целостности и готовности сети систем.
- **Нарушение процесса аутентификации** [b-ENISA]. Эта угроза может воздействовать на различные точки входа в сеть, такие как абонентское оборудование (мобильные устройства и IoT), интерфейсы эксплуатации и управления, роуминг и отраслевые услуги. Она связана с использованием злоумышленниками таких методов нарушения аутентификации систем IMT-2020, как кража учетных данных пользователей, взлом учетных записей и паролей, маскировка личности пользователя и нарушение аутентификации групп IoT.
- **Кража или подделка учетных данных** [b-ENISA]. Кража представляет собой преднамеренное использование чужих учетных данных. Угроза заключается в том, что злоумышленник может определить учетные данные легитимного пользователя и осуществлять дальнейшие атаки от его имени. Подделка учетных данных – это действия по присвоению идентичности другого лица с последующим использованием этой идентичности для достижения своих целей. Это угроза, которая может затронуть любой программный компонент или любое лицо. Злоумышленник подменяет идентичность легитимного управляющего и взаимодействует с сетевыми функциями, контролируемыми легитимным управляющим (то есть с элементами плоскости данных), инициируя атаку другого типа (например, провоцирование сетевых потоков, отвод трафика). В качестве методов подделки или кражи учетных данных также могут применяться методы социальной инженерии и подбор пароля/взлом учетной записи пользователя. Например, для раскрытия учетной записи абонента могут использоваться атаки перехвата международного идентификатора абонента подвижной связи (IMSI) абонентского оборудования. Такие атаки также могут осуществляться путем установки поддельной базовой станции, которую UE, потерявшее доступ к временному идентификатору абонента подвижной связи (TMSI), считает предпочтительной базовой станцией. В ответ абонент передает свой IMSI. К тому же в сетях IMT-2020 участвуют различные стороны, такие как операторы виртуальных сетей подвижной связи (VMNO), поставщики услуг связи (CSP) и поставщики сетевой инфраструктуры.

8.2 Угрозы для абонентского оборудования

Ниже перечислены угрозы для безопасности UE.

- **Заражение вредоносным ПО** [b-ENISA]. Если на UE установлено вредоносное программное обеспечение, злоумышленник может использовать зараженное UE для запуска какой-либо атаки, такой как кража личных данных, хранящихся в UE, запуск DDoS или попытка заражения другого UE. Примерами вредоносного программного обеспечения могут служить вредоносные программы, программы-вымогатели, вирусы, черви, трояны и мошеннические средства безопасности. Мобильное устройство, зараженное вредоносным ПО, включается в бот-сеть.
- **Угроза бот-сетей** [b-Khan]. Бот-сети – это вредоносные программы, способные управлять группой подключенных к интернету устройств. Мобильные бот-сети могут автоматически запускать различные атаки на системы IMT-2020 (например, DoS), используя множество мобильных устройств. Поскольку IMT-2020 обеспечивает связь между мобильными телефонами с большой вычислительной мощностью, эти угрозы становятся все серьезнее. Кроме того, подключение IoT-устройств открывает возможности для угроз новых типов. Таким образом, устройства IoT уязвимы для атак бот-сетей IoT. Примером может служить бот-сеть Mirai, охватившая миллионы IP-камер в 2016 году.
- **Угрозы мобильных вредоносных программ** [b-Khan]. Мобильное вредоносное ПО позволяет злоумышленникам красть данные PII, хранящиеся на мобильных устройствах, и даже инициировать атаки (например, DoS-атаки) на другие объекты, такие как другое UE, сети подвижного доступа и базовые сети операторов подвижной связи.

- **Несанкционированный доступ к пользовательским и сигнальным данным, их уничтожение, раскрытие или изменение**. Злоумышленник может получить несанкционированный доступ к пользовательским и сигнальным данным, передаваемым между UE и базовой станцией нового поколения, или их уничтожить, раскрыть или модифицировать.
- **Фальсификация абонентских учетных данных**. Злоумышленник может подделать абонентские учетные данные, используемые для аутентификации и обеспечения конфиденциальности.

8.3 Угрозы для сетей доступа

Ниже перечислены угрозы для безопасности сетей доступа.

- **Злонамеренный или случайный всплеск трафика** [b-NGMN]. По мере увеличения пропускной способности сетей и количества элементов UE повышается риск значительных случайных или злонамеренных изменений поведения сетевого трафика в результате серьезных событий. При этих масштабах невозможно различить намерение всплесков сетевого трафика, поэтому предотвращение вредоносных событий является важной задачей, но включает оба сценария.
- **Утечка ключей между каналами связи разных операторов** [b-NGMN]. Ключ шифрования (а иногда и ключ целостности) радиоинтерфейса вычисляется в домашней базовой сети, а затем передается в гостевую беспроводную сеть по каналу сигнализации, такому как SS7 (система сигнализации № 7) [b-ITU-T Q.700] или Diameter [b-RFC 3588]. Это очевидная точка воздействия и возможное место утечки ключей.
- **Взлом плоскости пользователя** [b-NGMN]. Существует угроза перехвата всего сеанса связи и его использования для внедрения в подвижное соединение подложных данных (или потери данных в результате их передачи в потерянную конечную точку обслуживания).
- **Необязательная реализация средств безопасности** [b-Khan], [b-NGMN]. Эта угроза возникает из-за необязательной реализации средств безопасности. Существует множество правил безопасности, которые не влияют на функциональное взаимодействие (в основном на взаимодействие с UE), и традиционно соответствующие средства безопасности рассматривались как не обязательные к применению. Такой вариант может привести к рискам, которым оператор подвергается не по своей вине, а из-за действий других операторов. Это также ставит под угрозу предположения о безопасности на уровне системы. Без этого этапа аутентификации уровень ключей не может достичь одной из своих целей, то есть защитить клиентов от дефектных базовых станций.
- **Угрозы, основанные на ложных отчетах о состоянии буфера** [b-Khan]. Для достижения своих злонамеренных целей злоумышленники могут использовать отчеты о состоянии буфера компонентов сети доступа, таких как базовые станции, чтобы получить такую информацию, как планирование пакетов, выравнивание нагрузки и алгоритмы управления доступом. Затем они могут от имени законного UE передавать ложные отчеты о состоянии буфера, ставя под угрозу работу сети.
- **Угрозы внедрения сообщений** [b-Khan]. Внедрение сообщений позволяет запускать DoS-атаки в сетях IMT-2020. Например, может быть перегружено устройство SDN с некорректным обновлением таблицы потоков. Злоумышленник также может внедрить в систему во время ее выхода из спящего режима блоки данных протокола управления (C-PDU) для выполнения DoS-атак на вновь прибывающее UE.
- **Угрозы со стороны микросот** [b-Khan]. Физический размер базовых станций существенно сократился, и теперь они размещаются в помещениях, таких как торговые центры, общественные учреждения, стадионы и больницы. Кроме того, использование новых частот, таких как частота mmWave, также облегчает использование этих базовых микростанций. Однако физически они не так безопасны, как базовые макростанции, использовавшиеся в сетях, предшествующих IMT-2020. Более того, с увеличением количества базовых станций увеличивается число потенциальных уязвимостей в сетях IMT-2020.

- **Перехват сеанса** [b-ENISA]. Перехват сеанса радиоинтерфейса – это атака, при которой злоумышленник перехватывает абонентский сеанс связи. Если легитимный аутентифицированный сеанс перехвачен, злоумышленник контролирует весь сеанс передачи определенного трафика и может проводить атаки других типов.
- **Угрозы со стороны поддельной сети доступа** [b-ENISA]. Если взломана базовая станция, злоумышленник может провести атаку через посредника от имени легитимной базовой станции или изменить сетевой трафик. Эта атака ведет к фальсификации сеанса связи между мобильным UE и сетью в целях выполнения других действий.
- **Манипуляции с данными конфигурации сети доступа** [b-ENISA]. Если взломан элемент сети доступа, такой как базовая станция, злоумышленник может подделать данные конфигурации и выполнять другие атаки (например, DoS).
- **Угрозы перехвата идентификатора абонента (IMSI)** [b-ENISA]. Если используются протоколы сотового пейджинга, злоумышленник может связать программный идентификатор жертвы с событием пейджинга. Это позволит ему получать информацию о местоположении жертвы, внедрять сфабрикованные пейджинговые сообщения и запускать атаки типа отказ в обслуживании.
- **Нарушение обслуживания из-за подложного запроса на установление RRC-соединения.** Если злоумышленник подделал сообщение с запросом на установление RRC-соединения, переданное открытым текстом, он может использовать временную идентификационную информацию жертвы для дальнейшей блокировки ее сетевого соединения. Подробный сценарий такой атаки описан в Дополнении II.

8.4 Угрозы для сетей с программируемыми параметрами

Угрозы для SDN описаны в [ITU-T X.1038].

8.5 Угрозы для базовой сети

Ниже перечислены известные угрозы для безопасности базовой сети.

- **DDoS** [b-Khan]. Атаки DDoS могут осуществляться в форме усиления сигнализации и насыщения AUSF и UDM с помощью бот-сетей, контролирующих множество зараженных устройств UE.
- **Угрозы, связанные с протоколами безопасности транспортного уровня (TLS)/уровня защищенных разъемов (SSL)** [b-Khan]. Связь на основе протоколов TLS/SSL, используемых в базовых сетях SDN, уязвима для таких атак, как атаки TCP/SYN (синхронизированные) DDoS, искажение RC4 в TLS, атаки с использованием эксплойта браузера против SSL/TLS (BEAST), атаки с использованием алгоритмов сжатия данных CRIME (compression ratio info-leak made easy), атаки типа LUCKY 13 [b-Goodin] и атаки типа POODLE (padding oracle on downgraded legacy encryption) [b-Möller].
- **Сканирование SDN** [b-Khan]. Злоумышленник может проанализировать трафик SDN и вручную собрать информацию о сети, такую как протокол инфраструктуры и основные сетевые элементы контроллера SDN. Собранная информация может использоваться для различных атак, таких как атаки DoS, сброс TCP, повторная передача и спуфинг.
- **Злонамеренное перенаправление трафика** [b-ENISA]. Взлом элемента сети позволяет злоумышленникам перенаправлять потоки трафика и прослушивать сетевой трафик. Перенаправление трафика – это угроза, относящаяся к сетевым элементам плоскости данных. Типичным примером перенаправления трафика в виртуализированных сетях является проникновение в отрезок сети. Эта угроза возникает, когда в каком-либо активном узле нарушена изоляция между отрезками сети или когда обойден либо неправильно настроен принудительный доступ к отрезку сети в периферийном оборудовании.
- **Злонамеренное использование инструментов контроля** [b-ENISA]. Операторы сети используют инструменты контроля для мониторинга активности сети и получения информации, которую можно использовать для различных целей, таких как оптимизация, обеспечение безопасности или коммерческие цели. Злоумышленники могут воспользоваться программными инструментами этого типа для целей зондирования перед атакой.

Для получения конфиденциальной информации обычно используют инсайдера оператора мобильной сети (MNO), имеющего привилегированный доступ к таким инструментам.

- **Утечка долговременного ключа к данным аутентификации/авторизации пользователя** [b-ENISA]. Эта угроза связана с раскрытием долгосрочных ключей аутентификации и средств обеспечения безопасности, осуществляемым через инсайдера либо враждебно настроенного или нелояльного сотрудника, работающего с базовой сетью.
- **Эксплуатация неправильно настроенных или плохо сконфигурированных систем/сетей** [b-ENISA]. Если системы и сети неправильно настроены или плохо сконфигурированы, злоумышленники могут получить доступ к критически важным ресурсам. Воспользовавшись системой, которая без злого умысла была неправильно настроена, злоумышленник может получить доступ к критически важным ресурсам сети. Ошибки конфигурации могут возникать на разных этапах жизненного цикла системы, например в процессе установки и технического обслуживания.
- **Анализ трафика** [b-ENISA]. Используемый злоумышленниками анализатор (сниффер), представляет собой программный или аппаратный инструмент для перехвата, регистрации и анализа сетевого трафика и данных. С помощью анализа злоумышленник также может перехватывать данные из элементов сети или компоновать и красть конфиденциальную информацию. Анализ может осуществляться везде, где имеется постоянный трафик.
- **Регистрация вредоносных сетевых функций** [b-ENISA]. Эта угроза возникает, когда в сети IMT-2020 устанавливаются вредоносные сетевые функции. Несанкционированная сетевая функция или функция, содержащая троянского коня, внедренная в сеть инсайдером (оператора подвижной связи) или продавцом/поставщиком услуг, может быть неправомерно установлена в SBA и зарегистрирована в базовой сети через функцию репозитория сетевых функций (NRF), чтобы установить другие вредоносные API. Установив или активировав несанкционированную сетевую функцию (NF), злоумышленник может получить доступ к конфиденциальным ресурсам сети для осуществления других атак, таких как отказ в обслуживании, распространение вредоносного программного обеспечения или кража конфиденциальной информации.
- **Небезопасное предоставление сетевых функций для функции сторонних приложений** [b-Ta-Hao Ting]. Предоставление сетевых функций внутренней сети для решения задач внешней сети позволяет динамично и гибко развертывать сети IMT-2020. Если же сообщение подделано или изменено, оно причинит ущерб всей базовой сети.
- **Небезопасный интерфейс на основе услуг** [b-TS 33.501]. Вмешательство в сообщение, переданное через интерфейс на основе услуг (SBI) между элементами сети, может привести к его изменению или раскрытию.

8.6 Угрозы, связанные с нарезкой сети

Ниже перечислены угрозы, связанные с нарезкой сети.

- **Угрозы для межсетевого обмена данными отрезков сети** [b-Khan]. Злоумышленник может нарушить сообщение между отрезками сети, воспрепятствовав надлежащему управлению их жизненным циклом.
- **Атака под видом законного пользователя** [b-Khan]. Злоумышленник может попытаться выделить недоступные ресурсы, выдавая себя за физическую хост-платформу. Более того, выдав себя за менеджера отрезка сети, он может попытаться похитить параметр создания отрезка сети.
- **Несоблюдение правил безопасности** [b-Khan]. Наличие разных правил и протоколов безопасности для разных отрезков сети позволяет злоумышленникам получить доступ к системе нарезки сети и управлять объектами через наименее защищенный отрезок.
- **DoS** [b-Khan]. Злоумышленник предпринимает DoS-атаку на виртуализированную сеть или на физические ресурсы, чтобы исчерпать доступные сетевые ресурсы для других отрезков сети.
- **Побочный канал** [b-Khan]. Злоумышленник получает доступ к одному отрезку сети и атакует ряд отрезков сети, пользующихся одним и тем же базовым оборудованием.

- **Утечка конфиденциальной информации** [b-Khan]. Поставщики инфраструктуры или VNF крадут информацию о пользователях из разных отрезков сети.
- **Угрозы, связанные с гипервизором** [b-Khan]. Атаки на гипервизор в целях нарушения виртуализации ресурсов. К этим атакам относятся ошибки программирования гипервизора, лазейка через операционную систему хостинга, DoS-атаки и атаки на аппаратные ресурсы.

8.7 Угрозы для периферийных вычислений с множественным доступом

Ниже перечислены известные угрозы для периферийных вычислений.

- **Ложный или мошеннический шлюз MEC** [b-ENISA]. Открытый характер периферийных шлюзов позволяет создать сценарий атаки, при котором злоумышленники устанавливают свои собственные шлюзовые устройства. Эта угроза приводит к тому же эффекту, что и атака через посредника.
- **Перегрузка периферийного узла** [b-ENISA]. Если определенные мобильные приложения или устройства IoT инициируют бомбардировку периферийного узла запросами или трафиком в адрес этого компонента, может произойти перегрузка периферийного узла на локальном уровне или на уровне обслуживания. Эта атака исходит из периферийных сетей, состоящих из устройств IoT, нарушающих работу соседних узлов затронутой сети.
- **Злоупотребление открытыми API на периферии сети** [b-ENISA]. При эксплуатации уязвимостей в приложениях типа MEC открытые API-интерфейсы в узлах MEC могут подвергаться злоупотреблению. Открытые API-интерфейсы в MEC, как правило, нужны для поддержки федеративных услуг и взаимодействия с различными поставщиками и создателями контента. Эта угроза может быть связана с DoS-атакой, атакой через посредника, утечкой конфиденциальной информации и манипулированием виртуальными машинами.
- **Физическое вмешательство в устройства**. Физическое вмешательство в устройства более вероятно, поскольку вычислительные ресурсы в архитектуре периферийных вычислений расположены ближе к злоумышленникам. Злоумышленник может вывести из строя периферийные узлы, что в свою очередь поставит под угрозу эффективность всей сети.

8.8 Угрозы для виртуализации сетевых функций

Ниже перечислены угрозы для NFV.

- **Злоупотребление протоколом соединения центров обработки данных (DCI)** [b-ENISA]. Эксплуатируя уязвимости протоколов DCI, злоумышленник может инициировать подложный трафик. Если в центрах обработки данных развернуты виртуализированные системы, это создаст угрозу для их безопасности, с которой необходимо считаться.
- **Злоупотребление ресурсами облачных вычислений** [b-ENISA]. Применяя простой процесс регистрации у поставщика услуг облачных вычислений, злоумышленник может использовать в своих целях мощную вычислительную инфраструктуру, включающую как программные, так и аппаратные компоненты. Используя преобладающую вычислительную мощность облачных сетей, злоумышленники могут организовать атаки за очень короткое время. Например, злоупотребляя мощью облачных вычислений, злоумышленник может запускать атаки типа прямого перебора и DoS-атаки.
- **Обход виртуализации сети** [b-ENISA]. Проблемы, связанные с некачественной реализацией и конфигурацией или неправильной изоляцией нарезки сети, могут привести к нарушению конфиденциальности данных (перехвату данных/трафика объектами других отрезков). Если сеть используется разными арендаторами, необходимо гарантировать, что в отрезок/из отрезка сети входит или выходит только законный трафик, а также что любой коммутирующий элемент проверяет и обеспечивает изоляцию трафика, устанавливая правила легитимного потока, предотвращающие вторжение в отрезок сети. На уровне базовой сети злоумышленник может использовать уязвимости гипервизора и конфигурацию правил потока, чтобы нарушить изоляцию отрезков сети и раскрыть данные, принадлежащие другим арендаторам.
- **Злоупотребление виртуализированным хостом** [b-ENISA]. Если приложения выполняются на виртуализированных хостах, это может привести к злоупотреблению общими ресурсами виртуализированной среды. Некоторый набор действий в виртуальной среде, где арендаторы

используют общие физические ресурсы, может приводить к раскрытию конфиденциальной информации. Например, в виртуализированных средах угроза раскрытия информации при сборе мусора еще серьезнее, чем в физических системах. Распространенная в физических системах (например, в сетевых средах) угроза перехвата представляет еще большую опасность в виртуальных средах, поскольку позволяет проводить перекрестный анализ потоков данных разных арендаторов, а также делать выводы о топологии, которые могут послужить основой для организации DoS-атак.

- **Угроза целостности инфраструктуры** [b-Alwakeel]. Выдавая себя за поставщика услуг, злоумышленник может представиться участником процесса предоставления реальных услуг NFV и получить доступ к пользовательским данным.
- **Злоупотребление ресурсами** [b-Alwakeel]. Злоумышленник высвобождает некоторые ресурсы и использует их в своих целях.
- **Изменение определения функции NFV** [b-Alwakeel]. Злоумышленник изменяет некоторые операции в функциональном обеспечении, определении NFV или даже организует DoS-атаки. Обычно это делается с помощью внедрения кода.
- **Изменение привилегий** [b-Alwakeel]. Злоумышленник изменяет привилегии пользователей в ходе атаки против неконтролируемых данных, несанкционированно расширяя или ограничивая их права доступа к объектам системы.
- **Атака в целях нарушения конфиденциальности с использованием общих ресурсов** [b-Alwakeel]. Используя атаку по побочному каналу, злоумышленники могут получить несанкционированный доступ к некоторой конфиденциальной информации о других пользователях общих услуг.
- **Злонамеренный инсайдер** [b-Alwakeel]. Пользующиеся доверием члены организации используют свои полномочия для несанкционированного доступа к конфиденциальным данным пользователей.

8.9 Угрозы для управления

Ниже перечислены угрозы для управления.

- **Небезопасный интерфейс управления** [b-TR 33.811]. Это угроза, связанная с незащищенным интерфейсом. Он позволяет злоумышленникам получать несанкционированный доступ к средствам управления сетью и создавать экземпляры отрезков сети, требующие значительных сетевых ресурсов, или большое количество экземпляров отрезков сети.
- **Раскрытие данных надзора и отчетности, связанных с функцией управления** [b-TR 33.811]. Эта угроза связана с незащищенными надлежащим образом операциями контроля данных и отчетности. В результате злоумышленник может подделать результаты контроля/отчетности и перехватить данные контроля и отчетности при их передаче, а также извлечь конфиденциальную информацию, которую можно использовать для осуществления атак на действующие экземпляры отрезков сети.
- **Несанкционированный доступ к интерфейсу управления** [b-Ta-Hao Ting]. Если интерфейс взломан, то такие сетевые функции, как SDN, NFV и нарезка сети, могут быть подвержены злонамеренным воздействиям, таким как несанкционированное изменение сетевых функций, создание ненадлежащих конфигураций сети и модификация сетевых функций.

9 Требования для обеспечения безопасности, связанные с компонентами и функциями

9.1 Средства обеспечения безопасности, связанные с абонентским оборудованием

Ниже перечислены рекомендуемые средства обеспечения безопасности UE.

- **Средства защиты UE от вредоносных программ**. Антивредоносное ПО предназначено для профилактики, обнаружения и удаления вредоносных программ в UE. Для защиты UE от заражения вредоносными программами используются три метода: обнаружение вредоносных программ по сигнатурам, обнаружение вредоносных программ по поведению и помещение в песочницу.

- **Средства защиты идентичности абонента (IMSI) посредством шифрования**. Рекомендуется шифровать IMSI кратковременным ключом шифрования с использованием симметричного криптографического алгоритма. Предварительным условием является наличие у UE собственного IMSI и открытого асимметричного ключа домашней сети, а также наличие у каждого оператора мобильной связи (называемой здесь домашней сетью) пары открытого и секретного асимметричных ключей. Предполагается, что секретный асимметричный ключ домашней сети хранится в домашней сети, а открытый асимметричный ключ домашней сети предварительно передается в мобильные устройства вместе с абонентскими IMSI.
- **Средства проверки идентичности**. Проверяют идентичность пользователя для предоставления услуг роуминга и облачных услуг.
- **Средства управления ключами**. Обеспечивают проверку идентичности пользователя и взаимную аутентификацию между UE и элементом сети.
- **Средства защиты данных о местоположении**. Обеспечивают защиту данных о местоположении пользователя.
- **Аутентификация обслуживающей сети**. Рекомендуется, чтобы UE проверяло идентификатор обслуживающей сети посредством неявной аутентификации ключа, то есть чтобы в последующих процедурах эта аутентификация обеспечивалась посредством успешного использования ключей в соответствии с соглашением об аутентификации и ключах.
- **Конфиденциальность и целостность пользовательских данных и данных сигнализации** [b-ITU-T X.1811]. UE имеет возможность обеспечивать конфиденциальность данных с помощью алгоритмов шифрования, а также защиту целостности и защиту от повторной передачи пользовательских данных между UE и сетевыми узлами.
- **Средства безопасного хранения и обработки абонентских учетных данных** [b-Craven]. UE имеет возможность обеспечить защиту целостности учетных данных и их долгосрочных ключей с помощью оборудования, защищенного от несанкционированного доступа. Рекомендуется, чтобы за пределами оборудования, защищенного от несанкционированного доступа, долгосрочные ключи были недоступны в незашифрованном виде. Рекомендуется, чтобы программа работала на оборудовании, защищенном от несанкционированного доступа с использованием алгоритма аутентификации и абонентских учетных данных.

9.2 Средства обеспечения безопасности, связанные с сетью доступа

Ниже перечислены рекомендуемые средства обеспечения безопасности в сети доступа.

- **Средства обеспечения безопасности канала**. Обеспечивают конфиденциальность и целостность связи для каналов управления и каналов пользовательского трафика в UE.
- **Средства аутентификации UE**. Рекомендуется, чтобы обслуживающая сеть определяла постоянный идентификатор абонента в процессе установления соглашения об аутентификации и ключах между UE и сетью.
- **Средства авторизации UE** [b-Craven]. Рекомендуется, чтобы обслуживающая сеть авторизовала UE, используя профиль абонента, полученный из домашней сети.
- **Средства авторизации сети обслуживания в домашней сети** [b-Craven]. Рекомендуется, чтобы UE удостоверялось, что оно подключено к обслуживающей сети, авторизованной домашней сетью.
- **Средства авторизации сети доступа** [b-Craven]. Рекомендуется, чтобы сеть доступа была авторизована обслуживающей сетью для предоставления услуг UE.
- **Средства обеспечения конфиденциальности данных пользователей и данных сигнализации** [b-Craven]. Рекомендуется, чтобы сеть доступа поддерживала шифрование пользовательских данных при передаче и данных сигнализации RRC.
- **Средства обеспечения целостности данных пользователей и данных сигнализации** [b-Craven]. Рекомендуется, чтобы узлы, как и UE, поддерживали защиту целостности и защиту от повторной передачи пользовательских данных между UE и следующей базовой станцией.

- **Средства установки и настройки** [b-Craven]. Рекомендуется, чтобы при установке и настройке систем эксплуатации и управления (O&M) следующая базовая станция была аутентифицирована и авторизована центром регистрации и центром сертификации (RA/CA) так, чтобы злоумышленники не могли изменить ее настройки и конфигурацию программного обеспечения.
- **Средства управления ключами на следующей базовой станции** [b-Craven]. Необходимо защищать элементы ключей шифрования, передаваемые из базовой сети IMT-2020 на следующую базовую станцию.
- **Средства обработки данных плоскости пользователя и плоскости управления** [b-Craven]. Эти средства управления ключами аналогичны средствам управления ключами при работе с данными плоскости пользователя и плоскости управления следующей базовой станции.
- **Средства обеспечения безопасной среды** [b-Craven]. К безопасной среде, в которой используются все эти незашифрованные данные, также предъявляются определенные требования. Рекомендуется, чтобы она поддерживала безопасное хранение, например, долгосрочных секретных ключей шифрования и важных данных конфигурации.
- **Средства устранения угроз нарушения обслуживания из-за запросов на установление RRC-соединения**. Для предотвращения угрозы злонамеренных запросов на установление RRC-соединения базовая станция должна поддерживать RRC-соединение с текущим абонентом в течение длительного времени. В результате время соединения базовой станции превышает время срабатывания таймера ожидания для текущего RRC-соединения. Кроме того, рекомендуется использовать на базовой станции параметры "ограничение времени соединения" и "ограничение количества повторов" и добавить процесс контроля наличия атаки. Подробный сценарий такой атаки описан в Дополнении II.

9.3 Средства обеспечения безопасности, связанные с сетями с программируемыми параметрами

Ниже перечислены рекомендуемые средства безопасности для SDN [ITU-T X.1038].

- **Средства аутентификации** приложения SDN для аутентификации контроллера/пользователя/администратора SDN.
- **Средства авторизации** приложения SDN для авторизации пользователя/администратора в целях предоставления доступа к системной информации.
- **Средства обеспечения конфиденциальности данных** приложения SDN для защиты конфиденциальности системной информации, хранящейся на платформе приложений, и защиты конфиденциальности при передаче данных через интерфейс управления приложениями.
- **Средства управления ключами/сертификатами** приложения SDN для поддержки управления ключами/сертификатами.
- **Средства управления безопасностью** приложения SDN для поддержки ведения журналов регистрации событий и аудита.
- **Средства защиты приложений** SDN для защиты от уязвимостей приложений.
- **Средства обеспечения целостности данных** приложений SDN для защиты целостности данных при их транспортировке через интерфейс управления приложениями.
- **Средства аутентификации** контроллера SDN для аутентификации администраторов/приложений SDN/коммутаторов SDN.
- **Средства авторизации** контроллера SDN для авторизации администраторов/приложений SDN в целях управления контроллером SDN.
- **Средства управления средствами аутентификации и безопасности** контроллера SDN для защиты от DoS-атак.
- **Средства обеспечения целостности данных контроллера SDN** для защиты целостности данных конфигурации и пользовательских данных, хранящихся в контроллере SDN, а также данных, передаваемых через интерфейс управления приложениями и интерфейс управления ресурсами.

- **Средства управления ключами/сертификатами** контроллера SDN для управления ключами/сертификатами.
- **Средства обеспечения конфиденциальности данных контроллера SDN** для защиты конфиденциальности данных конфигурации и пользовательских данных, хранящихся в контроллере SDN, а также данных, передаваемых через интерфейс управления приложениями и интерфейс управления ресурсами.
- **Средства усиления защиты операционной системы контроллера SDN** для поддержки функций усиления защиты операционной системы.
- **Средства аутентификации уровня ресурсов SDN** для аутентификации администраторов/контроллера SDN.
- **Средства авторизации уровня ресурсов SDN** для авторизации администраторов, управляющих коммутаторами SDN.
- **Средства управления безопасностью уровня ресурсов SDN** для поддержки ведения журналов регистрации событий и аудита.
- **Средства обеспечения целостности данных уровня ресурсов SDN** для защиты целостности данных конфигурации, хранящихся в коммутаторах SDN, а также данных, передаваемых между коммутаторами SDN, и данных, передаваемых через интерфейс управления ресурсами.
- **Средства управления ключами/сертификатами уровня ресурсов SDN** для управления ключами/сертификатами.
- **Средства обеспечения конфиденциальности данных уровня ресурсов SDN** для защиты конфиденциальности данных конфигурации, хранящихся в коммутаторах SDN, а также данных, передаваемых между коммутаторами SDN, и данных, передаваемых через интерфейс управления ресурсами.
- **Средства предотвращения переполнения таблицы потоков на уровне ресурсов SDN**. Контроллер SDN должен динамически вести таблицу потоков, вставляя и удаляя записи о потоках.

9.4 Средства обеспечения безопасности, связанные с базовой сетью

Ниже перечислены рекомендуемые средства обеспечения безопасности.

- **Средства обнаружения и защиты от атак типа DoS и DDoS** для защиты центральной станции управления SDN.
- **Средства проверки конфигурации** для проверки соблюдения правил управления потоками в элементах сети SDN.
- **Средства управления доступом** для ограничения доступа к SDN и элементам базовой сети.

Рекомендуется, чтобы поддерживались следующие средства обеспечения безопасности функции представления сети и интерфейса на основе услуг.

- **Безопасные средства представления функций сети** [b-TS 33.501]. Рекомендуется осуществлять взаимную аутентификацию на основе сертификатов клиента и сервера между функцией представления сети и функциями сторонних приложений, внешних по отношению к домену оператора IMT-2020, через безопасный туннель, такой как TLS. Рекомендуется использовать трафик между функцией представления сети (NEF) и функциями приложений для защиты целостности, защиты от повторной передачи и защиты конфиденциальности.
- **Конфиденциальность, целостность данных и аутентификация элементов сети через интерфейс на основе услуг** [b-TS 33.501]. Трафик между элементами сети через SBI должен обеспечивать защиту целостности, защиту от повторной передачи и защиту конфиденциальности данных, а также аутентификацию элементов сети через безопасный туннель, такой как TLS.

9.5 Средства обеспечения безопасности, связанные с нарезкой сети

Ниже перечислены рекомендуемые средства обеспечения безопасности, связанные с жизненным циклом отрезка сети [b-Olimid].

- **Средства обеспечения безопасности жизненного цикла отрезка сети**. Рекомендуется, чтобы безопасность обеспечивалась на всех четырех этапах, поскольку уязвимость на одном этапе может привести к возникновению уязвимостей на других.
- **Надлежащие средства ведения журналов регистрации событий и аудита**. Рекомендуется, чтобы журналы регистрации событий велись на разных уровнях в отдельных отрезках сети в зависимости от различных факторов, таких как нормативные требования, целевой уровень безопасности услуг, выделенный тип клиентских устройств (например, используемых человеком или машиной). Рекомендуется, чтобы журналы регистрации событий и отчеты были защищены, так как их раскрытие приведет к утечке конфиденциальной информации.
- **Средства защиты шаблона нарезки сети**. Рекомендуется, чтобы были защищены конфиденциальность и целостность шаблона нарезки сети при передаче и хранении, а его источник был аутентифицирован.
- **Средства согласования служб безопасности**. Рекомендуется, чтобы отдельные службы безопасности были согласованы и развернуты в соответствии с требованиями безопасности соответствующих вертикальных отраслей [b-ITU-T X.1047].
- **Средства изоляции отрезков сети**. Рекомендуется, чтобы при создании отрезка сети обеспечивалась его изоляция, а во время выполнения производился ее контроль и при необходимости обновление [b-ITU-T X.1047].
- **Средства обеспечения безопасности API**. Рекомендуется, чтобы API были безопасными в отношении прав доступа и эксплуатации и не раскрывали данные о трафике; также рекомендуется, чтобы API разрешали доступ к функциональным возможностям и данным только по согласованию между сторонами юридическим путем.
- **Средства вывода из эксплуатации**. Рекомендуется, чтобы при выводе из эксплуатации конфиденциальные данные уничтожались (или при необходимости надежно сохранялись), а ресурсы и сетевые функции высвобождались.

Рекомендуется, чтобы поддерживались перечисленные ниже средства безопасности внутри отрезка сети.

- **Средства обеспечения сквозной безопасности**. Отрезки сети представляют собой сквозные логические сети, поэтому рекомендуется учитывать требования сквозной безопасности [b-ITU-T X.1047].
- **Средства надлежащего использования механизмов безопасности**. Рекомендуется, чтобы во всех соединениях (например, между отрезком сети и уровнем ресурсов, отрезком сети и менеджером отрезков сети, подотрезками сети или между абонентским устройством и точкой доступа в сеть) использовались надлежащие механизмы для обеспечения целевого уровня безопасности; минимальные требования включают обеспечение конфиденциальности, целостности и подлинности данных, а также взаимную аутентификацию между одноранговыми объектами.
- **Средства аутентификации UE**. Рекомендуется, чтобы клиентские устройства IMT-2020 строго аутентифицировались с использованием первичной и предпочтительно вторичной аутентификации.
- **Средства безопасного потребления ресурсов**. Все ресурсы и сетевые функции, используемые отрезком сети, должны быть защищены.
- **Средства обеспечения безопасности арендаторов**. Рекомендуется, чтобы новые ресурсы, вводимые в строй арендаторами (например, сетевые функции, конфигурации, услуги), и их интеграция были надлежащим образом защищены во избежание уязвимостей, которые могут быть использованы в дальнейшем.
- **Средства защиты идентичности**. Рекомендуется, чтобы конфиденциальные идентификаторы были защищены и чтобы не было корреляции между идентификаторами.
- **Санкционированный перехват**. Рекомендуется, чтобы санкционированный перехват был возможен как на уровне отрезка сети, так и на уровне обслуживания.
- **Средства обеспечения доступа, прав и возможностей настройки конфигурации арендаторов** должны соответствовать юридическим соглашениям между сторонами.

Рекомендуется, чтобы поддерживались следующие средства обеспечения безопасности, относящиеся к связи между отрезками сети.

- Рекомендуется, чтобы для каждого отрезка сети обеспечивался минимальный уровень безопасности.
- **Средства изоляции отрезков сети**. Рекомендуется, чтобы изоляция между отрезками сети была достаточно надежной для предотвращения атак через менее защищенные отрезки сети [b-ITU-T X.1047].
- **Минимальные средства обеспечения безопасности связи**. Рекомендуется, чтобы связь между отрезками сети была сведена к минимуму, определялась строгими правилами и осуществлялась по защищенным каналам.
- **Средства управления ключами**. Рекомендуется, чтобы никакие криптографические ключи (и другие конфиденциальные параметры) не использовались несколькими отрезками сети.
- **Средства минимального выделения ресурсов**. Рекомендуется, чтобы распределение ресурсов гарантировало минимальный уровень готовности каждого отрезка сети; в частности чтобы механизмы безопасности могли работать независимо от потребления ресурсов.
- Отрезки сети, значительно различающиеся по уровню безопасности, не должны использовать одни и те же ресурсы или сетевые функции; в частности никогда не следует запускать отрезки сети в тестовом режиме вместе с рабочими отрезками сети.
- **Независимые средства обеспечения безопасности**. Рекомендуется, чтобы отдельные механизмы аутентификации, авторизации и управления доступом каждого отрезка сети не зависели друг от друга.

9.6 Средства обеспечения безопасности, связанные с периферийными вычислениями с множественным доступом

Рекомендуются следующие средства обеспечения безопасности.

- **Средства защиты от DDoS-атак** для защиты облачных веб-услуг.
- **Средства управления доступом** для ограничения доступа к элементам сети периферийных вычислений с множественным доступом.
- **Средства проверки целостности** для защиты данных и накопителей в системе облачных вычислений.
- **Средства управления доступом к услугам** для ограничения элемента облачных вычислений на основе услуг.
- **Средства физической защиты**. Рекомендуется обеспечить физическую защиту всех периферийных узлов, не находящихся в высокозащищенных периферийных центрах обработки данных, например дополнительные методы физической защиты во время производства или внедрение механизмов блокировки и другие физические средства защиты в полевых условиях.

9.7 Средства обеспечения безопасности, связанные с виртуализацией сетевых функций

Ниже перечислены рекомендуемые средства обеспечения безопасности.

- **Средства изоляции трафика**. Используются для обеспечения виртуальных отрезков сети и виртуальных сетевых функций.
- **Средства предотвращения DoS-атак** [b-Alwakeel]. Рекомендуется использовать элементы сети, например межсетевые экраны и устройства выравнивания нагрузки, для отражения DoS/DDoS-атак.
- **Средства обеспечения целостности инфраструктуры** [b-Alwakeel]. Рекомендуется использовать цепочку доверия и доверенный модуль платформы (TPM) для обеспечения безопасности различных поставщиков услуг VNF.

- **Средства предотвращения злоупотребления ресурсами** [b-Alwakeel]. Рекомендуется использовать усовершенствованный планировщик гипервизора, обеспечивающий справедливое распределение ресурсов между процессами, ограничивая максимально допустимое их количество для каждой виртуальной службы.
- **Средства защиты от изменения определения функций NFV** [b-Alwakeel]. Рекомендуется хранить копию пользовательских виртуальных служб в отдельном хранилище для предотвращения атак с внедрением вредоносных программ. Для этого используется таблица размещения файлов (FAT), содержащая информацию о службах и программном обеспечении, исполняемых пользователями.
- **Средства предотвращения изменения привилегий** [b-Alwakeel]. Рекомендуется предусмотреть защиту объекта виртуализации от несанкционированного доступа путем добавления правил, ограничивающих доступ к ресурсам.
- **Средства предотвращения атак при совместном использования ресурсов** [b-Alwakeel]. Рекомендуется использовать средства предотвращения атак по побочному каналу, ограничив доступ к образам VM и компонентам инфраструктуры виртуализации сетевых функций (NFVI) и контролируя использование ресурсов. Это можно сделать с помощью виртуального межсетевого экрана для предотвращения несанкционированного доступа к системе.
- **Средства защиты от злонамеренных инсайдеров** [b-Alwakeel]. Внутренние атаки можно предотвратить с помощью разных средств, одним из которых является журнал регистрации обращений к среде NFV, который затем можно использовать для внутреннего аудита в целях обнаружения подозрительных действий. Другой механизм – настройка строгих правил аутентификации и авторизации пользователей, имеющих права доступа.

9.8 Средства обеспечения безопасности, связанные с функцией управления

Рекомендуются следующие средства обеспечения безопасности [b-TR 33.811].

- **Средства взаимной аутентификации** между потребителем услуг управления и поставщиком услуг управления с использованием безопасного туннеля, такого как TLS, основанные либо (1) на сертификатах клиента и сервера, либо (2) на предварительном обмене ключами (PSK) с использованием TLS-PSK.
- **Средства защиты целостности, защиты от повторной передачи и защиты конфиденциальности данных** для интерфейса между поставщиком услуг управления и потребителем услуг управления, находящимся за пределами доверенного домена TLS оператора 3GPP.
- **Средства безопасности PI для интерфейса управления**. Рекомендуется, чтобы API были безопасными в отношении прав доступа и эксплуатации и не раскрывали данные о трафике; также рекомендуется, чтобы API к интерфейсам управления разрешали доступ к функциональным возможностям и данным только по согласованию между сторонами юридическим путем.

Приложение A

Архитектура безопасности системы связи IMT-2020

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

На рисунке 4-1 в [b-TS 33.501] представлен обзор архитектуры безопасности системы связи IMT-2020.

На рисунке 4-1 в [b-TS 33.501] показаны следующие домены безопасности.

– Безопасность доступа в сеть (I) – набор функций безопасности, позволяющий UE безопасно аутентифицировать услуги и получать к ним доступ через сеть, включая получение доступа через сеть 3GPP и сеть доступа не-3GPP, и, в частности, обеспечивающий защиту от атак через (радио) интерфейсы. Кроме того, он осуществляет передачу контекста безопасности из обслуживающей сети (SN) в сеть доступа (AN) для обеспечения безопасного доступа.

– Безопасность домена сети (II) – набор функций безопасности, позволяющий узлам сети безопасно обмениваться данными сигнализации и данными плоскости пользователя.

– Безопасность домена пользователя (III) – набор функций безопасности, обеспечивающих безопасный доступ пользователей к оборудованию подвижной связи.

– Безопасность домена приложений (IV) – набор функций безопасности, позволяющий приложениям в домене пользователя и в домене поставщика безопасно обмениваться сообщениями. Безопасность домена приложений выходит за рамки сферы применения настоящей Рекомендации.

– Безопасность домена SBA (V) – набор функций безопасности, которые позволяют сетевым функциям архитектуры SBA безопасно обмениваться данными в пределах домена SN и с другими доменами сети. К таким функциям относятся регистрация сетевых функций, аспекты безопасности, относящиеся к обнаружению и авторизации, а также защита интерфейсов на основе услуг. Безопасность доменов SBA – это новая функция безопасности, не описанная в [b-TS 33.401].

– Видимость и возможность настройки параметров безопасности (VI) – набор функций, который позволяет информировать пользователя о том, работает ли функция безопасности.

Дополнение I

Общая архитектура безопасности сети для обеспечения сквозной безопасности сети

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В этом Дополнении описана общая архитектура безопасности сети для обеспечения сквозной сетевой безопасности, как указано в [b-ITU-T X.805], что составляет основу настоящей Рекомендации.

В [b-ITU-T X.805] определена архитектура безопасности для обеспечения сквозной безопасности сети. Данная архитектура может применяться к различным видам сетей, в которых должны обеспечиваться сквозная безопасность и функционирование, независимо от технологии, лежащей в основе сети. В Рекомендации [b-ITU-T X.805] определены общие связанные с безопасностью архитектурные элементы, необходимые для обеспечения сквозной защиты. Цель [b-ITU-T X.805] состоит в том, чтобы служить основой для разработки детальных рекомендаций для сквозной сетевой защиты.

В Рекомендации [b-ITU-T X.805] определены восемь измерений защиты:

1) управление доступом;
2) аутентификация;
3) сохранность информации;
4) конфиденциальность данных;
5) безопасность связи;
6) целостность данных;
7) доступность; и
8) секретность.

В Рекомендации [b-ITU-T X.805] также определены три уровня защиты, один поверх другого, для обеспечения сетевых решений:

1) уровень защиты инфраструктуры;
2) уровень защиты услуг; и
3) уровень защиты приложений.

Кроме того, в [b-ITU-T X.805] определены три плоскости защиты:

1) плоскость защиты управления;
2) плоскость защиты контроля; и
3) плоскость защиты конечного пользователя.

Дополнение II

Угроза нарушения обслуживания в результате подделки запроса на соединение RRC и его параметров

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Обзор

Запрос на установление RRC-соединения представляет собой сообщение, передаваемое открытым текстом, когда UE получает доступ к сети. Он включает в себя глобальный временный уникальный идентификатор (GUTI) или S-TMSI – временный идентификатор UE. Существует несколько способов раскрыть временный идентификатор конкретного пользователя. Если злоумышленник перехватит этот запрос на установление RRC-соединения и внесет изменения в это сообщение, переданное на предыдущем шаге открытым текстом, то он сможет использовать этот временный идентификатор жертвы для постоянной блокировки ее сетевого соединения.

II.2 Сценарий атаки

Злоумышленник может перехватить сообщение с запросом на установление RRC-соединения, переданное открытым текстом, и получить временный идентификатор GUTI или S-TMSI. Используя этот временный идентификатор в подложном сообщении запроса на установление RRC-соединения, злоумышленник неправомерно использует временную идентификационную информацию, выдавая свое сообщение за сообщение, отправленное абонентским оборудованием жертвы. Хотя RRC-соединение злоумышленника прерывается из-за ошибки аутентификации MAC (кода аутентификации сообщения) во время передачи сигналов NAS (уровень "без доступа"), злоумышленник может продолжать блокировать радиосоединение жертвы, повторяя одно и то же фальшивое сообщение. Кроме того, временный идентификатор воссоздается через регулярные промежутки времени в соответствии с определенными правилами на основе IMSI. Если S-TMSI изменен, злоумышленник может обнаружить это изменение и возобновить передачу вредоносного сообщения. Чтобы заблокировать радиодоступ UE жертвы, злоумышленнику нужно передать фальшивое сообщение с запросом RRC-соединения. Для этой атаки должны соблюдаться два предварительных условия: 1) мобильное устройство злоумышленника должно находиться в той же соте, что и UE жертвы, чтобы перехватить радиотрафик; 2) UE злоумышленника должно иметь возможность передавать поддельные сообщения.

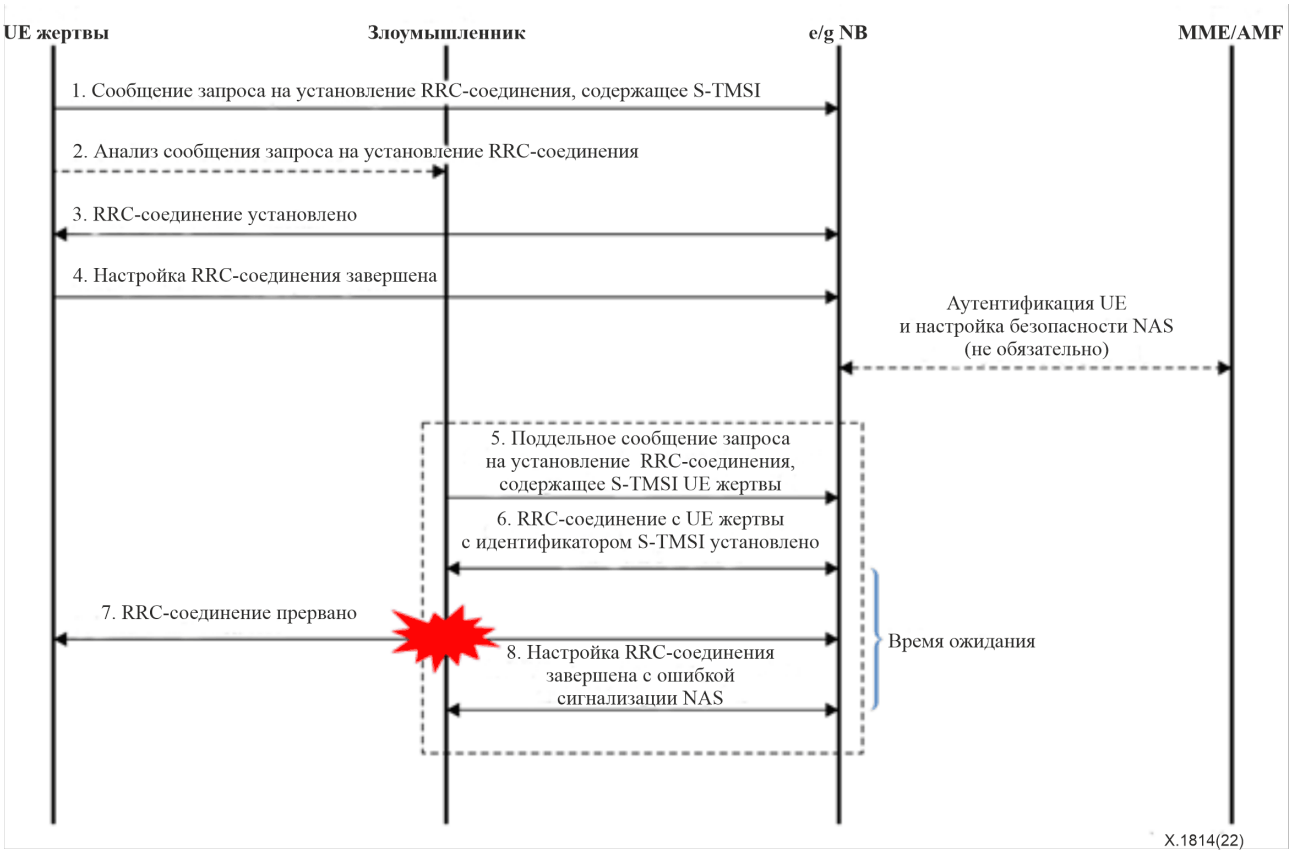

Рисунок II.1 – Сценарий атаки с фальшивым запросом на установления RRC-соединения

II.3 Последствия

При отсутствии проверки подлинности сообщений эта уязвимость приводит к тому, что оборудование радиосети (e/gNodeB) прерывает существующее соединение с UE жертвы в соответствии с сообщением, переданным злоумышленником, и подключается к UE злоумышленника. UE жертвы может оставаться в состоянии, когда оно не может получить доступ к сети нормальным образом.

II.4 Контрмеры

Самая простая и эффективная мера противодействия состоит в том, чтобы базовая станция сохраняла RRC-соединение с текущим пользователем в течение определенного периода времени. Когда злоумышленник установит RRC-соединение, используя краденный идентификатор жертвы, соединение прерывается из-за ошибки сигнализации NAS. Следовательно, если текущее соединение жертвы сохраняется до прерывания RRC-соединения злоумышленника, то радиосвязь может продолжаться. Обычно с момента попытки злоумышленника установить RRC-соединение до прерывания RRC-соединения из-за ошибки сигнализации NAS проходит столько же времени, сколько требуется базовой станции для установления RRC-соединения и ожидания завершения процесса установления RRC-соединения. Следовательно таймер ожидания[1] в e/gNodeB должен отсчитывать время с момента передачи запроса на установление RRC-соединения в UE до получения подтверждения завершения процесса установления RRC-соединения. Рекомендуется добавить процесс, в результате которого базовая станция сохраняла бы соединение дольше времени срабатывания таймера ожидания текущего RRC-соединения, по которому передается запрос с дубликатом идентификатора, и текущее соединение сохраняется, если новое соединение прерывается в течение соответствующего времени. Время сохранения соединения должно быть минимальным с учетом его влияния на качество связи и работу оборудования.

[1] Например T352, как указано в TS 25.331 3GPP.

Злоумышленник может повторять запросы к базовой станции на установление RRC-соединения, поддерживая статус нарушения обслуживания жертвы. Для предотвращения этой ситуации рекомендуется установить на e/gNodeB ограничение времени соединения и ограничение количества повторов, добавив процесс, при котором в случае повторения событий установления и прерывания RRC-соединения с превышением пределов времени соединения и количества повторов базовая станция предупреждала бы оператора сети о необходимости отслеживать атаки.

Библиография

[b-ITU-T Q.700] Recommendation ITU-T Q.700 (1993), *Introduction to CCITT Signalling System No. 7.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open systems interconnection – The directory: Public-key and attribute certificate frameworks.*

[b-ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами.*

[b-ITU-T X.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration.*

[b-ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology.*

[b-ITU-T X.1406] Recommendation ITU-T X.1406 (2021), *Security threats to online voting systems using distributed ledger technology.*

[b-ITU-T X.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology.*

[b-ITU-T X.1811] Рекомендация МСЭ-Т X.1811 (2021 г.), *Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность.*

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

[b-ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network.*

[[b-ITU-T Y.3150] Recommendation ITU-T Y.3150 (2020) *High-level technical characteristics of network softwarization for IMT-2020.*

[b-ITU-T Y.4807] Recommendation ITU-T Y.4807 (2020) *Agility by design for telecommunication/ICT systems security used in the Internet of things.*

[b-ITU workshop] Third annual ITU IMT-2020/5G Workshop and Demo Day (July 18, 2018), *5G security activities and future plan in ITU-T SG17.*

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

[b-ISO 81001-1] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

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

[b-RFC 3588] IETF RFC 3588 (2003), *Diameter base protocol.*

[b-TR 33.811] 3GPP TR 33.811 (2018), *Study on security aspects of 5G network slicing management.*

[b-TS 33.401] 3GPP TS 33.401 (2021), *3GPP System Architecture Evolution (SAE); Security architecture.*

[b-TS 33.501] 3GPP TS 33.501 (2022), *Security architecture and procedures for 5G System.*

[b-Alwakeel] Alwakeel, A.M., Alnaim, A., Fernández, E.B., *A Survey of Network Function Virtualization Security*, IEEE Southeast Conf. 2018.
https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security

[b-Craven] Craven, C., *5G Security Standards: What Are They?* 10 June 2020.
https://www.sdxcentral.com/5g/definitions/5g-security-standards/

[b-ENISA] European Union Agency for Cybersecurity (ENISA) (2019), *ENISA Threat Landscape for 5G Networks.*

[b-Goodin] Goodin, D. (2013), *Lucky Thirteen attack snarfs cookies protected by SSL encryption* Ars Technica. https://arstechnica.com/security/2013/02/lucky-thirteen-attack-snarfs-cookies-protected-by-ssl-encryption/

[b-Khan] Khan, R., Kumar, P., Jayakody, D.N.K, and Liyanage, M. (2019), *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions*, IEEE Communications Surveys and Tutorials, Vol. 22, No. 1, July, pp. 196-248.

[b-Möller] Möller, B, Duong, T, and Kotowicz, K. (2014), *This POODLE Bites: Exploiting The SSL 3.0 Fallback*. https://www.openssl.org/~bodo/ssl-poodle.pdf

[b-NGMN] The Next Generation Mobile Networks Alliance (NGMN Alliance) (2016), *5G security recommendations package.*

[b-Olimid] Olimid, R., and Nencioni, G. (2020) *5G Network Slicing: A Security Overview*, IEEE Access, Vol. 8, June, 99999-100009.

[b-SQL] OWASP, *SQL injection.* https://owasp.org/www-community/attacks/SQL_Injection

[b-Ta-Hao Ting] Ta-Hao Ting, Tsung-Nan Lin, Shan-Hsiang Shen, Yu-Wei Chang, *Guidelines for 5G end to end architecture and security issues*, 21 December 2019. https://arxiv.org/abs/1912.10318

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 межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2023 г.