ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1816 (03/2023)

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

Безопасность сетей IMT-2020

Руководящие указания и требования для классификации возможностей обеспечения безопасности в отрезке сети IMT-2020

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 распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
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.1816

Руководящие указания и требования для классификации возможностей обеспечения безопасности в отрезке сети IMT-2020

Резюме

Определение основных функций и процессов технологии нарезки сети заложило прочную основу для первой волны развертывания сетей IMT-2020 и коммерческого использования услуг с нарезкой сети. В качестве сквозной логической сети, которая настраивается по запросу, нарезка может обеспечить различные возможности обеспечения безопасности: во-первых, нарезка сети IMT-2020 обеспечивает вспомогательные меры безопасности для реализаций дифференцированной сети. Во-вторых, сеть IMT-2020 поддерживает некоторые дополнительные меры безопасности на уровне отрезка сети. Некоторые меры безопасности могут обеспечить несколько способов обеспечения безопасности, и операторы могут применять разные средства защиты. Эти меры могут обеспечить разную степень гарантии безопасности или эффективности функционирования, не связанной с безопасностью. Пользователи отрезков сети также могут предъявлять особые требования к безопасности и запрашивать у операторов настраиваемые отрезки сети с различными уровнями защиты. При выборе возможностей обеспечения безопасности в отрезке сети пользователи отрезков или операторы отрезков сталкиваются с определенными проблемами, такими как высокая стоимость управления, несогласованность определений и т. д. Цель настоящей Рекомендации – представить описание различных возможностей обеспечения безопасности в отрезке сети IMT-2020 и руководящие указания по классификации возможностей обеспечения безопасности в отрезке сети IMT-2020 и безопасности отрезка сети IMT-2020, для того чтобы помочь экосистеме более точно понять и выбирать возможности обеспечения безопасности отрезков сети.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1816	03.03.2023 г.	17-я	11.1002/1000/15114

Ключевые слова

Классификация, IMT-2020, отрезок сети, возможности обеспечения безопасности.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора 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, 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 МСЭ-Т, доступным на веб-сайте МСЭ-Т, по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1816

Руководящие указания и требования для классификации возможностей обеспечения безопасности в отрезке сети IMT-2020

1 Сфера применения

Цель настоящей Рекомендации – представить руководящие указания и требования для классификации возможностей обеспечения безопасности в отрезке сети IMT-2020. В этой Рекомендации содержатся:

- определения различных возможностей обеспечения безопасности в отрезке сети IMT-2020;
- принципы и методы классификации возможностей обеспечения безопасности в отрезке сети IMT-2020.

2 Справочные документы

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

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

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

[3GPP TS 33.501] Technical Specification 3GPP TS 33.501 V17.1.0 (2021), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 17).*

3 Определения

3.1 Термины, определенные в других документах

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

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

ПРИМЕЧАНИЕ 1. – Отрезки сети позволяют создавать настраиваемые сети для получения гибких решений в различных коммерческих сценариях, где предъявляются различные требования к функциональным возможностям, рабочим характеристикам и распределению ресурсов.

ПРИМЕЧАНИЕ 2. – Отрезок сети может обладать способностью объявлять о своих возможностях.

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

3.1.2 экземпляр отрезка сети (network slice instance) [b-ITU-T Y.3100]: Экземпляр отрезка сети, созданный на основе схемы отрезков сети.

3.1.3 подсеть отрезка сети (network slice subnet) [b-ETSI TS 128 530]: Представление аспектов управления набором управляемых функций и необходимых ресурсов (вычислительных ресурсов, ресурсов хранения данных, сетевых ресурсов и т. п.).

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

AAA	Authentication, Authorization, and Accounting	Аутентификация, авторизация и учет
ACL	Access Control List	Список управления доступом
AMF	Access and Mobility Management Function	Функция управления доступом и мобильностью
CN	Core Network	Базовая сеть
CU	Central Unit	Центральный блок
DDoS	Distributed Denial-of-Service	Распределенный отказ в обслуживании
DU	Distributed Unit	Распределенный блок
EAP	Extensible Authentication Protocol	Расширяемый протокол аутентификации
ENSI	External Network Slice Information	Информация о внешнем отрезке сети
gNB	NR Node B	Узел B NR
IMT-2020	International Mobile Telecommunications-2020	Международная подвижная электросвязь-2020
NAT	Network Address Translation	Трансляция сетевых адресов
NFV	Network Function Virtualization	Виртуализация сетевых функций
ng-eNB	Next Generation Evolved Node-B	Улучшенный узел B нового поколения
NSSAI	Network Slice Selection Assistance Information	Вспомогательная информация по выбору отрезков сети
S-NSSAI	Single Network Slice Selection Assistance Information	Вспомогательная информация по выбору одного отрезка сети
PDU	Protocol Data Unit	Блок данных протокола
PNF	Physical Network Function	Физическая сетевая функция
RAN	Radio Access Network	Сеть радиодоступа
RB	Radio Bearer	Радиоканал передачи данных
TLS	Transport Layer Security	Безопасность транспортного уровня
UE	User Equipment	Оборудование пользователя
URL	Uniform Resource Locator	Унифицированный указатель ресурса
VNF	Virtual Network Function	Виртуальная сетевая функция
WAF	Web Application Firewall	Брандмауэр веб-приложения

5 Соглашения по терминологии

В настоящей Рекомендации:

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

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

6 Введение в классификацию возможностей обеспечения безопасности в отрезке сети IMT-2020

Необходимым условием внедрения технологии нарезки сети является обеспечение безопасности отрезка сети. Пользователям услуг передачи данных на основе отрезков сети необходима соответствующая гарантия безопасности, адаптированная к их реализации отрезков сети; к тому же они могут предъявлять особые требования безопасности, основанные на используемых ими услугах на основе отрезков сети. Таким образом, они могут запрашивать у операторов отдельные отрезки сети с разной степенью защиты. У операторов отрезков сети, которые проектируют, строят и эксплуатируют сети и предоставляют отрезки сети, в нарезку сети входит множество доменов (беспроводных, передающих, базовой сети, управления и т. п.), и они могут предоставлять различные средства обеспечения безопасности. Во-первых, нарезка сети IMT-2020 обеспечивает меры безопасности для реализации дифференцированной сети. Во-вторых, сеть IMT-2020 поддерживает некоторые дополнительные меры безопасности на уровне отрезков сети. Некоторые меры безопасности также могут обеспечить несколько вариантов безопасности, и операторы могут располагать разными ресурсами безопасности, которые способны обеспечивать разную степень гарантии безопасности или эффективности функционирования, не связанной с безопасностью. Таким образом, средства обеспечения безопасности для одного отрезка сети следует определять на основе требований пользователей и способности сети обеспечить те или иные функции безопасности. Пользователи и операторы, выбирающие средства обеспечения безопасности своих отрезков сети, сталкиваются с рядом проблем:

- требования безопасности, предъявляемые пользователями, могут быть расплывчатыми, немногочисленными и недостаточными для выбора возможностей обеспечения безопасности;
- пользователи могут предъявлять слишком высокие требования безопасности, выходящие за рамки возможностей сети;
- уровень знаний заинтересованных сторон в области возможностей обеспечения безопасности и различий между ними может варьироваться, и комбинация выбранных ими функций может оказаться нерациональной. Например, способ защиты, обеспечиваемый выбранными функциями, может оказаться недопустимым для некоторых доменов или заинтересованных сторон;
- количество комбинаций возможностей обеспечения безопасности в отрезке сети может быть огромным, и затраты операторов на управление и оркестровку могут оказаться относительно высокими.

Здесь рекомендуются различные возможности обеспечения безопасности в отрезке сети IMT-2020 и приводится методика их классификации и комбинирования, преследующая следующие цели:

- помочь отрасли прийти к единому пониманию возможностей обеспечения безопасности в отрезке сети и различий между ними (например, по характеристикам);
- предложить общую базовую классификацию средств обеспечения безопасности в отрезке сети IMT-2020, чтобы помочь отрасли сформировать правильное представление о возможностях обеспечения безопасности, которые может предоставить нарезка сети, и добиться лучшего соответствия для большинства промышленных применений;
- помочь в реализации роуминга между разными отрезками сети, а также облегчить повторное использование отрезков сети;
- предоставить пользователям отрасли справочную информацию по выбору подходящих отрезков сети, отвечающих их требованиям;
- предоставить отраслевым надзорным органам справочную информацию для составления планов развития и стратегий выбора отрезков сети;
- предоставить поставщикам услуг справочную информацию для развертывания услуг в соответствующих отрезках сети;
- предоставить операторам справочную информацию для составления планов развития отрезков сети и оценки их ценности и стоимости;
- предоставить производителям оборудования справочную информацию по планированию дорожных карт развития технологии нарезки сети и наращивания производства в этой области.

Методика охватывает следующие аспекты:

- составление общего перечня различных возможностей обеспечения безопасности в отрезке сети в структурированной форме, включая название, описание, параметр безопасности и варианты средств обеспечения безопасности. Этот аспект рассматривается в разделе 7;
- для каждого параметра безопасности можно определить несколько уровней защиты, перечислив комбинации разных вариантов соответствующих возможностей обеспечения безопасности в отрезке сети на основе определенных принципов. Этот аспект рассматривается в разделе 8;
- кроме того, можно составить перечень основных типов возможностей обеспечения безопасности в отрезке сети, выбрав по одному уровню безопасности для каждого параметра безопасности на основе определенных принципов. Этот аспект рассматривается в разделе 9;
- заинтересованные стороны могут использовать принцип, методы и результаты классификации для выбора возможностей обеспечения безопасности определенного отрезка сети. Этот аспект рассматривается в разделе 10.

7 Возможности обеспечения безопасности в отрезке сети IMT-2020

7.1 Шаблон описания возможностей обеспечения безопасности в отрезке сети

В разделе 7 приведен общий перечень возможностей обеспечения безопасности сети IMT-2020; эти возможности могут различаться для разных отрезков сети. Описание возможностей обеспечения безопасности должно быть четким, кратким и недвусмысленным. Каждое описание должно включать следующие разделы.

- Описание возможности: подробное описание отдельного средства обеспечения безопасности в отрезке сети IMT-2020.
- Название возможности: уникальное имя и сокращенное условное обозначение, присвоенные каждому средству обеспечения безопасности.
- Параметр безопасности: конкретный аспект безопасности, для обеспечения которого предназначено средство. Существует восемь параметров безопасности: управление доступом, аутентификация, предотвращение отказа, конфиденциальность данных, безопасность связи, целостность данных, доступность и секретность [ITU-T X.805].
- Возможные варианты: существует несколько вариантов каждой возможности обеспечения безопасности, которые могут различаться в зависимости от отрезка сети. В настоящей Рекомендации каждый вариант обозначается порядковым номером при названии возможности.

  Примечание. – Варианты носят общий характер и не связаны с конкретной реализацией сети. Можно провести их дальнейшее подразделение в соответствии с конкретной реализацией.

7.2 Отдельные возможности обеспечения безопасности в отрезке сети IMT-2020

7.2.1 Аутентификация и авторизация в конкретном отрезке сети

- Описание возможности: система IMT-2020 обеспечивает возможность аутентификации и авторизации в конкретном отрезке сети [3GPP TS 33.501] между оборудованием пользователя (UE) и сервером аутентификации, авторизации и учета (AAA-S), который может принадлежать внешней сторонней организации. После первоначальной аутентификации процесс аутентификации и авторизации в конкретном отрезке сети может инициироваться на основе информации, помогающей выбрать один определенный отрезок сети (S-NSSAI). Сервер AAA также может инициировать отзыв авторизации, повторную аутентификацию и повторную авторизацию в конкретном отрезке сети.
- Название возможности: аутентификация и авторизация в конкретном отрезке сети (NSSAA).
- Параметры безопасности: аутентификация, управление доступом.
- Возможные варианты:
  - NSSAA.0: выключена;

– NSSAA.1: включена.

7.2.2 Изоляция сетевых ресурсов отрезка сети

- Описание возможности: отрезки сети IMT-2020 работают на унифицированных ресурсах инфраструктуры оператора. Существует множество способов изоляции, предотвращающих возможности доступа элементов отрезка сети к элементам других отрезков сети или влияния на них через общие ресурсы инфраструктуры.

  В отношении доменов подсети отрезка сети:

  – Для сети доступа (AN). В случае радиоинтерфейса для распределения ресурсов доступны совместное использование ресурсов динамического радиоканала передачи данных (RB) и резервирование ресурсов статического RB. Первое отличается более гибким покрытием и более эффективным использованием ресурсов, а последнее – более высокой надежностью и стоимостью. В случае базовой станции центральный блок (CU) и распределенный блок (DU) разных отрезков сети могут быть одними и теми же. Для более высоких уровней изоляции они могут быть изолированы физически путем выделения оборудования или логически с помощью виртуализации сетевых функций (NFV) (например, виртуальной машины/контейнера) для совместного использования оборудования.

  – Для транспортной сети (TN). Изоляция в транспортных сетях может быть физической (физическая изоляция сетевых функций, физическая изоляция сетевых каналов и т. д.), логической (логическая изоляция сетевых функций, логическая/виртуальная изоляция сетевых каналов и т. д.) или отсутствовать [ITU-T X.1047].

  – Для базовой сети (CN). К физической изоляции ресурсов базовой сети относятся изоляция одной или нескольких выделенных физических сетевых функций (PNF), физическая изоляция выделенных сетевых каналов, изоляция географического местоположения, изоляция вычислительных ресурсов, изоляция памяти, изоляция устройства хранения данных, PNF, изоляция на основе функций защиты и т. д. К логической изоляции ресурсов базовой сети относятся изоляция одной или нескольких виртуальных сетевых функций (VNF), изоляция виртуальных каналов, изоляция технологий виртуализации, изоляция виртуальных вычислений, изоляция виртуальной оперативной памяти, изоляция виртуального устройства хранения данных, изоляция по географическому местоположению аппаратуры, которая виртуализирована для предоставления виртуальных ресурсов, изоляция на основе VNF-защиты и т. д. [ITU-T X.1047].

  В отношении типов ресурсов и методов изоляции:

  – для ресурсов радиоинтерфейса: совместное использование или резервирование RB;

  – для ресурсов сетевой функции AN/TN/CN: физическая изоляция, логическая изоляция или отсутствие изоляции.

- Название возможности: изоляция отрезка сети в отношении сетевых ресурсов (SIR).
- Параметры безопасности: управление доступом, доступность, секретность.
- Возможные варианты:
  – SIR.0: изоляция отсутствует;
  – SIR.1: логическая изоляция + общий RB;
  – SIR.2: логическая + физическая изоляция + общий RB;
  – SIR.3: физическая изоляция + общий RB;
  – SIR.4: логическая изоляция + резервирование RB;
  – SIR.5: логическая + физическая изоляция + резервирование RB;
  – SIR.6: физическая изоляция + резервирование RB.

7.2.3 Защита данных плоскости пользователя

- Описание возможности: система IMT-2020 может обеспечивать различные возможности защиты данных плоскости пользователя на уровне отрезка сети. Улучшенный узел B нового поколения (ng-eNB)/узел B NR (gNB) могут решать, следует ли активировать защиту конфиденциальности и/или целостности плоскости пользователя для каждого сеанса PDU,

в соответствии с принятой политикой безопасности плоскости пользователя. Политику безопасности плоскости пользователя можно настроить так, чтобы она указывала "требуется" или "не требуется". Существуют дополнительные алгоритмы шифрования [3GPP TS 33.501].

- Название возможности: защита данных плоскости пользователя (UPDP).
- Параметры безопасности: конфиденциальность данных, целостность данных.
- Возможные варианты:
  - UPDP.0: не задействовать защиту конфиденциальности и/или целостности данных плоскости пользователя;
  - UPDP.1: задействовать защиту конфиденциальности и/или целостности данных плоскости пользователя с помощью дополнительных алгоритмов шифрования.

7.2.4 Защита границ

- Описание возможности: важно защитить отрезок сети от сетевых атак, развернув функции/компоненты управления безопасностью на его границе, особенно на границе CN (например, установив конфигурацию N6Protection интерфейса N6) [b-3GPP TS 28.541]. Для разных пользователей отрезка сети функции/параметры управления безопасностью могут различаться и динамически изменяться в соответствии с требованиями. К функциям управления безопасностью относятся брандмауэр, трансляция сетевых адресов (NAT), защита от вредоносных программ, родительский контроль, защита от распределенных атак типа "отказ в обслуживании" (DDoS) и т. д. [b-3GPP TS 28.541]. К компонентам относятся правила переадресации, правила фильтрации, настройка параметров и т. д. В число требований могут входить управление доступом к сети передачи данных и механизм туннелирования.
- Название возможности: защита границ (BP).
- Параметры безопасности: управление доступом, доступность, безопасность связи.
- Возможные варианты:
  - BP.0: функции управления безопасностью отсутствуют;
  - BP.1: функции/компоненты управления безопасностью установлены.

7.2.5 Защита услуг приложения

- Описание возможности: операторы могут устанавливать устройства или модули обеспечения безопасности на стороне сети, чтобы обеспечить различные функции защиты услуг приложения, использующих отрезки сети, и пользователей услуг таких приложений. Например, сеть оператора может обеспечивать обнаружение аномальных терминалов, очистку сетевого трафика, обнаружение вредоносных унифицированных указателей ресурсов (URL), работу брандмауэра веб-приложений (WAF), защиту от DDoS-атак и т. д.
- Название возможности: защита услуг приложения (ASP).
- Параметры безопасности: безопасность связи, управление доступом, доступность.
- Возможные варианты:
  - ASP.0: защита услуг приложения отсутствует;
  - ASP.1: защита услуг приложения установлена.

7.2.6 Защита секретности идентификатора EAP во время сеанса NSSAA

- Описание возможности: для аутентификации конкретного отрезка сети могут использоваться разные методы расширяемого протокола аутентификации (EAP) [b-IETF RFC 3748]. Для защиты секретности идентификатора EAP, используемого для NSSAA на основе протокола EAP [3GPP TS 33.501], можно использовать один из методов EAP с возможностью защиты секретности, например защиту транспортного уровня (TLS) на основе протокола EAP [b-IETF RFC 5216], EAP-TTLS [b-IETF RFC 5281]).
- Название возможности: защита секретности идентификатора EAP во время сеанса NSSAA (PPEAP).
- Параметр безопасности: секретность.
- Возможные варианты:

– PPEAP.0: методы защиты секретности EAP не используются;

– PPEAP.1: методы защиты секретности EAP используются.

7.2.7 Защита секретности (S-)NSSAI

- Описание возможности: NSSAI используется для идентификации отрезка сети/типа услуг. Из NSSAI и по характеру ее использования можно получить определенные сведения о сети оператора и пользователях. Сеть IMT-2020 предоставляет возможности для защиты секретности (S-)NSSAI, позволяя не использовать NSSAI или использовать альтернативную информацию за пределами домена оператора. Во время процедуры регистрации функция управления доступом и мобильностью (AMF) может передавать UE в сообщении о принятии регистрации параметр режима включения NSSAI для установления соединения уровня доступа, указывающий, должно ли UE включать информацию NSSAI при установлении соединения уровня доступа в соответствии с различными режимами, и если да, то когда. По умолчанию в режиме доступа 3GPP UE не должно предоставлять NSSAI на уровне доступа, если только ему не дано указание работать в других режимах [b-3GPP TS 23.502]. Во время сеанса NSSAA, если используемый сервер AAA принадлежит третьей стороне, S-NSSAI которой служит внутренним ядром сети IMT-2020, то в сети оператора информация может дополнительно преобразовываться в информацию о внешнем отрезке сети (ENSI), которая передается и используется вне домена оператора [3GPP TS 33.501].
- Название возможности: защита секретности (S-)NSSAI (PPSI).
- Параметр безопасности: секретность.
- Возможные варианты:
  – PPSI.0: NSSAI используется за пределами домена оператора;
  – PPSI.1: NSSAI не используется за пределами домена оператора или используется альтернативная информация.

7.3 Классификация возможностей обеспечения безопасности в отрезке сети IMT-2020

Возможности обеспечения безопасности в отрезке сети IMT-2020 можно классифицировать по их параметрам безопасности, как показано в таблице 7-1.

Таблица 7-1 − Классификация возможностей обеспечения безопасности в отрезке сети IMT-2020 по параметрам безопасности

Параметр безопасности **Возможность обеспечения безопасности в отрезке сети**	**Аутентификация и авторизация в конкретном отрезке сети (NSSAA)**	**Изоляция отрезка сети в отношении сетевых ресурсов (SIR)**	**Защита данных плоскости пользователя (UPDP)**	**Защита границ (BP)**	**Защита услуг приложения (ASP)**	**Защита секретности идентификатора EAP во время сеанса NSSAA (PPEAP)**	**Защита секретности (S-)NSSAI (PPSI)**
Управление доступом	√	√		√	√		
Аутентификация	√						
Предотвращение отказа							
Конфиденциальность данных			√				
Безопасность связи				√	√		
Целостность данных			√				
Доступность		√		√	√		
Секретность		√				√	√

8 Классификация параметров безопасности, достигаемых за счет возможностей обеспечения безопасности в отрезке сети

8.1 Метод и принцип классификации параметров безопасности на основе возможностей обеспечения безопасности в отрезке сети

Рекомендуется следующий метод классификации каждого параметра безопасности:

1) перечислить возможности обеспечения безопасности, относящиеся к параметру безопасности, и их варианты. Если влияние какой-либо возможности обеспечения безопасности на параметр безопасности маловероятно, она может факультативно не указываться для данного измерения защиты, а указываться лишь для других параметров безопасности, на которые она главным образом влияет;

2) перечислить комбинации различных вариантов возможностей обеспечения безопасности и составить разные уровни параметров безопасности. Если параметр безопасности достигается с помощью нескольких средств обеспечения безопасности, то при комбинировании вариантов этих средств каждый уровень эффективности защиты должен оставаться согласованным для нескольких доменов или заинтересованных сторон. Запись xx.nn (например AC.1, …, DI.0) представляет собой имя уровня параметра безопасности xx.

В разделе 8.2 приведен общий список восьми параметров безопасности с уровнями, основанными на возможностях обеспечения безопасности и их вариантах, перечисленных в разделе 7.

8.2 Параметры безопасности с уровнями, основанными на возможностях обеспечения безопасности в отрезке сети IMT-2020

8.2.1 Управление доступом на основе возможностей обеспечения безопасности в отрезке сети IMT-2020

Управление доступом может обеспечиваться с помощью нескольких вариантов возможностей, в частности аутентификации и авторизации в отрезке сети, изоляции ресурсов отрезка сети, защиты границ и защиты услуг приложения. Существует множество комбинаций различных вариантов, обеспечивающих разные уровни управления доступом. Они приведены ниже на основании раздела 7.

Таблица 8-1 − Уровни управления доступом

Параметр безопасности: управление доступом (AC)														
Возможности	**Аутентификация и авторизация в конкретном отрезке сети (NSSAA)**		**Защита услуг приложения (ASP)**		**Изоляция отрезка сети в отношении сетевых ресурсов (SIR)**							**Защита границ (BP)**		**Наименование уровня**
Варианты	**NSSAA.0**	**NSSAA.1**	**ASP.0**	**ASP.1**	**SIR.0**	**SIR.1**	**SIR.2**	**SIR.3**	**SIR.4**	**SIR.5**	**SIR.6**	**BP.0**	**BP.1**	
Комбинации	NSSAA.0		ASP.0		SIR.0							BP.0		AC.0000
					SIR.0							BP.1		AC.0001
					SIR.1 SIR.4							BP.0		AC.0010 AC.0040
					SIR.1 SIR.4							BP.1		AC.0011 AC.0041
					SIR.2 SIR.5							BP.0		AC.0020 AC.0050
					SIR.2 SIR.5							BP.1		AC.0021 AC.0051
					SIR.3 SIR.6							BP.1		AC.0031 AC.0061
			ASP.1		SIR.0							BP.0		AC.0100
					SIR.0							BP.1		AC.0101
					SIR.1 SIR.4							BP.0		AC.0110 AC.0140

Таблица 8-1 − Уровни управления доступом

Параметр безопасности: управление доступом (AC)														
Возможности	**Аутентификация и авторизация в конкретном отрезке сети (NSSAA)**		**Защита услуг приложения (ASP)**		**Изоляция отрезка сети в отношении сетевых ресурсов (SIR)**							**Защита границ (BP)**		**Наименование уровня**
Варианты	**NSSAA.0**	**NSSAA.1**	**ASP.0**	**ASP.1**	**SIR.0**	**SIR.1**	**SIR.2**	**SIR.3**	**SIR.4**	**SIR.5**	**SIR.6**	**BP.0**	**BP.1**	
						SIR.1 SIR.4							BP.1	AC.0111 AC.0141
						SIR.2 SIR.5							BP.0	AC.0120 AC.0150
						SIR.2 SIR.5							BP.1	AC.0121 AC.0151
						SIR.3 SIR.6							BP.1	AC.0131 AC.0161
	NSSAA.1		ASP.0			SIR.0							BP.0	AC.1000
						SIR.0							BP.1	AC.1001
						SIR.1 SIR.4							BP.0	AC.1010 AC.1040
						SIR.1 SIR.4							BP.1	AC.1011 AC.1041
						SIR.2 SIR.5							BP.0	AC.1020 AC.1050
						SIR.2 SIR.5							BP.1	AC.1021 AC.1051
						SIR.3 SIR.6							BP.1	AC.1031 AC.1061
			ASP.1			SIR.0							BP.0	AC.1100
						SIR.0							BP.1	AC.1101
						SIR.1 SIR.4							BP.0	AC.1110 AC.1140
						SIR.1 SIR.4							BP.1	AC.1111 AC.1141
						SIR.2 SIR.5							BP.0	AC.1120 AC.1150
						SIR.2 SIR.5							BP.1	AC.1121 AC.1151
						SIR.3 SIR.6							BP.1	AC.1131 AC.1161

8.2.2 Аутентификация на основе возможностей обеспечения безопасности в отрезках сети IMT-2020

Аутентификация может обеспечиваться с помощью таких средств (возможностей), как аутентификация и авторизация в отрезке сети. Существует два уровня аутентификации. Они приведены ниже.

Таблица 8-2 − Уровни аутентификации

Параметр безопасности: аутентификация (Au)			
Возможность	**Аутентификация и авторизация в конкретном отрезке сети (NSSAA)**		**Наименование уровня**
Варианты	**NSSAA.0**	**NSSAA.1**	
Комбинации	NSSAA.0		Au.0
	NSSAA.1		Au.1

8.2.3 Предотвращение отказа на основе возможностей обеспечения безопасности в отрезках сети IMT-2020

Ни одна из возможностей, перечисленных в разделе 7, не обеспечивает предотвращение отказа.

8.2.4 Обеспечение конфиденциальности данных на основе возможностей обеспечения безопасности в отрезке сети IMT-2020

Конфиденциальность данных может обеспечиваться такими средствами, как защита данных плоскости пользователя. Существует два уровня аутентификации. Они приведены ниже.

Таблица 8-3 − Уровни конфиденциальности данных

Параметр безопасности: конфиденциальность данных (DC)			
Возможность	**Защита данных плоскости пользователя (UPDP)**		**Наименование уровня**
Варианты	**UPDP.0**	**UPDP.1**	
Комбинации	UPDP.0		DC.0
	UPDP.1		DC.1

8.2.5 Обеспечение безопасности связи на основе возможностей обеспечения безопасности в отрезке сети IMT-2020

Безопасность связи может обеспечиваться такими средствами, как защита границ и защита услуг приложения. Существует несколько комбинаций различных вариантов функций, обеспечивающих разные уровни безопасности связи. Они приведены ниже.

Таблица 8-4 − Уровни безопасности связи

Параметр безопасности: безопасность связи (CS)					
Возможности	**Защита границ (BP)**		**Защита услуг приложения (ASP)**		**Наименование уровня**
Варианты	**BP.0**	**BP.1**	**ASP.0**	**ASP.1**	
Комбинации	BP.0		ASP.0		CS.00
	BP.0		ASP.1		CS.01
	BP.1		ASP.0		CS.10
	BP.1		ASP.1		CS.11

8.2.6 Обеспечение целостности данных на основе возможностей обеспечения безопасности в отрезке сети IMT-2020

Целостность данных может обеспечиваться такими средствами, как защита данных плоскости пользователя. Существует два уровня целостности данных. Они приведены ниже.

Таблица 8-5 − Уровни целостности данных

Параметр безопасности: целостность данных(DI)			
Возможность	**Защита данных плоскости пользователя (UPDP)**		**Наименование уровня**
Варианты	**UPDP.0**	**UPDP.1**	
Комбинации	UPDP.0		DI.0
	UPDP.1		DI.1

8.2.7 Обеспечение доступности на основе возможностей обеспечения безопасности в отрезках сети IMT-2020

Доступность может обеспечиваться такими средствами, как изоляция отрезка сети в отношении сетевых ресурсов, защита границ и защита услуг приложения. Существует множество комбинаций различных вариантов, обеспечивающих разные уровни доступности. Они приведены ниже.

Таблица 8-6 − Уровни доступности

<table>
<tr><th colspan="8">Параметр безопасности: доступность (Av)</th></tr>
<tr><th rowspan="2">Возможности</th><th colspan="2">Защита услуг приложения (ASP)</th><th colspan="2">Изоляция отрезка сети в отношении сетевых ресурсов (SIR)</th><th colspan="2">Защита границ (BP)</th><th rowspan="2">Наименование уровня</th></tr>
<tr><th>Варианты</th><th>ASP.0</th><th>ASP.1</th><th>SIR.1/SIR.2/SIR.3</th><th>SIR.4/SIR.5/SIR.6</th><th>BP.0</th><th>BP.1</th></tr>
<tr><td rowspan="8">Комбинации</td><td colspan="2" rowspan="4">ASP.0</td><td colspan="2" rowspan="2">SIR.1/SIR.2/SIR.3</td><td colspan="2">BP.0</td><td>Av.000</td></tr>
<tr><td colspan="2">BP.1</td><td>Av.001</td></tr>
<tr><td colspan="2" rowspan="2">SIR.4/SIR.5/SIR.6</td><td colspan="2">BP.0</td><td>Av.010</td></tr>
<tr><td colspan="2">BP.1</td><td>Av.011</td></tr>
<tr><td colspan="2" rowspan="4">ASP.1</td><td colspan="2" rowspan="2">SIR.1/SIR.2/SIR.3</td><td colspan="2">BP.0</td><td>Av.100</td></tr>
<tr><td colspan="2">BP.1</td><td>Av.101</td></tr>
<tr><td colspan="2" rowspan="2">SIR.4/SIR.5/SIR.6</td><td colspan="2">BP.0</td><td>Av.110</td></tr>
<tr><td colspan="2">BP.1</td><td>Av.111</td></tr>
</table>

8.2.8 Обеспечение секретности на основе возможностей обеспечения безопасности в отрезках сети сети IMT-2020

Секретность может обеспечиваться с помощью таких средств, как защита секретности идентификатора EAP во время сеанса NSSAA и защита секретности (S-)NSSAI. Существует множество комбинаций различных вариантов, обеспечивающих разные уровни секретности. Они приведены ниже.

Таблица 8-7 − Уровни секретности

<table>
<tr><th colspan="6">Параметр безопасности: секретность (Pr)</th></tr>
<tr><th rowspan="2">Возможности</th><th colspan="2">Защита секретности ID EAP во время сеанса NSSAA (PPEAP)</th><th colspan="2">Защита секретности (S-)NSSAI (PPSI)</th><th rowspan="2">Наименование уровня</th></tr>
<tr><th>Варианты</th><th>PPEAP.0</th><th>PPEAP.1</th><th>PPSI.0</th><th>PPSI.1</th></tr>
<tr><td rowspan="4">Комбинации</td><td colspan="2">PPEAP.0</td><td colspan="2">PPSI.0</td><td>Pr.00</td></tr>
<tr><td colspan="2">PPEAP.0</td><td colspan="2">PPSI.1</td><td>Pr.01</td></tr>
<tr><td colspan="2">PPEAP.1</td><td colspan="2">PPSI.0</td><td>Pr.10</td></tr>
<tr><td colspan="2">PPEAP.1</td><td colspan="2">PPSI.1</td><td>Pr.11</td></tr>
</table>

9 Руководящие указания и требования к способам обеспечения безопасности в отрезках сети

Способ обеспечения безопасности в отрезке сети может характеризоваться набором параметров безопасности в зависимости от категории услуг. Возможно множество разновидностей способов обеспечения безопасности в отрезке сети в зависимости от комбинации параметров безопасности различных уровней. Но не все комбинации являются рациональными.

При определении способов обеспечения безопасности в отрезке сети рекомендуется применять следующие методы и принципы:

1) сначала определить уровни параметров безопасности с более высоким приоритетом в соответствии с требованиями обслуживания и характеристиками уровней;

2) определить уровни оставшихся параметров безопасности в соответствии с требованиями обслуживания и характеристиками уровней;

3) проверить отсутствие конфликтов между всеми параметрами безопасности в целях координации. В каждом отрезке варианты возможностей обеспечения безопасности для разных параметров безопасности, содержащих одну и ту же возможность, должны быть согласованы;

4) при актуализации вариантов некоторых средств или уровней параметров безопасности для данного способа обеспечения безопасности в отрезке сети рекомендуется изменить соответствующие средства и параметры безопасности, чтобы сохранить согласованность.

10 Руководящие указания и требования по классификации возможностей обеспечения безопасности в отрезке сети для заинтересованных сторон

Операторам отрезков сети рекомендуется подготовить собственный перечень возможностей обеспечения безопасности в отрезке сети на основе общего перечня, приведенного в разделе 7, и частных возможностей обеспечения безопасности.

Операторам отрезков сети рекомендуется подготовить собственный перечень параметров безопасности с указанием уровней на основе общего списка параметров безопасности с указанием уровней и своих частных возможностей обеспечения безопасности или других параметров в соответствии с методом, описанным в разделе 8.

Операторам отрезков сети рекомендуется подготовить собственный перечень способов обеспечения безопасности в отрезке сети в соответствии с методом, описанным в разделе 9.

Операторам отрезков сети рекомендуется определить возможности обеспечения безопасности и их варианты для экземпляра отрезка сети (например, при подготовке [b-ETSI TS 128 531]) на основе своего перечня возможностей обеспечения безопасности в отрезке сети или перечня параметров безопасности с указанием уровней либо своих перечней способов обеспечения безопасности в отрезке сети путем сопоставления уровней параметров безопасности или способов обеспечения безопасности в отрезке сети.

Тем пользователям отрезков сети, которые хорошо знают свои требования безопасности и соответствующие возможности обеспечения безопасности, рекомендуется выбрать комбинации средств обеспечения безопасности и их вариантов из общего перечня возможностей обеспечения безопасности в отрезке сети или перечня возможностей обеспечения безопасности в отрезке сети оператора.

Пользователям отрезков сети, которым известен результат применения того или иного параметра безопасности, которого они хотят добиться, рекомендуется выбрать уровни соответствующих параметров безопасности по их характеристикам из общего перечня параметров безопасности с указанием уровня или из перечня параметров безопасности оператора с указанием уровня.

Пользователям отрезков сети, мало знакомым с конкретными аспектами возможностей обеспечения безопасности, рекомендуется выбрать способ из представленного оператором перечня способов обеспечения безопасности в отрезке сети.

Дополнение I

Характеристики вариантов возможностей обеспечения безопасности в отрезках сети IMT-2020

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

ПРИМЕЧАНИЕ. – Характеристики зависят от конкретных деталей реализации и могут изменяться по мере развития технологии.

- Характеристики вариантов NSSAA:
  - NSSAA.0: базовый уровень;
  - NSSAA.1: больше автономии (для вертикальной отрасли).
- Характеристики вариантов SIR:
  - SIR.0: изоляция отсутствует: базовый уровень;
  - SIR.1: логическая изоляция + совместное использование RB: SIR.1 обладает большей гибкостью и может требовать меньших затрат по сравнению с SIR.2 и SIR.3;
  - SIR.2: логическая + физическая изоляция + совместное использование RB: SIR.2 обладает большей гибкостью и может требовать меньших затрат по сравнению с SIR.3. SIR.2 обеспечивает более высокую надежность, чем SIR.1;
  - SIR.3: физическая изоляция + совместное использование RB: SIR.3 обеспечивает более высокую надежность и требует более крупных затрат ресурсов, чем SIR.1 и SIR.2;
  - SIR.4: логическая изоляция + резервирование RB: SIR.4 обладает большей гибкостью и может требовать меньших затрат по сравнению с SIR.5 и SIR.6;
  - SIR.5: логическая + физическая изоляция + резервирование RB: SIR.5 обладает большей гибкостью и может требовать меньших затрат по сравнению с SIR.6. SIR.2 обеспечивает более высокую надежность, чем SIR.4;
  - SIR.6: физическая изоляция + резервирование RB: SIR.6 обеспечивает более короткую задержку, повышенную надежность и требует более крупных затрат, чем остальные варианты.

Варианты с логической изоляцией могут требовать меньших затрат ресурсов сервера по сравнению с вариантами с физической изоляцией, но в то же время могут требовать бóльших затрат на контрмеры в области безопасности для достижения той же эффективности защиты.

Варианты с физической изоляцией могут обеспечить более высокий уровень управления доступом, чем варианты с логической изоляцией.

Варианты с совместным использованием RB отличаются более гибким покрытием и более эффективным использованием ресурсов по сравнению с вариантами с резервированием RB.

- Характеристики вариантов UPDP:
  - UPDP.0: отсутствующая защита данных в радиоинтерфейсе и более короткая задержка, чем у UPDP.1;
  - UPDP.1: обеспечивает защиту данных в радиоинтерфейсе с различными результатами в зависимости от дополнительных алгоритмов шифрования.
- Характеристики вариантов BP:
  - BP.0: базовый уровень;
  - BP.1: обеспечивает защиту границ с различными результатами в зависимости от установленных дополнительных функций/компонентов управления.

- Характеристики вариантов ASP:
  - ASP.0: базовый уровень;
  - ASP.1: обеспечивает защиту услуг приложения с различными результатами в зависимости от дополнительных средств защиты услуг приложения.
- Характеристики вариантов PPEAP:
  - PPEAP.0: идентичность UE открыта;
  - PPEAP.1: идентичность UE анонимна.
- Характеристики вариантов PPSI:
  - PPSI.0: (S-)NSSAI открыта;
  - PPSI.1: (S-)NSSAI нераскрыта.

Дополнение II

Пример основных способов обеспечения безопасности в отрезке сети IMT-2020

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Следующая таблица основных способов обеспечения безопасности в отрезке сети составлена на основе метода, описанного в разделе 9. Заинтересованные стороны могут непосредственно воспользоваться этим методом или адаптировать его для определения собственных основных способов обеспечения безопасности в отрезке сети.

Таблица II.1 − Примеры основных способов обеспечения безопасности в отрезке сети

Способ обеспечения безопасности в отрезках сети	Управление доступом	Аутентификация	Доступность	Безопасность связи	Конфиденциальность данных	Целостность данных	Предотвращение отказа	Секретность	Характеристика	Подходящие услуги
0	AC.0	Au.0	Av.0	CS.0	DC.0	DI.0	–	Pr.0	Базовая защита	Общедоступная сеть
1	AC.1161	Au.1	Av.111	CS.11	DC.1	DI.1	–	Pr.11	Высокая надежность, самая высокая стоимость	Услуги с высокими требованиями к безопасности, такие как частные линии для клиентов из сферы государственного управления, финансовых услуг, ценных бумаг и энергетики
2	AC.0000	Autor.0	Av.0	CS.0	–	–	–	–	Низкая стоимость	Недорогие услуги, услуги доступа в интернет и видео по технологии OTT
3	AC.xx61	–	Av.x11	–	–	–	–	Pr.xx4 Pr.xx6	Высокая степень изоляции, высокая стоимость	Услуги с требованием высокой степени изоляции
4	–	–	Av.x1x	–	DC.0	DI.0	–	–	Короткая задержка	Услуги с требованием короткой задержки, такие как облачные игры

ПРИМЕЧАНИЕ. – В порядковом номере наименования уровня x означает любое значение.

Библиография

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

[b-3GPP TS 23.502] 3GPP TS 23.502, *Procedures for the 5G System (5GS).*
https://www.3gpp.org/ftp/Specs/archive/23_series/23.502

[b-3GPP TS 28.541] 3GPP TS 28.541, *Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3.*
https://www.3gpp.org/ftp/Specs/archive/28_series/28.541

[b-IETF RFC 3748] IETF RFC 3748, *Extensible Authentication Protocol (EAP).*
https://tools.ietf.org/html/rfc3748

[b-IETF RFC 5216] IETF RFC 5216, *The EAP-TLS Authentication Protocol.*
https://www.rfc-editor.org/rfc/rfc5216.html

[b-IETF RFC 5281] IETF RFC 5281, *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0).*
https://datatracker.ietf.org/doc/html/rfc5281

[b-ETSI TS 128 530] Technical Specification ETSI TS 128 530 V17.1.0 (2022), *5G; Management and orchestration; Concepts, use cases and requirements* (3GPP TS 28.530 version 17.2.0 Release 17).
https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.02.00_60/ts_128530v170200p.pdf

[b-ETSI TS 128 531] Technical Specification ETSI TS 128 531 V16.9.0 (2021), *5G; Management and orchestration; Provisioning;* (3GPP TS 28.531 version 16.6.0 Release 16).
https://www.etsi.org/deliver/etsi_ts/128500_128599/128531/16.06.00_60/ts_128531v160600p.pdf

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2023 г.