Международный союз электросвязи

МСЭ-Т D.1140/X.1261

(08/2020)

СЕКТОР СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ D: ПРИНЦИПЫ ТАРИФИКАЦИИ И УЧЕТА И ЭКОНОМИЧЕСКИЕ И СТРАТЕГИЧЕСКИЕ ВОПРОСЫ МЕЖДУНАРОДНОЙ ЭЛЕКТРОСВЯЗИ/ИКТ

Рекомендации по экономическим и стратегическим вопросам международной электросвязи/ИКТ – Экономические и политические аспекты больших данных и цифровой идентичности в услугах и сетях международной электросвязи

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

Безопасность киберпространства – Управление определением идентичности

Политическая основа, включая принципы для инфраструктуры цифровой идентичности

Рекомендация МСЭ-Т D.1140/X.1261

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ D

ПРИНЦИПЫ ТАРИФИКАЦИИ И УЧЕТА И ЭКОНОМИЧЕСКИЕ И СТРАТЕГИЧЕСКИЕ ВОПРОСЫ МЕЖДУНАРОДНОЙ ЭЛЕКТРОСВЯЗИ/ИКТ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	D.0
ОБЩИЕ ПРИНЦИПЫ ТАРИФИКАЦИИ	
Аренда средств электросвязи для частного пользования	D.1–D.9
Принципы тарификации, применимые к службам передачи данных по специализированным сетям данных общего пользования	D.10–D.39
Начисление платы и учет в международной телеграфной службе общего пользования	D.40–D.44
Начисление платы и учет в международной службе телесообщений	D.45–D.49
Принципы, применимые к ГИИ-Интернет	D.50–D.59
Начисление платы и учет в международной службе телекс	D.60–D.69
Начисление платы и учет в международной факсимильной службе	D.70–D.75
Начисление платы и учет в международной службе видеотекс	D.76–D.79
Начисление платы и учет в международной фототелеграфной службе	D.80–D.89
Начисление платы и учет в службах подвижной связи	D.90–D.99
Начисление платы и учет в международной телефонной службе	D.100–D.159
Составление счетов и обмен счетами международной телефонной и телексной связи	D.160–D.179
Международная передача программ звукового вещания и телевидения	D.180–D.184
Начисление платы и учет по услугам международной спутниковой связи	D.185–D.189
Передача ежемесячных сведений, относящихся к международной финансовой отчетности	D.190–D.191
Служебная и привилегированная электросвязь	D.192–D.195
Погашение сальдо международных счетов за электросвязь	D.196–D.209
Принципы начисления платы и учета для услуг международной электросвязи, предоставляемых ЦСИС	D.210–D.260
Экономические и политические факторы, имеющие отношение к эффективному предоставлению услуг международной электросвязи	D.261–D.269
Принципы начисления платы и учета для сетей последующих поколений (СПП)	D.270–D.279
Принципы начисления платы и учета для универсальной персональной электросвязи	D.280–D.284
Принципы начисления платы и учета для услуг, предоставляемых интеллектуальной сетью	D.285–D.299
РЕКОМЕНДАЦИИ ДЛЯ РЕГИОНАЛЬНОГО ПРИМЕНЕНИЯ	
Рекомендации, применимые в Европе и бассейне Средиземного моря	D.300–D.399
Рекомендации, применимые в Латинской Америке	D.400–D.499
Рекомендации, применимые в Азии и Океании	D.500–D.599
Рекомендации, применимые в Африканском регионе	D.600–D.699
Рекомендации для Региональной группы ИКЗ МСЭ-Т для Арабского региона (РегГр-АРБ ИКЗ)	D.700–D.799
Рекомендации для Региональной группы ИКЗ МСЭ-Т для Восточной Европы, Центральной Азии и Закавказья (РегГр-ВЕЦАЗ ИКЗ)	D.800–D.899
РЕКОМЕНДАЦИИ ПО ЭКОНОМИЧЕСКИМ И СТРАТЕГИЧЕСКИМ ВОПРОСАМ МЕЖДУНАРОДНОЙ ЭЛЕКТРОСВЯЗИ/ИКТ	
Механизмы начисления платы и учета/расчетов за услуги международной электросвязи	D.1000–D.1019
Экономические и политические факторы, имеющие отношение к эффективному предоставлению услуг международной электросвязи	D.1020–D.1039
Международные интернет-соединения, а также вопросы тарифов и начисления платы применительно к соглашениям о взаиморасчетах за использование транснациональной наземной электросвязи	D.1040–D.1059
Вопросы, связанные с международным мобильным роумингом	D.1060–D.1079
Альтернативные процедуры вызова, а также неправомерное присвоение и неправомерное использование оборудования и услуг	D.1080–D.1099
Экономическое и регуляторное воздействие интернета, конвергенции (услуг или инфраструктуры) и новых услуг	D.1100–D.1119
Определение надлежащих рынков, политика в области конкуренции и выявление операторов, обладающих значительным влиянием на рынке (SMP)	D.1120–D.1139
Экономические и политические аспекты больших данных и цифровой идентичности в услугах и сетях международной электросвязи	**D.1140–D.1159**
Экономические и стратегические вопросы, относящиеся к мобильным финансовым услугам (МФУ)	D.1160–D.1179

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

Рекомендация МСЭ-T D.1140/X.1261

Политическая основа, включая принципы для инфраструктуры цифровой идентичности

Резюме

В Рекомендации МСЭ-T D.1140/X.1261 сформулирована политическая основа, включая принципы для инфраструктуры цифровой идентичности, при этом признается суверенное право каждого Государства-Члена регулировать свою электросвязь.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-T D.1140/X.1261	28.08.2020 г.	3-я	11.1002/1000/14270

Ключевые слова

Цифровая идентичность.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует 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 с целью стандартизации электросвязи на всемирной основе.

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Введение

По мере того как мир становится все более соединенным, государственные органы и поставщики услуг предоставляют онлайновый доступ ко все большему числу услуг. Хотя участие в такой цифровой революции приветствуется, одним из препятствий для этого остается необходимость решения сложной задачи идентификации. Обеспечение возможности доступа для всех слоев общества к экономике, ее инфраструктуре и учреждениям может оказаться сложной задачей в связи с отсутствием механизма проверки идентичности, который признавался бы во всех областях. Людям необходимо идентифицировать друг друга и идентифицировать себя, чтобы получить доступ ко множеству государственных и негосударственных услуг. Отсутствие легко проверяемого механизма идентичности приводит к неравноправию, если человек не может подтвердить свою личность, что может оказаться препятствием для получения им доступа к услугам электросвязи/другим услугам (банкинг, доступ к кредитам)/льготам и субсидиям, предоставляемым правительствами. Таким образом, удостоверение личности становится одной из предпосылок социально-экономического развития.

Механизм, позволяющий однозначно идентифицировать законную форму данных, в том числе отдельного человека или структуру, и обеспечить мгновенную проверку и аутентификацию идентичности, обладает целым рядом преимуществ. Способность легко и незамедлительно подтвердить чью-либо идентичность может снизить транзакционные издержки и повысить степень удовлетворенности пользователя. Одним из путей достижения этой цели является использование программ *цифровой идентичности (цифровой ИД)*, центральных реестров, в которых хранятся персональные данные в цифровой форме, и регистрационных данных, которые используют в большей степени цифровые, а не физические механизмы проверки идентичности их обладателя.

Несмотря на это, как правило, существуют два резко противоположных мнения о способах защиты цифровой идентичности: i) создание мощных защитных механизмов для сохранения конфиденциальности личной информации; или ii) предоставление частным компаниям и государственным органам возможности делать все необходимое для реализации экономического потенциала больших данных, источником которых является использование цифровой идентичности. Государства-Члены, регуляторные органы, инициативные группы и отдельные лица обеспокоены возможностью неправомерного использования личной информации. Очевидно, что необходимо найти баланс между максимальными экономическими результатами и защитой неприкосновенности частной жизни людей. В нынешней ситуации формирование политической основы, включающей принципы для программ цифровой идентичности, стало ключевой приоритетной областью для Государств − Членов МСЭ.

Рекомендация МСЭ-Т D.1140/X.1261

Политическая основа, включая принципы для инфраструктуры цифровой идентичности

1 Сфера применения

В настоящей Рекомендации предлагается политическая основа для цифровой идентичности, включая принципы проектирования инфраструктуры цифровой идентичности.

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 статуса Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации определены следующие термины:

3.1.1 атрибут (attribute) [b-ITU-T X.1252]: Информация, связанная с объектом, которая означает какую-либо его характеристику.

3.1.2 аутентификация (authentication) [b-ITU-T X.1252]: Процесс, используемый для достижения достаточной меры доверия в связи между объектом и представленной идентичностью.

3.1.3 авторизация (authorization) [b-ITU-T Y.2720] и [b-ITU-T X.800]: Предоставление прав и, на основе этих прав, предоставление доступа.

3.1.4 цифровая идентичность (digital identity) [b-ITU-T X.1252]: Цифровое представление информации, известной о конкретном лице, группе или организации.

3.1.5 объект (entity) [b-ITU-T X.1252]: Что-либо, что существует отдельно и обособленно и может быть определено в контексте.

ПРИМЕЧАНИЕ. – Объектом может быть физическое лицо, животное, юридическое лицо, организация, активный или пассивный предмет, устройство, применение программного обеспечения, услуга и т. п., или группа таких объектов. В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, применения программного обеспечения, услуги и устройства, интерфейсы и т. п.

3.1.6 идентификация (identification) [b-ITU-T X.1252]: Процесс опознания объекта по контекстуальным характеристикам.

3.1.7 идентификатор (identifier) [b-ITU-T X.1252]: Один или несколько атрибутов, используемых для идентификации объекта в том или ином контексте.

3.1.8 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ITU-T X.1252]: Любая информация, a) которая идентифицирует или может использоваться для идентификации, обращения или установления местоположения лица, к которому такая информация относится; b) на основе которой может быть осуществлена идентификация или получение контактной информации частного лица; или c) которая прямо или косвенно связана либо может быть связана с физическим лицом.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 инфраструктура цифровой идентичности (digital identity infrastructure): Система, обладающая набором функций (например, присвоения, администрирования, управления и технического обслуживания, обнаружения, обмена сообщениями, обеспечения реализации политики, аутентификации и утверждения, безопасности) для идентификации, аутентификации и авторизации цифровой идентичности объекта (например, идентификаторы, атрибуты) и т. п.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

API	Application Programme Interface	Интерфейс прикладного программирования
DII	Digital Identity Infrastructure	Инфраструктура цифровой идентичности
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PKI	Public Key Infrastructure	Инфраструктура открытых ключей

5 Соглашения

Отсутствуют.

6 Политическая основа и принципы для инфраструктуры цифровой идентичности

6.1 Политическая основа

6.1.1 Государствам-Членам настоятельно рекомендуется создавать инфраструктуру цифровой идентичности (DII) для присвоения цифровой идентичности, которая может использоваться для целенаправленного предоставления государственных услуг, в том числе субсидий, льгот и услуг. DII может использоваться для различных программ социального обеспечения. Коммерческие предприятия, поставщики услуг и другие структуры могут также использовать DII для адресного предоставления своих услуг. Государствам-Членам следует работать над обеспечением координации между соответствующими государственными учреждениями **и заинтересованными сторонами**, которые будут участвовать в развертывании и управлении DII.

6.1.2 Государствам-Членам следует поощрять присвоение цифровой идентичности, которая должна быть достаточно безопасной и надежной, чтобы исключить возможность ее подделки или копирования, и которую можно было бы проверить и аутентифицировать экономичным способом.

6.1.3 Государствам-Членам следует поощрять предоставление возможностей использования цифровой идентичности для получения широкого диапазона услуг через открытые и безопасные интерфейсы.

6.1.4 Государствам-Членам следует обеспечить, чтобы DII выполняла три основные функции:

- идентификация (для установления личности);
- аутентификация (для подтверждения личности); и
- авторизация (для разрешения использовать цифровую идентичность).

6.1.5 В рамках программ цифровой идентичности, созданных Государствами-Членами, следует обеспечить, чтобы каждый житель/пользователь, который имеет право на присвоение цифровой идентичности, получал ее при предоставлении необходимой информации.

6.1.6 Государствам-Членам следует также рассмотреть возможность принятия специальных мер для присвоения цифровой идентичности представителям уязвимых слоев общества, в частности женщинам, детям, престарелым, лицам с ограниченными возможностями, а также жителям, которые

проживают в районах с недостаточным уровнем обслуживания и могут не иметь постоянного адреса, и для содействия этому процессу.

6.1.7 Государствам-Членам следует принять надлежащие меры для защиты цифровой идентичности от киберугроз.

6.1.8 Каждая страна обладает суверенным правом регулировать свою электросвязь и, соответственно, регулировать предоставление инфраструктуры цифровой идентичности (DII) в контексте национальных законов о защите данных.

6.2 Руководящие принципы для инфраструктуры цифровой идентичности

6.2.1 При создании инфраструктуры цифровой идентичности Государствам-Членам следует применять на этапах технического проектирования и разработки принципы и политические соображения, касающиеся универсальности, доступности, контролируемости и защиты информации, позволяющей установить личность (PII).

6.2.2 При проектировании инфраструктуры цифровой идентичности следует принимать во внимание следующие принципы:

- Простота
  - Легко внедрять и использовать
- Развязывание
  - Атрибуты не связаны с объектом
- Минимизация
  - Количество атрибутов, которые используются для создания цифровой идентичности, следует поддерживать на необходимом и пропорциональном уровне
- Уникальность
  - Каждому жителю/пользователю Государство-Член присваивает только одну цифровую идентичность для доступа к государственным услугам
- Открытость
  - Основана на открытых интерфейсах прикладного программирования (API)
- Безопасность
  - Инфраструктуру следует защищать от несанкционированного доступа, утечек, проникновений, кражи и т. д. путем использования, в том числе, инфраструктуры открытых ключей (PKI).

6.2.3 Проектирование DII должно быть гибким и масштабируемым для соответствия будущим требованиям, возникающим по мере дальнейшего развития цифровых технологий.

Библиография

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

[ITU-T X.1250] Рекомендация МСЭ-Т X.1250 (2009 г.), *Базовые возможности для улучшенного доверия и функциональной совместимости при глобальном управлении определением идентичности.*

[ITU-T X.1251] Рекомендация МСЭ-Т X.1251 (2009 г.), *Структура осуществляемого пользователем управления в отношении цифровой идентичности.*

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

[ITU-T X.1255] Рекомендация МСЭ-Т X.1255 (2010 г.), *Структура обнаружения информации по управлению определением идентичности.*

[ITU-T X.1258] Рекомендация МСЭ-Т X.1258 (2016 г.), *Улучшенная аутентификация объектов на основании объединенных атрибутов.*

[ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.), *Структура управления определением идентичности в СПП.*

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (11/2015), *Big Data − Cloud computing based requirements and capabilities.*

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	X.1140–X.1149
Протоколы безопасности (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.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
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
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
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

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

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, 2021 г.