Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1605

(03/2020)

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

Безопасность облачных вычислений –
Проектирование безопасности облачных вычислений

# Требования безопасности к открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений

Рекомендация МСЭ-Т X.1605

ITU-T

Международный союз электросвязи

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 распределения реестра | X.1400–X.1429 |
| Безопасность технологии распределения 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 | X.1700–X.1729 |

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

# Рекомендация МСЭ-Т X.1605

## Требования безопасности к открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений


### Резюме

Функционирование платформ инфраструктуры как услуги (IaaS) и виртуализированных услуг сопряжено с различными и, возможно, более многочисленными проблемами и угрозами по сравнению с работой традиционной инфраструктуры и приложений информационных технологий. Платформы IaaS, которые совместно используют услуги вычислений, хранилища данных и сетевые службы, нуждаются в средствах защиты, соответствующих угрозам, которые возникают в среде IaaS. Цель Рекомендации МСЭ-Т X.1605 заключается в описании требований безопасности к открытой IaaS в помощь поставщикам IaaS при повышении безопасности платформы IaaS на этапах планирования, создания и эксплуатации.



### Хронологическая справка

| Издание | Рекомендация | Утверждено | Исследовательская комиссия | Уникальный идентификатор* |
|---|---|---|---|---|
| 1.0 | МСЭ-Т X.1605 | 26.03.2020 г. | 17-я | 11.1002/1000/14094 |

### Ключевые слова

Облачные вычисления, IaaS, требования безопасности, виртуальные ресурсы.


* 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, 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**

# Рекомендация МСЭ-Т X.1605

## Требования безопасности к открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений

### 1 Сфера применения

В настоящей Рекомендации представлен анализ проблем безопасности, с которыми сталкиваются поставщики инфраструктуры как услуги (IaaS) в среде IaaS, и определены требования безопасности к открытой IaaS в среде облачных вычислений. Настоящая Рекомендация предназначена для поставщиков открытой IaaS.

В Рекомендации приведено высокоуровневое описание требований безопасности реализации IaaS. Детальное руководство по реализации не входит в сферу применения настоящего документа.

### 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.1642] Рекомендация МСЭ-Т X.1642 (2016 г.), *Руководящие указания по эксплуатационной безопасности облачных вычислений.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3513] Recommendation ITU-T Y.3513 (2014), *Cloud computing – Functional requirements of Infrastructure as a Service*.

[ISO/IEC 27002] ИСО/МЭК 27002:2013, *Информационные технологии – Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью*.

[ISO/IEC 27031] ISO/IEC 27031:2011, *Information technology –Security techniques– Guidelines for information and communication technology readiness for business continuity*.

### 3 Определения

#### 3.1 Термины, определенные в других документах

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

**3.1.1 облачные вычисления (cloud computing)** [b-ITU-T Y.3500]: Парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу.

**3.1.2 облачная услуга (cloud service)** [b-ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений, обращение к которым производится с помощью заявленного интерфейса.

**3.1.3 потребитель облачной услуги (cloud service customer, CSC)** [b-ITU-T Y.3500]: Сторона, которая состоит в коммерческих отношениях применительно к использованию облачных услуг.

**3.1.4 партнер по облачной услуге (cloud service partner)** [b-ITU-T Y.3500]: Сторона, участвующая в поддержке деятельности поставщика или потребителя облачной услуги или того и другого либо оказывающая помощь в этой деятельности.

**3.1.5 поставщик облачной услуги (cloud service provider, CSP)** [b-ITU-T Y.3500]: Сторона, которая предоставляет облачные услуги.

**3.1.6 инфраструктура как услуга (infrastructure as a service, IaaS))** [b-ITU-T Y.3500]: Категория облачных услуг, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, являются возможности инфраструктуры.

**3.1.7 проблема безопасности (security challenge)** [b-ITU-T X.1601]: Отличная от непосредственной угрозы безопасности "трудность", включающая "косвенные" угрозы, которая обусловлена характером и рабочей средой облачных услуг.

**3.1.8 уязвимость (vulnerability)** [b-NIST-SP-800-30]: Слабое место информационной системы, процедур обеспечения безопасности системы, внутренних средств управления или реализации, на которое может быть направлено действие источника угрозы.

## 3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

# 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

| | | | |
|---|---|---|---|
| ACL | Access Control List | | Список управления доступом |
| API | Application Programming Interface | | Интерфейс прикладного программирования |
| BIA | Business Impact Analysis | | Анализ последствий для деятельности |
| CPU | Central Processing Unit | | Центральный процессор |
| CSC | Cloud Service Customer | | Потребитель облачной услуги |
| CSP | Cloud Service Provider | | Поставщик облачной услуги |
| DDoS | Distributed Denial of Service | | Распределенный отказ в обслуживании |
| DRO | Disaster Recovery Object | | Объект восстановления после чрезвычайных ситуаций |
| DSP | Digital Service Provider | | Поставщик цифровых услуг |
| IAM | Identity and Access Management | | Управление определением идентичности и доступом |
| IaaS | Infrastructure as a Service | | Инфраструктура как услуга |
| ICT | Information and Communication Technology | ИКТ | Информационно-коммуникационные технологии |
| IdM | Identity Management | | Управление определением идентичности |
| I/O | Input/Output | | Ввод/вывод |
| NIC | Network Interface Card | | Карта сетевого интерфейса |
| OS | Operating System | ОС | Операционная система |
| OTT | Over The Top | | Over The Top |
| PaaS | Platform as a Service | | Платформа как услуга |
| RPO | Recovery Point Objective | | Целевая точка восстановления |
| RTO | Recovery Time Objectives | | Целевые сроки восстановления |
| SaaS | Software as a Service | | Программное обеспечение как услуга |
| SLA | Service Level Agreement | | Соглашение об уровне обслуживания |

| | | |
|---|---|---|
| SQL | Structured Query Language | Язык структурированных запросов |
| VDC | Virtual Data Centre | Виртуальный центр обработки данных |
| VLAN | Virtual Local Area Network | Виртуальная локальная сеть |
| VM | Virtual Machine | Виртуальная машина |
| VXLAN | Virtual Extensible Local Area Network | Виртуальная расширяемая локальная сеть |
| XSS | Cross Site Script | Межсайтовый сценарий |

## 5 Соглашения

В настоящей Рекомендации ключевые слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевое слово "рекомендуется" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии 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 функция может быть активирована по желанию оператора сети/поставщика услуг дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии настоящей спецификации.

В тексте настоящей Рекомендации и приложений к ней иногда встречаются слова "должен", "не должен", "следует" и "может", и в таком случае их следует понимать соответственно как "требуется", "запрещается", "рекомендуется" и "возможно". Такие фразы или ключевые слова, фигурирующие в дополнении или материалах, явно помеченных как информационные, должны толковаться как не несущие нормативного смысла.

## 6 Обзор

Инфраструктура как услуга (IaaS) – это категория облачных услуг, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги (CSC), является тип возможностей инфраструктуры [b-ITU-T Y.3500]. IaaS обеспечивает для CSC возможность использования ресурсов облачной инфраструктуры (вычислительные ресурсы, ресурсы хранилища или сетевые ресурсы), которые могут быть оперативно предоставлены и высвобождены при минимальных управляющих действиях. Услуги открытой IaaS позволяют CSC быстро и без трудностей начать свою деятельность без необходимости создания новой инфраструктуры информационно-коммуникационных технологий (ИКТ), и CSC могут при необходимости использовать эти ресурсы для разработки, размещения и функционирования услуг и приложений по требованию гибким и масштабируемым образом.

На рисунке 6-1 представлена высокоуровневая концепция требований безопасности IaaS, в основе которой лежит многоуровневая структура, разработанная совместно с ИСО/МЭК и описанная в [ITU-T Y.3502], и концепция высокого уровня IaaS, описанная в [ITU-T Y.3513].


**Рисунок 6-1 – Высокоуровневая концепция требований безопасности IaaS**

Пользовательский уровень – это интерфейс пользователя, по которому CSC взаимодействует с поставщиком облачной услуги (CSP). Функциональные компоненты пользовательского уровня включают функцию пользователя, бизнес-функцию и функцию администратора, которые взаимодействуют с облачными услугами, предоставляемыми CSP, выполняют связанные с CSC административные действия и осуществляют мониторинг облачных услуг. В соответствии с распределением функций между CSP и CSC, ответственность за механизмы безопасности пользовательского уровня должны нести CSC, так как CSC обычно используют собственные инструменты и системы для доступа к услуге IaaS. В противном случае, если инструменты и системы пользовательского уровня предоставляет CSP, CSP должен обеспечивать инструменты и системы, отвечающие передовому опыту отрасли в области безопасности. Требования безопасности пользовательского уровня не входят в сферу применения настоящей Рекомендации.

Уровень доступа обеспечивает общий интерфейс для ручного и автоматического доступа к возможностям, предоставляемым на уровне услуг. Функциональные компоненты уровня доступа включают контроль доступа и управление соединениями. Ответственность уровня доступа заключается в представлении возможностей услуг IaaS через один или несколько механизмов доступа, например веб-интерфейсы и интерфейсы прикладного программирования (API). Требования безопасности уровня доступа определены в разделе 8.

Уровень услуг содержит реализацию услуг IaaS, которые предоставляет CSP. Этот уровень содержит и контролирует программные компоненты, реализующие услуги IaaS, и выполняет их упорядочение для предложения этих услуг CSC через уровень доступа. Требования безопасности уровня услуг определены в разделе 9.

Компоненты уровня ресурсов включают абстрактное представление ресурсов и управление ресурсами, а также физические ресурсы, как это определено в [ITU-T Y.3502]. С помощью программной абстракции происходит создание виртуализированных ресурсов и управление ими. Требования безопасности уровня ресурсов определены в разделе 10.

Управление безопасностью обеспечивает основные возможности управления межуровневой безопасностью, которые реализуются на пользовательском уровне, уровне доступа, уровне безопасности и уровне ресурсов и описаны выше. Требования к управлению безопасностью управления определением идентичностью и управления доступом, аудита безопасности, управления уязвимостями, реагирования на чрезвычайные ситуации, восстановления после чрезвычайных ситуаций и резервного копирования определены в разделе 11.

## 7 Проблемы безопасности в среде IaaS

IaaS, в силу огромного числа обеспечиваемых преимуществ, стала одной из важнейших услуг CSP, в особенности для традиционных операторов электросвязи, поставщиков услуг over the top (OTT) и цифровых услуг (DSP), и получила широкое распространение. В условиях быстрого развития IaaS вопросы обеспечения безопасности по-прежнему составляют серьезную и важную проблему, которую нельзя игнорировать. Функционирование платформ и услуг IaaS сопряжено с более многочисленными проблемами и угрозами по сравнению с работой традиционной инфраструктуры и приложений информационных технологий, особенно в результате широкой реализации технологий виртуализации, совместного использования ресурсов для множества пользователей-арендаторов и т. д.

В открытой IaaS может работать большое число сосуществующих CSC из самых различных организаций, поэтому важнейшими факторами при выборе CSC услуг открытой IaaS являются безопасность и защита конфиденциальности.

Проблемы безопасности, которые возникают при функционировании открытой IaaS, могут быть обусловлены нижеследующими факторами.

1) Виртуализация: как одна из важнейших технических особенностей облачных вычислений, технология виртуализации позволяет различным виртуальным машинам (VM) работать под управлением одного гипервизора, но также делает файлы, содержащиеся в VM, уязвимыми к незаконному изменению. Кроме того, при эксплуатации уязвимостей гипервизора все работающие в его среде VM подвергаются одинаковым рискам безопасности. Эти риски могут быть вызваны:
   - ненадлежащей конфигурацией и сетевой изоляцией физических хостов: злоумышленники могут напрямую использовать уязвимости гипервизора;
   - уязвимостями интерфейсов между VM и гипервизором: злоумышленники могут использовать уязвимости для управления гипервизором, что называется выводом VM.
2) Открытые API: в качестве предпосылки автоматического управления VM открытые API могут расширять области атаки в результате злонамеренного использования или эксплуатации таких уязвимостей, как отсутствие аутентификации, авторизации или проверки целостности, что приведет к уничтожению большого числа приложений.
3) Сетевые и интернет-соединения: сетевые угрозы, такие как распределенная атака типа "отказ в обслуживании" (DDoS), атака через посредника, атака типа IP-спуфинга и т. д., могут предприниматься не только из традиционной сети, но и из VM в той же хост-машине, защиту от которых значительно сложнее обеспечить в среде виртуализированной сети с нечеткими границами.
4) Высокий уровень совместного использования ресурсов: эта техническая особенность может обусловить более точную цель. В случае нарушения физической хост-машины или физической сети пострадают все работающие в их среде VM. Удаление отслуживших свой срок или замененных запоминающих устройств связано с вопросом обеспечения конфиденциальности всех данных CSC. Такое совместное использование может также усложнить изолирование разных CSC. В случае ненадлежащей конфигурации изолирования разных VM может существенно возрасти вероятность утечки данных или даже сетевых атак между разными VM. Любые инциденты могут привести к значительным рискам нарушения безопасности и серьезным последствиям.
5) Масштабируемость виртуальных ресурсов: гибкое расширение виртуальных ресурсов и динамическая настройка периметра безопасности виртуальной сети вызывают быстрый рост сетевых потоков восток-запад и новые сложные требования безопасности. Это требует, чтобы средства безопасности были гибкими и могли работать совместно, однако большинство оборудования и систем безопасности работают индивидуально, и в них отсутствует механизм эффективного взаимодействия.

6) Управление конфигурацией: в среде облачных вычислений существует огромное число активов разных типов, а также услуги различных типов, которые обусловливают высокие требования к конфигурации, включая управление доступом, изолирование, резервное копирование и т. д. Ненадлежащая конфигурация может создать новую область атаки или даже привести к прямой утечке конфиденциальной информации.

7) Проблемы, связанные с ведением журналов регистрации: данные различных журналов регистрации операционных систем, приложений, а также оборудования безопасности помогут операторам не допустить чрезвычайной ситуации и даже определить основную причину инцидентов безопасности. В среде облачных вычислений сбор, защита и синхронизация по времени данных журналов регистрации постоянно усложняются. Например, отсутствие защиты журнала регистрации приведет к риску злонамеренной подделки, а отсутствие синхронизации по времени усложнит корреляцию разнородных журналов регистрации.

## 8 Требования безопасности уровня доступа IaaS

Уровень доступа IaaS отвечает за представление CSC возможностей службы IaaS для доступа и управления с использованием одного или нескольких механизмов доступа. К механизмам доступа относятся в том числе:

– веб-доступ;

– доступ через API.

Другие задачи уровня доступа заключаются в реализации надлежащих механизмов управления соединением для обеспечения выполнения политики QoS, распределения нагрузки и безопасной передачи применительно к трафику и соединениям в направлении от функциональных компонентов пользовательского уровня и/или к ним.

### 8.1 Требования безопасности веб-доступа

1) Требуется, чтобы CSP IaaS применял меры аутентификации и авторизации при доступе CSC к службе IaaS через веб-доступ, например аутентификацию запроса с использованием учетных данных CSC и проверку авторизации CSC.

2) Требуется, чтобы CSP IaaS применял механизм управления доступом при использовании CSC соответствующих возможностей услуг.

3) Рекомендуется, чтобы CSP IaaS обеспечивал для CSC защищенный туннель связи при использовании веб-доступа.

4) Рекомендуется, чтобы CSP IaaS обеспечивал для CSC защиту веб-доступа, такую как проверка действительности при вводе-выводе, проверка целостности запроса, возможности защиты от веб-вторжения злоумышленников, например ввод языка структурированных запросов (SQL), межсайтовые сценарии (XSS), дистанционное исполнение команд и т. д.

5) Требуется, чтобы CSP IaaS поддерживал для веб-доступа возможности защищенного от подделки ведения журналов регистрации, выполнения анализа и аудита безопасности.

### 8.2 Требования безопасности доступа через API

1) Требуется, чтобы CSP IaaS поддерживал для CSC аутентификацию и авторизацию учетных данных пользователя при обращении к API услуги, например регистрацию в API для обеспечения работы только законных авторов вызова.

2) Требуется, чтобы CSP IaaS обеспечивал для CSC механизм управления доступом при вызове API услуги.

3) Рекомендуется, чтобы CSP IaaS обеспечивал для CSC защищенный туннель связи при использовании доступа к API.

4) Рекомендуется, чтобы CSP IaaS обеспечивал для CSC защиту интерфейса API, такую как проверка целостности запроса, возможности защиты от атак злоумышленников, например атак типа повторного воспроизведения, ввода кода и т. д.

5) Требуется, чтобы CSP IaaS поддерживал для вызова API возможности ведения журналов регистрации, выполнения анализа и аудита безопасности.

## 9 Требования безопасности уровня услуг IaaS

Уровень услуг IaaS содержит реализацию услуг, которые предоставляет CSP. Уровень услуг содержит и контролирует программные компоненты, реализующие услуги IaaS (такие, как услуги вычисления, сетевые услуги, услуги хранилища и т. д.), и выполняет их упорядочение для предложения этих услуг CSC через уровень доступа.

### 9.1 Требования безопасности услуг вычисления

1) Требуется, чтобы CSP IaaS обеспечивал механизмы изолирования виртуальных ресурсов, включая изолирование центрального процессора (ЦП), внутренней сети, памяти и хранилища и т. д., и разрешал только такую связь, которая отвечает политике безопасности среди разных блоков виртуального ресурса, например VM.

2) Требуется, чтобы CSP IaaS поддерживал настройку верхнего предела занятости ресурса для блока виртуального ресурса на физическом хосте, что позволит не допустить ухудшения производительности вследствие чрезмерной занятости конкретного блока виртуального ресурса.

3) Рекомендуется, чтобы CSP IaaS поддерживал автоматическую миграцию услуг блока виртуального ресурса в случае сбоя размещенного сервера, что позволит не допустить прерывания работы услуги в виртуальном ресурсе.

4) Требуется, чтобы CSP IaaS поддерживал проверку целостности копий блока виртуального ресурса для предотвращения злонамеренной подделки и обеспечивал возможность одновременной установки логического тома только одним блоком виртуального ресурса.

5) Требуется, чтобы CSP IaaS поддерживал миграцию политики безопасности с соответствующей одновременной синхронизацией с блоком виртуального ресурса.

6) Требуется, чтобы CSP IaaS обеспечивал для администратора CSC возможность настройки политики безопасности на блоках виртуального ресурса.

7) Требуется, чтобы CSP IaaS обеспечивал для CSC возможность полного удаления собственных данных. После того, как CSC удалит блок виртуального ресурса, должны быть одновременно уничтожены файлы копий, снимки данных и резервные копии.

### 9.2 Требования безопасности услуги хранилища

1) Рекомендуется, чтобы CSP IaaS поддерживал механизм дублирования данных. Следует гарантировать наличие не менее двух резервных копий данных CSC в различных физических местах, и этот механизм должен быть прозрачным для CSC.

2) Рекомендуется, чтобы CSP IaaS поддерживал управление совмещенным вводом/выводом (I/O) и безопасный параллельный доступ для нескольких VM, использующих одну и ту же систему хранения.

3) Требуется, чтобы CSP IaaS гарантировал управление доступом к хранимым данным, которое может выполняться как на логических, так и физических объектах хранения и которое не может быть обойдено в результате любого изменения физического местоположения хранилища.

4) Требуется, чтобы CSP IaaS гарантировал полное уничтожение данных CSC, в том числе:

   – полное уничтожение данных должно выполняться до переназначения ресурса хранилища новому CSC;

   – после удаления файлов/объектов CSC соответствующая область хранения в физическом томе должна быть надлежащим образом перезаписана или помечена как предназначенная только для записи, для того чтобы не допустить несанкционированного восстановления данных;

   – после переноса данных CSC требуется, чтобы немедленно были уничтожены метаданные CSC.

### 9.3 Требования безопасности сетевой услуги

1) Рекомендуется, чтобы CSP IaaS обеспечивал для CSC возможность контролировать сетевой трафик север-юг и восток-запад своих собственных виртуальных ресурсов.

2) Рекомендуется, чтобы CSP IaaS обеспечивал для CSC возможность реализации управления пропускной способностью сетевого интерфейса для виртуальных ресурсов.

3) Требуется, чтобы CSP IaaS обеспечивал меры изолирования между виртуализированной сетью CSC и платформой IaaS и сетью управления, например запрет доступа CSC к хост-машине или узлу управления.

4) Требуется, чтобы CSP IaaS реализовал механизм списка управления доступом (ACL) к сети для обеспечения изолирования в целях безопасности и управления доступом в виртуализированных сетях.

5) Рекомендуется, чтобы CSP IaaS поддерживал защиту от сетевых атак, например скачкообразные переходы виртуальной локальной сети (VLAN) или виртуальной расширяемой локальной сети (VXLAN).

## 10 Требования безопасности уровня ресурсов IaaS

В соответствии с составом функциональных компонентов уровня ресурсов IaaS требования безопасности уровня ресурсов IaaS включают следующие:

– требования безопасности абстрактного представления ресурсов и управления ресурсами;

– требования безопасности физических ресурсов.

### 10.1 Требования безопасности абстрактного представления ресурсов и управления ресурсами

Функциональный компонент абстрактного представления ресурсов и управления ресурсами позволяет CSP обеспечивать такие качественные характеристики, как оперативная эластичность, объединение ресурсов и самообслуживание по требованию. Этот компонент включает пул виртуальных ресурсов (например, виртуальный вычислительный ресурс, виртуальный сетевой ресурс и т. д.) и платформу управления виртуальными ресурсами. Требования безопасности абстрактного представления ресурсов и управления ресурсами определяются в аспекте представления виртуальных ресурсов и управления виртуальными ресурсами.

#### 10.1.1 Требования безопасности пула виртуальных ресурсов

##### 10.1.1.1 Требования безопасности виртуальных вычислительных ресурсов

1) Требуется, чтобы блоки виртуального вычислительного ресурса (такие, как виртуальная машина, контейнер и т. д.) были логически изолированы друг от друга.

2) Требуется, чтобы на блок виртуального вычислительного ресурса не оказывали воздействия другие блоки или хост-машины в случае нештатного происшествия или отказа.

3) Требуется, чтобы виртуальные вычислительные ресурсы не мог использоваться за пределами соответствующей им квоты.

4) Рекомендуется, чтобы были запрещены команды "копировать", "вставить" и другие команды между разными блоками виртуального вычислительного ресурса или разными хост-машинами.

5) Рекомендуется, чтобы CSP IaaS поддерживал контроль виртуальных ресурсов в режиме реального времени во внутриполосном или во внеполосном режиме и направлял сигналы тревоги при обнаружении отклонений. Для каждого блока виртуального ресурса контролируемые объекты должны включать статус выполнения, потребление ресурса и статус переноса ресурса и т. д.

#### 10.1.1.2 Требования безопасности виртуальных сетевых ресурсов

1) Требуется, чтобы виртуальные сети CSC были логически изолированы одна от другой путем реализации таких мер как VLAN, VXLAN, ACL и т. д.

2) Требуется, чтобы была обеспечена возможность контроля сетевого трафика между разными блоками виртуального ресурса.

3) Требуется, чтобы была обеспечена возможность управления скоростью передачи данных в виртуальных портах.

4) Рекомендуется обеспечить возможность обнаружения и предотвращения выполнения сетевых атак (таких, как IP-спуфинг, черви и т. д.), инициируемых из виртуальных ресурсов.

5) Требуется, чтобы был запрещен неизбирательный режим работы портов карты интерфейса виртуальной сети (NIC) для предотвращения анализа сетевого трафика.

#### 10.1.1.3 Требования безопасности виртуального ресурса хранилища

1) Требуется, чтобы пул виртуальных ресурсов хранилища был изолирован от других CSC.

2) Требуется, чтобы меры безопасности в отношении хранимых данных выполнялись как в логических, так и в физических объектах хранения.

3) Требуется, чтобы был запрещен прямой доступ к физическим ресурсам хранилища.

4) Требуется, чтобы поддерживалась возможность управления совмещенным I/O и безопасный параллельный доступ для нескольких блоков виртуального ресурса, использующих одни и те же объекты хранения.

5) Рекомендуется, чтобы виртуальные ресурсы хранилища могли поддерживать эластичное расширение без прерывания обычных услуг хранилища.

### 10.1.2 Требования безопасности платформы управления виртуальными ресурсами

1) Требуется, чтобы были надлежащим образом реализованы меры управления доступом для предотвращения незаконного доступа к платформе управления виртуальными ресурсами.

2) Требуется, чтобы были установлены только необходимые компоненты и приложения и чтобы порты неприменимых услуг были закрыты, согласно принципу минимизации рисков.

3) Требуется, чтобы была обеспечена возможность своевременно обнаружить атаку, направленную на платформу управления виртуальными ресурсами, и подать сигнал тревоги, и должна быть выполнена регистрация в журналах, включая указание IP-адреса источника, типа атаки, метку времени и т. д.

4) Требуется, чтобы была обеспечена возможность контроля виртуальных ресурсов в режиме реального времени, включая состояние выполнения, занятость ресурса, перенос и т. д.

5) Рекомендуется обеспечить возможность отключения ресурсов, которые не требуются или не используются.

6) Требуется, чтобы команды управления на платформе управления виртуальными ресурсами передавались по защищенному туннелю.

7) Рекомендуется, чтобы была предусмотрена возможность ограничения привилегированных команд при их удаленном исполнении.

8) Требуется, чтобы была обеспечена возможность изолирования незаконных блоков виртуального ресурса и их надлежащее удаление, с тем чтобы минимизировать последующее воздействие на всю совокупность виртуальные ресурсов.

9) Требуется, чтобы была обеспечена возможность обнаружения и удаления вредоносных кодов.

10) Требуется, чтобы была обеспечена возможность переноса политики безопасности одновременно с переносом блоков виртуального ресурса.

11) Требуется, чтобы была обеспечена своевременная реализация обновлений (патчей) для системы безопасности или конфигурация усиления безопасности в случае обнаружения уязвимости безопасности компонентов управления виртуальными ресурсами (таких, как гипервизор, процессор контейнера, компоненты управления и т. д.) и чтобы эти средства поддерживались на уровне современных требований.

12) Требуется, чтобы было обеспечено управление отказами для поддержания непрерывности услуг верхнего уровня, то есть, чтобы блоки виртуального ресурса на отказавшей хост-машине могли быть своевременно перенесены на другую хост-машину.

13) Требуется, чтобы была обеспечена регистрация в журнале всех действий и событий на платформе управления виртуальными ресурсами для последующего отслеживания и аудита.

### 10.2 Требования безопасности физических ресурсов

К физическим ресурсам относятся аппаратные ресурсы, такие как компьютеры, сетевое оборудование, компоненты хранилищ данных и другие элементы физической вычислительной инфраструктуры, которые необходимы CSP для выполнения предоставляемых CSC услуг IaaS и управления ими.

#### 10.2.1 Требования безопасности физической среды

Требования безопасности физической среды для IaaS описаны в [ISO/IEC 27002].

##### 10.2.1.1 Требования безопасности физических ресурсов

К физическим ресурсам относятся аппаратные ресурсы, такие как физическая сетевая инфраструктура, устройства хранения данных, хост-машины, терминалы управления и другие элементы физической инфраструктуры.

1) Требуется, чтобы была обеспечена возможность обнаружения и локализации отказа в физических ресурсах (таких, как сетевое оборудование, хост-машины, устройства хранения данных и т. д.), для того чтобы поддерживать готовность и надежность базовой физической инфраструктуры.

2) Рекомендуется обеспечить возможность своевременного обнаружения и маркирования замены физических ресурсов.

3) Рекомендуется, чтобы была обеспечена возможность восстановления данных в случае сбоя некоторых физических компонентов.

4) Требуется, чтобы была обеспечена возможность защиты платформы IaaS от DDoS.

5) Требуется, чтобы инфраструктурная сеть была разделена на разные домены безопасности сети, логически изолированные друг от друга.

6) Требуется, чтобы были реализованы механизмы обнаружения мониторинга трафика сети и действий по проникновению в сеть, при этом на границе сети должны быть развернуты устройства защиты, включая управление определением идентичности и доступом (IAM), IPS, брандмауэр и т. д.

7) Рекомендуется, чтобы была предусмотрена возможность обнаружения и предотвращения предпринимаемых исходящих атак, инициируемых из ресурсов IaaS.

8) Требуется, чтобы была обеспечена возможность обнаружения и удаления вредоносного кода, в особенности применительно к терминалам управления, хост-машинам и другим серверам приложений.

9) Требуется, чтобы был реализован базовый уровень политики безопасности и чтобы доступ к платформе IaaS имели только терминалы и серверы, отвечающие требованиям политики безопасности.

10) Требуется, чтобы была обеспечена регистрация в журнале всех действий и событий в физических ресурсах для последующего отслеживания и аудита.

## 11 Требования к управлению безопасностью

Управление безопасностью отвечает за применение относящихся к безопасности средств управления для смягчения угроз безопасности в среде облачных вычислений. Функциональные компоненты управления безопасностью охватывают все средства безопасности, требуемые для поддержки облачных услуг.

К функциональным компонентам управления безопасностью относятся:

- управление определением идентичности и доступом;
- аудит безопасности;
- управление уязвимостями;
- реагирование на чрезвычайные ситуации;
- восстановление после чрезвычайных ситуаций; а также
- резервное копирование.

### 11.1 IdM и управление доступом

Платформа IaaS должна обеспечивать для CSC и администраторов платформы IaaS функции унифицированного управления определением идентичности (IdM) и доступом.

1) Требуется, чтобы идентичность CSC на протяжении жизненного цикла была уникальной в каждой услуге IaaS и связанной с аудитом безопасности. Требуется, чтобы идентичность CSC была управляемой, сопровождаемой и защищенной от несанкционированного доступа, изменения или удаления.
2) Требуется, чтобы платформа IaaS обеспечивала для CSC управление политикой паролей, которая включает в том числе следующие требования:
   – требуется использовать политику сложности пароля;
   – требуется использовать механизм периода переустановки пароля;
   – требуется использовать случайную генерацию начального ключа CSC, и начальный ключ должен быть изменен при первом входе в систему.
3) Рекомендуется, чтобы платформа IaaS поддерживала для идентичности CSC обнаружение отклонений и чтобы сигналы тревоги могли передаваться в соответствующие CSC.
4) Требуется, чтобы платформа IaaS поддерживала для CSC многофакторную аутентификацию и чтобы методы аутентификации включали в том числе пароли, цифровые сертификаты, карты IC или биометрическую валидацию.
5) Требуется, чтобы при осуществлении доступа поддерживалась стратегия авторизации высокой степени детализации в зависимости от CSC и определения группы ресурсов. Требуется, чтобы платформа IaaS обеспечивала защиту конфиденциальности и целостности учетных данных аутентификации CSC.
6) Требуется, чтобы подробные журналы регистрации аутентификации, авторизации и других операций CSC, связанных с IdM, сохранялись для последующего аудита.
7) Рекомендуется, чтобы платформа IaaS поддерживала стыковку с системой IdM потребителя облачной услуги.
8) Требуется, чтобы функции и связанные с ними привилегии администратора платформы IaaS предоставлялись отдельной учетной записи.
9) Требуется, чтобы платформа IaaS использовала для администраторов многофакторную аутентификацию.
10) Требуется, чтобы платформа IaaS использовала для администраторов принцип минимальных полномочий.
11) Требуется, чтобы выполнялось шифрование конфиденциальных данных, таких как данные аутентификации, данные авторизации и т. д., в процессе их хранения и передачи.

### 11.2 Аудит безопасности

1) Требуется, чтобы платформа IaaS использовала для аудита безопасности различные регистрационные записи, которые включают в том числе следующие:
   - журналы регистрации, информация для аутентификации и авторизации идентичности CSC и администраторов платформы IaaS;
   - регистрационные записи, относящиеся к эксплуатации и обслуживанию инфраструктуры, которые ведут администраторы платформы IaaS;
   - журналы регистрации, относящиеся к эксплуатации ресурсов CSC, которые ведут администраторы платформы IaaS;
   - журналы регистрации, относящиеся к эксплуатации собственных ресурсов CSC, которые ведут CSC;
   - журналы регистрации, относящиеся к эксплуатации и обслуживанию в ходе выполняемых платформой IaaS процессов.
2) Требуется, чтобы на платформе IaaS были реализованы механизмы безопасности для защиты от подделки различных регистрационных записей.
3) Требуется, чтобы поддерживалась синхронизация всех сетевых часов на всей платформе IaaS, с тем чтобы обеспечить систематическую регистрацию доступа и работы.
4) Регистрационные записи аудита безопасности должны включать указание предмета, объекта, времени, типа и результата события безопасности.
5) Требуется, чтобы записи аудита потребителей облачной услуги были изолированы друг от друга.
6) Требуется, чтобы CSC мог собирать и просматривать записи аудита, относящиеся к его собственным ресурсам.
7) Требуется, чтобы записи аудита были надежно защищены, например путем запрета несанкционированного доступа к записям аудита, предотвращения их случайного удаления, изменения, переопределения и потери.
8) Требуется, чтобы срок хранения записей аудита соответствовал требованиям законодательства и определенным CSC требованиям к хранению.
9) Рекомендуется, чтобы платформа IaaS обеспечивала для CSC возможность использовать внешнюю систему или интерфейс аудита для целей выполнения аудита в рамках сферы ответственности CSC.

### 11.3 Управление уязвимостями

Уязвимости платформы IaaS могут существовать в процессах, управлении, конфигурации, аппаратном оборудовании, программном обеспечении и т. д.

1) Требуется, чтобы информация обо всех активах и версиях платформы IaaS была зарегистрирована и регулярно обновлялась.
2) Требуется, чтобы был реализован механизм оценки уязвимостей, в котором следует определить объекты, частоту и стратегию оценки уязвимостей.
3) Требуется, чтобы регулярно выполнялась оценка уязвимостей всех активов платформы IaaS, составлялись отчеты по результатам оценки уязвимостей и формулировались рекомендации по устранению уязвимостей.
4) Требуется, чтобы осуществлялось управление процессом обновления и устранения:
   - требуется, чтобы выполнялось отслеживание угроз безопасности и обновлений для системы безопасности, выпускаемых различными поставщиками, и определялись обновления, которые следует установить на платформе IaaS;
   - требуется, чтобы до установки обновлений для системы безопасности проводилось их тестирование, с тем чтобы обеспечить совместимость обновлений с существующей системой и приложением;

– требуется, чтобы для всех компонентов платформы IaaS был составлен план актуализации обновлений, чтобы в соответствии с этим планом выполнялась установка обновлений и в процессе установки создавались регистрационные записи.

5) Требуется, чтобы был описан базовый уровень конфигурации безопасности платформы IaaS и чтобы в соответствии с этим базовым уровнем была выполнена конфигурация компонентов платформы IaaS.

6) Требуется, чтобы регулярно проводилась проверка базового уровня безопасности всех активов платформы IaaS, составлялся отчет о базовом уровне и формулировались рекомендации по устранению недостатков.

7) Требуется, чтобы проводился аудит изменений стратегии конфигурации платформы IaaS, для того чтобы подтвердить правильность, согласованность, полноту и эффективность каждого элемента конфигурации, а также убедиться, что изменения конфигурации не создают новых дефектов безопасности.

### 11.4 Реагирование на чрезвычайные ситуации

Соображения по реагированию на чрезвычайные ситуации для IaaS соответствуют изложенным в пункте 8.9 [b-ITU-T X.1642].

### 11.5 Восстановление после чрезвычайных ситуаций

Соображения по восстановлению после чрезвычайных ситуаций, относящиеся к IaaS, должны соответствовать существующим общим нормам ИТ-технологий, например стандарту [ИСО/МЭК 27031:2011]. Вместе с тем, учитывая что восстановление после чрезвычайных ситуаций IaaS является быстро развивающейся технологией, следует учитывать нижеприведенные аспекты.

1) Определение для каждого CSC объектов восстановления после чрезвычайных ситуаций. Требуется, чтобы с целью определения для различной деятельности объектов восстановления после чрезвычайных ситуаций был инициирован анализ последствий для деятельности (BIA), который основан на выявлении ключевых компонентов и основных рисков безопасности на платформе IaaS. Объекты восстановления после чрезвычайных ситуаций могут определяться по приоритетам, RPO/RTO и т. д. Различные DRO определяют соответствующее SLA и архитектуру услуг, включая технологию обеспечения высокой готовности между удаленными виртуальными центрами обработки данных (VDC), межрегиональное резервное копирование данных и т. д.

2) Регулярное резервное копирование систем и данных. Требуется, чтобы поддерживалась возможность межрегионального хранения данных и устойчивость к чрезвычайным ситуациям. Кроме того, для арендаторов платформы IaaS следует обеспечить резервное копирование на уровне системы и резервное копирование на уровне данных, а также соответствующую возможность восстановления после чрезвычайных ситуаций, которые помогут CSP и CSC реализовать обработку отказов. Что касается CSC, они могут даже выполнять регулярное резервное копирование данных другому CSP, для того чтобы избежать риска длительного прерывания работы, связанного с одним CSP.

3) Регулярное подтверждение плана восстановления после чрезвычайных ситуаций. Системы и данные потребителей облачных услуг поддерживаются в относительно постоянном состоянии, однако возможно появление новых рисков безопасности в результате обновлений инфраструктуры, выполняемых поставщиками облачных услуг. Ввиду этого следует регулярно проводить тренировочное восстановление после чрезвычайных ситуаций и регистрировать ключевую информацию, в том числе сведения о готовности, целостности и действительности планов восстановления после чрезвычайных ситуаций, а также о проблемах и соответствующих решениях, определенных в ходе работы, и т. д.

4) Регулярная оценка рисков. Для того чтобы поддерживать непрерывность бизнес-процессов CSC, CSP должны оценивать риски безопасности, которые могут влиять на план CSC по обеспечению непрерывности деятельности, включая отказ службы IaaS, сбой сети между CSP и CSC, прекращение предоставления облачных услуг и т. д., и результаты этой оценки следует должным образом доводить до сведения CSC. Кроме того, меры по реагированию на чрезвычайные ситуации, планы восстановления после чрезвычайных ситуаций и меры по

поддержке непрерывности деятельности CSC должны быть объявлены заблаговременно, а также адаптированы к требованиям CSC.

### 11.6 Резервное копирование

Рекомендации по резервному копированию для IaaS соответствуют изложенным в пункте 8.10 [ITU-T X.1642].

# Библиография


[b-ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2015 год), *Основы безопасности облачных вычислений*.

[b-ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014 год) | ISO/IEC 17788:2014, *Информационные технологии – Облачные вычисления – Обзор и терминология*.

[b-NIST 500-291] NIST SP 500-291,2011, *NIST Cloud Computing Standards Roadmap*.

[b-NIST-SP-800-30] NIST Special Publication 800-30, 2012, *Guide for Conducting Risk Assessments*.

## 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, 2020 г.