Международный союз электросвязи

МСЭ-Т

X.1602

(03/2016)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасность облачных вычислений –
Обзор безопасности облачных вычислений

Требования к безопасности прикладной среды программного обеспечения как услуги

Рекомендация МСЭ-Т X.1602

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	
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	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	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
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

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

Рекомендация МСЭ-Т X.1602

Требования к безопасности прикладной среды программного обеспечения как услуги

Резюме

В Рекомендации МСЭ-Т X.1602 проводится анализ уровней зрелости приложения "программное обеспечение как услуга" (SaaS) и предлагаются требования к безопасности для обеспечения согласованной и безопасной среды выполнения услуг для приложений SaaS. Эти предлагаемые требования исходят от поставщиков облачных услуг (CSP) и партнеров по облачным услугам (CSN), поскольку им необходима прикладная среда SaaS, отвечающая их требованиям к безопасности. Такие требования имеют общий характер и не зависят от какой-либо услуги или модели, определяемой сценарием (например, веб-услуги или передача репрезентативного состояния (REST)), допущений или решений.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1602	23.03.2016 г.	17-я	11.1002/1000/12615

Ключевые слова

Требования к безопасности, прикладная среда программного обеспечения как услуги (SaaS), уровень зрелости SaaS.

* 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 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

Рекомендация МСЭ-Т X.1602

Требования к безопасности прикладной среды программного обеспечения как услуги

1 Сфера применения

В настоящей Рекомендации рассматриваются в основном требования к безопасности прикладной среды программного обеспечения как услуги (SaaS) на основе уровня зрелости приложения SaaS. Настоящая Рекомендация предназначена в первую очередь поставщикам облачных услуг (CSP) и партнерам по облачным услугам (CSN), таким, например, как разработчики приложений.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 облачная услуга (cloud service) [b-ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений, которые активируются через определенный интерфейс.

3.1.2 категория облачной услуги (cloud service category) [b-ITU-T Y.3500]: Группа облачных услуг, которая обладает некоторым общим набором характеристик.

3.1.3 потребитель облачной услуги (cloud service customer) [b-ITU-T Y.3500]: Сторона, которая состоит в деловых отношениях для целей использования облачных услуг.

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

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

3.1.6 пользователь облачной услуги (cloud service user) [b-ITU-T Y.3500]: Физическое лицо или объект, действующий от его лица, связанные с потребителем облачной услуги, который пользуется облачными услугами.

3.1.7 рабочий стол как услуга (desktop as a service) [b-ITU-T Y.3500]: Возможности, которые предоставляются потребителю облачной услуги, составляют возможности построения, конфигурирования, управления, сохранения, выполнения и предоставления пользовательских функций рабочего стола дистанционно.

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

3.1.9 программное обеспечение как услуга (software as a service (SaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, является тип возможностей приложения.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ASP	Application Service Provider		Поставщик прикладных услуг
CaaS	Communications as a Service		Связь как услуга
CRM	Customer Relationship Management		Управление отношениями с клиентами
CSC	Cloud Service Customer		Потребитель облачной услуги
CSN	Cloud Service Partner		Партнер облачной услуги
CSP	Cloud Service Provider		Поставщик облачной услуги
DaaS	Desktop as a Service		Рабочий стол как услуга
IaaS	Infrastructure as a Service		Инфраструктура как услуга
IAM	Identity and Access Management		Управление определением идентичности и доступом
IdM	Identity Management		Управление определением идентичности
OLAP	OnLine Analytical Processing		Интерактивная аналитическая обработка
OS	Operating System	ОС	Операционная система
PaaS	Platform as a Service		Платформа как услуга
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
REST	Representational State Transfer		Передача репрезентативного состояния
SaaS	Software as a Service		Программное обеспечение как услуга
SAP	Service Access Point		Точка доступа к услуге
SLA	Service Level Agreement		Соглашение об уровне обслуживания

5 Условные обозначения

Отсутствуют.

6 Обзор

Прикладная среда "программное обеспечение как услуга (SaaS)" – это ориентированная на услугу мультиарендная среда разработки, развертывания и выполнения, в которой программное обеспечение (ПО) и связанные с ним данные имеют центральное размещение и, как правило, доступны по запросу пользователей с помощью клиента, например веб-браузера, через интернет.

При том что настоящая Рекомендация касается, в первую очередь, SaaS, некоторые понятия, изложенные в настоящей Рекомендации, могут также применяться к другим категориям облачных услуг, которые включают в том числе тип возможностей приложения, например связь как услуга (CaaS).

На рисунке 1 представлена концептуальная модель прикладной среды SaaS. Основополагающие возможности, которые обеспечивают инфраструктура как услуга (IaaS), платформа как услуга (PaaS) и рабочий стол как услуга (DaaS), будут инкапсулированы в услуги и будут обеспечивать бесперебойный защищенный доступ с использованием экспортируемой точки доступа к услуге (SAP). В контексте настоящей Рекомендации IaaS может обеспечивать вычислительные услуги, услуги хранения и сетевые услуги, PaaS может обеспечивать услугу платформы, а DaaS может обеспечивать услугу рабочего стола для прикладной среды SaaS. Все эти услуги составляют базовые структурные блоки для разработки приложений.

Среда также обеспечивает ряд необходимых функций управления услугами, в том числе регистрацию услуг, конфигурацию услуг, комбинирование услуг, проверку зависимости от услуги, контроль доступа к услугам, изолирование услуг, мониторинг услуг и другие функции управления услугами.

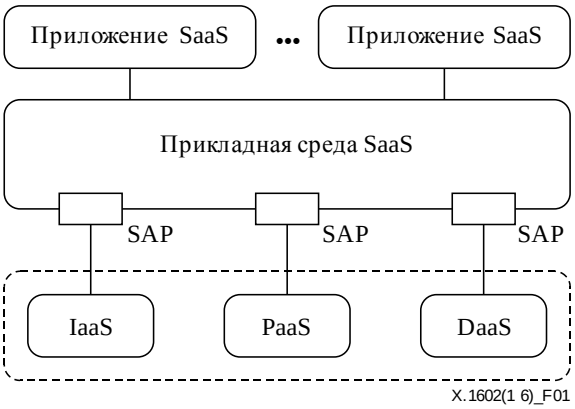
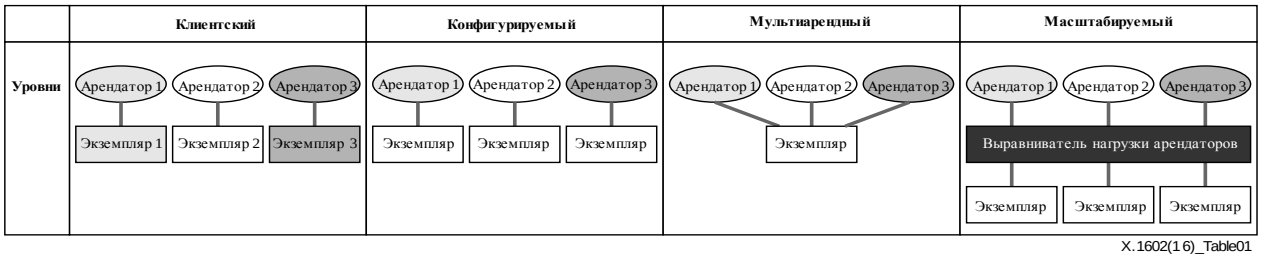


Рисунок 1 – Концептуальная модель прикладной среды SaaS

7 Уровни зрелости приложения SaaS

В отрасли зрелость SaaS классифицируется по четырем уровням, которые кратко могут быть названы как клиентский уровень, конфигурируемый уровень, мультиарендный уровень и масштабируемый уровень. Каждый уровень охватывает характеристики предыдущего уровня и обеспечивает расширенные характеристики. В таблице 1 представлена диаграмма, отражающая характеристики разных моделей зрелости SaaS.

Таблица 1 – Диаграмма уровней зрелости приложения SaaS



Различные уровни зрелости приложения SaaS характеризуются различными требованиями безопасности к прикладной среде SaaS, и эти требования будут рассмотрены в разделе 8 с позиции CSP и CSN.

7.1 Уровень 1: клиентское приложение SaaS

Клиентское приложение SaaS аналогично традиционной модели поставки программного обеспечения поставщика прикладных услуг (ASP). Каждый клиент имеет собственное пользовательское решение приложения SaaS и запускает свой отдельный экземпляр приложения на облачном сервере. Как показано на рисунке 2, экземпляр клиентского приложения состоит из полной среды выполнения, включая операционную систему (ОС), систему управления данными и промежуточное ПО, характерные для данного арендатора, и поставщик среды SaaS должен поддерживать несколько экземпляров. Эту модель сложно масштабировать в целях удовлетворения возрастающих потребностей клиентов, и ее эксплуатация может оказаться дорогостоящей.

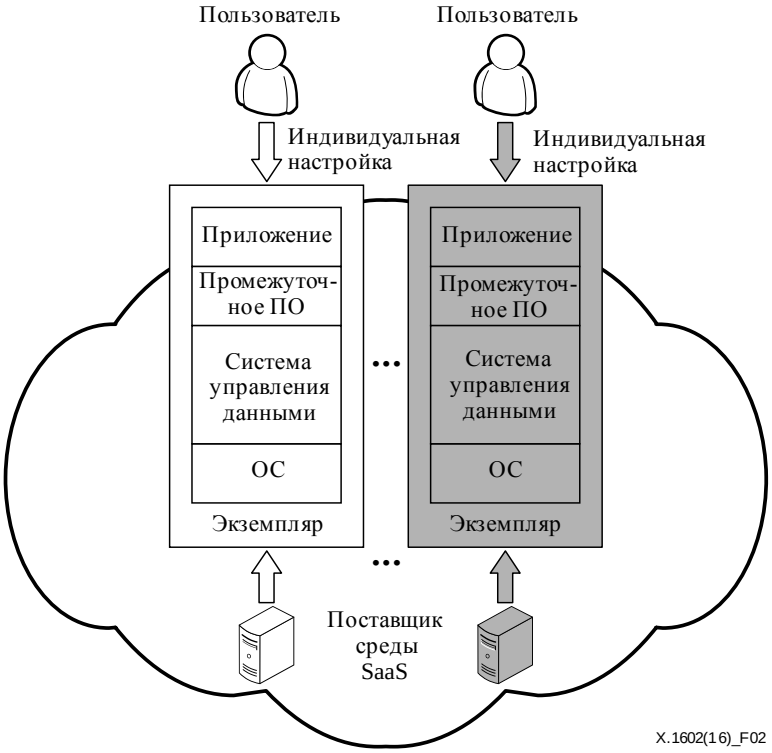


Рисунок 2 – Архитектура клиентского приложения SaaS

Типовые приложения на основе модели клиент-сервер могут легко трансформироваться в клиентские приложения SaaS путем перемещения серверов в облако с относительно небольшим объемом модификаций. Подходящие для данного сценария приложения разрабатываются, как правило, в соответствии со специальными требованиями предприятия или организации. Основное внимание будет уделяться безопасности в самой системе, следовательно, обычный способ заключается в группировании множества физических машин в закрытой зоне и развертывании системы управления данными (которая предоставляет абстрактные методы сохранения состояния и функционирования для различных типов данных) и соответствующего программного обеспечения на них. Система предназначена исключительно для внутреннего использования с жестким контролем доступа. Шаблон экземпляра приложения аналогичен для всех клиентов и обеспечивает ограниченные конфигурационные возможности. Однако экземпляр каждого клиента абсолютно независим от любого другого экземпляра.

7.2 Уровень 2: конфигурируемое приложение SaaS

В случае некоторых коллективно используемых приложений, не являющихся адаптированными, как например система самостоятельного создания веб-сайтов, поставщики приложений SaaS предлагают для таких приложений общие шаблоны и несколько наборов среды исполнения для экземпляров этих приложений. Используя в качестве основы тот же шаблон, клиенты могут создавать – путем конфигурирования внешних атрибутов и режимов работы приложения – множество раздельных экземпляров приложения, которые развертываются и исполняются на отдельных виртуальных или физических машинах для выполнения специализированных требований этих клиентов. Экземпляры приложения изолированы один от другого. Архитектура показана на рисунке 3.

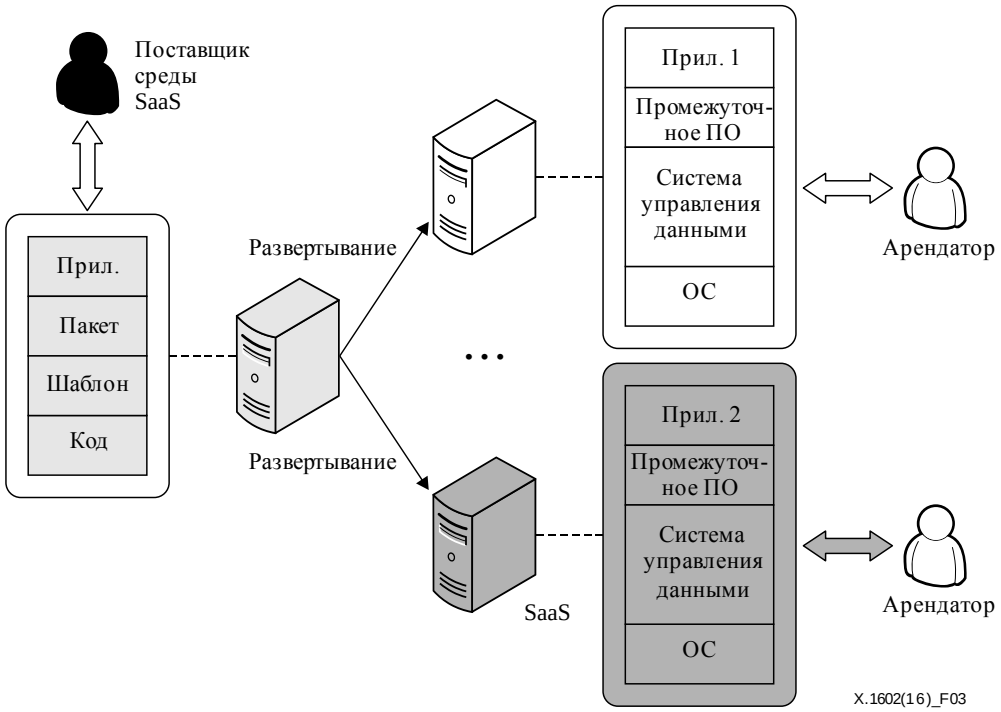


Рисунок 3 – Архитектура конфигурируемого приложения SaaS

Конфигурируемое приложение SaaS обладает следующими характеристиками.

1) Приложение при первом развертывании является копией стандартного продукта, и арендаторы конфигурируют это приложение в соответствии с собственными требованиями. Однако, конфигурационные опции продукта ограничены.

2) Для поставщиков приложения SaaS: любые изменения в кодах продукта могут быть легко применены для всех арендаторов немедленно. Однако для каждого экземпляра возможны лишь некрупное обновление или оптимизация, так как в результате обновления или оптимизации может возникнуть проблема прямой совместимости.

3) Арендаторы хранят данные на своих собственных виртуальных машинах или физических машинах, которые изолированы одна от другой. Вследствие этого, поставщик среды SaaS должен обеспечить достаточный объем ресурсов, таких как хранилища данных, для поддержки потенциального большого числа работающих одновременно экземпляров приложения.

По мере развития и совершенствования программных технологий приложение будет обеспечиваться достаточным объемом конфигурационных опций для удовлетворения индивидуальных требований пользователей, а процесс конфигурирования и использования должен стать более интеллектуальным и автоматизированным. Поставщики приложения SaaS разделят продукт на несколько версий, соответствующих разным уровням арендаторов.

7.3 Уровень 3: приложение SaaS с множеством арендаторов

На этом уровне поставщик приложения SaaS с помощью конфигурируемых метаданных может предоставлять единичный экземпляр, который обслуживает параллельно множество арендаторов. Режим с множеством арендаторов возможен на разных уровнях, включая ОС, систему управления данными, промежуточное ПО и приложение. Для разделения различных клиентов вводится идентификатор арендатора. Если в системе управления данными используется база данных, то схема базы денных расширяется в целях включения параметра идентичности арендатора для сохранения данных всех клиентов в том же наборе таблиц. Идентичность арендатора необходима также в запросах к базе данных с целью получения данных для конкретного клиента. На рисунке 4 показана общая архитектура приложения SaaS с множеством арендаторов.

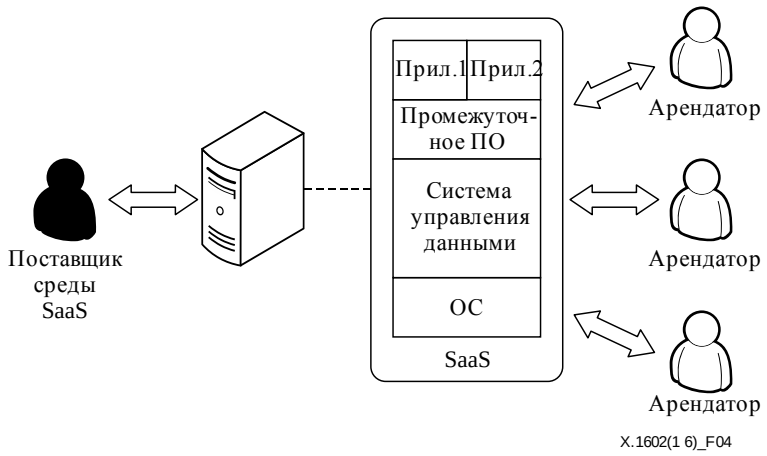


Рисунок 4 – Архитектура приложения SaaS с множеством арендаторов

Типовой реализацией этого уровня считается интеллектуальный анализ данных SaaS, например управление отношениями с клиентами (CRM). Для обеспечения онлайновых приложений интеллектуального анализа данных до настоящего времени прилагались дополнительные усилия для объединения средств организации хранилищ данных и облачных вычислений с SaaS. Хранилища данных размещаются в центре обработки данных, а приложения интеллектуального анализа данных и модели данных заранее определяются для использования с весьма незначительной дополнительной настройкой. Арендаторам необходимо только выбирать элементы данных, требуемые приложениями интеллектуального анализа данных, и определять порядок отображения данных из источников данных в хранилище данных и модель данных. Система выполнит интеграцию данных из нескольких систем источников в хранилище данных для поддержки приложений интерактивной аналитической обработки (OLAP), используя для этого автоматически генерируемые сценарии. Как правило, в течение времени прогона один экземпляр приложения интеллектуального анализа данных параллельно обслуживает нескольких арендаторов, используя средства метаданных. Процедуры авторизации и стратегии безопасности обеспечивают изолированность доступа к данным и приложению каждого клиента от доступа к данным и приложению других клиентов.

Это уровень обеспечивает более высокую эффективность использования вычислительных ресурсов и ресурсов хранения и, следовательно, может обеспечить размещение большего числа арендаторов. С помощью методов разделения данных и параллельных процессов возможно также достижение сопоставимой производительности, масштабируемости и эластичности.

Возможность изменения конфигурации и эффективность режима работы с множеством арендаторов являются отличительными характеристиками этого уровня приложения SaaS.

7.4 Уровень 4: масштабируемое приложение SaaS

Большинство поставщиков веб-услуг общего пользования обслуживают произвольно большое число клиентов как множественных арендаторов. Вследствие этого требуется, чтобы каждый уровень архитектуры основной платформы – от аппаратных средств до приложения – был легко масштабируемым для приложений и услуг, как показано на рисунке 5. Таким образом, может быть добавлено большее число арендаторов и большее число пользователей в рамках одного арендатора без необходимости дополнительного изменения архитектуры приложений.

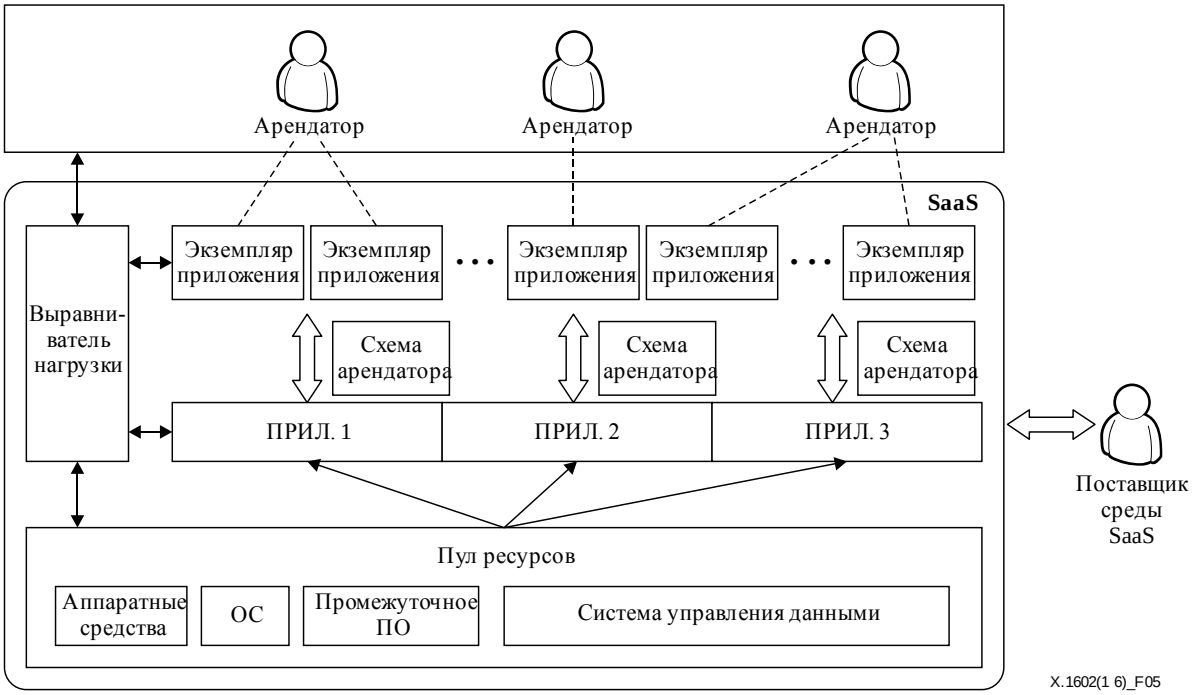


Рисунок 5 – Архитектура масштабируемого приложения SaaS

На прикладном уровне при введении нового арендатора будет создан один или несколько экземпляров приложения в соответствии с определяемыми арендаторами требованиями или будет выбран подходящий существующий экземпляр в соответствии с требованиями на основе механизма выравнивателя нагрузки. Требуется, чтобы все экземпляры приложений в такой среде создавались динамически.

Базовые ресурсы масштабируемых приложений SaaS поддерживают также эластичное масштабирование. Управление любыми аппаратными средствами, промежуточным ПО, ПО и данными необходимо осуществлять в пуле ресурсов. Приложения получают все ресурсы, которые им необходимы, динамически из пула ресурсов. Новые ресурсы могут добавлять при необходимости без повторного выполнения комбинации и организации архитектуры.

В связи с технологиями динамического масштабирования, включая выбор масштабирования, распределение ресурсов, соглашение об уровне обслуживания (SLA) и т. д., имеется несколько соображений, касающихся проектного решения. Новый арендатор может быть реализован как единичный экземпляр или может сосуществовать с другими арендаторами, работая с совместно используемым экземпляром. Разные экземпляры, запускаемые арендаторами разных типов, могут быть распределены по разным ресурсам. Поставщик среды SaaS, используя распределитель нагрузки и коллективные ресурсы, должен учитывать разные SLA для разных арендаторов.

8 Требования к безопасности для прикладной среды SaaS

На рисунке 6 показана взаимосвязь между потребителем облачных услуг (CSC), CSP и CSN применительно к прикладной среде SaaS, где CSP и CSN играют разные роли в выполнении разных функций. CSN может обслуживать CSP как поставщик контента, поставщик ПО, интегратор или аудитор системы, в то время как и CSN и CSP – оба – могут разрабатывать приложения для CSC. CSP и CSN имеют интерфейсы с прикладной средой SaaS, а CSC взаимодействует только с приложениями, созданными на ее основе. Вследствие этого, настоящая Рекомендация посвящена в основном требованиям к безопасности прикладной среды SaaS для CSP и CSN в разной модели зрелости. Требования к безопасности для прикладной среды SaaS исходят от CSP и CSN, так как им необходима прикладная среда SaaS для обеспечения возможности удовлетворения своих требований по безопасности.

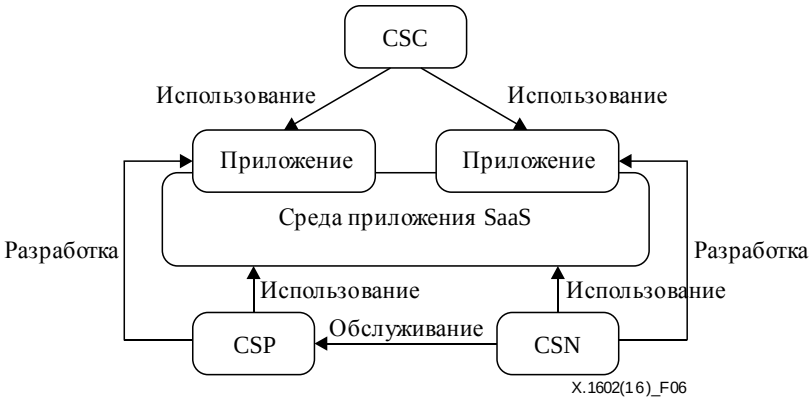


Рисунок 6 – Взаимосвязь между CSC, CSP и CSN

CSP и CSN имеют свои собственные требования к безопасности, касающиеся среды на разных уровнях SaaS. В таблице 2 отражены требования к безопасности CSP и CSN в прикладной среде SaaS. Требования, применимые как для CSP, так и для CSN, являются общими требованиями.

Таблица 2 – Требования к безопасности CSP и CSN в прикладной среде SaaS

	Прикладная среда SaaS
Общие требования	Управление определением идентичности и доступом, безопасность данных, оценка и аудит безопасности, безопасность интерфейсов, укрепление безопасности.
CSP	Готовность, гарантия функциональной совместимости/переносимости услуг, защита программных средств, нормативно-правовое соответствие, верификация безопасности для исходных кодов.
CSN	Безопасность аудита, безопасность ПО, удобство сопровождения ПО.

8.1 Общие требования к безопасности

В прикладной среде SaaS CSP и CSN – оба – имеют ряд общих требований к безопасности.

8.1.1 Управление определением идентичности и доступом (IAM)

8.1.1.1 Управление определением идентичности (IdM)

В прикладной среде SaaS действует множество администраторов и пользователей, при этом доступ к ней и ее использование осуществляются внутренним (CSP) и внешним (CSN) образом. Управление определением идентичности (IdM) необходимо не только для защиты идентичностей, но и для упрощения процессов управления доступом, аутентификации, авторизации и аудита транзакций в такой динамичной и открытой прикладной среде SaaS.

Для всех моделей зрелости необходимо, чтобы IdM обеспечивало возможность реализации однократной регистрации и/или федерации идентичностей для прикладной среды SaaS с использованием различных механизмов аутентификации в разных доменах безопасности.

8.1.1.2 Модель доверия

Требуется, чтобы прикладная среда SaaS включала в себя общую модель доверия как для уровня с множеством арендаторов, так и для масштабируемого уровня. Такая модель доверия позволит создавать острова и/или федерации доверенных объектов. В результате, система управления прикладной средой SaaS, основные ресурсы, гипервизоры, виртуальные машины и приложения, построенные на основе прикладной среды SaaS, смогут проводить аутентификацию идентичностей и санкционированных прав других объектов и компонентов. Каждый остров или федерация доверия будут основаны на одном или нескольких доверенных органах (например, органе выдачи сертификатов инфраструктуры открытых ключей (PKI).

8.1.1.3 Управление доступом

Администраторы прикладной среды SaaS должны обеспечивать механизмы, делегирующие авторизацию администраторам арендаторов. Администраторы арендаторов предоставляют права доступа к своим соответствующим ресурсам. Управление доступом такой прикладной среды SaaS должно поддерживать несколько моделей контроля доступа, такие как модель на основе идентичностей, модель на основе стратегий, модель на основе ролей, модель на основе задач и т. д.

Для приложений SaaS клиентского и конфигурируемого уровней базовым требованием является обеспечения модели контроля доступа на основе ролей. Например, CSN, который поддерживает построение услуги от CSP, может руководить некоторыми приложениями, но не имеет прав администрирования всей системы облачных услуг. Кроме того, CSN может иметь разрешение на доступ только к части ресурсов, имея предоставленные права. Однако CSN может сделать свои ресурсы совместно используемыми, предоставляя прикладные интерфейсы к другим CSN.

Для мультиарендного и масштабируемого уровня необходима интеграция модели контроля доступа для каждого отдельного участника и каждой отдельной группы. Для контроля доступа на базе ролей должны использоваться разделяемые несколькими арендаторами ресурсы в соответствии с группами задач в рабочем потоке и прав, предоставленных этим задачам. Таким образом, когда выполняется эта группа задач, прикладная среда SaaS должна определять механизм поддержки контроля доступа на основе задач. Такой механизм используется для обеспечения возможности временного предоставления и отзыва прав доступа арендаторов к основным ресурсам и предотвращения несанкционированного использования основных ресурсов.

8.1.2 Безопасность интерфейсов

В прикладной среде SaaS требует обеспечивать защиту интерфейсов, открытых для CSP или CSN, через которые осуществляет доставка или разработка различных видов услуг облачных вычислений, а также требуется обеспечивать защиту связи, базирующейся на этих интерфейсах. К имеющимся механизмам обеспечения безопасности интерфейсов относятся, в том числе, односторонняя/взаимная аутентификация, контрольная сумма для проверки целостности, цифровая подпись и т. д.

8.1.3 Безопасность данных

8.1.3.1 Изолирование данных

Данные могут быть изолированы физически и логически. Физическое изолирование должно выполняться с помощью контроля доступа к физическим хранилищам данных. В отношении прикладной среды SaaS должно действовать требование хранения данных разных арендаторов в разных областях физического хранилища данных или реализации контроля доступа к данным для разных арендаторов с использованием разрешения на доступ, домена данных или любых иных методов. Логическое изолирование данных означает, что разные арендаторы не должны иметь возможности доступа к данным другим арендаторов с помощью таких методов, как виртуализация, даже если все данные хранятся вместе.

В случае приложений SaaS клиентского и конфигурируемого уровня данные каждого арендатора сохраняются отдельно и изолированы от данных других арендаторов на физическом уровне.

В случае приложений SaaS мультиарендного и масштабируемого уровня данные всех арендаторов сохраняются в облаке. Следовательно, требуется, чтобы прикладная среда SaaS обладала достаточным уровнем интеллекта для разделения данных разных арендаторов и поддержания изолирования данных разных арендаторов в процессе хранения, обработки и передачи. Граница между каждым арендатором должна обеспечиваться на физическом уровне или на логическом уровне, что определяется требуемой степенью дробления изолирования и конкретным развертыванием программных и аппаратных средств облачных вычислений.

8.1.3.2 Конфиденциальность данных

В большинстве случаев данные арендатора хранятся и используются вне помещения и подвержены внешнему воздействию. Вследствие этого, требуется, чтобы прикладная среда SaaS поддерживала механизмы шифрования для обеспечения конфиденциальности данных во время передачи, в процессе обработки или в период хранения и предотвращала утечку в результате уязвимостей защиты в приложении.

Услуга шифрования данных требуется для всех уровней SaaS. Критические данные должны подвергаться шифрованию во избежание внешнего воздействия.

В случае мультиарендного и масштабируемого уровня, учитывая, что данные всех арендаторов должны храниться в одной базе данных или даже в одной большой таблице, требуется, чтобы прикладная среда SaaS обеспечивала надлежащий механизм управления ключами, для того чтобы обеспечить невозможность взлома данных другими арендаторами.

8.1.3.3 Целостность данных

Данные, в том числе системные данные и данные пользователей, такие как журналы регистрации и данные конфигурации, обусловливают предъявляемые к прикладной среде SaaS требования поддержки механизмов целостности для предупреждения неразрешенного использование этих данных во время передачи, в процессе обработки или в период хранения.

Требуется, чтобы не вносились изменения в журнал регистрации и журнал приложения. В случае внесения изменений, если произойдет отказ или ненадлежащее использование, CSP и вредоносное ПО будут защищены от прослеживания измененными журналами регистрации скрываемого процесса.

Приложение SaaS может требовать от CSC выполнять его конфигурацию по требованию. Требуется, чтобы в данные конфигурации, такие как конфигурационный файл, не вносились изменения без разрешения.

В прикладной среде SaaS данные пользователей хранятся в облаке, которым управляет CSP. В этом случае верификация целостности данных становится одним из существенных требований безопасности. Кроме того, требуется осуществлять верификацию целостность массовых данных.

8.1.3.4 Надежность данных

Для поддержки надежности данных требуется, чтобы прикладная среда SaaS поддерживала механизмы резервного копирования или дублирования данных, с тем чтобы обеспечить арендаторам возможность доступа к данным, даже если выйдет из строя часть узлов облачного хранилища.

Для размещенных данных требуется реализация многосайтного резервного копирования, в противном случае, данные станут полностью непригодными. Требуется, чтобы прикладная среда SaaS обладала возможностью полного своевременного восстановления данных, а также поддержания синхронности данных для обеспечения согласованности нескольких копий.

8.1.3.5 Прослеживаемость и контроль данных

Требуется, чтобы прикладная среда SaaS обеспечивала соответствие физического местонахождения данных применимым законам и местным нормам, а также любым ограничениям, определенным в юридических соглашениях. Требуется, чтобы прикладная среда SaaS обеспечивала для CSC методы указания местонахождения своих хранилищ данных и верификации надлежащего размещения своих данных.

Основные сомнения, связанные с совместно используемой и виртуализированной инфраструктурой, касаются не только утраты пользователями контроля над своими данными, но и размещения данных и контроля за их полным жизненным циклом. Требуется, чтобы в любой данный момент времени прикладной среде SaaS было известно точное место хранения и обработки системных и пользовательских данных и чтобы она обеспечивала верификацию местонахождения данных для CSC. И в процессе использования и после него не должна допускаться возможность прослеживания движения данных неавторизованными третьими сторонами (в том числе другими CSP).

8.1.4 Оценка и аудит безопасности

Требуется, чтобы прикладная среда SaaS инициировала в случае изменения, взлома или ненадлежащей работы основных ресурсов процедуру оценки безопасности, для того чтобы определить, затронуты ли определенные службы безопасности или их применимые стратегии обеспечения безопасности, а также предлагается ли индикации и инструкции для указания того, что они не могут удовлетворять заранее определенным условиям. Верификацию того, что прикладная среда SaaS отвечает применимым требованиям к безопасности, следует делегировать авторизованной стороне. Оценка безопасности или аудит безопасности могут осуществляться CSC, CSP или третьей стороной (CSN), а сертификация средств безопасности может выполняться авторизованной третьей стороной (CSN).

Для предоставления надежных, независимых и беспристрастных оценок уровня безопасности или аудита безопасности следует использовать независимые доверенные третьи стороны.

8.1.5 Укрепление безопасности

Прикладная среда SaaS предназначена в основном для предоставления возможности многоарендного развития, развертывания и среды выполнения с множеством арендаторов для приложений SaaS, ориентированных на безопасное обслуживание. Функции обеспечения безопасности приложений SaaS в ряде случаев недостаточны или недостаточно развиты. Требуется, чтобы прикладная среда SaaS находила и верифицировала эти ограниченные функции безопасности приложений SaaS и обеспечивала механизмы дифференцированного укрепления безопасности для усиления приложений SaaS исходя из этих ограниченных функций безопасности, с тем чтобы отвечать требованиям к безопасности различных арендаторов в различных условиях. Функции безопасности приложений включают функции статической безопасности, когда приложения находятся в состоянии простоя, и функции динамической безопасности, когда происходит работа приложений.

8.2 Требования к безопасности, предъявляемые CSP

Наряду с общими требованиями к безопасности CSP предъявляет конкретные требования к безопасности в прикладной среде SaaS.

8.2.1 Готовность

Для CSP требуется, чтобы прикладная среда SaaS обеспечивала постоянное обслуживание CSC, что требует обработки отказов аппаратных/программных средств, атак типа "отказ в обслуживании" и т. д. Важно обеспечивать для CSC минимальное время ожидания.

8.2.2 Гарантия функциональной совместимости/переносимости услуг

В том случае, когда CSC хочет перенести всю или часть своей системы к другому CSP, первоначальный CSP требует, чтобы прикладная среда SaaS обеспечивала гарантию функциональной совместимости/переносимости услуг для минимизации ущерба деятельности CSC. Наряду с этим требуется, чтобы прикладная среда SaaS гарантировала, что соответствующие данные будут безвозвратно удалены у предыдущего CSP и не будут восстановлены какой-либо иной стороной.

8.2.3 Защита программных средств

Требуется, чтобы в прикладной среде SaaS осуществлялась защита программных средств (таких как приложения, внутренние данные приложений, сценарии, макросы, библиотека кодов функций, лицензия на использование ПО и т. д.).

CSP требует, чтобы прикладная среда SaaS защищала конфиденциальность и целостность любых программных средств, которые обеспечиваются CSP или CSN, то есть что отсутствует возможность копирования, незаконного завладения, искажения, передачи или какого-либо иного использования этих программных средств неразрешенным образом.

8.2.4 Нормативно-правовое соответствие

При том что CSP может использовать механизмы резервного копирования и дублирования данных, для обеспечения надежности данных CSC, требуется, чтобы прикладная среда SaaS не допускала существования копий данных, длительность которого превышает период хранения данных, разрешенный применимым законом о защите данных.

8.2.5 Верификация безопасности для исходных кодов

В прикладной среде SaaS CSN может предоставлять CSP прикладные коды, контент или ПО, поэтому требуется, чтобы прикладная среда SaaS обеспечивала механизмы, помогающие CSP в верификации кодов и предотвращении проникновения вредоносных кодов.

8.3 Требования к безопасности, предъявляемые CSN

В прикладной среде SaaS CSN может быть разработчиком приложений, разработчиком контента, разработчиком ПО, интегратором и аудитором системы. Наряду с общими требованиями к безопасности CSN предъявляет конкретные требования к безопасности в прикладной среде SaaS.

8.3.1 Безопасность аудита

Если CSN является аудитором, требуется, чтобы прикладная среда SaaS обеспечивала механизмы, помогающие CSN в сборе событий аудита, информации регистрации и отчетной информации с детализацией по арендаторам и приложению. Такая информация используется для гарантирования соответствия осуществляемого CSP обслуживания государственным нормативным требованиям и юридическим соглашениям, заключенным с арендаторами. Требуется также, чтобы прикладная среда SaaS предоставляла механизмы, помогающие CSN в обеспечении того, что информация, собираемая и сообщаемая компонентами аудита в системе CSP, является верной и не подвергается искажению или манипулированию.

Наряду с этим требуется, чтобы прикладная среда SaaS обеспечивала для CSN возможность регистрации изменений важных данных и мониторинга готовности данных в онлайновом режиме, с тем чтобы своевременно направлять сигнал о нарушении безопасности и, тем самым, уменьшать потери.

8.3.2 Безопасность ПО

В том случае если CSN является разработчиком облачного контента или ПО, требуется, чтобы прикладная среда SaaS предоставляла механизмы, помогающие CSN в обеспечении соответствия их кодов или иных компонентов, подаваемых в CSP, любым ограничениям на программирование, которые требует CSP. Наряду с этим коды или компоненты не должны содержать вредоносного ПО или нарушать целостности облачных услуг CSP.

8.3.3 Удобство сопровождения ПО

В том случае если CSN является разработчиком облачного ПО, требуется, чтобы прикладная среда SaaS поддерживала механизмы, помогающие CSN в предоставлении исходных кодов или иных функциональных средств системе CSP. Требуется, чтобы исходные коды или функциональные средства содержали средства управления версиями и другие соответствующие методы, с тем чтобы обеспечивать возможность их сопровождения на протяжении жизненного цикла услуги. К таким методам относятся, в том числе, обеспечение обновлений для устранения известных уязвимостей, устранение зависимости от других компонентов, имеющих известные уязвимости, и повышение общего уровня безопасности системы.

Библиография

[b-ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2014 г.), *Основы безопасности облачных вычислений*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

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, 2017 г.