



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

**МСЭ-Т**

СЕКТОР СТАНДАРТИЗАЦИИ  
ЭЛЕКТРОСВЯЗИ МСЭ

**Y.2201**

(04/2007)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ  
ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА  
ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – **Аспекты  
обслуживания: возможности услуг и архитектура  
услуг**

---

**Требования к сетям последующих поколений  
версии 1**

Рекомендация МСЭ-Т Y.2201

---

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y  
ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ  
МЕЖСЕТЕВОГО ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
<b>Аспекты обслуживания: возможности услуг и архитектура услуг</b>	<b>Y.2200–Y.2249</b>
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
<b>Безопасность</b>	<b>Y.2700–Y.2799</b>
Обобщенная мобильность	Y.2800–Y.2899

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

**Требования к СПП версии 1**

**Резюме**

В Рекомендации МСЭ-Т Y.2201 представлены требования высокого уровня к услугам и функциональным возможностям сети последующего поколения (СПП) версии 1.

**Источник**

Рекомендация МСЭ-Т Y.2201 утверждена 27 апреля 2007 года 13-й Исследовательской комиссией МСЭ-Т (2005-2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

**Ключевые слова**

Учет, адресация, аутентификация, авторизация, возможности, требования к возможностям, начисление платы, идентификация, взаимосвязь, взаимодействие, управление, мобильность, присвоение имен, СПП версия 1, нумерация, ОАМ, открытая среда услуг, политика, секретность, профиль, эмуляция ТфОП/ЦСИС, моделирование ТфОП/ЦСИС, QoS, безопасность, подключение услуги.

## ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. 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 I 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 носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т.п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

## ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получал извещений об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это 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/>.

© ITU 2008

Все права сохранены. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо средств без предварительного письменного разрешения МСЭ.

## СОДЕРЖАНИЕ

	Стр.
1 Сфера применения .....	1
2 Справочные документы .....	1
3 Определения .....	3
3.1 Термины, определенные в других документах .....	3
3.2 Термины, определенные в настоящей Рекомендации .....	4
4 Сокращения и акронимы .....	5
5 Условные обозначения .....	6
6 Требования к функциональным возможностям для СПП версии 1 .....	6
6.1 Возможности подключений для транспорта .....	7
6.2 Режимы связи .....	7
6.3 Управление ресурсами среды передачи .....	7
6.4 Кодеки .....	8
6.5 Сеть доступа и подключение к сети .....	8
6.6 Сети пользователей .....	9
6.7 Присоединение, функциональная совместимость и взаимодействие .....	9
6.8 Маршрутизация .....	11
6.9 Качество обслуживания .....	11
6.10 Учет и начисление платы .....	13
6.11 Нумерация, присвоение имен и адресация .....	13
6.12 Идентификация, аутентификация и авторизация .....	15
6.13 Безопасность .....	19
6.14 Управление мобильностью .....	19
6.15 ОАМ .....	20
6.16 Живучесть .....	22
6.17 Управление .....	23
6.18 Открытая среда услуг .....	24
6.19 Управление профилем .....	27
6.20 Управление на основе заданных правил .....	28
6.21 Подключение услуги .....	29
6.22 Эмуляция и моделирование ТфОП/ЦСИС .....	35
6.23 Аспекты общественных интересов .....	36
6.24 Защита важной инфраструктуры .....	38
6.25 Неразглашение информации в интерфейсах NNI .....	39
6.26 Обмен информацией, связанной с пользователями, между поставщиками .....	39
Дополнение I – Отображение услуг для подключений услуги .....	40
Список литературы .....	41



## Рекомендация МСЭ-Т Y.2201

### Требования к сетям последующих поколений (СПП) версии 1

#### 1 Сфера применения

В данной Рекомендации определяются высокоуровневые требования для разработки набора Рекомендаций МСЭ-Т, которые будут служить основой для СПП версии 1.

Высокоуровневые требования и соответствующие функциональные возможности, определенные в данной Рекомендации, соответствуют основным целям и требованиям, которые зафиксированы в [ITU-T Y.2001], и основаны на требованиях к СПП версии 1, определенных в [b-ITU-T Y-Sup.1]. В СПП должен быть представлен, как минимум, один уровень обслуживания, в котором предоставляются возможности, идентичные или лучшие, чем возможности, предоставляемые сетями с коммутацией каналов.

Более подробные сведения о требованиях к услугам выходят за рамки данной Рекомендации. В то время как требования к оборудованию пользователя остаются за рамками данной Рекомендации, требования, связанные с организацией доступа, находятся в сфере применения данной Рекомендации.

Известно, что конкретная реализация СПП может быть составлена произвольным набором или расширенным набором услуг, поддерживаемых в СПП версии 1, и функциональных возможностей, как указано в данной Рекомендации.

Администрации могут потребовать, чтобы поставщики услуг СПП при реализации данной Рекомендации принимали во внимание национальные регуляторные требования и требования государственной политики

#### 2 Справочные документы

В нижеследующих Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые, посредством ссылок в настоящем тексте, составляют положения настоящей Рекомендации. На время публикации указанные здесь издания были действительными. Все Рекомендации и другие справочные документы постоянно пересматриваются, поэтому всем пользователям данной Рекомендации настоятельно рекомендуется изучить возможность использования последних изданий, перечисленных ниже Рекомендаций и других справочных документов. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей Рекомендации на какой-либо документ не придает этому отдельному документу статуса Рекомендации.

- |                 |   |
|-----------------|---|
| [ITU-T E.106]   | Рекомендация МСЭ-Т E.106 (2003 г.), <i>Международная схема аварийных приоритетов (IEPS) для операций по ликвидации последствий чрезвычайных ситуаций.</i>           |
| [ITU-T E.107]   | Рекомендация МСЭ-Т E.107 (2007 г.), <i>Служба электросвязи в чрезвычайных ситуациях (ETS) и основа для взаимодействия реализованных на национальном уровне ETS.</i> |
| [ITU-T E.164]   | Рекомендация МСЭ-Т E.164 (2005 г.), <i>Международный план нумерации электросвязи общего пользования.</i>  |
| [ITU-T E.212]   | Рекомендация МСЭ-Т E.212 (2004 г.), <i>Международный план идентификации для мобильных терминалов и пользователей подвижной связи.</i>                               |
| [ITU-T G.711]   | Рекомендация МСЭ-Т G.711 (1988 г.), <i>Импульсно-кодовая модуляция (ИКМ) голосовых частот.</i>  |
| [ITU-T G.780]   | Рекомендация МСЭ-Т G.780/Y.1351 (2004 г.), <i>Термины и определения для сетей синхронной цифровой иерархии (СЦИ).</i>   |
| [ITU-T G.808.1] | Рекомендация МСЭ-Т G.808.1 (2006 г.), <i>Обобщенная защитная коммутация – Линейная защита канала и подсети.</i>   |
| [ITU-T I.610]   | Рекомендация МСЭ-Т I.610 (1999 г.), <i>Принципы и функции эксплуатации и обслуживания В-ЦСИС.</i>   |

- [ITU-T M.3050.0] Рекомендация МСЭ-Т М.3050.0 (2007 г.), *Расширенная карта бизнес-процессов оператора электросвязи (eTOM) – Введение.*
- [ITU-T M.3050.1] Рекомендация МСЭ-Т М.3050.1 (2007 г.), *Расширенная карта бизнес-процессов оператора электросвязи (eTOM) – Структура бизнес-процессов.*
- [ITU-T M.3060] Рекомендация МСЭ-Т М.3060/Y.2401 (2006 г.), *Принципы управления сетями последующих поколений.*
- [ITU-T Q.825] Рекомендация МСЭ-Т Q.825 (1998 г.), *Определение приложений TMN в интерфейсе Q3: Запись подробностей вызова.*
- [ITU-T Q.1703] Рекомендация МСЭ-Т Q.1703 (2004 г.), *Структура функциональных возможностей служб и сети аспектов сети для систем, не входящих в IMT-2000.*
- [ITU-T Q.1706] Рекомендация МСЭ-Т Q.1706/Y.2801 (2006 г.), *Требования управления мобильностью для СПП.*
- [ITU-T Q.1741.1] Рекомендация МСЭ-Т Q.1741.1 (2002 г.), *Ссылки из IMT-2000 для версии 1999 года эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN.*
- [ITU-T Q.1741.2] Рекомендация МСЭ-Т Q.1741.2 (2002 г.), *Ссылки из IMT-2000 для версии 4 эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN.*
- [ITU-T Q.1741.3] Рекомендация МСЭ-Т Q.1741.3 (2003 г.), *Ссылки из IMT-2000 для версии 5 эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN.*
- [ITU-T Q.1741.4] Рекомендация МСЭ-Т Q.1741.4 (2005 г.), *Ссылки из IMT-2000 для версии 6 эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN..*
- [ITU-T X.462] Рекомендация МСЭ-Т X.462 (1996 г.), *Информационная технология – Управление системами обработки сообщений (MHS): Информация о регистрации.*
- [ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами.*
- [ITU-T Y.101] Рекомендация МСЭ-Т Y.101 (2000 г.), *Терминология инфраструктуры глобальной информации: Термины и определения.*
- [ITU-T Y.110] Рекомендация МСЭ-Т Y.110 (1998 г.), *Принципы и структурная архитектура инфраструктуры глобальной информации.*
- [ITU-T Y.1271] Рекомендация МСЭ-Т Y.1271 (2004 г.), *Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов.*
- [ITU-T Y.1541] Рекомендация МСЭ-Т Y.1541 (2006 г.), *Требования к сетевым показателям качества для служб, основанных на протоколе IP/*
- [ITU-T Y.1710] Рекомендация МСЭ-Т Y.1710 (2002 г.), *Требования для функциональных возможностей эксплуатации и обслуживания в сетях MPLS.*
- [ITU-T Y.1730] Рекомендация МСЭ-Т Y.1730 (2004 г.), *Требования к функциям ОАМ в сетях на основе Ethernet и служб Ethernet.*
- [ITU-T Y.2001] Рекомендация МСЭ-Т Y.2001 (2004 г.), *Общий обзор СПП.*
- [ITU-T Y.2012] Рекомендация МСЭ-Т Y.2012 (2006 г.), *Функциональные требования и архитектура СПП версии 1.*
- [ITU-T Y.2091] Рекомендация МСЭ-Т Y.2091 (2007 г.), *Термины и определения для сетей последующего поколения.*

- [ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования безопасности для СПП версии 1.*  
[ITU-T Z.100] Рекомендация МСЭ-Т Z.100 (2002 г.), *Язык описания и спецификаций (SDL).*

### 3 Определения

#### 3.1 Термины, определенные в других документах

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

**3.1.1 Учет (accounting) [ITU-T X.462].** Деятельность по сбору информации об операциях, осуществленных в рамках системы, и их последствиях.

**3.1.2 Адрес (address) [ITU-T Y.2091].** Адрес представляет собой идентификатор для конкретного пункта завершения связи и используется для маршрутизации в этот пункт завершения.

**3.1.3 Интерфейс приложение-сеть (application network interface) (ANI) [ITU-T Y.2012].** Интерфейс, обеспечивающий канал взаимодействия и обмена между приложениями и элементами СПП. ANI обеспечивает возможности и ресурсы, необходимые для внедрения приложений.

**3.1.4 Выставление счетов (billing) [ITU-T Q.1703].** Административная функция для подготовки счетов потребителям услуг, для своевременной оплаты, получения выручки и работы с рекламациями клиентов.

**3.1.5 Начисление платы (charging) [ITU-T Q.825].** Набор функций, необходимых для определения цены, назначаемой за пользование услугами.

**3.1.6 Корпоративная сеть (corporate network) [ITU-T Y.2701].** Частная сеть, которая поддерживает множество пользователей и которая может располагаться во многих местах, например, на предприятии, в университетском городке.

**3.1.7 Клиент (customer) [ITU-T M.3050.1].** Клиент приобретает продукты и услуги у предприятия либо получает бесплатные предложения или услуги. Потребитель может быть лицом или предприятием.

**3.1.8 Конечный пользователь (end user) [ITU-T M.3050.1].** Конечный пользователь является фактическим пользователем продуктов или услуг, предлагаемых предприятием. Конечный пользователь потребляет продукт или услугу. См. также "Абонент".

**3.1.9 Эстафетная передача абонента (handover) [ITU-T Q.1706].** Возможность предоставлять услуги, которая некоторым образом влияет на соглашения об уровне обслуживания, движущемуся объекту во время и после передвижения.

**3.1.10 Домашняя сеть (home network) [ITU-T E.212].** Сеть, связанная с оператором/поставщиком услуг, на услуги которой подписан данный абонент.

**3.1.11 Идентификатор (identifier) [ITU-T Y.2091].** Идентификатор представляет собой серию цифр, букв и символов или данных в любой другой форме, используемую для идентификации абонента(ов), пользователя(ей), элемента(ов) сети, функции(й), объекта(ов) сети, предоставляющего(их) услуги/приложения, или других объектов (например, физические или логические объекты). Идентификаторы могут использоваться для регистрации или авторизации. Они могут быть либо открытыми для всех сетей и используемыми совместно ограниченным количеством сетей, либо частными для конкретной сети (частные ID как правило не раскрываются третьим сторонам).

**3.1.12 Интернет (internet) [ITU-T Y.101].** Совокупность присоединяемых сетей, использующих протокол Интернет, который позволяет им функционировать как единой, крупной виртуальной сети.

**3.1.13 Мобильность (mobility) [ITU-T Y.2001].** Возможность для пользователя или других подвижных объектов осуществлять связь и иметь доступ к услугам вне зависимости от изменений местоположения или технических условий. Степень доступности услуги может зависеть от нескольких факторов, включая возможности сети доступа, соглашения об уровне обслуживания между домашней сетью пользователя и визитной сетью (если это применимо) и т. д. Мобильность включает возможность обеспечения электросвязи с непрерывным предоставлением услуг или без непрерывного предоставления услуг.

ПРИМЕЧАНИЕ. – В Рекомендации [ITU-T Y.2001] это понятие называется универсальной мобильностью.

**3.1.14 Управление мобильностью (mobility management) [ITU-T Q.1706].** Набор функций, используемых для обеспечения мобильности.

ПРИМЕЧАНИЕ. – Такие функции включают аутентификацию, авторизацию, уточнение местоположения, пейджинг, загрузку информации пользователя и т. д.

**3.1.15 Кочевничество (nomadism) [ITU-T Q.1706].** Возможность для пользователя изменять при передвижении свой пункт доступа к сети; при изменении пункта доступа к сети сеанс обслуживания пользователя полностью останавливается и затем вновь начинается, т. е. непрерывный сеанс или передача абонента невозможны. Считается, что обычный способ использования следующий: пользователь завершает свой сеанс обслуживания до перемещения в другой пункт доступа.

**3.1.16 Персональная мобильность (personal mobility) [ITU-T Q.1706].** Означает мобильность для тех сценариев, при которых пользователь изменяет оконечное оборудование, используемое для доступа к сети в различных пунктах. Возможность пользователя получить доступ к услугам электросвязи с любого оконечного оборудования на основе персонального идентификационного номера, а также возможность сети предоставлять эти услуги определяется в профиле услуги пользователя.

**3.1.17 Роуминг (roaming) [ITU-T Q.1706].** Означает возможность пользователей получать доступ к услугам в соответствии со своим профилем пользователя, находясь при этом вне своей домашней абонентской сети, т. е. используя пункт доступа визитной сети. Для этого необходима возможность доступа к визитной сети, наличие интерфейса между домашней сетью и визитной сетью, а также соглашение о роуминге между соответствующими сетевыми операторами.

**3.1.18 Плавная эстафетная передача абонента (seamless handover) [ITU-T Q.1706].** Особый случай мобильности с непрерывностью обслуживания, так как он сохраняет способность предоставлять услуги движущимся объектам во время и после движения без какого-либо влияния на соглашения об уровне обслуживания.

**3.1.19 Услуга (service) [ITU-T Z.100].** Набор функций и средств, предлагаемых поставщиком услуг пользователю.

**3.1.20 Непрерывность обслуживания (service continuity) [ITU-T Q.1706].** Возможность для подвижного объекта сохранять предоставляемое обслуживание, включая текущее состояние, такое как сетевая среда пользователя и сеанс для предоставления услуги.

**3.1.21 Абонент (subscriber) [ITU-T M.3050.1].** Лицо или организация, ответственные за заключение контрактов на абонируемые услуги и за оплату этих услуг.

**3.1.22 Мобильность оконечного оборудования (terminal mobility) [ITU-T Q.1706].** Означает мобильность для тех сценариев, при которых одно и то же оконечное оборудование перемещается или используется в разных пунктах. Возможность оконечного оборудования получить доступ к услугам электросвязи из различных пунктов и во время движения, а также возможность сети определять и устанавливать местоположение этого оконечного оборудования.

**3.1.23 Сеть пользователя (user network) [ITU-T Y.2701].** Частная сеть, состоящая из оконечного оборудования, которая может иметь множество пользователей.

**3.1.24 Визитная сеть (visited network) [ITU-T Q.1706].** Сеть, которая в конфигурации роуминга является местной для клиента.

## **3.2 Термины, определенные в данной Рекомендации**

В данной Рекомендации определяются следующие термины.

**3.2.1 Классификация по приоритетности (priority classification).** Классификация классов трафика в соответствии с различными уровнями приоритетов.

**3.2.2 Механизм включения приоритетности (priority enabling mechanisms).** Механизмы, с помощью которых может включаться режим передачи трафика в сети, соответствующий приоритету.

**3.2.3 Сигнализация приоритетности (priority signalling).** Часть механизмов включения приоритетности, в которой используется сигнализация.

**3.2.4 Однократная регистрация входа (single sign-on).** Возможность использовать утверждение аутентификации от одного оператора сети/поставщика услуг в сети другого оператора/поставщика услуг для пользователя, запрашивающего доступ к услуге или возможность роуминга в визитной сети.

**3.2.5 Идентификатор оконечного оборудования (terminal equipment identifier).** Уникальный идентификатор оконечного оборудования.

**3.2.6 Пользователь (user).** Понятие "пользователь" включает в себя окончательного пользователя (Рек. МСЭ-Т У.2091), физическое лицо, абонента, систему, оборудование, терминал, например, факс, персональный компьютер, (функциональный) блок, процесс, приложение, поставщика или корпоративную сеть.

**3.2.7 Атрибут пользователя user (attribute).** Характеристика, которая описывает пользователя, например, время жизни идентификатора пользователя, статус пользователя в значении "доступен", "не беспокоить" и т. д.

**3.2.8 Идентификатор пользователя (user identifier).** Тип пароля, образа или псевдонима, связанного с пользователем, который назначается и передается между операторами и поставщиками услуг для идентификации пользователя, аутентификации ее/его личности и/или для авторизации пользования услугой. Примерами могут служить SIP (протокол инициации сеанса связи), URI (унифицированный идентификатор ресурса) и т. д.

## 4 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения и акронимы:

ANI	Application Network Interface	Интерфейс приложение-сеть
API	Application Programming Interface	Программный интерфейс приложения
ATM	Asynchronous Transfer Mode	Асинхронный режим переноса
B2B	Business-to-Business	Взаимодействие бизнес-бизнес
CC	Content of Communication	Содержимое передаваемой информации (контент)
CD/DVD	Compact Disk/Digital Versatile Disk	Компакт диск/цифровой видеодиск
DNS	Domain Name System	Система доменных имен
DTMF	Dual Tone Multi Frequency	Двухтональный многочастотный набор
ENUM	tElephone NUmber Mapping	Отображение телефонного номера в IP-сети
ETS	Emergency Telecommunications Service	Служба электросвязи в чрезвычайных ситуациях
IEPS	International Emergency Preference Scheme	Международная приоритетная схема для оказания помощи в чрезвычайных ситуациях
IM	Instant Messaging	Мгновенный обмен сообщениями
IMS	IP Multimedia Subsystem	Мультимедийная подсистема IP
IN	Intelligent Network	Интеллектуальная сеть
IP	Internet Protocol	Протокол Интернет
IP-CAN	IP Connectivity Access Network	Сеть доступа с возможностью соединения по протоколу IP
IPv4	Internet Protocol version 4	Протокол Интернет версия 4
IPv6	Internet Protocol version 6	Протокол Интернет версия 6
IRI	Intercept Related Information	Сведения, полученные в результате перехвата данных
ISDN	Integrated Services Digital Network	Цифровая сеть с интеграцией служб (ЦСИС)
IT	Information Technology	Информационная технология
LEA	Law Enforcement Agencies	Правоохранительные органы
MMS	Multimedia Messaging Service	Служба передачи сообщений мультимедиа
MPLS	Multi-Protocol Label Switching	Многопротокольная коммутация на основе признаков
NAI	Network Access Identifier	Сетевой идентификатор доступа
NAPT	Network Address Port Translation	Трансляция сетевых адресов и портов
NAT	Network Address Translation	Трансляция сетевых адресов
NGN	Next Generation Network	Сети последующих поколений

NNI	Network-Network Interface	Межсетевой интерфейс
OAM	Operations, Administration and Maintenance	Эксплуатация, администрирование и техническое обслуживание
OMA	Open Mobile Alliance	Открытый альянс мобильной связи
OS	Operating System	Операционная система
OSA	Open Service Access	Открытый доступ к услугам
OTN	Optical Transport Network	Оптическая транспортная сеть
QoS	Quality of Service	Качество обслуживания
PBX	Private Branch Exchange	Телефонная система для частного пользования
PC	Personal Computer	Персональный компьютер
PDA	Personal Digital Assistant	Персональный цифровой секретарь
PLMN	Public Land Mobile Network	Сухопутная подвижная сеть общего пользования
POTS	Plain Old Telephone Service	Обычная аналоговая телефонная служба
PSTN	Public Switched Telephone Network	Коммутируемая телефонная сеть общего пользования
RACF	Resource and Admission Control Functions	Функции управления ресурсами и доступом
SIP	Session Initiation Protocol	Протокол инициации сеанса связи
SLA	Service Level Agreement	Соглашение об уровне обслуживания
SMS	Short Message Service	Служба коротких сообщений
SR	Service Resiliency	Способность услуги к восстановлению
TDR	Telecommunications for Disaster Relief	Электросвязь для помощи при стихийных бедствиях
TE	Terminal Equipment	Оконечное оборудование
UDDI	Universal Discovery, Description and Integration	Универсальное обнаружение, описание и интеграция
UMTS	Universal Mobile Telecommunications System	Универсальная система подвижной электросвязи
UNI	User to Network Interface	Интерфейс пользователь-сеть
URI	Uniform Resource Identifier	Унифицированный идентификатор ресурса
VPN	Virtual Private Network	Виртуальная частная сеть
xDSL	Various types of Digital Subscriber Lines	Различные типы цифровой абонентской линии

## 5 Условные обозначения

Нет.

## 6 Требования к функциональным возможностям для СПП версии 1

В последующих разделах представлены высокоуровневые требования и соответствующие им функциональные возможности для обеспечения целевых показателей услуг сетей СПП версии 1, определенных в [b-ITU-T Y-Sup.1].

Эти требования, в основном, исходят из перспектив высокого уровня и не предназначены для формирования точных функциональных требований для различных объектов СПП.

Более подробные сведения о требованиях к конкретным услугам в данной Рекомендации не рассматриваются.

В данной Рекомендации приведены только требования к функциональным возможностям сети СПП. Хотя требования к оборудованию пользователя здесь не приведены, приводятся требования, связанные с организацией доступа.

### **6.1 Возможности подключений для транспорта**

Для транспортного уровня СПП версии 1 [У.2012] должен использоваться IP протокол с целью обеспечения общих возможностей подключения повсеместно и на глобальном уровне. IP протокол может передаваться с помощью различных базовых технологий транспортировки на участках доступа и в центральной части транспортного уровня, например xDSL, ATM, MPLS, ретрансляция кадров, OTN, в соответствии со средой передачи, используемой оператором.

ПРИМЕЧАНИЕ. – Это не мешает операторам предоставлять услуги непосредственно пользователю с применением конкретных технологий (например, ATM, MPLS, ретрансляция кадров, OTN).

Возможности подключения должны предусматривать:

- 1) использование протоколов IPv4 и IPv6;
- 2) обеспечение связи в режиме реального времени и не в режиме реального времени;
- 3) возможность подключения по сценарию "один к одному";
- 4) возможность подключения по сценарию "один ко многим".

### **6.2 Режимы связи**

Сеть СПП должна поддерживать следующие режимы связи:

- один к одному;
- один ко многим;
- многие ко многим;
- многие к одному.

### **6.3 Управление ресурсами среды передачи**

Механизмы управления ресурсами среды передачи обычно используются в сочетании с традиционными услугами обработки речи и взаимодействия пользователей посредством речевого общения и DTMF. В СПП они должны быть расширены за счет новых услуг передачи данных, видео услуг и услуг передачи контента.

Сети СПП должны поддерживать различные ресурсы передачи и возможности управления ресурсами передачи с целью реализации широкого диапазона приложений.

Функциональные возможности ресурса передачи включают:

- запись медиа-данных, например, для предоставления услуг голосовой почты;
- воспроизведение записанных медиа-данных, например, прослушивание голосовой почты, сигналов, объявлений;
- распознавание сигналов DTMF, например, для предоставления услуг интерактивного голосового ответа;
- улучшенное распознавание речи, например, для предоставления услуг интерактивного голосового ответа;
- преобразование медиа-данных, например, преобразование текста в речь, речи в текст, факсимильных сообщений в электронную почту;
- перекодировку;
- параллельную передачу видео/текста/звука/данных, например, для конференц-связи;
- дублирование медиа-данных, например, для реализации сценариев законного перехвата данных;
- вставка медиа-данных.

## 6.4 Кодеки

Общие требования для кодеков включают следующее:

- 1) По мере возможности следует избегать перекодирования.
- 2) Сеть СПП должна поддерживать сквозное согласование любого кодека между объектами СПП (оконечными устройствами, элементами сети). За согласование и выбор общего кодека для каждого сквозного сеанса передачи данных отвечают объекты, расположенные на границах СПП, например, оконечные устройства СПП и оборудование пользователя, и сетевое оборудование с которого передается и на котором завершается передача IP потоков медиа-данных СПП. СПП должна поддерживать сквозное согласование текстовых кодеков, например кодеков, указанных в Рекомендациях МСЭ-Т.

ПРИМЕЧАНИЕ. – Предполагается, что в оборудовании пользователя СПП будет использоваться широкополосный звуковой кодек.

- 3) Для обеспечения взаимодействия между СПП и другими сетями, включая ТфОП/ЦСИС, PLMN и другие СПП, сеть СПП должна иметь возможность приема и воспроизведения речи закодированной согласно G.711 [G.711], при взаимодействии с другой сетью.
- 4) Если размер пакета не был выбран во время согласования кодека между оконечными устройствами и/или сетевыми элементами, или он не установлен двусторонним соглашением, то для речи закодированной согласно G.711 [G.711], должен использоваться размер пакета с отсчетами длиной 10 мс; это значение рекомендуется как оптимальное для уравнивания сквозной задержки с загрузкой сети. Известно, что в сети могут быть ограничения, для которых требуется, чтобы двусторонним соглашением было согласовано более высокое значение; в таких случаях рекомендуется значение 20 мс.

ПРИМЕЧАНИЕ 2. – Если при согласовании кодека между оконечными устройствами и/или элементами сети размер пакета выбран, данная Рекомендация не налагает никаких требований к выбираемому значению.

ПРИМЕЧАНИЕ 3. – Перекодировка может использоваться в сценариях в качестве функции распределения, когда сквозное соглашение не приводит к использованию общего кодека.

ПРИМЕЧАНИЕ 4. – Требования, описанные выше, не обязывают, чтобы оконечные устройства поддерживали любой кодек, или чтобы СПП поддерживали перекодирование между любым произвольным звуковым кодеком и G.711 [G.711].

## 6.5 Сеть доступа и подключение к сети

Целью СПП является поддержка услуг и приложений независимо от технологий сети доступа. Таким образом:

- 1) Сеть СПП должна поддерживать различные технологии функций транспорта доступа.
- 2) Транспортный уровень должен поддерживать возможности установления IP соединения между функциями конечного пользователя и основными функциями транспортировки.
- 3) Сеть СПП не должна препятствовать тому, чтобы сети пользователя имели любой уровень сложности, конфигурации.
- 4) Сеть СПП должна поддерживать регистрацию на уровне сети доступа, инициализацию функций конечного пользователя для доступа к услугам СПП и управление пространством IP адресов сети доступа, включая функцию NAT.
- 5) В профиле пользователя должны содержаться данные аутентификации доступа пользователя и сведения, относящиеся к конфигурации доступа к сети.
- 6) Сеть СПП должна поддерживать перенастройку услуг доступных пользователю в том случае, если пользователь является кочующим и обращается к услугам из места, не являющегося местом подписки. Работа услуг может зависеть от одного или от всех далее приведенных факторов: устройства пользователя, сети доступа и соглашений (например, соглашений о роуминге) между поставщиком услуг и поставщиком сети доступа. В сети доступа ресурсы должны быть распределены в соответствии с предоставляемыми услугами.
- 7) Если сети с многостанционным доступом подключены к одной центральной сети СПП, то сеть доступа должна поддерживать аутентификацию/авторизацию доступа пользователем, посещающим данную сеть доступа в процессе роуминга из другой сети доступа.

- 8) Для обеспечения гарантированной доступности услуг роуминга, процедуры подключения сети доступа СПП должны поддерживать аутентификацию сети доступа, основанную на стандартизованном методе для идентифицирующего пользователя на уровне сети доступа, например, механизм идентификатора присоединения к сети (NAI), определенный в [b-RFC 2486].

## 6.6 Сети пользователей

Далее приведены общие требования сети СПП версии 1 к доступу через сети пользователей:

- 1) Сеть СПП не должна запрещать решения по предоставлению доступа через сеть пользователя к СПП с использованием NAT/NAPT и брандмауэров в среде пользователя, где назначение IP адресов оборудованию пользователя может быть выполнено сетью пользователя. Для таких адресов может отсутствовать возможность маршрутизации в СПП.
- 2) Решения по предоставлению доступа к СПП через сеть пользователя должны оказывать минимальное влияние на существующие модели развертывания сети пользователя.
- 3) Решения по предоставлению доступа к СПП через сеть пользователя должны поддерживать следующие конфигурации
  - прямое соединение и взаимодействие отдельных оконечных устройств и СПП;
  - опосредованное соединение и взаимодействие отдельных оконечных устройств и СПП, например, через офисные IP АТС (IP PBX).

Сети СПП версии 1 должны поддерживать одновременное использование одним оконечным устройством нескольких типов функций транспорта доступа, однако требования по согласованию связи отсутствуют. Поэтому, с точки зрения сети, такие оконечные устройства могут отображаться как два или несколько отдельных оконечных устройств.

ПРИМЕЧАНИЕ. – Хотя в требованиях данной Рекомендации, не упоминается оконечное оборудование, в них не подразумевается запрет присоединения оконечного оборудования, которое может позволять адаптацию интерфейса под различные нужды пользователей, включая людей с ограниченными возможностями, при помощи наиболее распространенных устройств интерфейса пользователя.

## 6.7 Присоединение, функциональная совместимость и взаимодействие

Функциональная совместимость и взаимодействие – это две отдельные функции, они определены соответственно в [ITU-T Y.101] и в сериях Рекомендаций Y.1400.

### 6.7.1 Присоединение

Различаются два типа присоединений между сетями СПП версии 1:

- "присоединение, ориентированное на обеспечение соединения", основывается на простом установлении IP соединений, независимо от уровней функциональной совместимости сетей;

ПРИМЕЧАНИЕ 1. – Присоединение данного типа не содержит сведений о конкретной услуге, предоставляемой в сквозном режиме, и как следствие, рабочие характеристики сети, требования к QoS и безопасности не могут быть гарантированы в обязательном порядке.

- "присоединение, ориентированное на услугу", дает возможность операторам и поставщикам услуг предлагать услугу с определенными уровнями функциональной совместимости.

ПРИМЕЧАНИЕ 2. – Примером являются услуги G.711, предоставляемые через IP присоединение. Определенные уровни функциональной совместимости сетей зависят от услуги или QoS, или безопасности и т. д.

Далее приведены требования для присоединения:

- 1) Должен поддерживаться тип присоединения между сетями СПП, ориентированный на обеспечение соединения.
- 2) Не исключается тип присоединения между сетями СПП, основанный на услуге.

### 6.7.2 Функциональная совместимость сетей

Для обеспечения предоставления определенных услуг по сквозному маршруту, состоящему из одного или нескольких доменов СПП, необходимо чтобы:

- 1) В пределах домена одной СПП взаимодействовали необходимые компоненты услуг;
- 2) Не исключалась функциональная совместимость присоединенных сетей СПП, в которых развернуты одинаковые наборы функциональных возможностей услуг.

### 6.7.3 Взаимодействие с не СПП сетями

Для предоставления определенных услуг СПП версии 1 должны поддерживать взаимодействие с различными видами сетей. Услуги, определенные для взаимодействия, должны беспрепятственно предоставляться по всей инфраструктуре, представляемой одним или несколькими поставщиками сетей. Сети СПП версии 1 предоставляют функциональные возможности, включающие наряду с другими, безопасность, ОАМ, устойчивость к внешним воздействиям, качество обслуживания и, там, где необходимо, перекодирование медиа-данных для поддержки сценариев межсетевое соединения с другими не СПП сетями с целью обеспечения беспрепятственной сквозной работы.

Для того, чтобы дать возможность предоставления определенных услуг на маршруте, состоящем из сочетания сетей СПП и сетей, не СПП:

- необходимо, чтобы сеть СПП могла взаимодействовать с другими не СПП сетями;
- сеть СПП должна по мере возможности поддерживать следующие возможности взаимодействия:
  - Маршрутизация;
  - Взаимодействие сигнализации;
  - Взаимодействие по нумерации, присвоению имен и/или адресации;
  - Обмен данными, относящимися к ведению учета и начислению платы;
  - Взаимодействие в области безопасности;
  - Взаимодействие в области QoS;
  - Обмен сведениями о профиле пользователя и оконечного устройства;
  - Взаимодействие на уровне сред передачи;
  - Взаимодействие в области управления;
  - Управление политикой, включая учет различий в правилах, например, в соответствии с междоменными правилами, может возникнуть необходимость сокрытия или удаления из информационного потока, передаваемого через интерфейс с другим доверенным или доверенным доменом, внутренней информации некоторого доверенного домена, включая информацию, связанную с пользователем.

ПРИМЕЧАНИЕ. – Под этим не подразумевается, что все службы и/или функциональные возможности службы могут взаимодействовать. Данные требования могут применяться только к взаимодействию между определенными особыми (и, наиболее вероятно, аналогичными или идентичными) службами и/или функциональными возможностями службы.

#### 6.7.3.1 Взаимодействие с ТфОП/ЦСИС

При соединении сети СПП и ТфОП/ЦСИС должны поддерживаться следующие функции:

- 1) Взаимодействие между услугами ТфОП/ЦСИС и услугами эмуляции ТфОП/ЦСИС. При межсетевом обмене должен обеспечиваться высокий уровень функциональной совместимости сети с услугами эмулированной ТфОП/ЦСИС. Обеспечиваемая степень функциональной совместимости сетей зависит от операторов и, в некоторых случаях, от национальных регуляторов.
- 2) Взаимодействие между услугами ТфОП/ЦСИС и услугами моделирования ТфОП/ЦСИС: При межсетевом обмене должна поддерживаться функциональная совместимость услуг моделирования ТфОП/ЦСИС с дополнительными услугами ТфОП/ЦСИС, хотя такое взаимодействие может привести к ограничению возможностей услуги.

- 3) Взаимодействие между ТфОП/ЦСИС и мультимедийными IP услугами сети СПП, хотя такое взаимодействие может привести к ограничению возможностей услуги.

ПРИМЕЧАНИЕ 1. – Под этим не подразумевается, что все услуги СПП и/или свойства услуг могут взаимодействовать с ТфОП/ЦСИС и наоборот. Данные требования могут применяться только к взаимодействию между определенными особыми (и, наиболее вероятно, аналогичными или идентичными) услугами и/или свойствами услуги, которые предлагаются как со стороны СПП, так и ТфОП/ЦСИС.

ПРИМЕЧАНИЕ 2. – Корпоративные сети с коммутацией каналов поддерживаются в версии 1 либо посредством соединения с сетью СПП через существующие сети ТфОП/ЦСИС, либо, когда реализована эмуляция ТфОП/ЦСИС, через шлюз взаимодействия.

### **6.7.3.2 Взаимодействие с другими сетями**

- 1) Сеть СПП должна обеспечивать возможность прямого присоединения для сетей с коммутацией каналов, включая, как минимум, кабельные сети, радиовещательные сети и сети сухопутной подвижной связи общего пользования. Для всех сетей с коммутацией каналов требования по взаимодействию, такие же как и требования к ТфОП/ЦСИС.

Сеть СПП версии 1 должна поддерживать возможность для присоединения, ориентированного на установление соединения с сетями, которые не являются СПП, но основаны на протоколе IP. СПП не должна исключать возможность присоединения, ориентированного на услугу с сетями, которые не являются СПП, но основаны на протоколе IP.

Если присоединенная сеть предусматривает все возможности взаимодействия, как указано в разделе 6.7.3, такие присоединения сетей могут поддерживаться в развертывании. Характеристики и функциональные возможности сетей, не являющихся сетями СПП, но основанных на протоколе IP, являются достаточно разнообразными и многочисленными, поэтому точные требования для присоединения в версии 1 установить невозможно.

- 2) В сети СПП не должно быть преднамеренного исключения присоединений с сетями, не являющимися сетями СПП, но основанными на протоколе IP.

ПРИМЕЧАНИЕ. – Требования безопасности содержатся в разделе 6.13.

## **6.8 Маршрутизация**

В сети СПП должны быть представлены возможности выбора нужного пути маршрутизации между конечной точкой, формирующей исходящий трафик, и конечной точкой, получающей трафик.

В СПП должны поддерживаться схемы маршрутизации, наиболее подходящие для поставщиков услуг СПП. В частности, сеть СПП должна поддерживать:

- 1) как статические, так и динамические схемы маршрутизации;
- 2) схемы маршрутизации, которые могут эффективно работать в пределах домена сети СПП;
- 3) схемы маршрутизации, которые могут эффективно работать между доменами сети СПП, таким образом, обеспечивая взаимодействие.

## **6.9 Качество обслуживания**

Для того чтобы обеспечить пользователям или приложениям требуемый уровень обслуживания, в сети СПП должно поддерживаться сквозное QoS при передаче через различные сети с различными технологиями инфраструктуры, которые предоставляются множеством операторов. В СПП должно поддерживаться множество уровней QoS, которые могут согласовываться между пользователем и поставщиком услуг. В поддержку уровня обслуживания QoS входит использование механизмов управления ресурсами и доступом, разграничение классов трафика, управление приоритетностью, механизмы сигнализации QoS, измерение и управление рабочими характеристиками для обеспечения гарантии качества и управление перегрузками/избыточной нагрузкой.

### **6.9.1 Общие требования QoS**

Сеть СПП должна соответствовать следующим требованиям QoS:

- 1) Допускать использование различных технологий и бизнес-моделей.
- 2) Поддерживать различные процессы, относящиеся к жизненному циклу услуги, например, абонентскую подписку/предоставление услуг, вызов функций, мониторинг.
- 3) Поддерживать различные функциональные возможности окончного оборудования, например некоторые виды окончного оборудования могут поддерживать сигнализацию QoS на транспортном уровне, а другие – нет.
- 4) Управлять транспортными ресурсами, относящимися к QoS, в пределах сетей с пакетной коммутацией и на границах сети в соответствии с их функциональными возможностями
- 5) Поддерживать управление ресурсами и доступом в пределах отдельного домена СПП и между доменами СПП.
- 6) Поддерживать как относительное управление QoS, так и абсолютное управление QoS.
- 7) Поддерживать управляемые приложениями требования QoS.

### **6.9.2 Классы QoS в сети**

- 1) Сеть СПП должна учитывать рабочие характеристики сети на транспортном уровне.
- 2) Сеть СПП должна поддерживать классы QoS сети СПП, основанные на [ITU-T Y.1541].

### **6.9.3 Приоритетность услуг/приложений**

Сеть СПП должна поддерживать приоритетность услуг/приложений, обеспечивая:

- 1) схемы классификации приоритетности для управления доступом и восстановления;
- 2) расширения сигнализации, указывающие уровни приоритетов на интерфейсах UNI и NNI;
- 3) механизмы включения приоритетности, которые выполняют желаемое действие приоритетности.

### **6.9.4 Управление QoS**

Сеть СПП должна поддерживать:

- 1) степень детализации управления QoS на уровне потока, сеанса, класса услуги;
- 2) динамические характеристики QoS (то есть, должна быть возможность изменения атрибутов QoS во время активного сеанса связи);
- 3) управление ресурсами QoS, основанное на распределенном, централизованном или смешанном подходе;
- 4) механизмы управления доступом и перегрузками;
- 5) механизмы, обеспечивающие гарантированную своевременную и надежную доставку пакетов сигнализации и управляющих пакетов;
- 6) механизмы для назначения приоритетов доставки для электросвязи в чрезвычайных ситуациях и приоритетной электросвязи.

### **6.9.5 Сигнализация QoS**

Сеть СПП должна использовать механизмы сигнализации для поддержки QoS.

Более подробные требования к сигнализации QoS выходят за рамки данной Рекомендации и содержатся в других особых Рекомендациях.

### **6.9.6 Измерение качественных показателей и управление**

Для обеспечения гарантированного QoS, в СПП должно поддерживаться измерение качественных показателей и управление ими.

Измерение качественных показателей и управление ими должны поддерживать:

- 1) гарантированную доставку поставщиком услуг качественных показателей (для сравнения с SLA);
- 2) предоставление сведений о качественных показателях поставщиком услуг предполагаемым пользователям;

- 3) устранение поставщиком услуг неисправностей в сетях в пределах определенных трасс;
- 4) предоставление внутренних сведений поставщиком услуг о влиянии на рабочие характеристики изменений произошедших в пределах их сетей;
- 5) взаимное наблюдение поставщиками за рабочими характеристиками сетей друг друга;
- 6) предоставление сведений для других функций СПП, например RACF.

Более подробные требования для измерения и управления рабочими характеристиками находятся вне области применения данной Рекомендации и содержатся в других конкретных Рекомендациях.

### **6.9.7 Обработка и управление перегрузкой трафика**

Во избежание обработки и перегрузки трафика и для удержания времени отклика достаточно низким при таких перегрузках, с целью предотвращения отказа пользователей от сделанных ими запросов на обслуживание, в СПП версии 1 должны быть представлены механизмы для обнаружения перегрузок и управления ими, включая такие расширенные элементы управления, как балансировка нагрузки и репликация ресурса как на уровне услуг, так и на транспортном уровне.

СПП должна иметь механизмы управления перегрузкой, которые:

- 1) передают в другие сети данные об условиях перегрузки и степени перегрузки;
- 2) оптимизируют эффективную пропускную способность перегруженного ресурса, например, допустимое количество запросов на услугу/сек или пакетов/сек, с учетом приоритетности услуги;
- 3) обеспечивают наличие такой пропускной способности на протяжении всего события перегрузки, вне зависимости от пропускной способности перегруженного ресурса или количества источников перегрузки;
- 4) позволяют сети, которая получает сообщение о перегрузке, управлять своим трафиком.

### **6.10 Учет и начисление платы**

В сетях СПП поддерживаются возможности по ведению учета и начислению платы с целью предоставления оператору сети данных об учете и начислении платы, связанных с использованием ресурсов сети.

Ниже приведены требования к СПП для ведения учета и начисления платы:

- 1) Функциональные возможности ведения учета и начисления платы должны обеспечивать сбор данных для последующей обработки (начисление оплаты в автономном режиме), а также близкое к реальному времени взаимодействие с такими приложениями, как услуги по внесению предоплаты за обслуживание (начисление оплаты в интерактивном режиме).
- 2) Для управления начислением оплаты, должны быть доступны открытые механизмы.
- 3) Должны выполняться различные правила начисления оплаты, например, начисление оплаты по фиксированной ставке и начисление оплаты за сеансы связи.
- 4) Возможности ведения учета и начисления платы должны поддерживать услуги с функциями многоадресной передачи.
- 5) Сети СПП должны поддерживать все возможные типы соглашений о ведении учета, включая передачу сведений учета/начисления оплаты между поставщиками услуг. Данное требование также включает соглашения об электронной коммерции.

Например, в сценариях услуг доставки контента с функциями многоадресной передачи, услуги могут быть предоставлены в результате совместной деятельности нескольких компаний, например, несколько поставщиков контента и поставщик сетевых услуг. В дополнение к возможностям начисления платы пользователям необходимо иметь возможности начисления платы между компаниями.

ПРИМЕЧАНИЕ. – Использование сведений о начислении платы, собранных СПП для выписки счетов, выходит за рамки данной Рекомендации.

### **6.11 Нумерация, присвоение имен и адресация**

Сеть СПП предназначена для обеспечения эффективной, безопасной и доверенной среды нумерации, присвоения имен и адресации для пользователей, операторов сетей и поставщиков услуг. Там где это необходимо, будут учтены требования по регулированию, а так же взаимодействие с ТфОП/ЦСИС.

Эволюция по направлению к СПП должна гарантировать, что независимость Государств–Членов МСЭ по отношению к плану нумерации, плану присвоения имен и адресации будет полностью сохранена, как описано в [ITU-T E.164] и других относящихся к данной тематике Рекомендациях и Спецификациях других организаций по стандартизации.

Далее приведены требования для поддержки возможностей нумерации, присвоения имен и адресации. Они применяются как на транспортном уровне, так и на уровне обслуживания, если не отмечено иного.

#### **6.11.1 Общие требования для присвоения номеров, имен и адресации**

- 1) Требуется поддерживать как динамический, так и статический режим присвоения адресов.
- 2) Возможности нумерации, присвоения имен и адресации могут быть реализованы с помощью отдельной схемы соответствия для каждой услуги, или через общую для различных услуг схему соответствия.
- 3) Требуется поддерживать динамическое обновление базы данных присвоения имен, например, в случае использования подвижного оконечного устройства, адреса на одном или нескольких уровнях могут динамически изменяться в зависимости от месторасположения оконечного устройства.

#### **6.11.2 Нумерация**

Далее приведены требования для присвоения номеров, применяемые к СПП.

- 1) В механизме адресации должна поддерживаться возможность различать планы набора номера, нумерации и адресации.
- 2) В механизмах адресации должна поддерживаться возможность преобразования последовательности набора номера в нумерацию и схему адресации.
- 3) В СПП должна поддерживаться нумерация E.164 (глобальные номера).
- 4) В СПП должна быть разрешена нумерация, не соответствующая E.164 (локальные номера).
- 5) В СПП должны быть разрешены короткие номера в национальных схемах набора номера.
- 6) Сеть СПП не должна препятствовать существованию систем частной и корпоративной нумерации (см. раздел 6.6).
- 7) При использовании нумерации или последовательностей набора номера, не соответствующих E.164 (локальных номеров), адресация в СПП должна определить область, в пределах которой будет допустимо использование локальных номеров.
- 8) В СПП должна поддерживаться возможность различия алфавитно-цифровых идентификаторов, в которых, случается, что содержатся только цифры, от телефонных номеров, которые должны обрабатываться в процедурах маршрутизации.

#### **6.11.3 Схемы присвоения номеров, имен и адресации**

- 1) На транспортном уровне сети СПП версии 1 должны поддерживать схемы IP адресации, основанные на версии протокола IPv4 или IPv6, или обе версии.

ПРИМЕЧАНИЕ 1. – Следует принимать во внимание, что комбинация IPv4 и IPv6 в пределах одного домена оператора может вызвать проблемы с оказанием услуг.

- 2) Домены сети СПП версии 1 могут поддерживать оборудование пользователя в интерфейсе "пользователь-сеть" при помощи только IPv4, только IPv6, или обеих версий.

ПРИМЕЧАНИЕ 2. – Подразумевается, что протокол IPv6, основанный на оборудовании пользователя, также может поддерживать протокол IPv4 в интерфейсе "пользователь-сеть".

- 3) Сеть СПП версии 1 должна поддерживать установление мультимедийной связи по протоколу IP (как на устройстве происхождения вызова, так и на оконечном), используя как минимум, телефонный унифицированный идентификатор ресурса E.164 (URI телефона), например тел:+4412345678, и унифицированный идентификатор ресурса SIP (SIP URI), например, sip:my.name@company.org, Для телефонных URI:

- должны поддерживаться глобальные номера;
- должен поддерживаться формат локальных номеров.

- 4) В некоторых сценариях услуг, например взаимодействия с ТфОП/ЦСИС, сеть СПП версии 1 должна поддерживать установление мультимедийной связи по IP протоколу (как на устройстве происхождения вызова, так и на оконечном), используя нумерацию E.164 с поддержкой там, где это необходимо, нумерации подобной ENUM.
- 5) Схемы адресации должны поддерживать одноадресные и многоадресные типы услуг.
- 6) Схемы адресации должны поддерживать радиовещательные типы услуг.
- 7) Могут поддерживаться другие схемы присвоения номеров, имен и адресации.

#### **6.11.4 Разрешение имен/номеров/адресов**

В [ITU-T Y.2001] представлены основные принципы и требования для разрешения (идентификации) имен, адресов и присвоения номеров. В соответствии с ними представлены следующие требования.

- 1) масштабируемость: сети СПП должны быть масштабируемыми, для обработки увеличивающихся запросов на разрешение имени/номера/адреса;
- 2) надежность: возможности разрешения имен/номеров/адресов не должны быть затронуты сбоем в каком-либо одном месте, используя, например, механизмы распределенного разрешения;
- 3) безопасность: для возможностей разрешения имен/номеров/адресов должны быть реализованы меры безопасности.

ПРИМЕЧАНИЕ. – Данные возможности могут использовать внутренние или внешние для СПП базы данных, например, базу данных DNS интернета. Примеры мер безопасности включают аутентификацию доступа пользователя, защиту данных, синхронизацию данных и восстановление при сбоях.

#### **6.11.5 Нумерация, присвоение имен и адресация при взаимодействии**

При необходимости, функции взаимодействия выполняют преобразование номеров, имен и адресов в сценариях взаимодействия сетей.

- 1) Сеть СПП должна поддерживать множество сценариев межсетевого взаимодействия адресов на транспортном уровне, без влияния на услугу, предоставляемую пользователям, то есть, сценарии взаимодействия между доменами с различной адресацией, например, доменами, основанными на схемах адресации по протоколу IPv4 или IPv6, и доменами, основанными на общих или частных схемах адресации.
- 2) Там где необходимо, возможности преобразования адреса должны использоваться для поддержки различий в формате адреса, как на транспортном уровне, так и на уровне обслуживания, без какого-либо влияния на услугу, предоставляемую пользователям.

#### **6.12 Идентификация, аутентификация и авторизация**

Требования, представленные в данном пункте не привязаны к какому либо определенному набору услуг или приложений сети СПП.

ПРИМЕЧАНИЕ. – Конкретные механизмы аутентификации и авторизации выходят за рамки данной Рекомендации.

##### **6.12.1 Общие требования**

Существуют требования для возможностей двусторонней идентификации, аутентификации и авторизации, как на транспортном уровне, так и на уровне обслуживания. На транспортном уровне существуют требования по использованию транспортных ресурсов сети СПП. Требования для уровня обслуживания направлены на взаимосвязь между пользователем и услугой или между пользователем и другим пользователем, включая случаи, когда эти два пользователя находятся в разных сетях СПП.

ПРИМЕЧАНИЕ 1. – Иногда фраза "поставщик услуг" используется для ссылки на поставщика услуг транспортного уровня. В данном подпункте, поставщик сетевых услуг обычно сокращается до "СПП", а "поставщик услуг" называется именно так "поставщиком услуг"; поставщик услуг может быть везде, и он не обязательно является поставщиком сетевых услуг.

Далее приведены общие требования для возможностей идентификации, аутентификации и авторизации.

- 1) В СПП должны поддерживаться функции двусторонней аутентификации и авторизации, как на транспортном уровне, так и на уровне обслуживания. Аутентификация на транспортном уровне требует, чтобы пользователь был идентифицирован сетью для получения доступа к сети и привилегированному использованию. Функция аутентификации может быть важным фактором в защите от несанкционированного использования сетей, например, для предотвращения незапрошенной передачи данных. С помощью функции авторизации можно установить доступ к сетевым ресурсам и предотвратить нарушение прав доступа.
- 2) Сеть СПП должна иметь возможность уникально идентифицировать пользователя с помощью одного или двух из следующих типов идентификатора пользователя:
  - открытый идентификатор пользователя; Сведения, которые обычно используются пользователем СПП для соединения или общения с другим пользователем СПП;
  - секретный идентификатор пользователя; Секретный идентификатор пользователя СПП может использоваться для идентификации пользователя СПП в его/ее сети СПП или у поставщика услуг. Секретный идентификатор пользователя является единственным компонентом, используемым для аутентификации.
- 3) В СПП должна поддерживаться раздельная идентификация, аутентификация и авторизация пользователей и окончного оборудования.
- 4) В СПП для некоторых определенных услуг должна поддерживаться проверка взаимосвязи между пользователем и окончным оборудованием пользователя.
- 5) Аутентификация, авторизация и учет, выполняемые поставщиком услуг СПП и поставщиком услуг, должны выполняться в защищенном режиме.
- 6) Поставщик услуг должен предоставить механизмы, которые обеспечивают отображение общего идентификатора инициатора связи там, где это необходимо и где разрешено.
- 7) Поставщиком услуг должны быть представлены механизмы, которые обеспечивают скрытие общего идентификатора инициатора связи, если отображение данных сведений ограничено инициатором связи или сетью.
- 8) Поставщик услуг, выполняющий аутентификацию, должен предоставить механизмы для определения достоверности представленного общего идентификатора пользователя для входящей связи
- 9) Поставщик услуг, выполняющий аутентификацию, должен поддерживать механизмы, обеспечивающие предоставление общего идентификатора пользователя подключенной стороны инициатору сеанса связи, если это необходимо и не наложено ограничений подключенной стороной или сетью.
- 10) В СПП должна поддерживаться возможность проверки секретных идентификаторов пользователей и окончного оборудования (при необходимости). Дополнительно должна поддерживаться возможность проверки аутентификации и авторизации пользователей и окончных устройств для использования ресурсов СПП.
- 11) Поставщик услуг должен иметь возможность проверки секретных идентификаторов тех пользователей, которым предоставляются услуги. Дополнительно поставщик услуг должен поддерживать возможность проверки аутентификации и авторизации пользователей для использования ресурсов, которыми он управляет.
- 12) Соответствующий оператор сети должен управлять секретными и общими идентификаторами (идентификаторы, которые используются для аутентификации и авторизации) пользователей СПП, использующих ресурсы транспортного уровня.
- 13) Соответствующий поставщик услуг должен управлять секретными и общими идентификаторами (идентификаторы, которые используются для аутентификации, авторизации и маршрутизации) пользователей услуг, использующих ресурсы уровня обслуживания, и такое управление должно предотвратить возможность изменения пользователями общих и секретных идентификаторов.
- 14) Секретные идентификаторы пользователя СПП, предоставляемые для аутентификации/авторизации, не должны быть видны другим пользователям.
- 15) Общие идентификаторы пользователя услуг СПП могут быть видны другим пользователям, если в процесс взаимодействия не включены промежуточные услуги и имеется разрешение пользователя.

- 16) Поставщик услуг может разрешить пользователю использовать для доступа к службе один и тот же общий или секретный идентификатор пользователя параллельно с несколькими оконечными устройствами.
- 17) Так как одному пользователю может быть разрешено использовать несколько секретных идентификаторов пользователя, введенных в процессе одной процедуры подписки, сеть СПП должна поддерживать использование множества секретных идентификаторов пользователя в одной процедуре подписки.
- 18) СПП может позволить аутентификацию и авторизацию отдельного пользователя для ее использования в работе с множеством услуг ("однократная регистрация входа").

ПРИМЕЧАНИЕ 2. – Даже в тех случаях, когда требуется выполнение только однократной аутентификации, может оставаться потребность в выполнении многократных авторизаций. Кроме того, выполнение однократного входа может быть реализовано на стороне клиента, чтобы даже если требуется многократное выполнение аутентификации, пользователю необходимо всего лишь один раз установить взаимоотношение аутентификации. Сеть СПП версии 1 не должна поддерживать возможности однократной регистрации. Однако там, где такая поддержка осуществляется существующими технологиями, ожидается, что она также будет использоваться для СПП версии 1.

Аутентификация идентификатора абонента или пользователя не предназначена для указания на положительную проверку субъекта.

### 6.12.2 Требования для идентификации

Сети СПП версии 1 представляют возможности для идентификации пользователей, позволяющие операторам сети и поставщикам услуг идентифицировать пользователей определенных услуг СПП и при необходимости использовать данные сведения, например, для процедур аутентификации и авторизации. Сети СПП версии 1 должны обеспечивать возможности пользователям для идентификации поставщика на каждом уровне, где существует взаимосвязь.

Требования к возможностям идентификации включают:

- 1) Использование нескольких идентификаторов пользователя.  
Так как пользователь СПП может иметь несколько общих и секретных идентификаторов, сеть СПП должна отличать один идентификатор от другого, например, для личного использования и для использования в бизнесе.
- 2) Переносимость идентификатора.  
Сеть СПП должна представлять возможности, эквивалентные переносу номера в средах ТфОП.
- 3) Независимость идентификатора.  
Общий идентификатор пользователя должен быть присвоен пользователю независимо от места хранения, оконечного устройства пользователя и базовых сетевых технологий. Однако обратная совместимость, например, для телефонных трубок ТфОП, может быть достигнута с помощью соответствующих функций взаимодействия.
- 4) Поддержка атрибутов идентификатора.  
Такие атрибуты секретного идентификатора, как время жизни данного идентификатора для пользователя, абонента, используемой сети и т. п., могут быть связаны с идентификатором пользователя.
- 5) Поддержка условий признака.  
Условия для атрибута пользователя, например, установка таймера в качестве условий достоверности, могут быть связаны с идентификатором пользователя у поставщика атрибута, например, сети, пользователя, участником, конечным пользователем.
- 6) Выборочная авторизация признака.  
Сеть СПП должна поддерживать выборочную авторизацию сведений атрибута секретного идентификатора пользователя поставщиком атрибута, например, время жизни идентификатора.
- 7) Поддержка программирования со стороны абонента.  
Сеть СПП должна поддерживать программирование абонентом различных разрешений для различных данных атрибута, например, использование и доступ к сведениям атрибута секретного идентификатора для каждого атрибута.

- 8) Привязка пользователя и оконечного устройства  
В СПП для определенных услуг должна поддерживаться динамическая привязка общего идентификатора пользователя и идентификатора оконечного устройства.
- 9) Взаимосвязь с несколькими оконечными устройствами  
Сеть СПП должна допускать взаимосвязь общего или секретного идентификатора пользователя с несколькими подвижными или фиксированными идентификаторами оконечных устройств, для определенных услуг. Пользователю может быть разрешено использование нескольких оконечных устройств в любое время.
- 10) Передача сведений идентификатора  
Сеть СПП должна поддерживать передачу сведений идентификатора пользователя пользователями СПП, если было получено разрешение от устройства ввода, поддерживающего пользователя, или на своем оконечном устройстве или на принимающем данные оконечном устройстве для определенных услуг, например, оконечных устройств пункта продажи.

### 6.12.3 Требования для аутентификации

Аутентификация является процессом установления доверия к идентификаторам пользователя и оконечного оборудования, а так же к предложениям по присоединению сети и предоставлению услуг. С точки зрения поставщиков, в СПП могут быть отличия между аутентификацией транспортной сети и аутентификацией услуги. С точки зрения абонентов, в СПП могут быть отличия между аутентификацией пользователя и аутентификацией оконечного оборудования. Сетевая аутентификация является процессом проверки идентификаторов пользователя/оконечного оборудования для доступа к сети, который выполняется только поставщиками сетевых услуг. Аутентификация услуги отвечает за проверку идентификаторов пользователя/оконечного оборудования для использования услуги. С точки зрения абонентов, сеть СПП должна предоставлять пользователям возможность аутентификации и идентификации поставщика транспортной сети.

С точки зрения абонентов, сеть СПП должна также предоставлять пользователям возможность аутентификации и идентификации поставщика услуг.

Также сеть СПП должна обеспечивать независимость данных возможностей.

Эти различные концепции аутентификации могут быть объединены в единую концепцию или применяться раздельно, в зависимости от технологии транспортировки или модели бизнеса. Например, если поставщик сети также является поставщиком услуг, то может обрабатываться один поток аутентификации.

Требования к возможностям аутентификации включают:

- 1) В СПП должны поддерживаться различные механизмы сетевой аутентификации в соответствии с базовыми технологиями сети доступа.
- 2) Аутентификация услуги должна быть не зависимой от технологий сетей доступа к СПП и поддерживать совместимый механизм аутентификации службы.
- 3) В СПП должна быть возможность выполнения запроса к пользователю/оконечному оборудованию ввести данные аутентификации, либо в явной или неявной форме.
- 4) В СПП должны поддерживаться как программные, так и аппаратные механизмы аутентификации.
- 5) Должна быть разрешена аутентификация оконечного оборудования, в которой используются данные профиля устройства.
- 6) В СПП должны быть представлены возможности взаимной аутентификации между поставщиком услуг и пользователем.
- 7) В СПП должны быть представлены возможности взаимной аутентификации между поставщиком транспортной сети и пользователем.

#### 6.12.4 Требования для авторизации

Требования к возможностям авторизации включают в себя:

- 1) Доступ к услуге в СПП должен предоставляться аутентифицированным пользователям и/или устройствам, на основе предоставленных им прав доступа, профилей пользователей и сетевой политики
- 2) Авторизация услуги должна по мере возможности быть независимой от технологий сетей доступа к СПП.
- 3) Там, где это применимо, авторизация должна поддерживать сценарии мобильности СПП версии 1.

#### 6.13 Безопасность

В СПП версии 1 должны содержаться функции безопасности, используемые в существующих сетях и позволяющие выполнять защищенное присоединение к другим сетям СПП или не СПП. Эти требования основаны на применении для СПП [ITU-T X.805] и поэтому сводятся к следующим аспектам безопасности СПП: управлению доступом, аутентификации, сохранности данных, конфиденциальности данных, безопасности связи, целостности данных, готовности к работе и защите персональной информации.

Сеть СПП должна обеспечивать:

- 1) защиту от несанкционированного использования сетевых ресурсов и несанкционированного доступа к информационным потокам и приложениям;
- 2) аутентификацию подлинности объектов связи, если это требуется политикой;
- 3) механизмы, обеспечивающие конфиденциальность данных;
- 4) механизмы, обеспечивающие целостность данных;
- 5) средства для ведения отчетности, в соответствии с которыми лицо признается ответственным за любые выполненные им действия;
- 6) готовность к работе и доступность сети при обращении авторизованного объекта;
- 7) механизмы сохранности данных для предотвращения ложного отказа одним из объектов или сторон, участвующих в передаче информации, от принятия полного или частичного участия в процессе передачи информации;
- 8) конфиденциальность данных пользователя, например, настроек, профилей, сведений о присутствии пользователя в сети, данных о доступности и расположении. Эти сведения должны быть защищены так, чтобы информация была доступной, только когда обеспечена правильная авторизация;
- 9) защиту для сведения к минимуму сетевых атак изнутри сети или снаружи;
- 10) защиту от преступлений в сети с помощью разрешения пользователю идентифицировать поставщика транспортной сети и поставщика услуг.

#### 6.14 Управление мобильностью

Управление мобильностью включает возможность перемещения между различными сетями (СПП или не поддерживающими СПП) мобильных объектов таких как пользователи, оконечные устройства и сети. В СПП версии 1 рассматриваются два различных типа мобильности: персональная мобильность и мобильность оконечного устройства [ITU-T Q.1706].

Для СПП версии 1, персональная мобильность имеет место в том случае, если пользователи могут использовать механизмы регистрации для сопоставления самих себя с оконечным устройством, которое может быть сопоставлено сетью с пользователем. Там где имеются интерфейсы между пользователями и оконечными устройствами, и между пользователями и сетями, предполагается, что данные интерфейсы будут использоваться для СПП версии 1.

Для СПП версии 1 мобильность оконечного устройства имеет место в том случае, когда для сопоставления оконечного устройства с сетью используются механизмы регистрации. Там где имеется поддержка оконечного устройства с непрерывностью предоставления услуги, ожидается, что такая поддержка также будет использоваться для СПП версии 1.

Далее представлены общие требования для управления мобильностью, акцентированные на поддержке потребностей пользователя.

Для услуг, которым свойственна мобильность, сеть СПП версии 1 должна обеспечивать:

- 1) кочевничество для персональной мобильности и мобильности оконечного устройства;
- 2) поддержка мобильности для существующих технологий доступа, возможностей QoS и средств защиты;
- 3) поддержка управления местоположением для регистрации, обновления сведений о местоположении и трансляции адреса с целью обеспечения мобильности при пересечении границ сетей поставщиков услуг;
- 4) поддержка управления данными подписки о роуминге и аутентификации;
- 5) обеспечение безопасности для предотвращения несанкционированного доступа и гарантии секретности пользователя, с учетом непрерывности обслуживания и эстафетной передачи абонента, где это применимо;
- 6) обеспечение конфиденциальности данных о местоположении для скрывания этих данных от недоверенных объектов;
- 7) поддержка персонального вызова для установления входящих вызовов с целью сохранения энергии в мобильных оконечных устройствах и уменьшения потоков сигнализации в сети.

## **6.15 ОАМ**

Известно, что возможности ОАМ весьма важны для сетей общего пользования, позволяя упростить эксплуатацию сети, проверку рабочих характеристик сети и уменьшить эксплуатационные расходы за счет сведения к минимуму перерывов в обслуживании, вероятностей ухудшения обслуживания и простоев. Возможности ОАМ особенно важны для сетей, в которых необходима доставка (и, следовательно, измерение) параметров рабочих характеристик сети и работоспособности [ITU-T Y.1710], [ITU-T Y.1730].

В СПП версии 1 должны быть представлены функции ОАМ как для уровня обслуживания, так и для транспортного уровня.

Для того чтобы предложить надежные услуги СПП, которые могут поддерживать требования SLA, услуги СПП должны иметь собственные возможности ОАМ.

ПРИМЕЧАНИЕ. – Возможности ОАМ, приведенные в данном пункте, являются дополнением к возможностям управления, описанным в пункте 6.17.

### **6.15.1 Общие требования ОАМ**

Далее приведены требования ОАМ к сетям СПП.

- 1) Должна поддерживаться возможность выбора поставщиком услуг или поставщиком сетевых услуг нужных функций ОАМ.
- 2) Должна поддерживаться возможность применения функций ОАМ в приложениях связи из-пункта-в-пункт, из-пункта-во-множество-пунктов и из-множества-пунктов-во-множество-пунктов.
- 3) Функции ОАМ должны обеспечивать эффективное масштабирование до больших размеров сети.
- 4) Должна поддерживаться возможность обнаружения ошибок, дефектов и сбоев.
- 5) Должны поддерживаться возможности диагностики, локализации и уведомления объектов управления сетью, а также и выполнение соответствующих действий по исправлению.
- 6) Должна поддерживаться возможность, позволяющая СПП предотвращать запуск пользователем каких либо функций ОАМ, относящихся к службе/поставщику сетевых услуг.
- 7) Должна поддерживаться возможность, позволяющая СПП не допускать обнаружение или локализацию пользователем неисправностей в сети, так как это является частью ответственности поставщика услуг или поставщика сетевых услуг.
- 8) Трафик ОАМ должен передаваться по тому же пути, что и трафик пользователя.

- 9) Следующие ошибки должны обнаруживаться автоматически:
- потеря данных;
  - потеря соединения;
  - ошибочные данные;
  - непреднамеренно самопроизвольно скопированные данные;
  - неправильно введенные данные [ITU-T Y.1730].
- 10) Функциями ОАМ должна поддерживаться обратная совместимость. В СПП должна быть возможность задействовать функции ОАМ незаметно для пользователя, без затрагивания трафика пользователя и без выполнения излишних действий.
- 11) Функции ОАМ должны надежно выполняться даже в условиях плохой передачи данных, например при возникновении ошибок.
- 12) Оценка статуса возможности подключения не должна зависеть от динамического характера трафика пользователя [ITU-T Y.1710], [ITU-T Y.1730].
- 13) Должны поддерживаться взаимоотношения уровня сервер-клиент ОАМ между нижними уровнями и верхними уровнями, например, сигнал сбоя/сигнал ухудшения работы, в случае использования многоуровневой сети.
- 14) В случае использования многоуровневой сети, событие неисправности в заданном сетевом уровне сервера не должно приводить к появлению множества аварийных событий, и необходимо избегать выполнения излишних действий по исправлению в любом более высоком сетевом уровне клиента. На сетевом уровне клиента должна поддерживаться блокировка аварийного предупреждения для уровня сервера, инициирующего дефекты, присутствие которых было передано средствами упреждающего отображения дефекта. На сетевом уровне клиента должна поддерживаться возможность упреждающего отображения дефекта [ITU-T Y.1710], [ITU-T Y.1730].
- 15) В случае использования многоуровневой сети, функции ОАМ в заданном уровне сети не должны зависеть от любых функций ОАМ, определенных более низких или более высоких уровней сети. Для архитектуры является критически важной гарантия того, что уровни сети могут развертываться, добавляться и удаляться без влияния на другие уровни сети.
- 16) В случае использования многоуровневой сети, функции ОАМ в заданном уровне сети должны быть в достаточной степени независимы от любой конкретной плоскости управления таким образом, чтобы изменения в плоскости управления не вносило изменений в плоскость пользователя ОАМ. Для архитектуры является критически важным гарантия того, что плоскость пользователя и плоскость управления работают, не влияя друг на друга.
- 17) Функции ОАМ должны поддерживаться в различных условиях поставщиков услуг/сетей.
- 18) Если услуги СПП предоставляются в различных условиях поставщиков услуг/сетей, то требуется обнаружить и отметить, кто из поставщиков услуг/сетей несет ответственность за дефект, для того чтобы можно было быстро среагировать. Дополнительно поставщик услуги/сети, который предлагает эту услугу клиенту, должен быть поставлен в известность о сбое в обслуживании, даже если этот сбой и место обнаружения расположены в сети другого поставщика услуг/сети.
- 19) У СПП должны быть механизмы, для того чтобы удостовериться в том, что потоки поставщиков услуги/сети ОАМ, которые предназначены для внутреннего использования, находятся внутри их сетей и не существует утечки данных к клиентам или к другим поставщикам услуг/сети.
- 20) Для реализации функций ОАМ в гибридных сетях таким образом, чтобы услуги могли предоставляться по сквозному тракту, состоящему из комбинации сетей СПП и не-СПП, функции ОАМ должны поддерживаться в сценариях взаимодействия (раздел 6.7.3).
- 21) Для того чтобы сделать возможным раздельное управление частью сети, ответственность за которую несет поставщик, а также гибко определять объекты технического обслуживания, должны поддерживаться как функция "сегмент" ОАМ, так и "сквозная" функция ОАМ.

ПРИМЕЧАНИЕ. – Сегмент – это часть сквозного соединения, которая определяется для задач эксплуатации и технического обслуживания.

- 22) Должна поддерживаться регистрация времени простоя услуги для оценки качества и надежности.
- 23) Информация, полученная с помощью функций ОАМ, должна быть организована таким образом, чтобы предоставить надлежащие сигналы индикации техническому персоналу для поддержания качества уровня обслуживания, предложенного клиентам [ITU-T I.610].
- 24) Должны поддерживаться возможности мониторинга качественных показателей.

## **6.16 Живучесть**

Функции живучести необходимы для реализации сетей с высокой надежностью.

### **6.16.1 Требования к защитной коммутации**

В СПП должны поддерживаться возможности защитной коммутации для реализации быстрых и детерминированных функций живучести для всех трактов трафика.

Основными требованиями для защитной коммутации транспорта СПП являются следующие:

- 1) Должны поддерживаться возможности для предотвращения запуска защитной коммутации более низкого уровня из-за дефекта в более высоком уровне.
- 2) Если в защитной коммутации участвует более одного уровня, то более низкие уровни должны иметь приоритет перед более высокими уровнями (это также известно, как стратегия межуровневого распространения).
- 3) Должны предоставляться как защитная коммутация 1+1, так и 1: n.
- 4) Неиспользованные ресурсы защиты транспорта могут использоваться для передачи трафика с наибольшей эффективностью.
- 5) Должно быть минимизировано влияние на производительность сети (например, дополнительная задержка, изменение задержки, ошибки в битах, потери пакетов и т. п.) из-за защитной коммутации.
- 6) Должны поддерживаться функции ручного управления, такие как блокировка защиты, принудительное подключение и подключение команд вручную.

Подробные требования для конкретных технологий предоставлены в разных Рекомендациях, таких как [ITU-T G.808.1].

### **6.16.2 Требования к повторной маршрутизации**

Если случаются серьезные аварии или происходят особые события, то может произойти ухудшение качества или, в самом худшем случае, сбой в сети. В этих случаях требуются такие возможности как повторная маршрутизация, с возможным понижением производительности или качества услуги и механизмы контроля трафика.

ПРИМЕЧАНИЕ. – Эти возможности могут также рассматриваться как часть функций целостности сети.

Основными требованиями для повторной маршрутизации СПП являются следующие.

- 1) Если в повторной маршрутизации участвует более одного уровня, то более низкие уровни должны иметь приоритет перед более высокими уровнями (стратегия межуровневого распространения).
- 2) Механизм повторной маршрутизации должен быть способен найти альтернативный маршрут за приемлемый период времени.
- 3) Влияние на производительность сети (например, дополнительная задержка, изменение задержки, ошибки в битах, потери пакетов и т. п.) из-за защитной коммутации должно быть сведено к минимуму.
- 4) Сеть СПП не должна исключать управление оператором.
- 5) При необходимости должна быть возможна повторная оптимизация сети после восстановления поврежденного трафика.
- 6) При возвращении в исходное состояние после сбоя или условий ухудшенного качества, должна быть восстановлена производительность уровня обслуживания, предшествовавшая сбою или условиям ухудшенного качества.

### 6.16.3 Требования к способности услуги к восстановлению

Условия способности услуги к восстановлению зависят от конкретной услуги, таким образом, они должны быть определены для каждой услуги.

Главными требованиями к способности услуги к восстановлению (SR) являются:

- 1) Сеть СПП должна иметь возможность для независимого присвоения разных уровней SR разным услугам.
- 2) Сеть СПП должна иметь возможность для независимого присвоения разных уровней SR разным услугам в различных потоках.
- 3) В зависимости от присвоенного уровня SR услуги, охваченные SR, должны иметь возможность представлять тот же уровень качества обслуживания, который был до сбоя.
- 4) Оконечное оборудование может по выбору передавать уровни SR сети СПП.
- 5) Сеть СПП должна иметь возможность присвоения и поддержки SR от точки входа до точки выхода в сети поставщика услуги.
- 6) Сеть СПП должна иметь возможность разделения панели пользователя и панели управления в потоках с задействованными SR.
- 7) Сеть СПП должна поддерживать возможность уведомления приложения/пользователя, если требуемый уровень SR не отвечает требованиям сетей СПП.

### 6.17 Управление

Возможности управления СПП поддерживают области управления, которые охватывают планирование, установку, эксплуатацию, администрирование, техническое обслуживание и предоставление сетей и услуг. Целью высокого уровня является предоставление живучих и рентабельных сетей.

Возможностями управления СПП также поддерживаются услуги мониторинга, управления услугами СПП и транспортными компонентами, за счет передачи управляющей информации через интерфейсы между компонентами СПП и системами управления, между вспомогательными системами управления СПП, а также между компонентами СПП и персоналом поставщиков сетей и услуг.

Возможности управления СПП выполняют задачи СПП с помощью:

- 1) предоставления возможности управления на протяжении всего жизненного цикла компонентов СПП, как физических, так и логических. Сюда входят ресурсы на транспортном уровне и на уровне обслуживания, функции доступа к транспортировке, взаимосвязанные компоненты, сети пользователя и окончное оборудование;
- 2) предоставления возможности управления компонентами услуг СПП независимо от транспортных компонентов СПП, и позволяя организациям, предоставляющим услуги СПП создавать для клиентов различные услуги (возможно, из услуг от различных поставщиков);
- 3) предоставления возможностей управления, которые позволяют организациям, предоставляющим услуги СПП, дать своим пользователям возможность персонализации услуг и создания новых услуг из различных возможностей СПП (от различных поставщиков услуг);
- 4) предоставления возможностей управления, которые позволяют организациям, предлагающим услуги СПП, добавить к ним улучшения, включая самообслуживание со стороны пользователя, например, предоставление услуги, сообщения о сбоях, онлайн-отчеты о выставлении счетов);
- 5) разработки архитектуры управления и услуг управления, которые позволят поставщикам услуг уменьшить время, необходимое для разработки, создания и доставки новых услуг;
- 6) поддержки безопасности информации управления, включая информацию о клиенте и информацию пользователя;

- 7) поддержки доступности услуг управления в любом месте, в любое время и для любой зарегистрированной организации или физического лица;
- 8) поддержания сетей электронного бизнеса (eBusiness), основанных на концепции ролей в бизнесе (клиент, поставщик услуг, исполнитель, посредник, поставщик, например, поставщик оборудования) [ITU-T Y.110], [ITU-T M.3050.0];
- 9) разрешения предприятию и/или физическому лицу исполнять множество ролей в разных сетях, а также множество ролей в пределах определенной сети, например, одна роль – это розничный поставщик услуг, а другая роль – это оптовый поставщик услуг [ITU-T M.3050.0];
- 10) поддержания процессов B2B между организациями, предоставляющими услуги и возможности СПП;
- 11) разрешения управления гибридными сетями, состоящими из СПП и не-СПП ресурсов;
- 12) объединения абстрактных точек зрения на ресурсы (сеть, вычисление и приложение), в которых кроются сложность и многообразие технологий и доменов.

Подробные требования к управлению СПП выходят за рамки данной Рекомендации и описаны в конкретных рекомендациях по управлению, таких как [ITU-T M.3060].

ПРИМЕЧАНИЕ. – См. также требования в разделе 6.10 "Учет и начисление платы".

### **6.18 Открытая среда услуг**

Возможности открытой среды услуг проистекают из основных характеристик СПП в части поддержки и формирования среды для создания расширенной, гибкой и открытой услуги и ее предоставления в рамках уровня обслуживания.

Реализация новых функций в существующих сетях может быть ограничена или невозможна из-за возможностей установленного оборудования. Предоставление программного обеспечения для реализации новых функций в оборудовании определенных поставщиков также ограничено, так как интерфейсы программных приложений (API) обычно являются чьей-то собственностью, т. е. не открыты.

Сети СПП требуют применения новых возможностей и поддержки широкого спектра новых услуг, включая услуги с улучшенными и комплексными функциональными возможностями. Благодаря усилиям таких третьих лиц, как поставщики приложений и поставщики услуг, по разработке новых приложений и возможностей, доступных через открытые и стандартные интерфейсы, существует все возрастающая потребность объединения усилий поставщиков сетей и поставщиков услуг для разработки стандартных приложений интерфейсов сети (ANI). Более того, должна поддерживаться возможность многократного использования программного обеспечения и его переносимость, а также использование коммерческого программного обеспечения для содействия экономически эффективному развитию.

Далее перечислены некоторые основные преимущества открытой среды услуг.

- Приложения и возможности могут легко создаваться поставщиками сетей, а также третьими лицами.
- Возможности можно сделать переносимыми и/или многократно используемыми в различных сетях.
- Открытые и стандартные интерфейсы ANI будут обеспечивать возможность взаимодействия между объектами и приложениями СПП, например, для создания услуг.

Внутри открытой среды услуг каждая возможность должна функционировать отдельно или совместно с другими возможностями для реализации приложений. Каждая возможность выполняет для нужного объекта, например, третьего лица, все соответствующие функции услуги. Приложения могут предоставляться в разных сетях, поэтому возможности должны быть способны работать независимо от технологий базовых сетей.

СПП должны удовлетворять следующим основным требованиям открытой среды услуг:

- 1) Независимость от поставщиков сетей. Функциональные возможности, эксплуатация и управление приложениями должны быть независимыми от поставщиков инфраструктуры базовых сетей и технологии сетей;

- 2) Независимость от производителей. Должна поддерживаться открытая среда услуг, предоставляющая пользователям широкий спектр услуг и приложений в конкурентной среде;
- 3) Прозрачность местоположения. В распределенной среде поставщики услуг должны иметь доступ к возможностям отовсюду, независимо от реального физического местоположения таких возможностей;
- 4) Прозрачность сети. Среда открытых услуг должна позволять приложениям и услугам быть независимыми от технологии или окончательного оборудования;
- 5) Прозрачность протокола. Должна быть достигнута прозрачность протокола, с помощью предоставления открытых стандартизованных инструментов для программирования интерфейса протокола с целью реализации независимого процесса управления услугами и сокрытия сложных технических деталей сети от открытой среды услуг.
- 6) Безопасный доступ к возможностям открытой среды услуг должен удовлетворять основным требованиям безопасности СПП, как это определено в пункте 6.13.

В следующих подразделах описаны возможности открытой среды услуг.

### **6.18.1 Координация услуг**

Требования для координации услуг открытой среды услуг включают следующее:

- 1) В СПП должна быть предложена координация приложений и услуг с возможностями.
- 2) Должны отслеживаться возможности или компоненты услуг, полученные от разных поставщиков услуг, а также связи между этими возможностями или компонентами услуг.
- 3) Для приложений и услуг должна быть доступна информация об изменении состояний возможностей или компонентов услуг, например, из-за модернизации.

### **6.18.2 Взаимодействие со средами создания услуг**

- 1) В открытой среде услуг СПП должна быть обеспечена возможность взаимодействия между средами создания услуг и объектами сети с целью создания и предоставления приложений и услуг.
- 2) В сетях СПП версии 1 должны поддерживаться следующие три класса сред создания услуг:
  - открытая среда создания услуг: примерами сред этого класса, использующего ANI, являются OSA/Parlay, Parlay X, OMA;
  - среда создания услуг на основе мультимедиа IP подсистемы (IMS) [ITU-T Q.1741.X];
  - среда создания услуг на основе интеллектуальной сети (IN): Примеры соответствующих протоколов интерфейсов для этого класса среды включают в себя протокол IN приложения (INAP), адаптированное приложение для расширенной логики мобильных сетей (CAMEL) и беспроводную интеллектуальную сеть (WIN).

### **6.18.3 Обнаружение услуги**

Обнаружение услуги часто является первым шагом к определению местоположения возможностей и/или услуг и приложений. Возможность обнаружения услуги существенна для ряда сценариев, таких как сценарии мобильности (для определения местоположения услуг в посещаемой сети) и доступ к услугам, не зависящий от оборудования пользователя.

Например, если такая возможность реализуется в веб-услугах, то для обнаружения услуги и подключения доступа к услугам может использоваться реестр услуг веб-сети общего пользования, например, реестр универсального поиска, описания и интеграции (UDDI).

К обнаружению услуги предъявляются следующие требования.

- 1) Сеть СПП должна поддерживать возможность обнаружения услуги, чтобы позволить пользователям найти интересующие их услуги по всем базовым сетевым технологиям.
- 2) Механизмы обнаружения услуги не должны зависеть от базовых сетевых технологий, чтобы они могли поддерживать разнотипные и изменяющиеся сетевые технологии.
- 3) Возможностью обнаружения услуги должен быть предусмотрен поиск как услуг, интересующих пользователя, так и услуг, интересных для устройств:
  - Услуги, интересующие пользователя, могут использоваться непосредственно пользователем. Примерами услуг, интересующих пользователя, являются справочные услуги, услуги по переводу и совместно используемое оборудование, например, информация IT поддержки.
  - Услуги, представляющие интерес для устройств, могут быть доступны для них напрямую, например, переносная трубка мобильного телефона или портативный ПК. Такие примеры включают принтеры, устройства для архивации, пишущие CD/DVD устройства, серверы аутентификации, IP-серверы распределения адресов. Услуги, представляющие интерес для устройств, и сетевая информация не всегда могут быть использованы напрямую пользователями-людьми.
- 4) Механизмы обнаружения услуги не должны ограничиваться только традиционными технологиями на основе клиент-сервер.

ПРИМЕЧАНИЕ. – Обнаружение услуги может быть реализовано с применением одноранговых технологий или комбинации технологии клиент-сервер и одноранговой технологии.

- 5) Возможность обнаружения услуги должна поддерживать разнообразие критериев обзора данных, например, местоположение и стоимость, для обеспечения надлежащего масштабирования.
- 6) Возможность обнаружения услуги должна поддерживать надлежащие механизмы для обеспечения безопасности и конфиденциальности.
- 7) Возможность обнаружения услуги должна учитывать расширяемость, например, нужно избегать механизмов радиовещательной рассылки.

#### **6.18.4 Регистрация услуги**

Эта возможность позволяет регистрировать другие возможности, услуги и приложения в справочниках открытой среды услуг, которые доступны для возможностей, услуг и приложений. Например, регистрация возможности может быть реализована в услугах веб-сети, когда желательно показать услугу веб-сети: услуги веб-сети могут быть зарегистрированы в "реестре" услуг веб-сети общего пользования. Реестр – это особый справочник, в котором пользователи не только могут найти указание на ресурс, но также могут с его помощью зарегистрировать услуги.

К регистрации услуги предъявляется следующее требование:

- 1) В открытой среде услуг должны предоставляться средства для регистрации возможностей, услуг и приложений. При выборе технологии должны быть гарантированы функции регистрации услуг и отмены регистрации, включая конфигурацию, активацию и публикацию.

#### **6.18.5 Поддержка развития для услуг**

Поддержка развития является ключевым аспектом в цепи доставки услуг как для поставщика услуги, так и для третьих лиц, которые могут расширить набор возможностей и общее предложение услуг. Для развития требуется сбор и публикация данных, доступность средств для ясной формулировки и конкретизации своих потребностей, а также идентификация интерфейсов для развития услуг.

Сеть СПП должна поддерживать развитие для:

- 1) разработки приложений и услуг;
- 2) испытания приложений и услуг, например, отслеживание и отладка;

- 3) ввод в действие приложений и услуг;
- 4) удаление приложений и услуг.

В поддержку развития должно быть включено:

- 1) (программный) компонент, дающий возможность многократного использования и взаимозаменяемости;
- 2) возможность смешивания и подбора компонентов с помощью управления интерфейсами и наличие согласованной семантики для данных/схем, совместно используемых в этих компонентах;
- 3) поддержка полного жизненного цикла компонентов, включая установку, конфигурацию, администрирование, публикацию, контроль версий, техническое обслуживание и удаление;
- 4) поддержка для разработки приложения с агностической доставкой, для того чтобы позволить реализацию приложений без переделки для каждого сценария развития;
- 5) отслеживание взаимозависимостей среди компонентов.

## **6.19 Управление профилем**

### **6.19.1 Профиль пользователя**

Профиль пользователя – это накопленная информация, связанная с пользователем (или абонентом). В среде СПП управление атрибутами профиля пользователя особенно важно, так как для реализации некоторых возможностей, включая аутентификацию, авторизацию, мобильность, определение местоположения, начисление платы и т.п. требуется информация пользователя. В профиль пользователя входит информация, связанная с транспортом, и информация, связанная с услугой. Профиль пользователя может храниться в отдельных базах данных уровня обслуживания и транспортного уровня и может иметь функции обмена между ними.

Основными требованиями к профилю пользователя являются следующие:

- 1) Для каждого пользователя должен существовать свой профиль, необходимый поставщику, который может состоять из нескольких "компонентов".
- 2) Эти компоненты могут быть распределены в домашней сети и в среде поставщика услуг; должны удовлетворяться критерии конфиденциальности и защиты данных.
- 3) Внутри домашней сети эти компоненты могут быть распределены по разным объектам.
- 4) Внутри домашней сети требуется функциональная возможность, позволяющая определить местоположение компонентов профиля пользователя. Данная возможность позволяет службам/приложениям не знать об истинном местоположении компонентов, и необходима для управления домашней сетью.
- 5) Услуги, приложения и другие объекты СПП должны быть способны получать полный профиль пользователя или избранные его части (по требованию) в одной транзакции; должны удовлетворяться критерии конфиденциальности и защиты данных.
- 6) Должны присутствовать эффективные средства поиска компонентов профиля отдельного пользователя с приемлемой задержкой для услуг, работающих в реальном времени.

**ПРИМЕЧАНИЕ.** – Хотя при управлении профилем пользователя не предпринимается попытка классификации данных, которые может содержать этот профиль, но может применяться распределение по категориям, например, основной информации пользователя или конкретной информации об услуге

Ожидается, что подробные требования, связанные с профилем пользователя, его использованием и управлением будут содержаться в следующей(их) Рекомендации(ях) МСЭ-Т.

### **6.19.2 Профиль устройства**

Профиль устройства – это набор накопленной информации, связанной с оборудованием пользователя. В среде СПП управление атрибутами профиля устройства также важно, так как информация об устройстве вместе с информацией о "профиле пользователя" часто требуется для ряда возможностей, включая аутентификацию, авторизацию, мобильность, определение местоположения, начисление платы и т. п. В профили устройств входит информация, связанная с транспортом, и

информация, связанная с услугой. Профили устройств могут храниться в отдельных базах данных уровня обслуживания и транспортного уровня и могут иметь функции обмена данными между ними.

ПРИМЕЧАНИЕ 1. – Данная информация может включать идентификацию окончного оборудования, адрес, имя, статические атрибуты, такие как поддерживаемая среда и протоколы передачи, данные об экране (размер в пикселях, цвета, разрешающая способность, время отклика и т.п.), скорость передачи данных, полоса пропускания, рабочая мощность; динамические атрибуты, такие как пользователь окончного оборудования, географическое положение, приложения, выполняющиеся на этом окончном оборудовании.

Профили устройств могут использоваться в следующих целях:

- чтобы проследить похищенные или незаконно присвоенные устройства;
- для определения типа и уровня обслуживания, которая может быть предоставлена пользователю, на основании возможностей устройства;
- для определения требуемого качества услуги для соединения между окончным оборудованием, на основании возможностей устройства;

К профилям устройств предъявляются следующие требования.

- 1) Для каждого оборудования пользователя может существовать один профиль устройства, который может состоять из нескольких "компонентов".
- 2) Эти компоненты могут быть распределены в домашней сети и/или в среде поставщика услуг стороннего лица.
- 3) Внутри домашней сети эти компоненты могут быть распределены по разным объектам.
- 4) Внутри домашней сети требуется функциональная возможность, позволяющая определить местоположение компонентов профиля пользователя. Данная возможность позволяет службам/приложениям не знать об истинном местоположении компонентов профиля устройства, и необходима для управления домашней сетью.
- 5) При одобрении пользователем, услуги, приложения и другие объекты СПП должны быть способны находить целый профиль пользователя или избранные его части (по требованию) в одной транзакции; должны удовлетворяться критерии конфиденциальности и защиты данных.
- 6) Должны присутствовать эффективные средства поиска компонентов профиля индивидуального устройства с приемлемой задержкой для услуг, работающих в реальном времени.

ПРИМЕЧАНИЕ 2. – Хотя при управлении профилем устройства не предпринимается попытка классификации данных, которые может содержать этот профиль, но может применяться распределение по категориям, например, основной информации устройства или конкретной информации об услуге

- Ожидается, что подробные требования, связанные с профилем пользователя, его использованием и управлением будут содержаться в следующей Рекомендации(ях) МСЭ-Т.

## **6.20 Управление на основе заданных правил**

Управление на основе заданных правил может использоваться в СПП чтобы:

- 1) убедиться в согласованности услуги во всем диапазоне технологий доступа и базовой сети. Оно также может применяться во многих сетях, предоставляющих услуги.

ПРИМЕЧАНИЕ 1. – Такое управление, применяемое в каждой сети, зависит от технологии сети и может конкретизироваться под каждую сетевую технологию;

- 2) обеспечить контроль доступа с учетом использования возможностей и ресурсов сети услугами и приложениями;
- 3) обеспечить регистрацию использования ресурсов сети;

ПРИМЕЧАНИЕ 2. – Это можно рассматривать как функцию, предоставляющую информацию, которая может быть использована другими возможностями сети, такими как учет и назначение цены.

- 4) скрыть услуги и приложения от сложных деталей реализации транспортной сети.

ПРИМЕЧАНИЕ 3. – Управление на основе заданных правил может быть использовано для нужд приложений, пока они остаются независимыми от развернутых сетевых технологий.

Вместе с основными областями применения, указанными выше, и применяемой с возможностью соединения, QoS и безопасностью, может быть предпринято еще много действий в сфере управления, которые принесут пользу службам СПП. Например, управление политикой может быть применено к:

- инициализации услуги;
- конфигурации услуги;
- авторизации, например, названия;
- доставке услуги;
- учету и начислению платы.

Управление на основе заданных правил может вводить правила для предоставления надежных, согласованных, однозначных результатов, называемых стратегическими решениями. Сложность этих правил зависит от их предполагаемого использования.

ПРИМЕЧАНИЕ 4. – Возможности управления QoS, такие как ресурс и контроль доступа (раздел 6.9) могут рассматриваться как часть общего управления набором возможностей на основе заданных правил.

Основными требованиями к управлению СПП версии 1 на основе заданных правил являются:

- 1) Возможности управления на основе заданных правил должны поддерживаться, для того чтобы гарантировать доступ к услуге, ее инициализацию и управление ею.
- 2) Возможности управления на основе заданных правил должны действовать в пределах конкретных услуг и в пределах конкретных доменов поставщиков или во всем множестве доменов поставщиков.
- 3) Возможности управления на основе заданных правил должны отвечать отказом или не отвечать на санкционированных запросы и отвечать на санкционированные запросы.

## **6.21 Подключение услуги**

В категории "подключение услуги" сгруппированы возможности, предоставляющие функциональные возможности для конкретных или улучшенных услуг или приложений, и/или дающих доступ к, и/или обрабатывающие конкретную информацию, предоставленную этими же возможностями.

### **6.21.1 Управление группой**

С помощью этой возможности предоставляются функциональные возможности, связанные с надежным и эффективным управлением группами сетевых объектов (оконечным оборудованием, пользователями, сетевыми узлами и т. п.). Она может использоваться приложениями и другими услугами в разных целях, включая приложения VPN, распределение видеоконтента, управление устройствами, инициализация и управление услугами и сетью, службы чрезвычайных ситуаций (оповещение общественности) и т. п.

Типичный случай, в котором требуется управление группой – это услуга VPN, предоставляемая оператором сети. В случае VPN закрытая группа лиц должна быть определена с помощью списка участников-пользователей услугой, и связь в пределах этой группы должна быть надежно защищена от других пользователей. Сети СПП должны управлять такими группами и обеспечивать надежную связь в группе.

Другим примером является одновременное распределение видеоконтента с помощью многоадресной рассылки от источника к множеству пользователей в группе. Для этого приложения возможность управления группой также важна. Требованиями к управлению группой являются следующие.

- 1) В СПП должна предоставляться возможность, которая активирует создание групп транспортного уровня.
- 2) В СПП должна предоставляться возможность, которая активирует создание группы и/или групп для конкретной услуги (уровень обслуживания).
- 3) Сеть СПП должна управлять группами и предоставлять надежную связь в группе.

### 6.21.2 Управление персональной информацией

Данная возможность обеспечивает управление статической и динамической информацией конкретного приложения, связанного с пользователем и с особенностями соединения. Примерами информации конкретного приложения являются контактная информация пользователя, членство в приложении (пароли и т. п.), загрузочные параметры приложения, полоса пропускания/предпочтения QoS, например, в соответствии с имеющимися сетями доступа, предпочтительные среды передачи, конкретные данные пользователя и т. п. Эта информация, доставленная с помощью приложений, например, услуги по уведомлению и информированию, в соответствии с предварительно определенными предпочтениями пользователя и стратегическими атрибутами, посредством разных мобильных устройств и типов сетей доступа, может накапливаться и управляться пользователем с помощью возможности управления персональной информацией.

Далее следуют требования для возможности управления персональной информацией.

- 1) Может быть предоставлена возможность управления персональной информацией. С помощью возможности управления персональной информацией можно собирать и управлять статической и динамической информацией конкретного приложения от лица пользователей; возможен также поиск этой информации из приложения от лица пользователей.
- 2) Информация, которая управляется возможностью управления персональной информацией, должна быть защищена от несанкционированного доступа/поиска или действий с ней и пр.
- 3) С помощью возможности управления персональной информацией должны поддерживаться разные варианты общения.

### 6.21.3 Обработка сообщений

В современных сетях некоторые услуги поддерживаются в условиях как проводной, так и беспроводной передачи, а другие могут быть найдены только в одной из них. Например, услуга коротких сообщений (SMS) была разработана для беспроводных сетей, хотя сейчас ее можно найти в некоторых выделенных сетях, в то время как мгновенные сообщения (IM) были разработаны для проводных сетей, хотя в некоторых мобильных сетях имеются услуги реализующие IM. Результаты, ожидаемые от разных услуг, также отличаются, в том смысле, что некоторые услуги разработаны для использования в восприятии "реального времени", а другие разработаны, как услуга "почтового ящика", где сообщения накапливаются и готовятся к доставке позднее.

Возможность обработки сообщений обеспечивает функциональные возможности для предоставления услуг, основанных на сообщениях. Такими функциональными возможностями являются управление услугой сообщений в реальном времени и не в реальном времени. Примерами сообщений в реальном времени являются IM и чат, а примерами сообщений не в реальном времени являются электронная почта, SMS и услуга мультимедийных сообщений (MMS).

Далее следуют основные требования.

- 1) Возможность обработки сообщений СПП должна поддерживать услуги сообщений, доступные как в выделенном оконечном оборудовании, так и в мобильном оконечном оборудовании, предназначенные для использования, как в доступе проводного транспорта, так и в доступе беспроводного транспорта.
- 2) Возможность обработки сообщений СПП должна поддерживать услуги сообщений, как в реальном времени, так и не в реальном времени.

ПРИМЕЧАНИЕ. – Возможность управления группой также может быть необходима для поддержки услуги сообщений.

Кроме того, существуют требования пользователей по обработке сообщений, которые задействуют возможности конфигурации услуг сообщений, таких как выбор, фильтрация, форматирование, управление группой и обработка (например, выделение больших объемов предоставленной электросвязи).

### 6.21.4 Поддержка многоадресной передачи

Эти возможности дают приложениям возможность доставки контента множеству пользователей одновременно, используя механизмы многоадресной передачи.

Для эффективного использования ресурса сети в дополнение к одноадресной рассылке, должны поддерживаться механизмы многоадресной передачи.

Для предоставления радиовещательных/многоадресных услуг как на транспортном уровне, так и на уровне обслуживания, должны быть предоставлены соответствующие возможности.

Основные требования включают в себя.

- 1) В СПП должны поддерживаться возможности многоадресной передачи для реализации эффективной и масштабируемой доставки данных.
- 2) В СПП должны предоставляться возможности реализации радиовещательных/многоадресных услуг в одной СПП и в нескольких СПП.

### **6.21.5 Наличие**

С помощью возможности (услуги) наличия предоставляется доступ к информации, имеющейся в наличии, и о ее доступности для пользователей и услуг. Наличие – это набор признаков, характеризующих текущие свойства объекта, например, состояние, местоположение и т. п.

Объектом в данном случае является любое устройство, услуга, приложение и т. п., способное предоставить информацию, имеющуюся в наличии. Доступность, с другой стороны, обозначает способность и намерение объекта передавать сообщения, основываясь на различных свойствах и стратегиях, связанных с этим объектом – например, времени дня, возможности устройства, предпочтения и возможности среды и т. п. Термины наличия и доступности почти всегда используются вместе для предоставления полного набора информации, имеющейся в наличии.

СПП должна поддерживать два типа пользователей: того кто поставляет информацию о наличии (иногда его называют "информатором" [b-121.905]), и того, кто запрашивает информацию о наличии (наблюдатель).

Услуга наличия предоставляется с помощью трех групп возможностей. Требования для каждой группы возможностей описаны ниже.

#### *Сбор информации о наличии*

- 1) СПП должна обеспечивать возможность сбора информации, описывающей состояние соединения с информатором, например, устройств(а), используемых(ого) пользователем.
- 2) СПП должна обеспечивать возможность сбора информации относительно местоположения информатора в соответствии с национальными регламентарными положениями и законами.

#### *Распределение информации о наличии*

- 3) СПП должна обеспечивать возможность объекта, например, пользователя, быть проинформированным о текущем статусе наличия информатора. Другим примером является использование этой возможности для включения другой услуги, чтобы получить доступ к информации пользователей, имеющейся в наличии, при разрешении пользователя.

#### *Управление информацией о наличии*

- 4) СПП должна обеспечивать управление наличием, то есть набор возможностей для управления собранной информацией, имеющейся в наличии.
- 5) Контроль доступа к информации, имеющейся в наличии, с использованием возможности распределения наличия, должен управляться в соответствии с конфиденциальностью информатора и требованиями правил доступа.
- 6) Возможности управления наличием должны включать возможность распределения, для того чтобы предоставлялась только требуемая часть информации, имеющейся в наличии.
- 7) Возможности управления наличием должны включать сбор запросов от определенных объектов для получения информации, имеющейся в наличии, для других объектов. Возможности управления наличием также предоставляют информатору возможность распределять предоставленную им информацию, например, принимать или отвергать запросы наблюдателей на информацию, имеющуюся в наличии.

### 6.21.6 Управление местоположением

Управление местоположением – это вспомогательная возможность для инициализации приложений и услуг, основанных на местоположении, в которых используется информация, касающаяся местоположения пользователей и устройств внутри сетей. Местоположение пользователей и приборов внутри сетей может быть связано с их физическим позиционированием и, следовательно, с расширением приложений с учетом местных условий и их значимостью.

Механизмы определения и сообщения информации о местоположении часто зависят от технологии сети доступа. Это значит, что внутри каждой технологии сети доступа необходима поддержка приложениям и услугам, основанным на местоположении.

Далее приведены требования для управления местоположением.

- 1) В сетях СПП должна предоставляться возможность управления местоположением для определения и сообщения информации, относящейся к местоположению пользователей и устройств внутри СПП в соответствии с национальными правилами и законами.
- 2) В СПП должны предоставляться дополнительные функциональные возможности для подтверждения правильности и аутентичности информации о местоположении, используемой приложениями и услугами, с целью уменьшения любых негативных воздействий, обусловленных искаженной или фальсифицированной информацией о местоположении.
- 3) При инициализации услуг и приложений, основанных на местоположении, нужно учитывать проблемы конфиденциальности.
- 4) Возможность управления местоположением должна предоставлять средство для передачи информации о местоположении, в соответствии с информацией, содержащейся в профилях пользователя/устройства.

### 6.21.7 Активная доставка

Активная доставка – это подключатель услуги, предоставляющий возможность передачи данных от отправителя к получателю, без предварительного запроса со стороны получателя, например, посредством механизма активной доставки на основе SIP.

В то время как у пользователя обычно есть возможность конфигурировать услуги активной доставки из диапазона услуг, предоставленных поставщиками услуг, получателю нет необходимости делать конкретный запрос на отправку требуемых данных. Данные могут отправляться или в результате единичного, связанного с конкретным приложением, инициированного вызова или периодически.

В качестве примера можно привести возможность использования активной доставки для предоставления уведомления о доступности сообщения MMS.

К активной доставке предъявляются следующие требования:

- 1) В СПП должна поддерживаться возможность активной доставки в соответствии с национальными регламентарными положениями и законами.

ПРИМЕЧАНИЕ. – Для инициации услуг активной доставки может потребоваться согласие пользователя.

### 6.21.8 Управление устройствами

Управление устройствами – это подключатель услуги, предоставляющий сетевые возможности для управления устройствами и контроля. Возможности управления устройствами могут использоваться для:

- управление конфигурацией аппаратного/программного обеспечения, например информацией об аппаратном обеспечении устройств, возможностями среды, версией программного обеспечения;
- дистанционная модернизация программного обеспечения как с участием, так и без участия пользователя, например, исправление ошибок, функциональных возможностей, OS, встроенных программ, клиентских приложений;
- дистанционная диагностика сбоев.

Ниже приведены общие требования для управления устройствами:

- 1) В СПП должна поддерживаться модернизация устройств.
- 2) В СПП должна поддерживаться автоконфигурация устройств.
- 3) В СПП должен поддерживаться сбор информации, связанной с устройствами, в соответствии с национальными регламентарными положениями и законами, например, адресов IP и местоположения.

- 4) Управление устройствами может предоставлять функции для регистрации, управления и модернизации информации об устройствах.
- 5) Управление устройствами может предоставлять функции для удаленной проверки состояния устройств, включая состояние изменений и модернизации, и создание отчетов о диагностике.
- 6) Управление устройствами должно быть безопасно и должно выполняться надежным объектом в соответствии с национальными регламентарными положениями и законами.

ПРИМЕЧАНИЕ 1. – Управление устройствами должно позволять установку предпочтений и приложений пользователя.

ПРИМЕЧАНИЕ 2. – Для инициации услуг управления устройствами может потребоваться согласие пользователя.

#### **6.21.9 Обработка сеанса связи**

В СПП должны предоставляться возможности установки, управления и завершения сквозной услуги сеансов связи, которые включают в себя, например, множество участников, группу конечных точек, связанную с этими участниками, и описание мультимедийных связей между этими конечными точками. Такие возможности обработки сеанса связи должны предоставляться как в выделенных, так и в мобильных сетях, для того чтобы учесть требования различных услуг, а также использовать для работы услуг подходящие серверы приложений.

В функции обработки сеанса связи входит следующее:

- создание сеанса связи;
- представление идентичности исходного участника и подключенного к нему участника сеанса связи;
- подавление идентичности исходного участника и подключенного к нему участника сеанса связи;
- доставка и подавление дополнительной информации, предоставленной пользователем, например, изображение, видео или текст во время создания сеанса связи;
- обработка входящего сеанса связи завершающей стороной;
- согласование возможности входящего сеанса связи;
- прием, игнорирование, перенаправление или отбрасывание входящего сеанса связи;
- согласование среды передачи и компонентов среды передачи во время создания сеанса связи;
- обработка текущего сеанса связи;
- модификация среды передачи и компонентов среды передачи в текущем сеансе связи;
- приостановка и возобновление текущего сеанса связи;
- окончание сеанса связи;
- завершение сеанса связи под управлением сети.

Далее приведены общие требования для обработки сеанса связи:

- 1) При обработке сеанса связи должна существовать возможность использования для работы услуги подходящих серверов приложений.
- 2) Сеть СПП должна позволять пользователю создавать один или несколько сеансов связи и активировать сопутствующие мультимедийные приложения внутри каждого сеанса связи.
- 3) В процессе обработки сеанса связи должны поддерживаться сеансы связи с различным типом сред передачи.
- 4) Должен поддерживаться контроль приема сеанса связи, основанный на определенных уровнях QoS, и безопасности.
- 5) Механизмы контроля приема сеанса связи должен охватывать множество типов услуг, например, голосовая, текстовая, видео.
- 6) Если в сеансе связи заняты один или два участника, то сеть должна завершать сеанс в любое время в течение сеанса связи по требованию одного из пользователей сеанса. Сеть может завершить сеанс связи в любое время в течение сеанса связи, например, при сбое.

- 7) Если в сеансе занято более двух участников, то сеть может завершать сеанс в любое время в течение сеанса по требованию любого из пользователей сеанса. Сеть может завершить сеанс в любое время в течение сеанса (например, при сбое).

#### **6.21.10 Поддержка приложений на основе интернет-технологий**

Применение поддержки приложений на основе интернет-технологий дает возможность расширенного использования возможностей устройств и характеристик сетей для приложений на основе интернет-технологий.

Возможности поддержки приложений на основе интернет-технологий предоставляют пользователям согласованную среду сети интернет, которая объединяет множество сетевых сред и множество устройств (PC, портативный компьютер, PDA, сотовый телефон и т. п.).

Поддержка приложений на основе интернет-технологий включает следующие взаимодействия:

- от сервера (приложений) к серверу;
- от сервера к оконечному оборудованию;
- от оконечного оборудования к серверу;
- от оконечного оборудования к оконечному оборудованию (или одноранговое).

Сеть СПП должна поддерживать приложения на основе интернет-технологий, соблюдая следующие требования:

- 1) функциональная совместимость в проводных и беспроводных сетевых средах;
- 2) безопасный доступ к приложениям;
- 3) кочевничество;
- 4) небольшое время запаздывания приложения и эффективное использование пропускной способности.

Сеть СПП должна поддерживать СПП приложения на основе интернет-технологий, соблюдая следующие требования:

- 5) многократное использование существующих технологий и компонентов СПП (например, аутентификации) для инициализации приложений на основе интернет-технологий;
- 6) многократное использование программных средств авторской разработки и объединенных программных средств;
- 7) согласованный опыт пользователя по сетям;
- 8) поддержка методов построения услуг;
- 9) масштабируемость приложений на основе интернет-технологий;
- 10) не снижаемая надежность СПП.

ПРИМЕЧАНИЕ. – СПП версии 1 могут быть ограничены в отношении возможностей поддержки приложений на основе интернет-технологий.

#### **6.21.11 Синхронизация данных**

Синхронизация данных определена как процесс установления эквивалентности двух наборов данных. Подключатель услуги синхронизации данных синхронизирует собранные в сети данные от разного оконечного оборудования, включая портативные компьютеры, мобильные телефоны, портативные и настольные компьютеры. Приложения, в которых может использоваться подключатель услуги синхронизации данных, включают в себя календарь, управление контактной информацией, управление данными предприятия, накопленными в базах данных, и управление документами сети Интернет.

В СПП должен поддерживаться подключатель услуги синхронизации данных со следующими функциональными возможностями:

- 1) синхронизация собранных в сети данных с оконечным оборудованием, поддерживающим эту возможность;
- 2) синхронизация оконечного оборудования с соответствующими собранными в сети данными;
- 3) синхронизация собранных в сети данных среди оконечных устройств.

Если поддерживается подключатель услуги синхронизации данных, применяются следующие требования:

- 1) Подключатель услуги синхронизации данных должен быть независимым от транспортных протоколов.
- 2) Должны поддерживаться случайные данные, собранные в сети.
- 3) При синхронизации следует знать об ограниченности ресурсов оконечного оборудования.

## **6.22 Эмуляция и моделирование ТфОП/ЦСИС**

Эволюция сетей в СПП зависит от выбора операторов и их потребностей. Операторы сетей будут выбирать эволюционный путь в зависимости от их реальных ресурсов, бизнес-планов и стратегий. Таким образом, они могут выбрать разные технологии и временные рамки.

За период передачи данных от ТфОП/ЦСИС к СПП, в СПП должны быть предоставлены следующие возможности:

На время переходного периода от ТфОП к СПП, требуется, чтобы СПП обеспечивала следующие возможности:

- 1) возможности эмуляции ТфОП/ЦСИС;
- 2) возможности моделирования ТфОП/ЦСИС.

Далее приведены требования к данным возможностям.

### **6.22.1 Требования к эмуляции ТфОП/ЦСИС**

#### **6.22.1.1 Основные требования к эмуляции ТфОП/ЦСИС**

Сеть СПП должна предоставлять услуги службы эмуляции ТфОП/ЦСИС, как минимум, одного уровня, представляющие возможности, которые идентичны или лучше предлагаемых сетью с коммутацией каналов.

#### **6.22.1.2 Требования к оконечному оборудованию для эмуляции ТфОП/ЦСИС**

Сеть СПП должна поддерживать действующие терминалы, например, традиционные телефоны ТфОП, текстовые телефоны, устройства факсимильной связи и другие типы существующего оконечного оборудования ТфОП/ЦСИС), которые соединены не с помощью интерфейса UNI СПП, а через ТфОП/ЦСИС, похожие на UNI.

ПРИМЕЧАНИЕ. – Существует вероятность того, что эмуляция всей услуги ТфОП/ЦСИС невозможна, а также поддержка услуги может быть ограничена для некоторых типов оконечного оборудования, то есть действующего оконечного оборудования или оборудования пользователя, которое ведет себя, как действующее оконечное оборудование.

#### **6.22.1.3 Требования услуги для эмуляции ТфОП/ЦСИС**

Требованиями услуги для эмуляции ТфОП/ЦСИС являются:

- 1) СПП должна поддерживать способность для поставщиков услуг эмулировать одну или более из их услуг ТфОП/ЦСИС.
- 2) СПП должна поддерживать описания возможности, унаследованные из действующей спецификации ТфОП/ЦСИС.

ПРИМЕЧАНИЕ – В конкретном применении СПП могут не поддерживаться все возможности и интерфейсы, представленные в ТфОП/ЦСИС.

### **6.22.2 Требования к моделированию ТфОП/ЦСИС**

#### **6.22.2.1 Основные требования для симуляции ТфОП/ЦСИС**

В СПП должны поддерживаться услуги моделирования ТфОП/ЦСИС, создающие у пользователя впечатление, что он работает в ТфОП/ЦСИС.

#### **6.22.2.2 Требования оконечного оборудования для моделирования ТфОП/ЦСИС**

Сеть СПП должна поддерживать нестандартное оконечное оборудование для услуг моделирования ТфОП/ЦСИС. Она также может поддерживать устройства адаптации для обеспечения возможности подсоединения стандартного оконечного оборудования к СПП (например, обычные телефоны, текстовые телефоны и устройства факсимильной связи).

#### **6.22.2.3 Требования услуги для моделирования ТфОП/ЦСИС**

Ниже приведены требования услуги для моделирования ТфОП/ЦСИС:

- 1) В СПП должны поддерживаться возможности аналогичных услуг ТфОП/ЦСИС, использующих управление сеансом связи посредством IP интерфейсов и инфраструктуры.
- 2) СПП должна предоставить поставщику услуг возможность моделировать услуги ТфОП/ЦСИС.

3) СПП не должна предоставлять услуги, идентичные услугам сетей ТфОП/ЦСИС.

ПРИМЕЧАНИЕ. – Предполагается, что в услугах моделирования ТфОП/ЦСИС не применяются модели вызовов или протоколы сигнализации ТфОП/ЦСИС.

### **6.23 Аспекты общественных интересов**

В СПП должны предоставляться возможности для поддержки услуг общественных интересов, востребованных правилами и законами государственных или региональных администраций и международными соглашениями. В эти услуги общественных интересов могут входить, кроме прочих, услуги, описанные в следующих пунктах данного раздела

#### **6.23.1 Законный перехват**

- 1) Поставщик транспорта СПП и/или поставщик услуг СПП должен выполнять требования законного перехвата. Таким образом, в СПП должны быть предоставлены механизмы, которые сделают законный перехват возможным, там где это необходимо согласно правилам или законам страны в их области применения.
- 2) С помощью механизмов законного перехвата должен предоставляться доступ к содержимому передаваемой информации (СС) и сведениям, полученным в результате перехвата (IRI) правоохранительными органами (LEA) по требованиям со стороны администраций или в соответствии с международными соглашениями.

Так как характер законного перехвата зависит от государственных/региональных регламентарных положений и законов, то требования зависят от регуляторной среды каждого государства.

#### **6.23.2 Идентификация злонамеренной связи**

В СПП должна быть включена возможность идентификации источника злонамеренной связи, например, получение идентификаторов оконечного оборудования или данных о местоположении инициатора связи.

#### **6.23.3 Незапрошенный объем трафика**

В СПП должны предоставляться возможности для предотвращения появления незапрошенного объема трафика.

#### **6.23.4 Электросвязь в чрезвычайных ситуациях**

В электросвязь в чрезвычайных ситуациях (включая поддержку и раннее предупреждение) входят:

- связь от отдельного субъекта к органу власти, например, вызов экстренных служб;
- связь между органами власти, например, связь для оказания помощи при бедствии (TDR);
- связь от органа власти к отдельному субъекту, например, услуги массового оповещения.

ПРИМЕЧАНИЕ. – Кроме электросвязи от органа власти к органу власти, TDR и служба электросвязи в чрезвычайных ситуациях (ETS) могут также использоваться для электросвязи от органа власти к отдельному субъекту.

В [ITU-T Y.1271], [ITU-T E.106] и [ITU-T E.107] представлены *"Структура требований к сетям и возможностям электросвязи в чрезвычайных ситуациях в развивающихся сетях с коммутацией каналов и с коммутацией пакетов"*, *"Международная схема предпочтений оказания помощи в чрезвычайных ситуациях (IEPS) для действий по оказанию помощи при бедствиях"* и *"Служба электросвязи в чрезвычайных ситуациях, и структура взаимодействия для государственной реализации ETS"*, соответственно.

В СПП должны быть созданы возможности сети, доступные для приложений раннего предупреждения, например, для предоставления информации о географическом местоположении для доставки предупредительных сообщений только тем, кто возможно будет затронут надвигающимся бедствием.

Для поддержания электросвязи в чрезвычайных ситуациях и раннего предупреждения от СПП требуется надежная работа и высокая готовность.

Сеть СПП необходима для:

- 1) реализации возможностей уровня обслуживания и транспортного уровня, для того чтобы электросвязь в чрезвычайных ситуациях поддерживалась с использованием схем приоритетности/предпочтения. У контроля вызова/сеанса электросвязи в чрезвычайных ситуациях и канала передачи трафика электросвязи в чрезвычайных ситуациях должно быть преимущество в условиях перегрузки/сбоя;
- 2) обеспечения необходимого взаимодействия и отображения механизмов приоритета между разными компонентами СПП, например, между сетью доступа и базовой сетью, и между уровнем обслуживания и транспортным уровнем, и между сетями СПП, например, между двумя базовыми сетями поставщиков услуг, чтобы обеспечить надлежащую сквозную электросвязь, с учетом приоритетности/предпочтения;
- 3) поддержки существующих услуг электросвязи, включая услуги, эквивалентные всем существующим услугам электросвязи ТфОП/ЦСИС, в чрезвычайных ситуациях, даже если один или несколько взаимодействующих объектов присоединены к СПП, а один или несколько объектов присоединены к ТфОП/ЦСИС;
- 4) активирования новых средств электросвязи в чрезвычайных ситуациях, например, услуги мгновенных сообщений, для того чтобы она поддерживалась властями, такими как поставщики услуг в чрезвычайных ситуациях, в будущих применениях;
- 5) обеспечения непрерывного взаимодействия органов электросвязи в чрезвычайных ситуациях по всем общественным сетям внутри административного домена чрезвычайной ситуации;
- 6) обеспечения маршрутизации электросвязи в чрезвычайных ситуациях к соответствующим органам власти;
- 7) обеспечения маршрутизации электросвязи в чрезвычайных ситуациях от органа власти к отдельным субъектам;
- 8) обеспечения, если это возможно, непрерывной электросвязи в чрезвычайных ситуациях между органом власти и отдельными субъектами до тех пор, пока орган власти не завершит сеанс, даже если отдельный субъект уже повесил трубку;
- 9) предоставления органу власти информации о географическом местоположении отдельного субъекта, а так же о его идентификаторе, в соответствии с требованиями государственных или региональных регламентарных положений. Если это требуется в соответствии с регламентарным положением или законом, то эта информация может быть получена органом власти, даже если отдельный субъект просил ее не сообщать;
- 10) предоставления возможности как санкционированного, так и не санкционированного доступа к услугам электросвязи в чрезвычайных ситуациях в соответствии с требованиями государственных или региональных регламентарных положений. Например, СПП должна предоставлять возможность аутентификации доступа пользователя к электросвязи ETS/TDR;
- 11) поддержки снятия с электросвязи в чрезвычайных ситуациях определенных ограничивающих функций управления сетью;
- 12) поддержки электросвязи в чрезвычайных ситуациях в альтернативной или множественной среде передачи, если это требуется, например, в соответствии с регламентарным положением или законом. Видео, текст и голос, и любая другая комбинация из этого набора, как и различные формы сообщений, имеют значение для электросвязи, предоставляемой экстренным службам для людей с ограниченными возможностями;
- 13) предоставления гарантии распространения только санкционированных сообщений раннего предупреждения;
- 14) предоставления возможности предотвращения бесцельных и не являющихся необходимыми сообщений, похожих на сообщения о раннем предупреждении.

#### **6.23.5 Представление идентификации пользователя и конфиденциальность**

- 1) В СПП должна быть возможность для представления идентификации исходного участника.
- 2) В СПП должна быть возможность для представления идентификации завершающего участника.
- 3) В СПП должна быть возможность для подавления представления идентификации исходного участника.

- 4) В СПП должна быть возможность для подавления представления идентификации завершающего участника.

ПРИМЕЧАНИЕ. – Требования для поддержки электросвязи в чрезвычайных ситуациях могут обходить подавление.

#### **6.23.6 Выбор поставщика услуги или сети**

В СПП должна поддерживаться возможность для выбора поставщика, если это необходимо, например, по предписанию или по закону.

#### **6.23.7 Пользователи с ограниченными возможностями**

Основная потребность пользователей с ограниченными возможностями заключается в том, что им требуются средства для контроля и использования оконечного оборудования и услуг альтернативными способами и в альтернативных режимах, подходящих для разных возможностей и предпочтений. Таким требованиям лучше всего отвечает совокупная разработка основного представления оконечного оборудования и услуг.

- 1) В СПП должно быть предоставлено средство, необходимое для вызова услуг ретрансляции. Услуги ретрансляции осуществляют преобразование в разные режимы связи, которые представляют интерес для людей с ограниченными возможностями, например, предпочтение объяснения знаками, чтение по губам, текст, голос. Вызов услуг ретрансляции может основываться на предпочтениях пользователя, на преобразовании адреса или команд пользователя.
- 2) В СПП должна существовать возможность вызова услуг ретрансляции любым участником электросвязи в чрезвычайных ситуациях.

ПРИМЕЧАНИЕ 1. – Другие потребности пользователей с ограниченными возможностями при пользовании услугами электросвязи в чрезвычайных ситуациях рассмотрены в разделе 6.23.4.

ПРИМЕЧАНИЕ 2. – См. также в списке литературы [b-ITU-T TR.TACL] и [b-ITU-T F.790].

#### **6.23.8 Переносимость номера**

Переносимость номера – это возможность сетей ТфОП/ЦСИС.

Эквивалентной возможностью в СПП является идентификация переносимости (пункт 6.12.2). Эмуляция ТфОП/ЦСИС не налагает новых требований для поддержки переносимости номера, потому что эмулированные услуги образованы от ТфОП/ЦСИС (см. раздел 6.22.1.3).

#### **6.23.9 Тарифное разделение услуг**

Во многих государственных сферах применения требуется, чтобы поставщики услуг "разделили тарифы" своих предложений, чтобы дать клиентам возможность выбрать поставщиков разнообразных услуг, а поставщикам – предлагать услуги клиентам на конкурентной основе.

Там где это требуется, например, в соответствии с регламентарным положением или законом, сеть СПП должна поддерживать механизмы реализации тарифного разделения услуг.

#### **6.24 Защита важной инфраструктуры**

Поставщики услуг должны иметь возможность защитить свои инфраструктуры СПП от злонамеренных атак, таких как отказ в обслуживании, перехват, получение доступа обманым путем, тайные действия с сообщениями (модификация, задержка, удаление, вмешательство, воспроизведение, изменение маршрута, неправильный маршрут или неправильный порядок сообщений), отказ от факта получения или отправления сообщения или подлог. В защиту может входить предупреждение, обнаружение и восстановление после атаки, а также меры по предотвращению перерывов в обслуживании.

Требования безопасности предоставлены в пункте 6.13.

### **6.25 Неразглашение информации в интерфейсах NNI**

Если требуется, например, в соответствии с регламентарным положением или законом, государственным или региональным условиям, то в СПП должна быть возможность, позволяющая:

- поставщикам услуг препятствовать раскрытию внутренней информации или информации пользователей услуг другим объектам в интерфейсах NNI;
- поставщикам сетей препятствовать раскрытию информации, содержащейся внутри сети, другим объектам в интерфейсах NNI.

### **6.26 Обмен информацией, связанной с пользователями, между поставщиками**

Если требуется, например, в соответствии с регламентарным положением или законом, то в СПП должны поддерживаться механизмы для обмена информацией, связанной с пользователем, между сетями СПП для совместимости услуг.

## Дополнение I

### Соответствие услуг для подключателей услуг

(Данное приложение не является неотъемлемой части данной Рекомендации)

В данном Дополнении представлен пример соответствия выбранных услуг для выбранных подключателей услуг в обслуживании (раздел 6.21). Данное соответствие не претендует на полноту и не представляет требования, которые необходимо поддерживать.

**Таблица I.1 – Иллюстративное отображение услуг для помощников в обслуживании**

Услуги/ помощники в обслуживании	Наличие	Управление местополо- жением	Управление группой	Обработка сообщений	Поддержка многоадресной передачи	Активная доставка	Обработка сеанса связи
Разговорные голосовые услуги в реальном времени							X
Текст в реальном времени							X
Услуги сообщений	X		X	X			X
Разговор в сетях СПП "нажми и говори"	X		X				X
Мультимедийные интерактивные услуги из пункта в пункт			X				X
Объединенные интерактивные услуги связи		X	X				X
Услуги по доставке контента		X				X	
Услуги на основе "нажми и говори"		X				X	
Услуги широкого вещания/ многоадресные					X		
Основные и транзитные услуги для предприятий			X				X
Информационные услуги	X	X				X	
Присутствие и основные услуги по уведомлению	X	X	X				
Услуги на основе OSA 3GPP версия 6 и 3GPP2 версия A	X	X	X	X	X	X	X
Приложения поиска данных	X					X	
Услуги VPN			X		X		

## Список литературы

В следующих документах содержится информация, которая может представлять ценность для читателей этой Рекомендации. В них представлена дополнительная информация о темах, охваченных данной Рекомендацией, но они не существенны для понимания данной Рекомендации.

### Рекомендации МСЭ

- [b-ITU-R M.1645] Рекомендация МСЭ-R M.1645 (2003 г.), *Структура и общие задачи будущих систем на основе ИМТ-2000 и систем, не входящих в ИМТ-2000.*
- [b-ITU-T E.351] Рекомендация МСЭ-T E.351 (2000 г.), *Маршрутизация мультимедийных соединений в сетях TDM, ATM и сетях на основе IP.*
- [b-ITU-T F.703] Рекомендация МСЭ-T F.703 (2000 г.), *Мультимедийные абонентские службы.*
- [b-ITU-T F.724] Рекомендация МСЭ-T F.724 (2005 г.), *Описание услуг и требования к услугам видеотелефонной связи, предоставляемым по IP-сетям.*
- [b-ITU-T F.733] Рекомендация МСЭ-T F.733 (2005 г.), *Описание услуг и требования к услугам мультимедийных конференций, предоставляемым через IP-сети.*
- [b-ITU-T F.741] Рекомендация МСЭ-T F.741 (2005 г.), *Описание услуг и требования к аудиовизуальным услугам по запросу.*
- [b-ITU-T F.742] Рекомендация МСЭ-T F.742 (2005 г.), *Описание службы и требования к службам дистанционного обучения.*
- [b-ITU-T F.790] Рекомендация МСЭ-T F.790 (2007 г.), *Рекомендации по доступности электросвязи для пожилых людей и людей с ограниченными возможностями.*
- [b-ITU-T G.722.2] Рекомендация МСЭ-T G.722.2 (2003 г.), *Широкополосное кодирование речи со скоростью примерно 16 кбит/с при помощи адаптивного многоскоростного кодера при широкополосной передаче (AMR-WB).*
- [b-ITU-T G.729] Рекомендация МСЭ-T G.729 (2007 г.), *Кодирование речи со скоростью 8 кбит/с при помощи линейного предсказания, возбуждаемого сопряженно-структурным алгебраическим кодом (CS-ACELP).*
- [b-ITU-T G.729A] Рекомендация МСЭ-T G.729, Приложение А (1996 г.), *Кодек речи CS-ACELP пониженной сложности 8 кбит/с.*
- [b-ITU-T G.780] Рекомендация МСЭ-T G.780/Y.1351 (2004 г.), *Термины и определения для сетей синхронной цифровой иерархии (SDH).*
- [b-ITU-T G.799.1] Рекомендация МСЭ-T G.799.1/Y.1451.1 (2004 г.), *Спецификации функциональных средств и интерфейса для оборудования транспортной сети ТфОП для взаимосвязи сети ТфОП и IP-сети.*
- [b-ITU-T G.805] Рекомендация МСЭ-T G.805 (2000 г.), *Общая функциональная архитектура транспортных сетей.*
- [b-ITU-T G.809] Рекомендация МСЭ-T G.809 (2003 г.), *Функциональная архитектура многоуровневых сетей без установления соединения.*
- [b-ITU-T G.1000] Рекомендация МСЭ-T G.1000 (2001 г.), *Качество обслуживания связи: Структура и определения.*
- [b-ITU-T G.1010] Рекомендация МСЭ-T G.1010 (2001 г.), *Категории мультимедийного QoS конечного пользователя.*
- [b-ITU-T H.263] Рекомендация МСЭ-T H.263 (2005 г.), *Кодирование видеосигнала для низкоскоростной связи.*

- [b-ITU-T H.264] Рекомендация МСЭ-Т H.264 (2005 г.), *Улучшенное кодирование видеосигнала для общих аудиовизуальных услуг.*
- [b-ITU-T H.510] Рекомендация МСЭ-Т H.510 (2002 г.), *Мобильность для мультимедийных систем и услуг H.323.*
- [b-ITU-T H-suppl] Приложение 1 к Рекомендациям МСЭ-Т серии H (1999 г.), *Профиль приложения – Язык жестов и общение в реальном времени с чтением по губам при помощи низкоскоростных средств видеосвязи.*
- [b-ITU-T I.230] Рекомендация МСЭ-Т I.230 (1988 г.), *Определение категорий услуг носителя.*
- [b-ITU-T I.250] Рекомендация МСЭ-Т I.250 (1988 г.), *Определение вспомогательных услуг.*
- [b-ITU-T M.3017] Рекомендация МСЭ-Т M.3017 (2003 г.), *Принципы интегрального управления смешанными сетями с коммутацией каналов/пакетов.*
- [b-ITU-T Q.833.1] Рекомендация МСЭ-Т Q.833.1 (2001 г.), *Асимметричная цифровая абонентская линия (ADSL) – Управление сетевыми элементами: модель SMIP.*
- [b-ITU-T Q.1200] Рекомендация серий Q.1200 МСЭ-Т (1997 г.), *Структура общей серии Рекомендаций интеллектуальной сети.*
- [b-ITU-T Q.1236] Рекомендация МСЭ-Т Q.1236 (1999 г.), *Набор 3 возможностей интеллектуальной сети – Требования и методология управления информационной моделью.*
- [b-ITU-T Q.1702] Рекомендация МСЭ-Т Q.1702 (2002 г.), *Долговременный обзор аспектов сети для систем, не входящих в ИМТ-2000.*
- [b-ITU-T Q.1742.4] Рекомендация МСЭ-Т Q.1742.4 (2005 г.), *Эталонные спецификации ИМТ-2000 (утверждены по состоянию на 30 июня 2004 года) для развитой базовой сети ANSI-41 с сетью доступа cdma2000.*
- [b-ITU-T Q.1761] Рекомендация МСЭ-Т Q.1761 (2004 г.), *Принципы и требования для сближения фиксированных и существующих систем ИМТ-2000.*
- [b-ITU-T T.140] Рекомендация МСЭ-Т T.140 (1998 г.), *Протокол для мультимедийного приложения текстового общения.*
- [b-ITU-T Y.1411] Рекомендация МСЭ-Т Y.1411 (2003 г.), *Взаимодействие сети ATM-MPLS – Взаимодействие в плоскости пользователя по методу ячеек.*
- [b-ITU-T Y.2111] Рекомендация МСЭ-Т Y.2111 (2006 г.), *Функции управления ресурсами и установлением соединениями в сетях последующих поколений.*
- [b-ITU-T Y-Sup.1] Приложение 1 к Рекомендациям МСЭ-Т серии Y.2000 МСЭ-Т (2006 г.), *Обзор СИП версии 1.*

## **Руководства МСЭ-Т**

- [b-ITU-T TR.TACL] Технический документ МСЭ-Т: Перечень доступности для использования в работах по стандартизации МСЭ-Т (2006 г.). (доступен по адресу [www.itu.int/ITU-T/studygroups/com16/accessibility/docs/tacl.pdf](http://www.itu.int/ITU-T/studygroups/com16/accessibility/docs/tacl.pdf))

## **Технические определения ETSI**

- [b-101.331] ETSI TS 101 331 V1.2.1 (2006-06), *Требования правоприменяющих органов.*
- [b-102.71] 3GPP TS 22.071 Проект партнерства третьего поколения; Технические определения групп услуг и системных аспектов; *Служба определения местоположения (LCS); Описание службы; Этап 1* (Выпуск 1999 г.).

- [b-121.905] ETSI TR 121 905 V7.3.0 (2007-03), *Словарь определений 3GPP.*
- [b-122.057] ETSI TS 122 057 V6.0.0 (2005-01), *Описание услуги подвижной функциональной среды (MExE); Этап 1.*
- [b-122.127] ETSI TS 122 127 V7.1.0 (2006-03), *Требования услуг открытого доступа к услугам (OSA); Этап 1.*
- [b-122.140] ETSI TS 122 140 V6.7.0 (2005-03), *Услуга мультимедийных сообщений (MMS); Этап 1.*
- [b-122.146] ETSI TS 122 146 V7.2.0 (2006-09), *Услуга а широкополосной/многоадресной передачи мультимедийных сообщений (MBMS); Этап 1.*
- [b-122.174] ETSI TS 122 174 V6.2.0 (2005-01), *Активная доставка; Этап 1.*
- [b-122.240] ETSI TS 122 240 V6.5.0 (2005-01), *Требования услуг для общего профиля пользователя (GUP) 3GPP; Этап 1.*
- [b-122.250] ETSI TS 122 250 V6.0.0 (2005-01), *Управление группой подсистемы передачи мультимедийных данных по IP-сетям (IMS); Этап 1.*
- [b-122.708] ETSI TS 122 078 V7.6.0 (2005-12), *Частные применения для специализированного приложения для усовершенствованной логики подвижной сети (CAMEL); Описание услуги.*
- [b-123.141] ETSI TS 123 141 V7.2.0 (2006-09), *Услуга присутствия; Описание архитектуры и функциональных особенностей; Этап 2.*
- [b-123.228] ETSI TS 123 228 V7.7.0 (2007-03), *Подсистема передачи мультимедийных данных по IP-сетям (IMS); Этап 2.*
- [b-126.235] ETSI TS 126 235 V6.4.0 (2005-03), *Мультимедийные разговорные приложения с коммутацией пакетов; Кодеки по умолчанию.*
- [b-133.106] ETSI TS 133 106 V7.0.1 (2006-01), *Требования узаконенного перехвата.*
- [b-142.033] ETSI TS 142 033 V7.0.0 (2007-06), *Законный перехват – Этап 1.*
- [b-181.005] ETSI TS 181 005 V1.1.1 (2006-03), *Требования услуг и возможностей.*

### **Стандарты Института национальных стандартов США (ANSI)**

- [b-JSTD025] ANSI J-STD-025-A-2003, *Узаконенное электронное наблюдение (CALEA).*
- [b-T1.678] ANSI ATIS 1000678-2006, *Узаконенное электронное наблюдение (LAES) за голосом в пакетных технологиях в проводных сетях электросвязи.*
- [b-T1.724] ANSI T1.724-2004, *Интерфейс эстафетной передачи UMTS для законного перехвата, Март, 2004 г.*
- [b-TIA-1066] TIA-1066 (2006г.), *Узаконенное электронное наблюдение (LAES) для передачи голоса в сети cdma2000 по IP-протоколу (VoIP).*
- [b-TIA-1072] TIA-1072 (2006 г.), *LAES для системы "нажми-и-говори" в сотовой сети cdma2000.*
- [b-TIA-1016-A] *Управляемый источником голосовой широкополосный многоадресный кодек с переменной скоростью (VMR-WB), возможности службы 62 и 63 для систем с расширенным спектром (TIA-1016-A-2006).*
- [b-TIA-127-A] *Расширенная возможность 3 службы кодека речи с переменной скоростью для широкополосных цифровых систем с расширенным спектром (ANSI/TIA-127-A-2004).*

## Определения IETF

- [b-RFC 2486] IETF RFC 2486 (1999 г.), *Идентификатор доступа к сети*.
- [b-RFC 4594] IETF RFC 4594 (2006 г.), *Рекомендации по конфигурации для классов услуг DiffServ*.

## Определения открытого альянса мобильной связи

- [b-OMA-DS] Синхронизация данных OMA V1.2 – **Статус:** Утвержденный помощник – **Дата выпуска:** 2006-07-10.
- [b-OMA-DM] Управление устройствами OMA V1.2 – **Статус:** Утвержденный помощник – **Дата выпуска:** 2007-02-09.
- [b-OMA-OSE] Среда услуг OMA V1.0 – **Статус:** Кандидат – **Дата выпуска:** 2007-03-13.
- [b-OMA-PoS] Сотовая система "нажми-и-говори" OMA V1.0.1 – **Статус:** Утвержденный помощник – **Дата выпуска:** 2006-11-28.
- [b-OMA-PS] Простое присутствие OMA V1.0.1 – **Статус:** Утвержденный помощник – **Дата выпуска:** 2006-11-28.
- [b-OMA-WS] Веб-услуги OMA V1.1 – **Статус:** Утвержденный помощник – **Дата выпуска:** 2006-03-28.
- [b-OMA-XML] Управление документами XML OMA V1.0.1 – **Статус:** Утвержденный помощник – **Дата выпуска:** 2006-11-28.
- [b-OMA-LS] Подвижная услуга определения местоположения OMA V1.1 – **Статус:** Кандидат в помощники – **Дата выпуска:** 2006-10-20.
- [b-OMA-XDM] Управление документами XML OMA V1.0.1 – **Статус:** Утвержденный помощник – **Дата выпуска:** 2006-11-28.
- [b-OMA-Push] Активная услуга OMA V2.1 – **Статус:** Кандидат в помощники – **Дата выпуска:** 2005-11-22.

## Открытый доступ к услугам (OSA)

- b-OSA-Parlay-X] *Открытый доступ к услугам (OSA), Веб-услуги Parlay X, Части 1-14, ETSI ES 202 391-[1-14] V1.1.1 (2006-12).*
- [b-OSA-Parlay-4] *Открытый доступ к услугам (OSA), Прикладной программный интерфейс (API), Части 1-14, ETSI ES 202 915-[1-14] V1.3.1 (2006-12).*
- [b-OSA-Parlay-5] *Открытый доступ к услугам (OSA), Прикладной программный интерфейс (API), Части 1-15, ETSI ES 203 915-[1-15] V1.1.1 (2007-01).*

## Службы ИС

- [b-TIA-771] TIA/EIA/IS 771-1 (1999 г.), *Беспроводная интеллектуальная сеть – Приложение 1 (2001).*
- [b-TIA-873] TIA/EIA 873.002 (2003 г.), *Все мультимедийные домены базовой сети на основе IP-протокола – Подсистема передачи мультимедийных данных по IP-сетям – Этап 2.*

## **Определения UDDI**

[b-UDDI]

Технический комитет по определениям UDDI, *Определения UDDI*, Версия 3.0.2.

## **Определения SOA**

[b-OASIS-SOA]

*OASIS, Эталонная модель для архитектуры, ориентированной на службы 1.0*,  
Определение комитета 1. 2 август 2006 г.





## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование услуг 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 услуг
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	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
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных услуг
Серия T	Оконечное оборудование для телематических услуг
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
<b>Серия Y</b>	<b>Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений</b>
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи