

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

У.1271

(07/2014)

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

Аспекты протокола Интернет – Архитектура, доступ,
возможности сетей и административное управление
ресурсами

**Принципы в отношении требований к сетям
и возможностей сетей для обеспечения
электросвязи в чрезвычайных ситуациях
по сетям связи, находящимся в стадии
перехода от коммутации каналов
к коммутации пакетов**

Рекомендация МСЭ-Т У.1271

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y
**ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ
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
IPTV по СПП	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: функциональная совместимость услуг и сетей в 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
Пакетные сети	Y.2600–Y.2699
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999

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

Рекомендация МСЭ-Т У.1271

Принципы в отношении требований к сетям и возможностей сетей для обеспечения электросвязи в чрезвычайных ситуациях по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов

Резюме

Требуется решение многих задач и рассмотрение множества проблем в ходе определения и создания функциональных возможностей для поддержания электросвязи в чрезвычайных ситуациях по сетям электросвязи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов. Настоящая Рекомендация представляет собой обзор основных требований, возможностей и концепций электросвязи в чрезвычайных ситуациях, которую способны обеспечить развивающиеся сети связи.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный ID*
1.0	МСЭ-Т У.1271	14.10.2004 г.	13-я	11.1002/1000/7047
2.0	МСЭ-Т У.1271	18.07.2014 г.	13-я	11.1002/1000/12177

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: <http://handle.itu.int/>, после которого следует уникальный идентификатор Рекомендации. Например, <http://handle.itu.int/11.1002/1000/11830-en>.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

© ITU 2014

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Определения	2
3.1 Термины, определенные в других документах	2
3.2 Термины, определенные в настоящей Рекомендации	2
4 Сокращения и акронимы	4
5 Безопасность	4
6 Общие соображения.....	4
6.1 Природа чрезвычайных ситуаций	4
6.2 Безотлагательные меры в случае чрезвычайной ситуации	5
6.3 Гарантированная электросвязь	5
7 Требования и возможности по обеспечению электросвязи в чрезвычайных ситуациях	6
7.1 Усовершенствованный приоритетный режим	7
7.2 Защищенные сети	9
7.3 Конфиденциальность местоположения	9
7.4 Восстанавливаемость	10
7.5 Межсетевые соединения	10
7.6 Функциональная совместимость	10
7.7 Мобильность	11
7.8 Повсеместное покрытие	11
7.9 Жизнеспособность/работоспособность	11
7.10 Передача голоса	11
7.11 Передача изображения	11
7.12 Передача данных.....	12
7.13 Масштабируемая полоса пропускания	12
7.14 Преимущественное обслуживание в механизмах управления перегрузками...	13
7.15 Надежность/эксплуатационная готовность.....	14
7.16 Использование облачной инфраструктуры в ETS	14
Приложение А – Возможные различия между обязательными и факультативными требованиями.....	16
Дополнение I – Сведения о возможных источниках чрезвычайных ситуаций	18
Библиография	20

Введение

Задачей электросвязи в чрезвычайных ситуациях является содействие аварийно-спасательным операциям с целью восстановления коммунальных инфраструктур и обеспечения населению нормальных условий жизни после серьезных бедствий. В некоторых странах аварийно-спасательные операции относятся к сфере ведения организаций, обеспечивающих общественную безопасность. Аварийно-спасательные бригады должны оценивать ущерб, координировать спасательные операции и медицинскую помощь, согласовывать усилия по восстановлению и т. д. Для достижения этой цели электросвязь в чрезвычайных ситуациях может быть обеспечена путем совместного использования ресурсов инфраструктуры электросвязи общего пользования, а в некоторых случаях путем использования дополнительных ресурсов корпоративных сетей (например, сети общественной безопасности), которые в настоящий момент находятся в стадии перехода от базовых сетей с коммутацией каналов к сетям с коммутацией пакетов, способным предоставить электросвязь с разнообразными возможностями.

Рекомендация МСЭ-Т Y.1271

Принципы в отношении требований к сетям и возможностей сетей для обеспечения электросвязи в чрезвычайных ситуациях по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов

1 Сфера применения

Для решения особых задач, с которыми сталкивается электросвязь в чрезвычайных ситуациях, необходимы и понимание контекста, и серьезные размышления. Настоящая Рекомендация представляет собой обзор основных требований, характеристик и концепций электросвязи в чрезвычайных ситуациях, которую способны обеспечить развивающиеся сети электросвязи. Настоящая Рекомендация дает операторам сетей электросвязи руководящие указания относительно требований и возможностей сетей по обеспечению электросвязи в чрезвычайных ситуациях и призвана предоставить спасателям (пользователям) информацию, полезную для (получения) запроса этих возможностей.

ПРИМЕЧАНИЕ. – Настоящая Рекомендация определяет требования к сетям, реализация которых должна содействовать поддержке служб электросвязи в чрезвычайных ситуациях и, при необходимости, упростить применение [ITU-T E.106] и [ITU-T E.107].

2 Справочные документы

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все рекомендации и другие источники являются предметом пересмотра; поэтому всем пользователям данной Рекомендации предлагается рассмотреть возможность применения последнего издания рекомендаций и других ссылок, перечисленных ниже. Перечень действующих на настоящий момент рекомендаций МСЭ-Т публикуется регулярно. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус рекомендации.

- [ITU-T E.106] Рекомендация МСЭ-Т E.106 (2003 г.), *Международная схема аварийных приоритетов (IEPS) для операций по ликвидации последствий чрезвычайных ситуаций.*
- [ITU-T E.107] Рекомендация МСЭ-Т E.107 (2007 г.), *Служба электросвязи в чрезвычайных ситуациях (ETS) и основа для взаимодействия реализованных на национальном уровне ETS.*
- [ITU-T J.260] Рекомендация МСЭ-Т J.260 (2005 г.), *Требования к предпочтительному использованию средств электросвязи в сетях IP-Cablecom.*
- [ITU-T J.261] Рекомендация МСЭ-Т J.261 (2009 г.), *Концепция внедрения преимущественной электросвязи в сетях IP-Cablecom и IP-Cablecom2.*
- [ITU-T M.3342] Рекомендация МСЭ-Т M.3342 (2006 г.), *Указания по определению шаблонов представления SLA.*
- [ITU-T X.1303] Recommendation ITU-T X.1303 (2007), *Common Alerting Protocol (CAP 1.1).*
- [ITU-T Y.2001] Рекомендация МСЭ-Т Y.2001 (2004 г.), *Общий обзор СПП.*
- [ITU-T Y.2205] Рекомендация МСЭ-Т Y.2205 (2011 г.), *Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения.*
- [ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements.*
- [ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements.*

- [ITU-T Y.3520] Recommendation ITU-T Y.3520 (2013), *Cloud computing framework for end to end resource management*.
- [ATIS-1000057] ATIS-1000057 (2014), *Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Network (NGN)*.
- [ETSI TS 122 011] ETSI TS 122 011 (2013), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Service accessibility (3GPP TS 22.011 version 11.3.0 Release 11)*.
- [ETSI TS 133 401] ETSI TS 133 401 (2013), *Digital cellular Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 11.7.0 Release 11)*.
- [IETF 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP)*.
- [IETF 5321] IETF RFC 5321 (2008), *Simple Mail Transfer Protocol*.
- [IETF 5670] IETF RFC 5670 (2009), *Metering and Marking Behaviour of PCN-Nodes*.
- [IETF 6679] IETF RFC 6679 (2012), *Explicit Congestion Notification (ECN) for RTP over UDP*.
- [IETF 6710] IETF RFC 6710 (2012), *Simple Mail Transfer Protocol Extension for Message Transfer Priorities*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 служба электросвязи в чрезвычайных ситуациях (emergency telecommunications service, ETS) [ITU-T E.107]: Национальная служба, предоставляющая приоритетную электросвязь для авторизованных пользователей ETS в случае бедствий и чрезвычайных ситуаций.

3.1.2 сети последующих поколений (СПП) (Next Generation Network (NGN)) [ITU-T Y.2001]: Сеть с коммутацией пакетов, которая может предоставлять услуги электросвязи и использовать многочисленные широкополосные технологии транспортировки с включенной функцией QoS и в которой связанные с услугами функции не зависят от лежащих в основе технологий, связанных с транспортировкой. Она обеспечивает беспрепятственный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или выбираемым ими услугам. Она поддерживает универсальную мобильность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 гарантированные возможности (assured capabilities): Возможность обеспечения высокого уровня надежности или достоверности того, что имеющая решающее значение электросвязь доступна и функционирует надежно.

3.2.2 аутентификация (authentication): Действие или метод, применяемый для проверки предъявляемой идентификационной информации.

3.2.3 санкционирование (authorization): Действие по определению конкретных прав, например, доступа к ресурсам электросвязи, которые могут быть предоставлены пользователю, представившему определенный пароль.

3.2.4 санкционированный пользователь средств электросвязи в чрезвычайных ситуациях (authorized emergency telecommunication user): Человек или организация, имеющие право приоритетного использования ресурсов во время национальных и/или международных чрезвычайных ситуаций.

- 3.2.5 сообщение о чрезвычайной ситуации (bottom up emergency declaration):** Заявление отдельных пользователей о наличии определенной или предполагаемой чрезвычайной ситуации. После этого пользователь или пользователи будут пользоваться ресурсами электросвязи в чрезвычайных ситуациях в соответствии с конкретными санкциями или указаниями властей.
- 3.2.6 излишняя сетевая буферизация (buffer-bloat):** Ситуация в сети с коммутацией пакетов, при которой большие буферы в различных сетевых узлах и оконечных системах вызывают чрезмерную задержку и дрожание, а также снижают общее качество работы сети. Эта ситуация может повлиять на то, как быстро сообщается о чрезвычайных ситуациях.
- 3.2.7 ограниченная чрезвычайная ситуация (confined emergency situation):** Чрезвычайная ситуация в пределах некоторой точно определенной относительно небольшой географической зоны (например, местная), не затрагивающая другие зоны.
- 3.2.8 объявленная чрезвычайная ситуация (declared emergency situation):** Чрезвычайная ситуация, публично признанная и официально подтвержденная компетентным(и) органом(ами) соответствующим(его) правительств(а).
- 3.2.9 чрезвычайная ситуация (emergency situation):** Серьезное происшествие, случившееся внезапно и неожиданно. Для восстановления нормального состояния и исключения дальнейшей угрозы для населения или имущества могут потребоваться незамедлительные широкомасштабные действия с привлечением средств электросвязи. В случае обострения такая ситуация может перерасти в кризис и/или бедствие.
- 3.2.10 международная чрезвычайная ситуация (international emergency situation):** Чрезвычайная ситуация, распространяющаяся через государственные границы, затрагивающая несколько стран.
- 3.2.11 метка (label):** Идентификатор, расположенный среди элементов данных или приложенный к ним.
- 3.2.12 чрезвычайная ситуация в масштабе всей страны (nationwide emergency situation):** Чрезвычайная ситуация, которая затрагивает все население, но ограничивается только одной страной.
- 3.2.13 обычная связь для чрезвычайной ситуации (ordinary emergency capability):** Особый тип электросвязи для чрезвычайных ситуаций (например, номера 911, 110 или 112), используемый на национальном уровне населением для передачи сообщений о местных или личных чрезвычайных ситуациях государственным служащим или иным официально назначенным гражданским органам власти.
- 3.2.14 политика (policy):** Правила (или методы) распределения ресурсов сетей электросвязи для передачи трафика различных типов, которые могут быть обозначены различными метками.
- 3.2.15 предпочтение (precedence):** Ситуация, когда существует привилегия по обеспечению возможности, содействию или первоочередному обслуживанию.
- 3.2.16 режим предпочтительного обслуживания (preferential):** Возможность, предоставляющая преимущества по сравнению с обычными возможностями.
- 3.2.17 преимущественное обслуживание в механизмах управления перегрузками (preferential treatment in congestion control mechanisms):** Методики управления ресурсами электросвязи для сведения к минимуму последствий перегрузок в отношении электросвязи в чрезвычайных ситуациях. Управлять перегрузками можно посредством ряда мер, в том числе структуры сети, механизмов сетевых элементов (например, средств управления машинными перегрузками) и эксплуатационных возможностей сети.
- 3.2.18 возможность приоритетного обслуживания (priority treatment capabilities):** Возможности первоочередного доступа к ресурсам сети электросвязи и/или первоочередного их использования.
- 3.2.19 общественная безопасность (public safety):** Общий термин, используемый в некоторых регионах для охвата операций по восстановлению в чрезвычайных ситуациях, наряду с другими службами, такими как пожарные и аварийно-спасательные, скорой и неотложной медицинской помощи, полиции и лицензированные службы охраны и т. п. для благополучия и защиты населения. Основная цель заключается в предотвращении угроз населению, таких как преступления и бедствия, и защите от них населения.
- 3.2.20 объявление чрезвычайной ситуации (top down emergency declaration):** Ситуация, когда ответственный(е) служащий(е), обладающий(е) признанной властью в правительстве или промышленности, объявляют чрезвычайную ситуацию.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CSP	Cloud Service Provider		Поставщик облачных услуг
DSL	Digital Subscriber Line	ЦАЛ	Цифровая абонентская линия
ETS	Emergency Telecommunications Service		Служба электросвязи в чрезвычайных ситуациях
GBR	Guaranteed Bit Rate		Гарантированная скорость передачи данных
IM	Instant Messaging		Мгновенная передача сообщений
IMS	IP Multimedia Subsystem		Мультимедийная подсистема IP
KQI	Key Quality Indicator		Ключевой показатель качества
LTE	Long Term Evolution		Долгосрочное развитие
NGN	Next Generation Network	СПП	Сеть последующего поколения
QoS	Quality of Service		Качество обслуживания
RACH	Random Access Channel		Канал случайного доступа
RAN	Radio Access Network		Сеть радиодоступа
SLA	Service Level Agreement		Соглашение об уровне обслуживания
SLS	Service Level Specification		Спецификация уровня обслуживания
SMS	Short Message Service		Услуга коротких сообщений
SMTP	Simple Mail Transfer Protocol		Простой протокол пересылки электронной почты
SP	Service Provider		Поставщик услуг

5 Безопасность

В соответствии с природой настоящей Рекомендации безопасность здесь рассматривается в общем смысле. Вместе с тем следует обратить особое внимание на разделы 6.3 и 7, в которых некоторые требования могут иметь серьезные последствия для безопасности, такие как: санкционирование (раздел 6.3), целостность сети (раздел 7.2), аспекты секретности отдельных пользователей (раздел 7.3), восстанавливаемость сети (раздел 7.4), функциональная совместимость (раздел 7.6), жизнеспособность/работоспособность (раздел 7.9) и надежность/эксплуатационная готовность (раздел 7.15). Другие Рекомендации МСЭ-Т могут дополнять настоящую Рекомендацию в том, что касается аспектов безопасности.

6 Общие соображения

6.1 Природа чрезвычайных ситуаций

Бедствия часто происходят внезапно и приводят к колоссальным повреждениям, потерям и разрушениям. Бедствия являются результатом действия природных сил или возникают из-за действий или вмешательства человека. Бедствия могут иметь огромную разрушительную силу, могут длиться очень долго и охватывать существенные географические зоны одной или нескольких стран. Другими словами, бедствия различны по силе (энергии), продолжительности (времени) и географическому охвату.

Ежегодно в мире происходят сотни бедствий; от них не застрахована ни одна страна. Ограниченное бедствие может быть достаточно разрушительным и в то же время местным по своей природе. Бедствия могут затрагивать целый регион, например в случаях общенациональной или международной чрезвычайных ситуаций. Каждое бедствие приносит страдания, финансовые потери и имеет социальные последствия. Электросвязь необходима для эффективного проведения аварийно-спасательных работ и спасания жизней, вне зависимости от типа бедствия.

В большинстве стран для прогнозирования бедствий и принятия при них эффективных мер разрабатываются и применяются планы и меры (такие как испытания, учения, тренировочные занятия). Вместе с тем иногда может возникнуть сценарий, известный как "черный лебедь". Неожиданное сочетание аномальных условий может оказаться слишком сложным для традиционных мер прогнозирования бедствия и смягчения его последствий или сделать невозможным их применение.

6.2 Безотлагательные меры в случае чрезвычайной ситуации

Все типы бедствий, будь они стихийными или антропогенными, могут произойти в любом месте и в любое время. Ликвидация последствий бедствий происходит поэтапно. Главной задачей спасателей, первыми появившихся на месте бедствия, является оценка ущерба и предотвращение дальнейших разрушений. Другие этапы быстро сменяют друг друга. На втором этапе приоритетом является лечение раненых и спасание жизней. К работам по третьему этапу часто привлекается дополнительный персонал, занимающийся восстановлением при бедствиях, оборудование и материальные ресурсы, возможно, получаемые с предварительно созданных баз, складов или мест сосредоточения. Четвертый этап – это расчистка и восстановление.

Ключевым средством упрощения операций на всех этапах восстановительных работ при бедствиях является использование быстрой, надежной, удобной электросвязи в чрезвычайных ситуациях, которая может быть организована посредством принятия технических решений и/или реализации административной политики. Следует понимать, что некоторые существующие планы первоначально предусматривали неблагоприятные ситуации, которые оказались более серьезными, чем меры по реагированию на них: так, землетрясение может оказаться сильнее, чем было принято при планировании мер.

6.3 Гарантированная электросвязь

Целью является обеспечение гарантированной электросвязи при чрезвычайных ситуациях. При бедствии может пострадать сама инфраструктура электросвязи. К типичным последствиям относятся: перегрузка и необходимость развернуть заново или расширить охват существующих линий электросвязи, с тем чтобы достичь новых географических зон, не охваченных существующей инфраструктурой. Даже если инфраструктура электросвязи не повреждена бедствием, во время таких событий спрос на услуги электросвязи резко возрастает.

Методы извещения органов власти о чрезвычайной ситуации чрезвычайно разнообразны. Граждане могут оповестить правительство о бедствии, используя обычную связь для чрезвычайных ситуаций. С другой стороны, о бедствии могут сообщить спасатели, прямо или косвенно взаимодействующие с жителями в зоне бедствия. Эта информация может привести к публикации заявления о чрезвычайной ситуации наделенным(и) полномочиями служащим(и) ответственного правительства. Последний случай является объявлением чрезвычайной ситуации.

Назначение участников спасательных операций может быть известно до возникновения реальной чрезвычайной ситуации. В таком случае их полномочия могут быть сохранены, что дает возможность их аутентификации для санкционированной электросвязи. В общем случае, когда предоставляется право на преимущественное или приоритетное использование электросвязи (например, предпочтение перед остальными пользователями), пользователи услуги должны иметь соответствующие разрешения и их личности должны аутентифицироваться. Вопрос о том, требуется ли санкционирование, решается на уровне соответствующей отдельной страны. Однако в отсутствие механизма санкционирования пользователи, не имеющие разрешений, могут злоупотреблять режимом предпочтительного обслуживания. Технические аспекты безопасности обсуждаются в разделе 11 Рекомендации МСЭ-Т [ITU-T Y.2205].

Реакция сети с коммутацией каналов и некоторых сетей с коммутацией пакетов (сети последующих поколений – СПП) на перегрузку выражается в отказе в предоставлении связи, если ресурсы исчерпаны. Некоторые сети могут обеспечивать режим предпочтительного обслуживания для запроса на вызов. Одним из вариантов, когда имеющие разрешение участники спасательных операций нуждаются в связи, является предоставление им права на получение связи до других инициаторов вызовов. Однако в некоторых типах сетей с коммутацией пакетов дополнительная нагрузка приводит к ухудшению показателей трафика индивидуальных пользователей во всей сети. Это происходит, когда сеть работает в режиме "максимальных усилий", при котором вся информация обрабатывается одинаково и просто выстраивается в очередь или сбрасывается, до тех пор пока не появятся доступные ресурсы сети.

Проведенные в последнее время исследования и измерения показывают, что явление, известное как "излишняя сетевая буферизация", может приводить к неприемлемым задержкам. Сокращение стоимости памяти привело к тому, что сетевые ресурсы (включая оборудование конечных пользователей в широкополосной сети) снабжаются большими буферами. Наличие таких буферов приводит к задержке своевременных уведомлений о перегрузке, что рассчитано на сведение к минимуму последствий перегрузки. Наличие этих больших буферов может иметь последствия не только для трафика в режиме "максимальных усилий", но и для приоритетного трафика, такого как электросвязь при чрезвычайных ситуациях.

Важным шагом к обеспечению гарантированных возможностей является предоставление режима предпочтительного обслуживания для электросвязи в чрезвычайных ситуациях и создание отказоустойчивых сетей, которые не входят в состояние отказа из-за неисправности одного из компонентов. Хотя отказоустойчивые сети – важный шаг на пути к обеспечению гарантированной связи, операторы сетей должны также иметь планы восстановления для ремонта сетей в случае неисправности.

7 Требования и возможности по обеспечению электросвязи в чрезвычайных ситуациях

Полномасштабная электросвязь в чрезвычайных ситуациях должна обеспечивать выполнение разнообразных эксплуатационных требований к средствам аварийно-спасательных работ. В таблице 1, ниже, перечислены конкретные задачи и требования, которые способны упростить обеспечение электросвязи для работ по ликвидации последствий чрезвычайных ситуаций. Воплощение этих требований в эксплуатационные возможности существенно упрощает эффективное и своевременное выполнение восстановительных операций при чрезвычайных ситуациях.

ПРИМЕЧАНИЕ. – В тех случаях, когда реализованы средства связи, соответствующие этим требованиям, они могут использоваться также для обеспечения обычной связи в чрезвычайных ситуациях, такой как традиционные службы 110, 112, 911 и т. п. Запросы по выполнению соответствующих требований и условия их выполнения должны решаться соответствующей страной на национальном уровне.

В таблице 1 перечислены задачи и функциональные требования.

**Таблица 1 – Электросвязь в чрезвычайных ситуациях
функциональные требования и возможности**

Усовершенствованный приоритетный режим
Защищенные сети
Конфиденциальность местоположения
Восстанавливаемость
Межсетевые соединения
Функциональная совместимость
Мобильность
Повсеместное покрытие
Жизнеспособность/работоспособность
Передача голоса
Передача изображения
Передача данных
Масштабируемая полоса пропускания
Надежность/эксплуатационная готовность
Преимущественное обслуживание в механизмах управления перегрузками

7.1 Усовершенствованный приоритетный режим

Для передачи трафика электросвязи в чрезвычайных ситуациях требуются гарантированные возможности вне зависимости от сетей, по которым он передается. Главным компонентом гарантированных возможностей является усовершенствованный приоритетный режим. Один из методов обеспечения приоритетности заключается в том, чтобы, во-первых, "идентифицировать" (например, классифицировать и/или обозначить меткой) трафик электросвязи в чрезвычайных ситуациях и затем применить к этому трафику сетевую политику с целью достичь желаемого гарантированного обслуживания. В сетях, ориентированных на установление соединений, когда соединение установлено, вызов становится "четко привязанным", при этом требуемое качество гарантируется и сохранения предпочтительного статуса не требуется. В то же время в сетях с коммутацией пакетов, т. е. в сетях без установления соединений, может потребоваться передавать в каждом пакете метку электросвязи в чрезвычайных ситуациях. Операторы сетей связи и поставщики услуг должны иметь возможность идентифицировать электросвязь в чрезвычайных ситуациях и придавать ей приоритетный статус в соответствии со своими SLA с пользователями.

Новые или временные (при операциях в чрезвычайных ситуациях) пользователи требуют от оператора сети предоставить линию доступа¹. Желательно, чтобы она предоставлялась на предпочтительной основе, для того чтобы иметь возможность оперативно использовать электросвязь в чрезвычайных ситуациях.

7.1.1 Предпочтительный доступ к средствам электросвязи

Существует множество способов доступа к ресурсам электросвязи для использования возможностей электросвязи в чрезвычайных ситуациях. Среди них аналоговая абонентская линия, беспроводная, спутниковая, кабельная, цифровая абонентская линия (ЦАЛ) и волоконно-оптическая линия. Для участника аварийно-спасательных работ существенным преимуществом была бы возможность доступа к услугам этих различных сетей электросвязи на приоритетной или предпочтительной основе. Это позволит значительно оперативнее наладить электросвязь в чрезвычайных ситуациях.

Традиционная сеть с коммутацией каналов, как правило, не предусматривает обозначения приоритетности запросов о доступе. Однако режим предпочтительного доступа может быть обеспечен при помощи особо отмеченных линий, или специально предусмотренных услуг "при снятии телефонной трубки", но такая возможность может быть реализована только для конкретной линии или географического положения, а не по запросу на электросвязь в чрезвычайной ситуации. В настоящее время нет возможности обеспечения приоритетного тонального сигнала или инициации услуги при доступе с обычного телефона. Тональный сигнал приходит в режиме запроса с ограниченного числа портов, и в условиях напряженного трафика, если спрос поглотил предлагаемые порты, доступ может быть осуществлен с задержкой. Следовательно, обеспечение предпочтительного доступа к услугам в развивающихся сетях – это требование, которое требует тщательного рассмотрения.

7.1.2 Предпочтительное установление соединения, использование остающихся эксплуатационных ресурсов и завершение трафика в чрезвычайных ситуациях

Трафик в чрезвычайных ситуациях необходимо идентифицировать, с тем чтобы отличить его от обычного трафика. В традиционных сетях с коммутацией каналов различить два типа трафика позволяет только протокол сигнализации. Однако в сетях с коммутацией пакетов идентификация при помощи меток, размещенных в элементах сигнализации или элементах данных, может упростить различение типов трафика. В сетях с коммутацией пакетов метки могут располагаться на различных уровнях и подуровнях.

После того как трафик электросвязи в чрезвычайных ситуациях идентифицирован, для его приоритетного прохождения должны применяться правила или методы политики сети электросвязи. В транспорте, ориентированном на установление соединений, такая политика потенциально предусматривает более высокую вероятность принятия вызова. В транспорте, не ориентированном на установление соединений, такая политика должна обеспечить более высокую вероятность успешной маршрутизации и доставки, чем при обычном трафике.

¹ Если термин "линия доступа" используется в таком контексте, она означает проводной или беспроводной доступ, канал, виртуальное соединение, туннель и т. д.

7.1.2.1 Завершение трафика при чрезвычайной ситуации в условиях перегрузки

При перегрузке сети на трафик электросвязи в чрезвычайной ситуации должно оказываться минимальное воздействие. В традиционных сетях с коммутацией каналов для уменьшения перегрузки применяются методы управления трафиком, такие как блокирование вызовов. Трафик электросвязи в чрезвычайной ситуации выделяется сведением блокирования к минимуму и обеспечением высокой степенью вероятности завершения по сравнению с обычным трафиком.

В СПП с коммутацией пакетов для предотвращения блокировки и обеспечения более высокой вероятности завершения трафика электросвязи в чрезвычайных ситуациях, чем обычного трафика, используются сигнализация приоритета, приоритетный транспорт сигнализации и носителей и различные механизмы предпочтительного обслуживания (в том числе механизмы управления перегрузками).

7.1.2.2 Освобождение от средств сетевого управления

На основании региональных/национальных требований и политики оператора сети электросвязь в чрезвычайных ситуациях следует освободить от средств контроля за сетевым управлением вплоть до той степени, в которой дальнейшее освобождение приведет к нестабильности сети. Средства управления перегрузками (например, средства управления машинными перегрузками), средства управления чрезмерной загруженностью и балансирование нагрузки не должны отрицательно сказываться на электросвязи в чрезвычайных ситуациях.

7.1.3 Предпочтительная маршрутизация трафика электросвязи в чрезвычайных ситуациях

В некоторых ситуациях трафик электросвязи в чрезвычайных ситуациях может направляться по альтернативным маршрутам, если маршрут по умолчанию использовать невозможно или он перегружен. В развивающихся сетях желательно, чтобы трафик электросвязи в чрезвычайных ситуациях не проходил через единые точки отказа и, следовательно, чтобы существовало несколько запасных маршрутов или альтернативные маршруты, которые можно было бы использовать во время перегрузки или неисправности сети. В сетях с коммутацией пакетов маршрутизация пакетов – это непрерывный процесс для данной реализации электросвязи, выполняемый до тех пор, пока сеанс не будет завершен. Вследствие этого средства контроля трафика и сетевого управления должны быть непрерывными, чтобы избежать последствий перегрузки соединений и систем. В дополнение к этому эффект перегрузок больших буферов может смещаться по различным элементам сети по мере колебания реально имеющейся ширины полосы. Таким образом, для управления буферами и избежания высокой степени задержки экстренного трафика требуются постоянные контроль и средства управления.

Кроме того, в последние годы появились несколько новых методов избежания перегрузок (в отличие от управления перегрузками), которые могут применяться для поддержки пользователей электросвязи в чрезвычайных ситуациях [IETF RFC 4412], [b-IETF RFC 5559], [IETF RFC 5670] и [IETF RFC 6679].

7.1.4 Факультативное прерывание трафика не относящейся к чрезвычайным ситуациям электросвязи

Хотя обычно концепция прерывания относится к связи с коммутацией каналов, определено и ее применение в некоторых сетях с коммутацией пакетов (СПП). Прерывание трафика не относящейся к чрезвычайным ситуациям электросвязи для высвобождения пропускной способности и ресурсов для электросвязи в чрезвычайных ситуациях является факультативным требованием; базовые положения об электросвязи в чрезвычайных ситуациях не предусматривают концепцию прерывания. Вместе с тем использование меток для придания приоритета электросвязи в чрезвычайных ситуациях является одним из подходов к определению и предоставлению ресурсов для трафика, относящегося к чрезвычайным ситуациям, за счет обычного трафика.

7.1.5 Допустимое ухудшение качества обслуживания по трафику при недоступности ресурсов инфраструктуры

QoS для различных режимов обслуживания при электросвязи в чрезвычайных ситуациях, как правило, определяется как наилучшее из возможного для обеспечения разборчивой беспомеховой электросвязи и передачи важной информации. Однако, когда ресурсы электросвязи работают в стрессовой ситуации, допустимое ухудшение QoS может быть приемлемо. Это может происходить, только если ресурсы

становятся недоступными до такой степени, что сеть не в состоянии поддерживать передачу обычного трафика, и отсутствуют достаточная пропускная способность и ресурсы для поддержания уровня QoS, обычно приемлемого для передачи трафика, относящегося к чрезвычайным ситуациям. Для операций в чрезвычайных ситуациях необходимо продолжать передачу критически важной информации, пусть даже и с ограничениями, чтобы не потерять способность осуществлять связь вообще.

В тех случаях, когда это оправдано, во время официально объявленных чрезвычайных ситуаций, когда ресурсы инфраструктуры электросвязи практически исчерпаны, может потребоваться обеспечить приоритет электросвязи в чрезвычайных ситуациях перед обычной электросвязью. Это может повлиять на QoS установленной электросвязи. В результате осуществляемая обычная электросвязь может ухудшиться или прерваться.

7.2 Защищенные сети

Обеспечение безопасности необходимо для предотвращения возможности использования несанкционированными пользователями дефицитных ресурсов электросвязи, требуемых для поддержки операций при чрезвычайных ситуациях.

7.2.1 Ускоренная аутентификация санкционированных пользователей электросвязи в чрезвычайных ситуациях

Электросвязь в чрезвычайных ситуациях предназначена только для санкционированных пользователей, участвующих в аварийно-спасательных операциях. Этих пользователей определяет соответствующий компетентный орган в каждой стране или местном сообществе. По запросу на предоставление средств электросвязи в чрезвычайных ситуациях для развивающихся сетей желательно потребовать внедрения инновационного метода поточной ускоренной аутентификации пользователей в этих развивающихся сетях электросвязи, включая сети подвижной связи, который проверяет идентификационную информацию пользователя для защиты ресурсов электросвязи от чрезмерного использования и злоупотребления во время чрезвычайных ситуаций. После того как аутентификация подтверждена и в сети передается трафик электросвязи в чрезвычайных ситуациях, такая аутентификационная информация может быть ассоциирована с метками, которые затем должны передаваться в течение всего времени от инициации вызова до его завершения. Может оказаться необходимым продолжать передачу этой метки на протяжении всего экстренного вызова.

7.2.2 Обеспечение безопасности трафика электросвязи в чрезвычайных ситуациях

В дополнение к аутентификации и санкционированию для электросвязи в чрезвычайных ситуациях требуются иные аспекты безопасности, например меры против спуфинга, проникновения и отказа в обслуживании. Желательно гарантировать обнаружение несанкционированного изменения объектов. При этом обычная электросвязь также будет пользоваться преимуществами повышенной защиты от проникновения и отказа в обслуживании. Сети должны иметь защиту от повреждения (мошеннического) повреждения трафика и средств управления, а также от несанкционированного доступа к ним, включая расширенные методы кодирования и аутентификации пользователя.

7.3 Конфиденциальность местоположения

Для некоторых типов электросвязи в чрезвычайных ситуациях могут применяться специальные дополнительные меры безопасности. Например, один из возможных сценариев разрушения предусматривает попытку помешать работам по ликвидации последствий чрезвычайных ситуаций. При таком сценарии необходимо обеспечить защиту электросвязи определенных пользователей в чрезвычайных ситуациях, в силу срочности и важности этой связи, от манипулирования, перехвата или помех со стороны других пользователей. Для предотвращения раскрытия местоположения определенных санкционированных пользователей электросвязи в чрезвычайных ситуациях несанкционированными сторонами должны применяться специальные механизмы защиты данных о том, где располагаются санкционированные пользователи. Такие особые требования безопасности не входят в сферу охвата настоящей Рекомендации.

Ограниченному количеству пользователей электросвязи в чрезвычайных ситуациях из числа руководителей высшего звена может потребоваться организовывать работы по оказанию помощи без риска раскрытия сведений об их нахождении.

7.4 Восстанавливаемость

Если ресурсы сети, являющиеся ключевыми для операций при чрезвычайных ситуациях, выходят из строя, их необходимо своевременно восстановить. Для сетей как с коммутацией каналов, так и с коммутацией пакетов, как правило, требуются физические линии доступа – проводные или беспроводные, до мест нахождения клиентов. Когда линии доступа повреждены, операторы сетей восстанавливают работоспособность сети, но время отсутствия доступа может оказаться продолжительным. Следовательно, восстановление должно осуществляться на предпочтительной основе, чтобы сделать возможным оперативное начало функционирования электросвязи в чрезвычайных ситуациях для пользователей с предпочтительным доступом.

В случае повреждения функции сети электросвязи должно быть возможным вновь предоставить, отремонтировать или восстановить до требуемых уровней на приоритетной основе.

7.5 Межсетевые соединения

Желательно, чтобы сети, обеспечивающие электросвязь в чрезвычайных ситуациях, были соединены с другими сетями, позволяя таким образом получить широкий охват. Обеспечение предпочтительных соединений в контрольных точках, которые считаются образующими международные и/или регуляторные границы между национальными сетями, обеспечивающими электросвязь в чрезвычайных ситуациях, может создать международную систему связи в чрезвычайных ситуациях, например в ситуациях, когда применимы [ITU-T E.106] и/или [ITU-T E.107].

ПРИМЕЧАНИЕ. – Чрезвычайные ситуации часто бывают региональными, но могут затрагивать несколько стран. В таких случаях для работ по ликвидации последствий данного бедствия могут потребоваться усилия нескольких стран для организации электросвязи в чрезвычайных ситуациях. Кроме того, в "мире, становящемся все более сетевым", многие страны часто оказывают поддержку работам по ликвидации последствий бедствия, не выходящего за пределы одной страны.

В определенных либерализованных и конкурентных системах может существовать:

- a) несколько операторов сетей в одной стране;
- b) операторы сетей, чьи сети охватывают сразу несколько стран.

В таких случаях необходимо рассмотреть возможность соединения сетей, обеспечивающих электросвязь в чрезвычайных ситуациях, с сетями других операторов и/или через контрольные точки на международных и/или регуляторных границах сетей.

7.6 Функциональная совместимость

Развивающиеся сети создадут ряд проблем, одной из которых является необходимость упорядоченного и прозрачного продолжения базовых [ITU-T E.106] функций предоставления электросвязи в чрезвычайных ситуациях режима предпочтительности. В периода конвергенции следует рассмотреть различные схемы взаимодействия технологий с коммутацией каналов и с коммутацией пакетов. Например, голосовые вызовы из телефонной сети или сети подвижной связи могут передаваться через сети с коммутацией пакетов, а затем завершаться либо в сети с коммутацией каналов, либо непосредственно в сети с коммутацией пакетов. Требования по взаимодействию для методов предпочтительного обслуживания в разнородных сетях рассматриваются для КТСОП и сетей IP-Cablecom в разделе 6 [ITU-T J.261] и в разделе 6.2 [ITU-T J.260]. Эти требования могут применяться и к другим разнородным сетям.

Существенной причиной проблем функциональной совместимости часто бывают вопросы конфигурации. Для обеспечения возможности функциональной совместимости между различными операторами, предлагающими услуги электросвязи в чрезвычайных ситуациях, наиболее удобной была бы общая конфигурация. Следует отметить, что это не означает, что все операторы должны одинаковым образом конфигурировать свои внутренние сети, если они должны поддерживать возможности электросвязи в чрезвычайных ситуациях. Это лишь означает, что они обеспечат требуемую конфигурацию в соответствующих местах входа/выхода. Этот метод также в большей степени способствует повсеместной связи, поскольку можно начать предоставлять любые услуги электросвязи в чрезвычайных ситуациях с любым имеющим на это контракт поставщиком услуг без изменения конфигурации.

Целью этого требования является обеспечение присоединения и функциональной совместимости всех сетей (развивающихся и существующих).

7.7 Мобильность

Мобильность требует, чтобы в инфраструктуру связи были включены передвижные, быстро развертываемые и полностью подвижные средства. Для того чтобы обеспечить возможность передвижения, общая конфигурация предусматривает ключевые элементы, предназначенные специально для упрощения реализации приложений для чрезвычайных ситуаций. Инфраструктура электросвязи должна поддерживать подвижность пользователя и терминала, включая электросвязь быстрого развертывания и полностью подвижную электросвязь. Поскольку большинство беспроводных терминалов поддерживают технологии как WiFi, так и сотовой связи, возрастает значение выгрузки данных для возможного увеличения голосового трафика в сетях подвижной связи. В чрезвычайных ситуациях трафик может быть передачей голоса или данных, и эти возможности выгрузки должны обеспечить предпочтительное обслуживание для трафика передачи как голоса, так и данных.

7.8 Повсеместное покрытие

Повсеместная доступность ресурсов электросвязи, которые обеспечивают поддержку услуг для населения, может послужить базисом для легко доступных средств электросвязи в чрезвычайных ситуациях. Благодаря тому, что такие возможности имеются, операции в чрезвычайных ситуациях не будут задержаны до развертывания специальных средств связи. Однако в тех ситуациях, когда существующие сети не соответствуют (или могут не соответствовать) требованиям/возможностям электросвязи в чрезвычайных ситуациях, пользователи электросвязи в чрезвычайных ситуациях будут по умолчанию использовать средства связи, доступные для населения в целом.

Следовательно, ресурсы инфраструктуры электросвязи общего пользования в обширных географических зонах должны образовывать основу для повсеместного покрытия электросвязи в чрезвычайных ситуациях.

7.9 Жизнеспособность/работоспособность

Основная сетевая инфраструктура, поддерживающая электросвязь в чрезвычайных ситуациях, должна быть максимально устойчивой, для того чтобы выстоять в случае бедствия.

Средства связи должны быть достаточно устойчивыми, чтобы поддерживать связь с выжившими пользователями в широком диапазоне условий, возникших вследствие стихийных бедствий или антропогенных катастроф.

7.10 Передача голоса

По традиции основным способом электросвязи в ходе аварийно-спасательных работ была и остается голосовая связь. Следовательно, сети должны быть оборудованы средствами для передачи голоса при операциях в чрезвычайных ситуациях. Сети с коммутацией каналов выполняют это требование по умолчанию, тогда как в сетях с коммутацией пакетов для обеспечения приемлемой интерактивной потоковой передачи голоса в режиме реального времени требуется обеспечить: малое фазовое дрожание, малые потери и малую задержку передачи. И сети с коммутацией каналов, и сети с коммутацией пакетов должны обеспечить пользователям электросвязи в чрезвычайных ситуациях требуемый уровень качества передачи голоса.

7.11 Передача изображения

Наряду с голосовой связью все более важным инструментом в операциях по восстановлению в чрезвычайных ситуациях становится интерактивная видеосвязь. В сетях с коммутацией пакетов видеослужбы могут предоставляться по той же ориентированной на сеансы эталонной архитектуре, которая используется для передачи голоса, при аналогичной сигнализации. Вместе с тем передача видеоданных включает аудио- и видеокomпоненты, с которыми могут быть связаны совершенно иные, чем при передаче голоса, требования к ширине полосы и показателям качества, и она может применяться в иных режимах, чем те, которые обычно предусматриваются для передачи голоса, например, в двусторонних аудиодиалогах с двусторонним видеорядом или двусторонних аудиодиалогах с односторонним видеорядом. Видеослужбы, используемые при восстановлении в чрезвычайных ситуациях, могут стать частью приоритетных услуг видеоконференц-связи, предлагаемых тем или иным поставщиком услуг.

7.12 Передача данных

Наряду с передачей голоса фундаментальное повсеместное присутствие интернета привело к увеличению возможностей передачи голоса и данных на основе пакетов. Многие поставщики услуг предлагают передачу голоса, изображений и данных по управляемой сети передачи данных, предусматривающей мультимедийную связь с различными устройствами, от портативных мобильных терминалов до фиксированных терминалов, находящихся в жилых домах и на предприятиях. Эти методы связи дают пользователям электросвязи в чрезвычайных ситуациях более широкий выбор как альтернативных трасс связи, так и альтернативных способов связи с районами, где инфраструктура может быть повреждена. Следует поддерживать максимально высокое качество обслуживания (QoS) в электросвязи в чрезвычайных ситуациях на основе стандартов. При таком сценарии сети передачи данных должны обеспечивать QoS в отношении минимальной потери пакетов.

В [ATIS-1000057] приводятся примеры двух типов услуг передачи данных, которые могут применяться для поддержки восстановления в чрезвычайных ситуациях: услуга передачи данных с гарантированной скоростью (GBR) и транспортирование данных (без GBR). В дополнение к этим услугам более широкий комплекс услуг передачи данных, используемых для поддержки операций по восстановлению в чрезвычайных ситуациях, может включать приоритетные версии следующих коммерческих услуг: веб-службы, передача файлов, электронная почта, служба коротких сообщений (SMS) по IP, и мгновенная передача сообщений (IM).

В электронной почте широко применяемый метод связан с использованием простого протокола пересылки электронной почты (SMTP). Хотя для указания в заголовке таких полей, как важность и приоритет, используются различные подходы, эти подходы (методики) зачастую используют сильно различающийся синтаксис, и поэтому получатели SMTP по-разному работают с этими подходами. Тем не менее, при подаче сообщения может применяться стандартный метод, см. "Подача сообщения для почты" [b-IETF RFC 6409] и см. "Простой протокол пересылки электронной почты" [IETF RFC 5321] по передаче, но с двумя следующими вариантами IETF: 1) определение параметра приоритета в команде "Отправитель" набором целых значений, обозначающих уровень приоритета, и 2) определение расширения заголовка SMTP, который используется при пересылке сообщения через агентов передачи, которые не поддерживают параметр, приведенный в 1) [IETF RFC 6710]. Хотя фактические значения и семантика приоритета зависят от применяемой политики, приводится пример набора значений для случая, когда ряд санкционированных пользователей используют SMTP для услуг электросвязи в чрезвычайных ситуациях. Принципы применения параметра или заголовка приоритета, определяемые этим подходом, могут рассматриваться для принятия, если узлы сети развертываются с этими расширениями.

Еще один пример передачи данных – необходимость передачи властями сигналов тревоги для граждан в связи с масштабными чрезвычайными ситуациями, например предупреждений о цунами и других стихийных и антропогенных бедствиях, с использованием таких механизмов, как протокол общего оповещения [ITU-T X.1303]. Такого рода связь состоит из двух этапов. На первом этапе оповещения могут направляться по списку рассылки, например родителям о закрытии школы или жителям конкретного географического района, как в случае предупреждения о цунами, без особого списка рассылки. Второй этап связан с надежной доставкой предупреждений.

7.13 Масштабируемая полоса пропускания

В тех случаях, когда это оправдано, во время объявленных чрезвычайных ситуаций, когда ресурсы инфраструктуры практически исчерпаны, может потребоваться обеспечить приоритетность электросвязи в чрезвычайных ситуациях по сравнению с обычной электросвязью. Одним из способов достижения этого является предоставление электросвязи в чрезвычайных ситуациях масштабируемой полосы пропускания, что дает возможность уменьшить полосу пропускания, предоставляемую обычной электросвязи, и это может оказать неблагоприятное воздействие на установленную электросвязь в отношении QoS. Качество обычной электросвязи может ухудшиться, или допускается определенное ухудшение качества обслуживания для электросвязи, не относящейся к чрезвычайной ситуации, по мере истощения ресурсов инфраструктуры.

Широкополосный доступ является потребностью пользователя, которую он может запросить при получении от оператора услуг электросвязи в чрезвычайных ситуациях. Санкционированные пользователи должны иметь возможность выбирать параметры электросвязи в чрезвычайных ситуациях для поддержки меняющихся требований к ширине полосы пропускания.

7.14 Преимущественное обслуживание в механизмах управления перегрузками

В случае сетей с коммутацией пакетов многие краевые и основные маршруты конфигурируются с пороговыми значениями и механизмами управления перегрузками для снижения уровня перегрузок. Результатом работы этих механизмов является сбрасывание пакетов как обычного, так и приоритетного трафика, в зависимости от уровня перегрузки. Электросвязь в чрезвычайных ситуациях может иметь более высокий приоритет, чем трафик "при максимальных усилиях", но если механизмы будут применяться ко всему трафику, они могут препятствовать электросвязи в чрезвычайных ситуациях. Эти механизмы управления перегрузками следует конфигурировать таким образом, чтобы трафик санкционированных пользователей электросвязи в чрезвычайных ситуациях продолжал передаваться даже на ухудшенном уровне и не подвергался воздействию этих механизмов.

Виды трафика можно идентифицировать при наличии поддержки сигнализации, например поля заголовка приоритета ресурсов в SIP. Для определения приоритета различных видов трафика применяются также метки. Механизмы управления перегрузками должны быть способны опознавать трафик электросвязи в чрезвычайных ситуациях и предлагать исключения для сведения к минимуму отброшенных пакетов такого трафика. К трафику электросвязи в чрезвычайных ситуациях при перегрузках должны применяться сокращенные меры по сравнению с обычным трафиком.

В сетях подвижной и фиксированной связи последующих поколений возрастает значение применения мультимедийной подсистемы IP (IMS), особенно в отношении сетей радиодоступа (RAN), таких как сети, работающие по технологии долгосрочного развития (LTE). Для мобильного доступа пользовательское оборудование для санкционированных пользователей электросвязи в чрезвычайных ситуациях конфигурируется с кодом защиты от перегрузок класса доступа, чтобы обеспечить приоритетный доступ в канале случайного доступа (RACH) во время перегрузки. Такие сетевые элементы, как базовые станции, MME и шлюзы, поддерживают параметры сигнализации (как, например, повышенный приоритет) при перегрузках для обеспечения приоритета электросвязи в чрезвычайных ситуациях при перегрузках. В [ETSI TS 133 401] и [ETSI TS 122 011] описывается развивающаяся архитектура 3GPP для безопасности и класса доступа, обеспечивающего защиту от перегрузок, соответственно.

С позиций поставщика услуг для управления трафиком при перегрузке обычно используются три показателя: на основании скорости, на основании объема и на основании приложения. К числу недостатков этих подходов относятся чрезмерное или недостаточное ограничение сети и аспекты политики, являющиеся следствием поддержки безопасности прикладного уровня (кодирование). Чтобы оператор мог провести не зависящие от приложения измерения и преодолеть неопределенность показателей, операторы оказывают отправителю поддержку для обеспечения сигналов подверженности перегрузке наряду с ответным уведомлением о перегрузке от получателя. Отправитель включает ожидаемую перегрузку в заголовок данных, и промежуточные узлы узнают о перегрузке на трассе из информации заголовка. Оператор может отслеживать эти сигналы о подверженности, в особенности в аномальных условиях, и принимать необходимые меры для повышения вероятности завершения трафика службы электросвязи в чрезвычайных ситуациях (ETS).

Трафик электросвязи в чрезвычайных ситуациях не должен испытывать больших задержек. Например, вышеописанное явление, установленное путем фактических измерений, представляет собой увеличение задержки вследствие наличия в сети больших буферов. При перегрузках воздействие этих больших буферов сводит на нет пользу управления перегрузками. Для высокой вероятности обеспечения приемлемой задержки решающее значение имеют конфигурирование этих буферов, их мониторинг и управление ими.

Были определены [b-Nichols] некоторые характеристики, которые имеют значение при управлении этими буферами для эффективного активного управления очередью. Контролируемое управление задержкой считается базирующимся на минимальном размере очереди, а не на его среднем значении, при переменном состоянии для отслеживания минимального размера очереди и времени, которое пакет остается в очереди. Считается, что это более эффективные меры управления большими буферами, чем, например, пороговые значения размера очереди или использование каналов, применяемые в настоящее время. Понимание управления очередью и применение соответствующих мер в сочетании со связанным с задержкой поведением на каждом транзитном участке, вероятно, будут способствовать уменьшению больших задержек для трафика электросвязи в чрезвычайных ситуациях.

Следует проектировать и поддерживать сети с помощью различных имеющихся механизмов для максимально оптимального поддержания стандартизованного QoS.

7.15 Надежность/эксплуатационная готовность

Для того чтобы быть максимально полезной, электросвязь в чрезвычайных ситуациях должна быть как надежной, так и доступной. Везде, где это возможно, доступ к управлению сетью или ее политикой может повысить вероятность успешного осуществления электросвязи благодаря предоставлению режима предпочтительности для электросвязи в чрезвычайных ситуациях.

Все компоненты, включая аппаратное и программное обеспечение и другие ресурсы электросвязи, должны функционировать согласованно и в точном соответствии с проектными требованиями и спецификациями и должны иметь возможность использования с высоким уровнем уверенности в соответствии со своими соглашениям об уровне обслуживания (SLA).

SLA могут содействовать уверенности клиента ETS в том, что в сети поставщика услуг соблюдены проектные требования и спецификации.

В Справочнике по управлению SLA организации TeleManagement Forum (TMF) [b-TMF GB917] описывается формальная методика, которая может применяться для заключения SLA между клиентами и поставщиками услуг. В Справочнике используется понятие спецификации уровня обслуживания (SLS) для определения измеримых параметров, которые следует включать в SLA. SLS используется для определения параметров ключевого показателя качества (KQI), наряду со связанными с ними пороговыми значениями, для включения в SLA. Также рекомендуется использовать шаблоны SLA, такие как указанные в [ITU-T M.3342].

В Справочнике TMF по SLA разработка спецификации SLA считается "бизнес-процессом". Этот бизнес-процесс далее подразделяется на бизнес-процессы более низкого уровня, к числу которых относятся:

- установка требований к SLA;
- подготовка проекта SLA;
- проверка полноты SLA;
- подтверждение спецификации SLA;
- подписание спецификации SLA.

Применение каждого бизнес-процесса подробно разъясняется с позиций клиента и поставщика услуг. Приводятся также примеры (именуемые "случаями использования"), показывающие, как эти бизнес-процессы могут применяться в контексте конкретных услуг (например, ETS).

Более углубленные примеры, именуемые "указателями по применению", обычно приводятся в отдельных документах. Так, [b-TMF GB934] представляет собой указание по применению, посвященное управлению SLA при передаче голоса по IP. В [b-TMF GB934] также обсуждается управление SLA при передаче голоса по IP в контексте ETS. Одним из основных отличий ETS от услуг общего пользования является значение KQI при аномальных условиях (например, перегрузке).

Для рассмотрения требований к эксплуатационной готовности и надежности сетей можно использовать примеры ETS, приведенные в [b-TMF GB917] и [b-TMF GB934], в особенности приводимое в [b-TMF GB934] обсуждение аспектов голосовых услуг. Дополнительная работа по управлению SLA конкретно в ETS, которая могла бы предусматривать разработку KQI для данных и видеоизображений, требует дальнейшего изучения.

7.16 Использование облачной инфраструктуры в ETS

В [ITU-T Y.3501] приводятся общие требования к облачным вычислениям и их возможностям. В Приложении А к этой Рекомендации содержится перечень функциональных требований к электросвязи в чрезвычайных ситуациях и ее возможностей. Необходимо обеспечивать эти требования, когда электросвязь в чрезвычайных ситуациях, включая ETS, предлагается поставщиком облачных услуг (CSP) [ITU-T Y.3510].

Являющаяся в настоящее время предметом определения инфраструктура облачных вычислений может использоваться поставщиками услуг (например, поставщиками СПП), с тем чтобы обеспечить предоставление сетевых услуг общего пользования, таких как электросвязь в чрезвычайных ситуациях, включая ETS. Если инфраструктура облачных вычислений используется для поддержки электросвязи в чрезвычайных ситуациях, включая ETS, применяются и должны учитываться сетевые ресурсы и

требования к базовой транспортной сети для приоритетного обслуживания, указанные в этой Рекомендации. Так, ETS обеспечивает приоритетную электросвязь для санкционированных пользователей при бедствиях и чрезвычайных ситуациях. В контексте управления облачными ресурсами, если облачная инфраструктура используется для поддержки сетевых услуг общего пользования, санкционированные пользователи ETS должны иметь возможность получать приоритетный доступ (т. е. предпочтительное обслуживание) к облачным ресурсам. Наряду с этим требования к электросвязи в чрезвычайных ситуациях, указанные в этой Рекомендации, применяются в нескольких уровнях эталонной облачной архитектуры, определенной в [ITU-T Y.3501] и [ITU-T Y.3510].

В [ITU-T Y.3520] дается обзор общих концепций требований к сквозному управлению ресурсами облачных вычислений. Если для поддержки ETS используются ресурсы облачных вычислений, то, согласно [ITU-T Y.3520], потребуются соответствующие функции управления ресурсами для обеспечения приоритетного обслуживания при использовании ресурсов облачных вычислений санкционированными пользователями.

В Дополнении IV к [ITU-T Y.3510] приводятся руководящие указания и подробности использования ETS ресурсов облачной инфраструктуры, относящиеся как к сетевым ресурсам, так и к требованиям к базовым транспортным сетям, приведенным в этой Рекомендации.

Приложение А

Возможные различия между обязательными и факультативными требованиями

(Данное приложение является неотъемлемой частью настоящей Рекомендации.)

Функциональные требования и возможности электросвязи в чрезвычайных ситуациях	Описание	Обязательные	Необязательные
Усовершенствованный приоритетный режим	Для передачи трафика связи в чрезвычайных ситуациях требуются гарантированные возможности передачи, вне зависимости от того, по каким сетям он передается.	X	
Защищенные сети	Сети должны иметь защиту от повреждения (фальсификации) трафика или сигналов управления, а также от несанкционированного доступа к ним (мошенничества), включая расширенные методы кодирования и аутентификации пользователя, в зависимости от случая.	X	
Конфиденциальность местоположения	Ограниченному количеству пользователей электросвязи в чрезвычайных ситуациях из числа руководителей высшего звена может потребоваться организовывать работы по оказанию помощи без риска раскрытия сведений об их нахождении.		X
Восстанавливаемость	Определенные сетевые функции должно быть возможным вновь предоставить, отремонтировать или восстановить до требуемых уровней на приоритетной основе.		X
Межсетевые соединения	Сети, обеспечивающие связь в чрезвычайных ситуациях, должны предусматривать возможность международных соединений везде, где это возможно, например в ситуациях, когда применимы [ITU-T E.106] и/или [ITU-T E.107].	X	
Функциональная совместимость	Обеспечивает присоединения и функциональную совместимость всех сетей (развивающихся и существующих).	X	
Мобильность	Инфраструктура электросвязи должна поддерживать мобильность пользователя и терминала, включая связь быстрого развертывания и полностью подвижную электросвязь.	X	
Повсеместное покрытие	Ресурсы инфраструктуры электросвязи общего пользования в обширных географических зонах должны образовывать основу для повсеместного охвата электросвязи в чрезвычайных ситуациях.	X	
Жизнеспособность/ работоспособность	Средства связи должны быть достаточно устойчивыми, чтобы поддерживать связь с выжившими пользователями в широком диапазоне условий.	X	
Передача голоса	И сети с коммутацией каналов, и сети с коммутацией пакетов должны обеспечить пользователям электросвязи в чрезвычайных ситуациях уровень обслуживания голосовой полосы.	X	

Функциональные требования и возможности электросвязи в чрезвычайных ситуациях	Описание	Обязательные	Необязательные
Передача изображения	Сети с коммутацией каналов и с коммутацией пакетов должны обеспечивать качество обслуживания при низком показателе ошибок пакетов и потери пакетов для пользователей электросвязи в чрезвычайных ситуациях.	X	
Передача данных	Сети с коммутацией пакетов должны обеспечивать качество обслуживания при низком показателе потери пакетов для пользователей электросвязи в чрезвычайных ситуациях.	X	
Масштабируемая полоса пропускания	Санкционированные пользователи должны иметь возможность выбирать параметры электросвязи в чрезвычайных ситуациях, для того чтобы выполнялись различные требования по ширине полосы пропускания.		X
Надежность/ эксплуатационная готовность	Электросвязь должна функционировать согласованно и в точном соответствии с проектными требованиями и спецификациями, и должна иметь возможность использования с высоким уровнем уверенности.	X	
Преимущественное обслуживание в механизмах управления перегрузками	Механизмы управления перегрузками должны поддерживать применение к трафику электросвязи в чрезвычайных ситуациях сокращенных мер по сравнению с обычным трафиком.		X

Дополнение I

Сведения о возможных источниках чрезвычайных ситуаций

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Причиной большинства стихийных бедствий являются силы двух типов. Это: экстремальные погодные условия (бури) и землетрясения. И те, и другие могут иметь различную силу и быть причиной разнообразных разрушений в различных по величине географических районах. Ураган (иногда называемый тайфуном или циклоном), как правило, охватывает огромные географические пространства и представляет собой наиболее разрушительные неблагоприятные штормовые погодные условия на земле. Ветер, дождь и вторичные явления, такие как наводнения, являющиеся результатом бури такого вида, часто причиняют широкомасштабный и долговременный ущерб зданиям и людям. Несмотря на то, что многие параметры (например, интенсивность и путь следования) бурь в некоторой степени могут прогнозироваться, что дает людям время для спасения, разрушения собственности и земли неизбежны. В отличие от экстремальных погодных условий землетрясения, по большому счету, непредсказуемы, но они затрагивают гораздо меньшие географические районы. Тем не менее, мощные силы природы все еще не приручены и часто приносят значительные разрушения и людские потери, особенно в густонаселенных районах мира.

Как правило, стихийные бедствия влекут за собой дополнительные природные явления. Например, следствием урагана может стать сильный паводок и грязевые оползни. Ураганы могут повлечь за собой выход рек из берегов, приводящий к гибели животных в затронутых районах. Люди могут остаться без электричества или без крыши над головой, им потребуется еда, одежда и жилье. Землетрясения продолжают свое разрушительное действие, так как за ними следуют дополнительные толчки. Иногда землетрясения создают приливные волны, которые приносят дополнительные разрушения в уже пострадавшие районы. Как стало недавно ясно, некоторые из бедствий могут создавать эффект каскада и не поддаваться воздействию планируемых для борьбы с ними мер. Землетрясение, например, может вызвать повреждение ядерной установки и цепь событий, не рассматривавшихся и не предусматривавшихся при планировании мер реагирования.

В таблице I.1 перечислены некоторые стихийные бедствия.

Таблица I.1 – Стихийные бедствия

Снежные лавины
Засуха
Землетрясения
Эпидемии
Сильный паводок
Голод
Наводнения
Лесные пожары
Сильные грозы
Ураганы
Грязевые оползни
Сильная стужа, снег, лед или жара
Сейсмическая волна
Торнадо
Цунами
Тайфуны
Извержения вулкана
Бури

Чрезвычайные события, причиной которых являются действия людей, могут также различаться по силе, географическому охвату, продолжительности и возможным разрушениям.

Антропогенные бедствия могут конкурировать с природными. Как и в случае стихийных бедствий, здесь могут существовать дополнительные разрушительные последствия, являющиеся результатом основного события. Например, пожар в угольной шахте может привести к смерти населения от огня и удушья. Такие пожары могут преградить людям выход из шахты и привести к взрывам. Список бедствий, вызванных действиями людей, приведен в таблице I.2.

Таблица I.2 – Антропогенные катастрофы

Поджог
Разливы химических веществ
Разрушение промышленных или жилых зданий
Взрывы
Пожары
Утечки газа
Ядерные взрывы
Прорывы трубопроводов
Крушения самолетов/вынужденные посадки
Отравление
Радиация
Кораблекрушения/столкновения судов
Паническое бегство
Столкновения поездов в метро/сход с рельсов
Терроризм
Столкновения поездов/сход с рельсов
Несчастные случаи на воде

Библиография

- [b-IETF RFC 5559] IETF RFC 5559 (2009), *Pre-Congestion Notification (PCN) Architecture*.
- [b-IETF RFC 6409] IETF RFC 6409 (2011), *Message Submission for Mail*.
- [b-Nichols] Nichols, K., Jacobson, V. (2012) *Controlling Queue Delay*. Association for Computer Machinery.
<<http://queue.acm.org/detail.cfm?id=2209336>>
- [b-TMF GB917] TMF GB917 (04/2012), *SLA Management Handbook Release 3.1*.
- [b-TMF GB934] TMF GB934 (06/2008), *Application Note to SLA Management Handbook, Release 2.0*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	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	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи