МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.2205

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2008)

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

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

Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения

Рекомендация МСЭ-Т Y.2205

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
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: 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
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899

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

Рекомендация МСЭ-Т Y.2205

Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения

Резюме

В Рекомендации МСЭ-Т Y.2205 (Y.NGN-ET-Tech) описываются технические соображения, которые могут применяться в сетях последующих поколений (СПП) для обеспечения электросвязи в чрезвычайных ситуациях (ЕТ). Кроме того, в этой Рекомендации приводятся основополагающие технические принципы, используемые для обеспечения ЕТ.

Источник

Рекомендация МСЭ-Т Y.2205 утверждена 12 сентября 2008 года 13-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

Ключевые слова

Архитектура, раннее предупреждение (EW), служба электросвязи в чрезвычайных ситуациях (ETS), СПП, приоритетная электросвязь, QoS (качество обслуживания), электросвязь для оказания помощи при бедствиях (TDR).

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

СОДЕРЖАНИЕ

Введение

В [ITU-T Y.1271] содержатся требования к сети и возможности сети для обеспечения электросвязи в чрезвычайных ситуациях. Как показывает опыт деятельности органов власти, ответственных за координацию операций по оказанию помощи при бедствиях с использованием сетей общего пользования, осуществление приоритетной электросвязи на основе этих требований может привести к созданию новых механизмов, а также к взаимодействию/повторному использованию существующих механизмов. Электросвязь в чрезвычайных ситуациях должна пользоваться преимущественным режимом по сравнению с обычными услугами сетей общего пользования. Идея приоритетной электросвязи, используемой в чрезвычайных ситуациях, не нова; в течение многих лет сети с коммутацией каналов обеспечивали работу таких систем, в основном, для голосовых вызовов (см., например, [ITU-T E.106]). Однако, что касается технических методов, используемых для обеспечения выполнения этих основополагающих требований к электросвязи в чрезвычайных ситуациях в среде СПП, то они развиваются. Традиционные методы установления приоритета, используемые при коммутации каналов, могут не применяться в СПП вследствие различий, присущих электросвязи с коммутацией каналов и с коммутацией пакетов.

В [ITU-T Y.1271] в общем виде изложены и теоретически описаны требования и возможности. [ITU-T Y.1271] является нейтральной в технологическом отношении.

В связи с тем, что СПП основаны на технологии коммутации пакетов, которая принципиально отличается от технологии коммутации каналов, требуется рассмотреть технические вопросы и возможные решения, которые могли бы использоваться для реализации возможностей электросвязи в чрезвычайных ситуациях в СПП.

В настоящей Рекомендации определяются технические соображения, которые могут применяться в СПП для обеспечения электросвязи в чрезвычайных ситуациях, а также для реализации используемых основополагающих принципов.

Рекомендация МСЭ-Т Y.2205

Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения

1 Сфера применения

В настоящей Рекомендации описываются технические соображения, которые могут применяться в сетях последующих поколений (СПП) для обеспечения электросвязи в чрезвычайных ситуациях (ЕТ). Кроме того, в данной Рекомендации приводятся основополагающие технические принципы, используемые для обеспечения ЕТ. В Рекомендации определяются требования и возможности ЕТ, помимо тех, которые установлены в отношении СПП в [ITU-T Y.2201] (как определено в [ITU-T Y.2001] и далее описано в [ITU-T Y.2011]).

К электросвязи в чрезвычайных ситуациях (включая обеспечение некоторых элементов раннего предупреждения (см. рисунок 1)) относится:

- электросвязь в чрезвычайных ситуациях между отдельным лицом и органом власти, например звонки оператору службы экстренного вызова;
- электросвязь в чрезвычайных ситуациях между органами власти;
- электросвязь в чрезвычайных ситуациях между органом власти и отдельным лицом, например службы оповещения общественности.

В Дополнении I представлена дополнительная информация, касающаяся перечисленных выше категорий ЕТ.

Определен также ряд требований и возможностей в отношении раннего предупреждения. Возможности электросвязи в чрезвычайных ситуациях между отдельным лицом и органом власти не рассматриваются и выходят за рамки сферы применении настоящей Рекомендации.

Некоторые технические средства, описанные в этом документе, могли бы также использоваться для электросвязи в чрезвычайных ситуациях между отдельным лицом и органом власти или между отдельными лицами, однако эти категории не рассматриваются в настоящей Рекомендации.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру, поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса рекомендации.

[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 H.248.1] Рекомендация МСЭ-Т H.248.1 (2005 г.), *Протокол управления шлюзом: Версия 3*.

[ITU-T H.323] ITU-T Recommendation H.323 (2006), *Packet-based multimedia communications systems*.

[ITU-T H.460.4] Рекомендация МСЭ-Т H.460.4 (2007 г.), *Обозначение приоритета вызова и идентификация сети страны/международной сети происхождения вызова для приоритетных вызовов по H.323*.

[ITU-T J.260] Рекомендация МСЭ-T J.260 (2005 г.), *Требования к предпочтительному использованию средств электросвязи в сетях IPCablecom*.

[ITU-T X.805] Рекомендация МСЭ-T X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами*.

[ITU-T X.1303] ITU-T Recommendation X.1303 (2007), *Common alerting protocol (CAP V1.1)*.

[ITU-T Y.110] ITU-T Recommendation Y.110 (1998), *Global Information Infrastructure principles and framework architecture*.

[ITU-T Y.1271] Рекомендация МСЭ -T 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-T Y.1541 (2006 г.), *Требования к сетевым показателям качества для служб, основанных на протоколе IP*.

[ITU-T Y.2001] Рекомендация МСЭ-T Y.2001 (2004 г.), *Общий обзор СПП*.

[ITU-T Y.2011] ITU-T Recommendation Y.2011 (2004), *General principles and general reference model for NGNs*.

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN of release 1*.

[ITU-T Y.2111] Рекомендация МСЭ-T Y.2111 (2008 г.), *Функции управления ресурсами и установлением соединений в сетях последующих поколений*.

[ITU-T Y.2171] Рекомендация МСЭ-T Y.2171 (2006 г.), *Уровни приоритета при управлении доступом в сетях последующих поколений*.

[ITU-T Y.2172] ITU-T Recommendation Y.2172 (2007), *Service restoration priority levels in IP networks*.

[ITU-T Y.2201] ITU-T Recommendation Y.2201 (2007), *NGN release 1 requirements*.

[ITU-T Y.2701] ITU-T Recommendation Y.2701 (2007), *Security requirements for NGN release 1*.

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP)-Version 1 Functional Specification*. <http://www.ietf.org/rfc/rfc2205.txt?number=2205>

[IETF RFC 3246] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior)*. <http://www.ietf.org/rfc/rfc3246.txt?number=3246>

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*. <http://www.ietf.org/rfc/rfc3261.txt?number=3261>

[IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP)*. <http://www.ietf.org/rfc/rfc3312.txt?number=3312>

[IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP)*. <http://www.ietf.org/rfc/rfc4412.txt?number=4412>

[IETF RFC 4542] IETF RFC 4542 (2006), *Implementing an emergency telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite*. <http://www.ietf.org/rfc/rfc4542.txt?number=4542>

[IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*. <http://www.ietf.org/rfc/rfc4594.txt?number=4594>

3 Определения

В настоящей Рекомендации используются следующие определения из: [ITU-T Y.1271], [ITU-T Y.2001], [ITU-T Y.2011] и [ITU-T Y.2201].

3.1 электросвязь в чрезвычайных ситуациях (emergency telecommunications) (ET): ET означает любую службу, связанную с чрезвычайными ситуациями, для которой требуется специальная

обработка со стороны СПП, по сравнению с другими службами. К таким службам относятся службы экстренного вызова, уполномоченные властями, и службы общественной безопасности.

3.2 служба электросвязи в чрезвычайных ситуациях (emergency telecommunications service) (ETS): [ITU-T E.107] Национальная служба, предоставляющая приоритетную электросвязь авторизованным пользователям ETS в период бедствий и чрезвычайных ситуаций

3.3 сети последующих поколений (next generation network) (СПП): [ITU-T Y.2001] Сеть с пакетной коммутацией, пригодная для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от применяемых технологий, обеспечивающих транспортировку. Она обеспечивает свободный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или выбираемым ими услугам. Она поддерживает универсальную подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.4 электросвязь для оказания помощи при бедствиях (telecommunications for disaster relief) (TDR): TDR представляет собой возможности использования международной и национальной электросвязи для целей оказания помощи при бедствиях. Для TDR могут использоваться на постоянной или совместной основе международные сетевые средства, которые уже введены в действие и эксплуатируются; временные сетевые средства, которые предоставляются конкретно для TDR, либо подходящая комбинация из этих двух вариантов.

4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

ASN.1	Abstract Syntax Notation One		Абстрактно-синтаксическая нотация 1
CAC	Call Admission Control		Управление допуском вызова
CAP	Common Alerting Protocol		Протокол общего оповещения
DoS	Denial of Service		Отказ в обслуживании
DSCP	Differentiated Services Code Point		Указатели кода дифференцированного обслуживания
EAS	Emergency Alert System		Система оповещения о чрезвычайной ситуации
EF	Expedited Forwarding		Срочная пересылка данных
ENI	ETS National Implementation		Реализованная на национальном уровне служба ETS
ET	Emergency Telecommunications		Электросвязь в чрезвычайных ситуациях
ETS	Emergency Telecommunications Service		Служба электросвязи в чрезвычайных ситуациях
EW	Early Warning		Раннее предупреждение
IEPS	International Emergency Preference Scheme		Международная система предпочтений при чрезвычайных ситуациях
IP	Internet Protocol		Протокол Интернет
ISDN	Integrated Services Digital Network	ЦСИС	Цифровая сеть с интеграцией служб
MMPS	Multimedia Priority Service		Приоритетное обслуживание мультимедийного трафика
NGN	Next Generation Network	СПП	Сети последующих поколений
NOAA	National Oceanic and Atmospheric Administration		Национальное управление океанических и атмосферных исследований
PHB	Per Hop Behaviour		Поведение на каждом шаге
PIN	Personal Identification Number		Персональный идентификационный номер
PLMN	Public Land Mobile Network		Сеть сухопутной подвижной связи общего пользования
PSAP	Public Safety Answering Point		Пункт сообщений общественной безопасности

PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
RACF	Resource and Admission Control Function		Функция управления ресурсами и допуском
RPH	Resource Priority Header		Заголовок приоритета ресурса
RSVP	Resource ReSerVation Protocol		Протокол резервирования ресурсов
QoS	Quality of Service		Качество обслуживания
SAME	Specific Area Message Encoding		Протокол кодирования сообщений для конкретного района
SCF	Service Control Function		Функция управления обслуживанием
SIP	Session Initiation Protocol		Протокол инициации сеанса
SLA	Service Level Agreement		Соглашение об уровне обслуживания
SS7	Signalling System № 7		Система сигнализации № 7
TCP	Transmission Control Protocol		Протокол управления передачей
UDP	User Datagram Protocol		Протокол дейтаграмм пользователя
UN/ISDR	United Nations International Strategy for Disaster Reduction		Международная стратегия ООН по уменьшению чрезвычайных ситуаций
VoIP	Voice over IP		Передача голоса по протоколу IP
W-CDMA	Wideband Code Division Multiple Access		Широкополосный многостанционный доступ с кодовым разделением каналов
WPS	Wireless Priority Service		Беспроводная приоритетная служба
xDSL	Any variant of Digital Subscriber Line		Любой вариант цифровой абонентской линии
XML	eXtensible Markup Language		Расширяемый язык разметки
XSD	XML Schema Definition		Определение схемы XML

5 Описание электросвязи в чрезвычайных ситуациях (ET) и раннего предупреждения

5.1 Общие положения

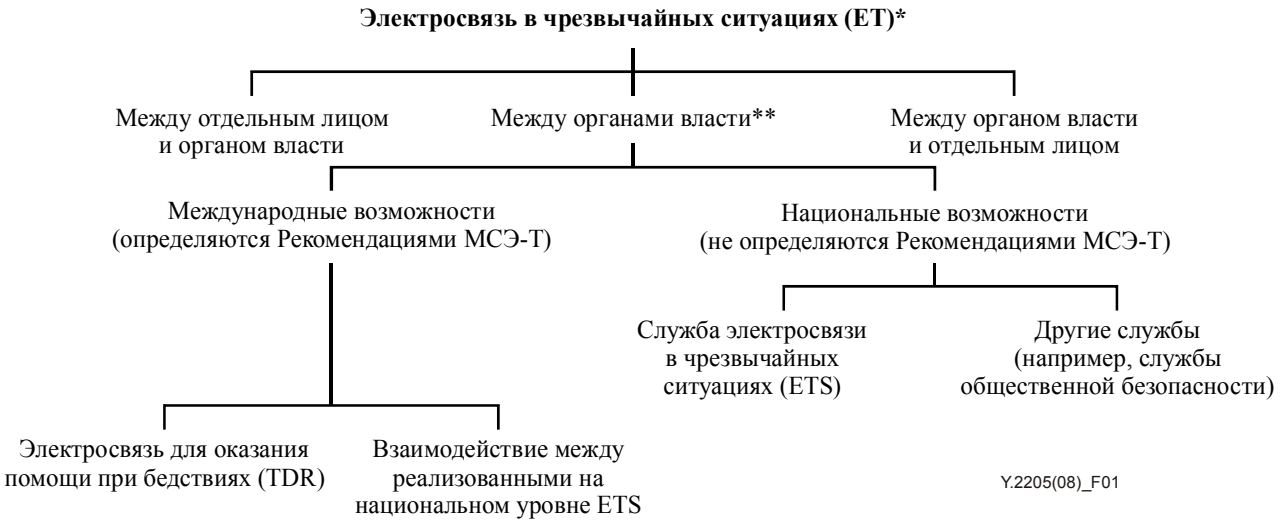
В настоящей Рекомендации используются следующие термины:

- Электросвязь в чрезвычайных ситуациях ET
- Служба электросвязи в чрезвычайных ситуациях ETS
- Электросвязь для оказания помощи при бедствиях TDR
- Раннее предупреждение EW

Важно отметить, что имеется согласие и понимание в отношении различных вариантов использования этих терминов. С этой целью приведенные ниже термины используются следующим образом:

- ET Обобщающий термин для любой службы, связанной с чрезвычайными ситуациями, для которой требуется специальная обработка со стороны СПП, по сравнению с другими службами.
- ETS Определение этого термина дано в [ITU-T E.107].
- TDR Общий термин для обозначения возможности использования электросвязи для целей оказания помощи при бедствиях.
- EW Общий термин для обозначения всех типов систем/возможностей/служб раннего предупреждения.

Для данного порядка формируется дерево, при этом в корне всех видов деятельности расположена ET. Использование терминов и их взаимосвязь изображено на рисунке 1, ниже.



* Включая некоторые аспекты раннего предупреждения
** Может также применяться к электросвязи между органом власти и отдельным лицом

Рисунок 1 – Терминологическая структура взаимосвязи для электросвязи в чрезвычайных ситуациях

5.2 Электросвязь в чрезвычайных ситуациях

Электросвязь в чрезвычайных ситуациях (ET) означает любую службу, связанную с чрезвычайными ситуациями, для которой требуется специальная обработка со стороны СПП, по сравнению с другими службами. К таким службам относятся службы экстренного вызова, уполномоченные властями, и службы общественной безопасности. Ниже приводятся конкретные примеры служб в рамках электросвязи в чрезвычайных ситуациях:

1) *Электросвязь для оказания помощи при бедствиях (TDR)*

   TDR представляет собой возможности использования международной и национальной электросвязи для целей оказания помощи при бедствиях. Для TDR могут использоваться на постоянной или совместной основе международные сетевые средства, которые уже введены в действие и эксплуатируются; временные сетевые средства, которые предоставляются конкретно для TDR, либо подходящая комбинация из этих двух вариантов.

2) *Служба электросвязи в чрезвычайных ситуациях (ETS)*

   ETS является национальной службой, предоставляющей приоритетную электросвязь авторизованным пользователям ETS в период бедствий и чрезвычайных ситуаций. Описание ETS определяется в [ITU-T E.107]. В [ITU-T E.107] приводится руководство, которое позволит обеспечивать электросвязь между одной реализованной на национальном уровне ETS (ENI) и другой (другими) ENI (электросвязь между органами власти).

3) *Национальные/региональные/местные службы экстренного вызова и общественной безопасности*

   К другим примерам ET относятся национальные/региональные/местные службы экстренного вызова и общественной безопасности. Они являются специализированными службами для целей обеспечения экстренного вызова и общественной безопасности на национальном/региональном/местном уровне. Эти службы экстренного вызова зависят от национальных/региональных/местных потребностей и подлежат стандартизации на национальном/региональном уровне.

5.3 Раннее предупреждение

В отчете [b-UN Global Survey] Генеральному секретарю Организации Объединенных Наций (ООН) за сентябрь 2006 года, подготовленном по линии Международной стратегии ООН по уменьшению чрезвычайных ситуаций (UN/ISDR) на тему "Глобальный обзор по системам раннего предупреждения", раннее предупреждение определяется как "своевременное и эффективное предоставление информации через определенные учреждения, которое позволяет частным лицам, подверженным опасности, принять меры, направленные на предупреждение и снижение риска для себя, а также подготовиться к эффективному реагированию". В данном отчете ООН приводится

оценка способностей, разрывов и возможностей, связанных с созданием всеобъемлющей глобальной системы раннего предупреждения обо всех стихийных бедствиях.

6 Общие соображения, касающиеся электросвязи в чрезвычайных ситуациях и раннего предупреждения

До разработки [ITU-T Y.1271] требования к возможностям электросвязи в чрезвычайных ситуациях относились прежде всего к сетям с коммутацией каналов, например коммутируемым телефонным сетям общего пользования (КТСОП).

Эти требования основывались на определенных характеристиках сетей с коммутацией каналов и пользовались преимуществами таких сетей. Например:

- при управлении допуском используется жесткая связь между ресурсами сигнализации и среды передачи;
- весь трафик медиаданных, для которого требуется равномерная полоса пропускания, передается с постоянной скоростью;
- полоса пропускания резервируется для каждого потока данных;
- разделение трафика управления и трафика данных.

Эти характеристики необязательно встречаются в современных сетях с коммутацией пакетов с негарантированным обслуживанием, при котором:

- в сетях с коммутацией пакетов обычно совместно используются ресурсы и организуются очереди, с тем чтобы компенсировать неравномерный характер трафика; сочетание этих способов обычно и составляет основу негарантированного обслуживания;
- управление допуском может вызывать трудности: многие приложения не сообщают о полосе пропускания, которая требуется для них, и сигнализация не связана со средой передачи;
- приложениям/услугам требуется разная полоса пропускания, и они могут передавать данные с динамически устанавливаемыми скоростями;
- для различных потоков пакетов совместно используется полоса пропускания, обеспечиваемая за счет статистического мультиплексирования;
- для трафика управления и данных могут совместно использоваться одни и те же ресурсы сети.

Кроме того, если не принимать специальных мер, то в СПП с пакетной коммутацией пакеты могут "бороться" за имеющуюся полосу пропускания. На чистом транспортном уровне пакетам не может быть свободно отказано в обслуживании и к ним не может быть свободно применено управление потоком. Кроме того, расчет нагрузки в сетях с коммутацией пакетов существенно отличается от расчета для сетей с коммутацией каналов в части, касающейся стандартных общепринятых подходов. На заданный "поток" пакетов могут воздействовать другие потоки пакетов, совместно использующие ресурсы, если соответствующим образом не применяются меры, доступные в СПП. С другой стороны, разделение обслуживания и транспортирования в СПП может обеспечивать преимущество с точки зрения предоставления более гибких и разнообразных возможностей для электросвязи в чрезвычайных ситуациях.

Эти условия означают, что предоставление возможностей электросвязи в чрезвычайных ситуациях не является чем-то совершенно понятным, очевидным и простым. Также нельзя просто воздействовать на транспортирование, как это было в случае сетей с коммутацией каналов. Другие существенные различия между сетями с коммутацией каналов и с коммутацией пакетов, а также между разными технологиями пакетной коммутации, будут оказывать воздействие на обеспечение и выполнение различных требований, указанных в [ITU-T Y.1271].

Следовательно, данная Рекомендация предназначена для того, чтобы указать, какие свойства и механизмы СПП могут быть использованы для содействия выполнению требований электросвязи в чрезвычайных ситуациях, а также некоторых аспектов раннего предупреждения.

7 Общие функциональные требования и возможности

К числу функциональных требований и возможностей относятся те, которые указаны в [ITU-T Y.1271] и [ITU-T Y.2201] для СПП варианта 1, а также те, которые выявлены по результатам проведенного ООН Глобального обзора по системам раннего предупреждения в отношении развития СПП [b-UN Global Survey].

7.1 Электросвязь в чрезвычайных ситуациях

В таблице 1 перечислены функциональные требования и возможности электросвязи в чрезвычайных ситуациях.

Таблица 1 – Список функциональных требований и возможностей электросвязи в чрезвычайных ситуациях

Электросвязь в чрезвычайных ситуациях Функциональные требования и возможности
Усовершенствованный приоритетный режим
Защищенные сети
Конфиденциальность данных о местоположении
Восстанавливаемость
Возможность установления соединения с сетью
Возможность взаимодействия
Мобильность
Повсеместное покрытие
Живучесть/долговечность
Передача в реальном времени: голос/текст в реальном времени и видео/изображения (если позволяет полоса пропускания)
Передача не в реальном времени: сообщения/потоки данных не в реальном времени (аудио/видео)
Расширяемость полосы пропускания
Надежность/доступность

Цель состоит в том, чтобы обеспечить высокую степень уверенности и вероятности того, что критически важная связь доступна авторизованным пользователям, например, имеющим непосредственное отношение к электросвязи в чрезвычайных ситуациях, и надежно работает. В [ITU-T Y.1271] приводятся "Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов".

Следует учитывать наличие полосы пропускания (например, вида ресурса) в отношении передачи видео и изображений.

7.2 Раннее предупреждение

К числу требований к системам раннего предупреждения в контексте СПП относятся:

- возможность непрерывной работы; системы должны находиться в исправном состоянии, быть надежными и доступными в любой момент времени;
- передача предупреждающих сообщений только тем, кто, возможно, будет затронут надвигающимся бедствием;
- предоставление требуемых возможностей электросвязи для передачи в реальном времени (например, сейсмической информации и данных об уровне моря);
- опора на согласованные на международном уровне стандарты;
- обеспечение передачи только авторизованных сообщений;
- предотвращение отправки нецелевых и ненужных сообщений (например, если сообщения передаются не по адресу и/или не содержат полезной и жизненно важной информации).

Дополнительные требования могут касаться возможностей обеспечения фильтрации сообщений, с тем чтобы эти сообщения достигали:

- избранной группы пользователей;
- избранных районов и т. д.

(например, вид "сотового вещания ").

8 Механизм и возможности обеспечения электросвязи в чрезвычайных ситуациях в СПП

8.1 Общие положения

Отделение управления обслуживанием/приложениями от транспортирования, позволившее раздельно предлагать прикладные услуги и транспортные услуги и обеспечивать их независимое развитие, является важной характеристикой СПП. Такое отделение можно представить в виде двух раздельных блоков или страт функциональных возможностей. Функции транспортирования располагаются в страте транспортирования, а функции управления обслуживанием, относящиеся к приложениям, например телефонии, располагаются в страте обслуживания. Каждая страта обычно имеет собственный набор ролей, участников и административных доменов (см. [ITU-T Y.110]). Роли, связанные с предоставлением услуги (услуг), не зависят от ролей, связанных с обеспечением возможности соединения для целей транспортирования. Каждая страта может рассматриваться отдельно с технической точки зрения. Функции управления ресурсами и допуском (RACF) исполняют роль арбитра для этих страт при выполнении резервирования (и проведении переговоров), связанных с QoS. В [ITU-T Y.2111] определяется функциональная архитектура и требования функциям управления ресурсами и допуском в сетях последующих поколений, в которых могут встречаться разнообразные технологии доступа и базовой транспортировки, а также может иметься множество доменов. Принимаемые RACF решения, связанные с QoS, опираются на SLA, приоритет обслуживания, профили пользователя, правила работы оператора сети, а также наличие ресурсов, как для сетей доступа, так и для базовых сетей. Требуется, чтобы пользователи электросвязи в чрезвычайных ситуациях были идентифицированы и чтобы, после того как они прошли аутентификацию и авторизацию, RAFC предоставила им приоритет в управлении допуском.

Если в СПП необходимо отличать трафик электросвязи в чрезвычайных ситуациях от обычного трафика, то требуется, чтобы были доступны соответствующие отличительные метки, также называемые маркерами. В данном контексте используется термин маркировка (трафика).

В сквозной (т. е. сегменты сети доступа и базовой сети) многоуровневой (т. е. страты транспортирования и обслуживания) архитектуре протоколов СПП возможно существование различных видов меток на разных уровнях протоколов, как вертикальных (т. е. взаимодействие между различными уровнями протоколов), так и горизонтальных (т. е. взаимодействие между устанавливающими связь сетевыми элементами). Метки могут передаваться в пакетах сигнализации и/или вставляться в заголовок пакетов данных для идентификации и маркировки вызовов/сеансов электросвязи в чрезвычайных ситуациях. Метки, используемые для идентификации и маркировки вызовов/сеансов или трафика электросвязи в чрезвычайных ситуациях, зависят от протокола. Для получения специализированного (например, предпочтительного/приоритетного) режима, являющегося сквозным для всех аспектов вызова/сеанса электросвязи в чрезвычайных ситуациях (например, управление вызовом/сеансом, трафик и управление несущей), требуется обеспечить соответствующее преобразование меток, используемых в различных протоколах, и взаимодействие между этими метками. Например, содержащаяся в заголовке протокола SIP информация о приоритете ресурса, используемая на уровне управления для идентификации приоритетного вызова/сеанса, могла бы преобразовываться в соответствующие указатели кода дифференцированного обслуживания (DSPC) для маркировки трафика электросвязи в чрезвычайных ситуациях на уровне IP-сети. Аналогично, указатели кода дифференцированного обслуживания (DSPC) на третьем уровне могли бы преобразовываться в конкретные параметры приоритета в сетях VLAN и Ethernet на втором уровне в транспортном протоколе. Протокол SIP описывается в [IETF RFC 3261], а его обновления – в [b-IETF RFC 3265], [b-IETF RFC 3853], [b-IETF RFC 4320], [b-IETF RFC 4916], [b-IETF RFC 4032] и [b-IETF RFC 5027].

В страте обслуживания услугами обычно используются конкретные заданные наборы протоколов. Следовательно, методы, которые могут эффективно использоваться для конкретных услуг электросвязи в чрезвычайных ситуациях, будут меняться в зависимости от рассматриваемых услуг и возможностей конкретного протокола (протоколов), о котором идет речь, связанного с услугой.

В плоскости транспортирования может использоваться протокол Интернет (IP). Точный состав базового стека протокола IP, вероятно, будет меняться в зависимости от поставщика.

Кроме того, протоколы, используемые в инфраструктурах локального (последняя миля) доступа, могут отличаться от протоколов, используемых в базовых инфраструктурах. Инфраструктуры локального доступа могут строиться с использованием проводных (т. е. фиксированный доступ) технологий, беспроводных технологий, или на основе их сочетания.

Таким образом, для организации заданного сквозного маршрута данных вызова/сеанса электросвязи в чрезвычайных ситуациях может использоваться широкий диапазон технологий транспортирования.

В следующих ниже пунктах описываются различные характеристики и/или возможности конкретных технологий, которые могут эффективно использоваться для удовлетворения требований электросвязи в чрезвычайных ситуациях.

В связи с тем, что в страте транспортирования возможно применение протокола IP (и ряда связанных с ним протоколов), которые определены IETF, например TCP или UDP, целесообразно использовать для обеспечения электросвязи в чрезвычайных ситуациях, где это применимо, определенные IETF соответствующие возможности. Эти вопросы будут обсуждаться в дальнейших пунктах.

Важно проводить различие между разработкой IETF спецификаций (RFC) и их применением в среде интернет и/или СПП. В обоих случаях, фактически используемые спецификации будут зависеть от того, какая сеть развернута конкретным заинтересованным поставщиком. Однако поскольку среда интернет выходит за пределы сферы применения МСЭ-Т, не могут быть сделаны никакие предположения относительно качества обслуживания или возможностей маршрутов на основе протокола Интернет, описанных в [b-IETF RFC 4190][1]. С другой стороны, более жесткие требования к международной электросвязи в чрезвычайных ситуациях в сетях СПП на основе протокола IP находятся в пределах сферы применения МСЭ-Т и могут быть предложены поставщикам услуг СПП в виде Рекомендаций МСЭ-Т.

В [IETF RFC 4542] описываются возможные решения в отношении "предпочтительного обслуживания в чрезвычайных ситуациях в интернете". Многие методы, изложенные в этом документе, применяются к ETS в среде СПП.

Из этого следует, что в СПП, где страты обслуживания и транспортирования независимы, следующие факторы влияют на успешное обеспечение электросвязи в чрезвычайных ситуациях:

i) идентификация и маркировка трафика электросвязи в чрезвычайных ситуациях;

ii) политика управления допуском;

iii) политика распределения полосы пропускания;

iv) аутентификация и авторизация настоящих пользователей электросвязи в чрезвычайных ситуациях.

8.1.1 Приоритетный режим

В целом, приоритетный режим является основным элементом обеспечения электросвязи в чрезвычайных ситуациях, которая по определению должна считаться более важной, чем обычные услуги электросвязи. Если на предоставление обычных услуг уходит подавляющая часть ограниченных ресурсов сети, то электросвязь в чрезвычайных ситуациях вынуждена конкурировать за те же самые ограниченные ресурсы, что может негативно сказаться на ней. Следовательно, следует разработать какие-то средства предоставления экстренным службам приоритетного режима по сравнению с обычными услугами электросвязи.

В первую очередь, к таким средствам относятся:

a) распознавание и авторизация пользователей электросвязи в чрезвычайных ситуациях;

b) предоставление авторизованным пользователям электросвязи в чрезвычайных ситуациях приоритета в обслуживании.

В уровневой архитектуре СПП, определенной в [ITU-T Y.2012], индикатор приоритета, передаваемый функцией управления обслуживанием (SCF) функции управления ресурсами и допуском (RACF), должен быть способен указывать категории приоритетов, предоставляемых пользователям, с тем чтобы позволить применение различных правил и установление различий между многими видами приоритетных приложений. Например, персоналу больницы может быть предоставлена более низкая категория приоритета пользователя, чем координаторам службы скорой помощи.

---

[1] В [b-IETF RFC 4190] указано, что:

"Постоянной неотъемлемой чертой развития интернета является предоставление наилучшего уровня обслуживания из возможных в качестве модели обслуживания по умолчанию"; и

"взаимодействие между доменами при ETS не должно основываться на повсеместной или даже широко распространенной поддержке по всему маршруту между оконечными точками".

8.1.2 Идентификация, аутентификация и авторизация, а также управление доступом

Необходимо предотвращать неавторизованный доступ к услугам и ресурсам электросвязи в чрезвычайных ситуациях, например, со стороны злоумышленников, маскирующихся под авторизованных пользователей. Следовательно, должны обеспечиваться механизмы и возможности аутентификации пользователей или устройств электросвязи в чрезвычайных ситуациях, либо и тех, и других, в зависимости от случая, а также авторизации доступа, на основе политики, применимой к конкретной службе (например, ETS или TDR).

Необходимо идентифицировать вызов/сеанс электросвязи в чрезвычайных ситуациях (например, с помощью специального набора номера, входных данных, профилей пользователя или подписки). Поставщики услуг СПП должны ускорять аутентификацию авторизованных пользователей электросвязи в чрезвычайных ситуациях. Требуется использовать конкретные механизмы и методы для аутентификации и авторизации, основные на политике, применимой к конкретным видам электросвязи в чрезвычайных ситуациях (например, использовать персональный идентификационный номер (PIN), а также профили пользователя и подписки). После того как пользователь или устройство, либо они оба, аутентифицированы и авторизованы на основе применяемой политики, трафик вызова/сеанса электросвязи в чрезвычайных ситуациях должен быть маркирован и указан в прямом направлении к последующим сетям. Также после прохождения аутентификации и авторизации требуется, чтобы приоритет предоставлялся по всем аспектам вызова/сессии электросвязи в чрезвычайных ситуациях, сигнализации/управлению, трафику несущей и любому применимому управлению.

Необходимо учитывать аутентификацию и авторизацию при эстафетной передаче и при приеме вызовов/сеансов электросвязи в чрезвычайных ситуациях между поставщиками услуг СПП, с учетом наличия многих поставщиков услуг и разделения управления обслуживанием и транспортирования. Аутентификация и авторизация поставщиков услуг СПП для эстафетной передачи и приема вызовов/сеансов и трафика электросвязи в чрезвычайных ситуациях должна основываться на SLA и применимой политике.

8.1.3 Соображения относительно управления допуском для обеспечения более высокой вероятности допуска

Одной из задач функции управления ресурсами и допуском (RACF) является обеспечение управления QoS, включая допуск к ресурсам и резервирование ресурсов, если пожелает поставщик услуги. В связи с этим в периоды высокой потребности в обслуживании со стороны пользователей, в некоторых запросах на обслуживание, возможно, придется отказать. Если такие отказы не происходят, то СПП не может полностью гарантировать качество обслуживания в чрезвычайных ситуациях. Процессы RACF, связанные с QoS, включают в себя авторизацию на основе профилей пользователя, SLA, правил работы оператора сети, приоритета обслуживания и наличия ресурсов для доступа и базовой транспортировки. В настоящей Рекомендации предполагается, что RACF должна иметь возможность установления приоритетов запросов на обслуживание путем использования приоритета обслуживания. (Сеть, которая просто выдает отказ авторизованным запросам вследствие мгновенной перегрузки, обеспечивала бы плохое обслуживание клиентов, неоднократно заставляя их повторно направлять запросы). Таким образом, в настоящей Рекомендации утверждается, что приоритет обслуживания является фактором первостепенной важности, который должен учитываться в методах планирования для принятия решения о распределении ресурсов применительно к допуску с ожиданием/общему допуску. Механизмы, позволяющие реализовать данную функциональную возможность, обсуждаются ниже.

Высокоуровневые требования RACF состоят в работе над авторизованными запросами в отношении QoS с использованием профилей и приоритета пользователя. Одно конкретное требование заключается в том, чтобы при управлении допуском для приоритетной обработки использовалась информация о приоритете обслуживания. Существуют различные методы, которые могут использоваться для приоритета обслуживания при управлении допуском на основе ресурсов.

Один из возможных методов состоит в том, чтобы для трафика электросвязи в чрезвычайных ситуациях использовались более высокие пороги допуска и, таким образом, обеспечивалась возможность некоторого дополнительного допуска для приоритетных запросов, когда обычным запросам выдается отказ. При применении данного метода временно повышается использование ресурсов сети. Однако вследствие большого объема ресурсов СПП и того обстоятельства, что на любом заметном временном интервале некоторые ресурсы, естественно, станут доступными (например, при завершении других сеансов), пропускная способность системы восстановится до

своего установленного рабочего текущего уровня. Более того, если предположить, что объем приоритетного трафика относительно невелик и что сеть редко или почти никогда не работает с полной 100-процентной пропускной способностью, становится очевидно, что более высокий порог решения о допуске для приоритетного трафика не должен создавать никакой угрозы общей работоспособности сети или QoS другого трафика.

Существуют системы управления допуском на основе резервирования, которые разрешают запросы на обслуживание только в том случае, если запрос в отношении требуемой полосы пропускания является успешным. В этом случае в методе обслуживания механизма планирования, в качестве первоочередной задачи, должен учитываться приоритет обслуживания.

В заключение отметим, что возможны также другие способы, позволяющие обойти механизм управления допуском (например, RACF для обхода приоритетным трафиком). Примером такого способа является использование протокола резервирования ресурсов, описанного в [b-IETF RFC RSVP].

8.1.3.1 Управление допуском вызова (CAC)

CAC представляет собой набор действий/правил, применяемых сетью на этапе установления вызова/сеанса, для того чтобы принять или отклонить обслуживание на основе запрашиваемой информации и критериев приоритета, а также наличия необходимых ресурсов.

В традиционной сети КТСОП/ЦСИС управление допуском вызова означает буквально то, что канал либо предоставляется, либо не предоставляется, на основе авторизации. Более того, предоставление канала по определению подразумевает наличие маршрута с требуемой полосой пропускания. В связи с тем что имеется информация о состоянии сети, касающаяся статуса отдельных каналов (речевых каналов), сеть КТСОП/ЦСИС может:

a) направлять экстренные вызовы по специально зарезервированным для экстренного трафика маршрутам (если имеются);

b) дожидаться, пока освободится канал (постановка в очередь).

Поскольку в сетях на основе протокола IP отсутствует информация о состоянии отдельных маршрутов или канала, с помощью лишь аутентификации и авторизации при входе в сеть нельзя гарантировать наличие сквозного маршрута или достаточной сквозной полосы пропускания для данного вызова/сеанса. В сети на основе протокола IP входной сетевой элемент не имеет или почти не имеет сведений о преобладающих состояниях сети за пределами своего домена. Следовательно, CAC во входном сетевом элементе является недостаточным для того, чтобы гарантировать наличие сквозного маршрута, если оно не было расширено с помощью дополнительных средств.

Из этого далее следует, что выходной сетевой элемент никаким образом не управляет удаленным входным сетевым элементом, который может пытаться установить с ним вызов/сеанс, или не имеет об этом элементе никаких сведений. Однако в сетях КТСОП/ЦСИС выходной сетевой элемент способен управлять возможным входным сетевым элементом, который пытается установить вызов/сеанс, с помощью механизмов связанной сигнализации.

В [ITU-T Y.2171] определяется приоритет управления допуском для сигналов услуг электросвязи, добивающихся вхождения в сеть, в частности, в период чрезвычайных ситуаций, когда ресурсы сети могут быть сокращены. В частности, рекомендованы три уровня приоритета управления допуском для сигналов служб, добивающихся вхождения в СПП. Уровень приоритета 1 (наибольший) рекомендован для электросвязи в чрезвычайных ситуациях (включая ETS) по СПП. Трафик с этим уровнем приоритета получает наибольшую гарантию допуска в СПП.

8.2 Страта обслуживания

8.2.1 Общие положения

У стран имеется или они создают ETS для того, чтобы позволять приоритетный режим в отношении авторизованного трафика с целью поддержки операций по оказанию помощи в чрезвычайных ситуациях и при бедствиях в пределах своих национальных границ. Однако могут возникать кризисные ситуации, при которых важно, чтобы пользователь ETS в одной стране мог связаться с доступными пользователями в другой стране. В этом случае важно, чтобы исходящий из какой-либо страны вызов/сеанс ETS получил сквозной приоритетный режим, т. е. приоритетный режим в стране-отправителе и в стране-получателе. Для этого может потребоваться взаимодействие двух реализованных на национальных уровнях ETS по международной сети, в которой либо

предоставляется возможность приоритетного режима, либо обеспечивается прозрачная передача приоритета между обеими странами.

В нижеследующих пунктах описывается ряд механизмов протоколов, используемых для подачи сигнала и получения приоритетного режима на уровне управления обслуживанием в контексте СПП с пакетной коммутацией. Также освещаются конкретные возможности применения этих механизмов протоколов к ETS. Эти возможности, обеспечиваемые протоколами, необходимы для международного применения, в случае осуществления связи между реализованными на национальных уровнях ETS по международной сети (например, взаимодействие двух реализованных на национальных уровнях ETS).

8.2.2 Приоритет ресурсов для SIP

В [IETF RFC 4412] к SIP добавлены два поля заголовков, а именно поле "приоритет ресурса" (Resource-Priority) и поле "принять приоритет ресурса" (Accept-Resource-Priority), а также определяются процедуры их использования. Поле заголовка "приоритет ресурса" может использоваться агентами пользователя SIP, шлюзовыми станциями и оконечным оборудованием коммутируемой телефонной сети общего пользования (КТСОП), а также серверами-посредниками SIP с целью воздействия на обработку ими запросов SIP.

Для того чтобы обеспечить эквивалентность некоторых существующих систем, приоритет, соответствующий нескольким различным "стандартизованным" системам, может быть обозначен путем определения "пространства имен", соответствующего конкретной системе, и количества уровней приоритета в этой системе. Приведенные ниже пространства имен и связанное с ними количество уровней приоритета, предназначенные для использования в ETS, определены в [IETF RFC 4412].

Пространства имен	Уровни
ets	5
wps	5

Все вызовы/сеансы ETS в среде с использованием протокола IP обозначаются с помощью пространства имен "ets", имеющего пять уровней приоритета, с помощью которых на прикладном уровне (в элементах SIP) передается информация о важности. Входящим вызовам/сеансам ETS присваивается обозначение "ets" в заголовке "приоритет ресурса". Вызовы/сеансы ETS распознаются по наличию значения заголовка "приоритет ресурса" в пространстве имен "ets" в сообщении SIP, и им предоставляется "высокий" приоритет для резервирования/присвоения ресурсов, при котором на транспортном уровне может быть установлен предпочтительный режим. Точно так же для выделения вызовов/сеансов может назначаться пространство имен "wps", которому соответствует пять уровней приоритета, в случае если ресурсы ограничены или перегружены, как, например, при радиодоступе в сетях беспроводной связи.

8.2.3 IEPS

В [ITU-T E.106] описываются функциональные требования к международной системе предпочтений при чрезвычайных ситуациях (IEPS), ее свойства, доступ к IEPS и оперативное управление системой. IEPS дает возможность взаимодействия различных систем приоритетов/предпочтений, реализованных на национальном уровне. Тем самым обеспечивается сквозной предпочтительный режим для авторизованных узкополосных голосовых вызов и вызовов для передачи данных.

Сфера применения [ITU-T E.106] сформулирована для случаев КТСОП, ЦСИС или сети сухопутной подвижной связи общего пользования (PLMN). IEPS предоставляет авторизованным пользователям приоритетный режим для службы международной телефонной связи на сетях электросвязи с установлением соединения. Следовательно, на основе двусторонних/многосторонних соглашений между странами/администрациям можно было бы использовать IEPS при таком сценарии для обеспечения взаимодействия реализованных на национальном уровне ETS.

8.2.4 Протоколы управления в системе H.323

В настоящем пункте описываются протоколы, используемые в системе H.323 для обеспечения приоритетной электросвязи.

В [ITU-T H.460.4] определяется обозначение приоритета вызова и идентификация сети страны/международной сети происхождения вызова для приоритетных вызовов в системе H.323.

Параметр для обозначения приоритета вызова в системе H.460.4 поддерживает индикатор приоритетного вызова и пять уровней приоритета.

В [ITU-T H.248.1] определяются протоколы, используемые между элементами физически распределенного мультимедийного шлюза, который применяется в соответствии с архитектурой, указанной в [ITU-T H.323]. Для санкционированных правительством экстренных служб (например, ETS), в [ITU-T H.248.1] определяются индикатор вызова и индикатор приоритета IEPS. В индикаторе вызова IEPS передается указание на приоритет между функциями контроллера и шлюза. В индикаторе приоритета передаются уровни приоритета между функциями контроллера и шлюза. Индикатор приоритета в системы H.248 поддерживает 16 уровней приоритета. Для служб общественной безопасности в [ITU-T H.248.1] определяются индикаторы экстренного вызова для передачи указания на приоритет между функциями контроллера и шлюза.

8.3 Страта транспортирования

8.3.1 Общие положения

В основе необходимости в специальных соглашениях (например, SLA) для обработки сигналов ET в СПП, которая надлежащим образом спроектирована и имеет подходящие размеры, лежит предположение о том, что сетевых ресурсов недостаточно для того объема трафика, который поступает в сеть, и что при таких условиях трафик электросвязи в чрезвычайных ситуациях мог бы оказаться отклоненным либо существенно задержанным и/или прерванным, ниже того уровня, при котором он может использоваться, либо даже его передача могла бы отмениться. В случае если объем принимаемого трафика, предусмотренный в статистической модели или в модели с максимально возможным уровнем обслуживания, превышает пропускную способность данного приемного сетевого элемента (например, IP-маршрутизатора) и/или выходную пропускную способность, которой обладает данный элемент, единственной возможностью, доступной для данного сетевого элемента, является прекращение передачи избыточного трафика. Это означает, что если не разрешены специальные мер предпочтительной обработки, передача трафика электросвязи в чрезвычайных ситуациях была бы прекращена наряду с трафиком, не являющимся трафиком электросвязи в чрезвычайных ситуациях.

В качестве решения иногда предлагаются методы избыточного обеспечения ресурсами. Однако во многих случаях избыточное обеспечение может оказаться невозможным или нецелесообразным. Что еще более важно, некоторые виды чрезвычайных ситуаций могут возникать в результате преднамеренного или случайного разрушения/повреждения участков сети, и, таким образом, исключаются любые пути или элементы с избыточным обеспечением, которые обычно могут быть доступными. Если СПП должна быть в состоянии справиться со всеми видами чрезвычайных ситуаций при неблагоприятных обстоятельствах, то будет необходимо обеспечить наличие конкретных средств для предоставления трафику электросвязи в чрезвычайных ситуациях предпочтительного режима.

В нижеследующих пунктах описывается ряд механизмов, используемых для получения приоритетного режима на транспортном уровне в условиях СПП с пакетной коммутацией.

8.3.2 Управление полосой пропускания с использованием RSVP

Одной из возможных характеристик сети на основе протокола IP, за счет которой обеспечивается определенное (грубое) соответствие распределенной полосе пропускания в сетях с коммутацией каналов, является применение механизма распределения и резервирования полосы пропускания на основе протокола IP. Данный механизм представляет собой процедуру, определенную IETF в своем протоколе резервирования ресурсов (RSVP), который указан в [IETF RFC 2205] и в его обновлениях: [b-IETF RFC 2750], [b-IETF RFC 3936] и [b-IETF RFC 4495].

Определение параметров управления ресурсами, которое необходимо для протокола инициации сеанса (SIP) в страте обслуживания и которое должно использоваться совместно с протоколом RSVP (в страте транспортирования), указано в [IETF RFC 3312]. Данное определение параметров позволяет использовать процедуры сигнализации RSVP до процедуры сигнализации SIP, во время них и/или вместе с ними. Ряд таких примеров приведен в Дополнении A к [IETF RFC 4542]. Однако в [IETF RFC 4542] используется метод преимущественного права.

В [b-IETF RFC RSVP] указываются расширения протокола RSVP, которые могут использоваться, чтобы обеспечивать возможность установления приоритета допуска на сетевом уровне. В этом документе указываются новые расширения протокола RSVP для повышения вероятности завершения вызова без применения преимущественного права. Для выполнения условий "приоритета допуска", который требуется на сети электросвязи в чрезвычайных ситуациях, поддерживающей протокол

RSVP, используются методы проектирования пропускной способности с использованием моделей распределения полосы пропускания. В частности, в настоящем документе указываются два новых элемента политики протокола RSVP, позволяющие передавать информацию о приоритете допуска в сообщениях сигнализации RSVP, с тем чтобы узлы RSVP могли исполнять решения, касающиеся управления выборочным допуском к полосе пропускания, на основе приоритета допуска вызова.

8.3.3 Управление очередностью с использованием дифференцированного обслуживания

В [IETF RFC 4594] излагается рекомендуемое преобразование классов обслуживания в указатели кода дифференцированного обслуживания (DSCP). На рисунке 3 в [IETF RFC 4594] приводится таблица преобразования, в которой для приложений телефонной связи выделяется класс срочной пересылки данных (EF). Это позволяет включать в пакеты протокола IP значения DSCP, выделенные для класса срочной пересылки данных.

Более того, в [ITU-T Y.1541] рекомендуется также, чтобы голосовой трафик в пакетах протокола IP маркировался (помечался) с использованием DSCP, соответствующего срочной пересылке данных. При получении пакетов, маркированных как EF, сетевые элементы (маршрутизаторы) в страте транспортирования обеспечат своевременную доставку трафика, требующего немедленной обработки, по сравнению с трафиком, не требующим немедленной обработки, с использованием правил срочной пересылки данных, которые определены для указателя кода EF и описаны в [IETF RFC 3246].

Однако код EF используется для обычного телефонного трафика. Следовательно, по-прежнему может существовать необходимость в том, чтобы каким-то образом различать трафик телефонной связи в чрезвычайных ситуациях от трафика, не являющегося трафиком телефонной связи в чрезвычайных ситуациях (см. следующий пункт).

8.3.4 EF DSCP для трафика, имеющего допуск к пропускной способности

В [b-IETF RFC DSCP] осуществляется распределение EF DSCP для трафика, имеющего допуск к пропускной способности. Это дает возможность передавать трафик в реальном времени, соответствующий правилам поведения на каждом шаге при срочной пересылке данных, с использованием процедуры CAC, которая предусматривает аутентификацию, авторизацию и допуск к пропускной способности (см. пп. 8.3.1 и 8.3.2, выше), в отличие от класса трафика в реальном времени, соответствующего поведению на каждом шаге при срочной пересылке данных, к которому не применяется допуск к пропускной способности.

Предлагается, чтобы запрашиваемый указатель имел название EF-ADMIT и чтобы ему присваивалось соответствующее значение.

8.4 Доступ к СПП

8.4.1 Общие положения

Существует много методов доступа к СПП, зависящих от технологии. В соответствии с [ITU-T Y.2012] сеть доступа включает функции, зависящие от сочетания метода доступа и технологии. Например, для технологии W-CDMA и доступа по xDSL. В зависимости от технологии, используемой для доступа к услугам СПП, сеть доступа включает функции, относящиеся к:

1) кабельному доступу;
2) доступу по xDSL;
3) беспроводному доступу (например, с использованием технологий IEEE 802.11 и 802.16, а также доступа по 3G RAN);
4) оптическому доступу.

Для обеспечения электросвязи в чрезвычайных ситуациях в сегменте доступа к СПП также необходимы специальные соглашения. В основе необходимости в специальных соглашениях лежит допущение о том, что ресурсы доступа ограничены точно так же, как и ресурсы базовой сети. Следовательно, в зависимости от объема трафика, который поступает в сегмент сети доступа, на трафик электросвязи в чрезвычайных ситуациях могло бы быть оказано воздействие (например, он мог бы оказаться отклоненным либо существенно задержанным и/или прерванным, ниже того уровня, при котором он может использоваться, либо даже его передача могла бы отмениться).

Следовательно, если СПП должна быть в состоянии справиться со всеми видами чрезвычайных ситуаций при неблагоприятных обстоятельствах, в сегменте доступа СПП должно быть обеспечено

наличие конкретных средств для предоставления трафику электросвязи в чрезвычайных ситуациях предпочтительного режима. Это включает в себя, помимо прочего, механизмы и возможности для:

- распознавания трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного доступа к ресурсам/средствам;
- предпочтительной/приоритетной маршрутизации трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного установления сеансов/вызовов электросвязи в чрезвычайных ситуациях.

8.4.2 Беспроводной радиодоступ

Требуется, чтобы сети беспроводного радиодоступа обеспечивали конкретные механизмы и возможности предоставления авторизованным сеансам/вызовам электросвязи в чрезвычайных ситуациях предпочтительного/приоритетного режима. Для предоставления такого режима могут использоваться механизмы и возможности, зависящие от технологии. Это включает в себя, помимо прочего, механизмы и возможности для:

- распознавания трафика электросвязи в чрезвычайных ситуациях: такое распознавание включает идентификацию и маркировку авторизованного трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного доступа к ресурсам/средствам: это облегчает доставку в СПП запроса на электросвязь в чрезвычайных ситуациях, если имеющиеся ресурсы доступа ограничены;
- предпочтительной/приоритетной маршрутизации трафика электросвязи в чрезвычайных ситуациях: это может предполагать такие свойства, как постановку в очередь на имеющиеся ресурсы, исключение из определенных ограничительных функций управления сетью и резервирование некоторых маршрутов/путей для трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного установления сеансов/вызовов электросвязи в чрезвычайных ситуациях.

Например, в стандарте 3GPP определяется приоритетное обслуживание или приоритетное обслуживание мультимедийного трафика в системах 3GPP. Приоритетное обслуживание и приоритетное обслуживание мультимедийного трафика позволяет авторизованным пользователям получать приоритетный доступ к ближайшим имеющимся радиоканалам (для голосового трафика или трафика данных) по сравнению с другими пользователями в ситуациях, когда перегрузка приводит к блокированию попыток вызова. При приоритетном обслуживании поддерживается приоритетное прохождение и завершение вызова, обеспечивающее "сквозной" приоритетный вызов между сетями подвижной связи, между сетями подвижной и фиксированной связи и между сетями фиксированной и подвижной связи. При приоритетном обслуживании мультимедийного трафика обеспечивается приоритетное прохождение и завершение мультимедийных сеансов, обеспечивающее "сквозные" приоритетные мультимедийные сеансы, в том числе между сетями подвижной связи, между сетями подвижной и фиксированной связи и между сетями фиксированной и подвижной связи. Приоритетное обслуживание и приоритетное обслуживание мультимедийного трафика в системах 3GPP описано в [b-3GPP TS 22.153].

Так же как и в 3GPP, в стандарте 3GPP2 определяется приоритетное обслуживание мультимедийного трафика (MMPS) для систем 3GPP2. Спецификация 3GPP2 для MMPS содержится в [b-3GPP2 S.R0117-0-v1.0].

8.4.3 Фиксированный доступ

Требуется, чтобы сети фиксированного доступа обеспечивали конкретные механизмы и возможности предоставления авторизованным вызовам/сеансам электросвязи в чрезвычайных ситуациях предпочтительного/приоритетного режима. Для предоставления такого режима могут использоваться механизмы и возможности, зависящие от технологии (например, 802.1p с xDSL, IPCablecom, Packet Cable 2). Это включает в себя, помимо прочего, механизмы и возможности для:

- распознавания трафика электросвязи в чрезвычайных ситуациях: такое распознавание включает идентификацию и маркировку авторизованного трафика электросвязи в чрезвычайных ситуациях;

- предпочтительного/приоритетного доступа к ресурсам/средствам: это облегчает доставку в СПП запроса на электросвязь в чрезвычайных ситуациях, если имеющиеся ресурсы доступа ограничены;
- предпочтительной/приоритетной маршрутизации трафика электросвязи в чрезвычайных ситуациях: это может предполагать такие свойства, как постановку в очередь на имеющиеся ресурсы, исключение из определенных ограничительных функций управления сетью и резервирование некоторых маршрутов/путей для трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного установления сеансов/вызовов электросвязи в чрезвычайных ситуациях.

Например, в [ITU-T J.260] определяются требования для предпочтительной электросвязи по сетям IPCablecom. Существенные аспекты предпочтительной электросвязи по сетям IPCablecom, содержащиеся в [ITU-T J.260], группируются по двум направлениям: установление приоритета и аутентификация. Эти два направления включают возможности обеспечения электросвязи в IPCablecom, для которой может потребоваться предпочтительный режим (например, TDR и ETS). Реализация приоритета и аутентификации необходима для обеспечения предпочтительной электросвязи в сетях IPCablecom.

9 Механизмы и возможности для обеспечения некоторых аспектов раннего предупреждения в СПП

9.1 Общие положения

Системы оповещения, используемые для раннего предупреждения, можно отнести к моделям двух классов: с принудительным оповещением и с оповещением по запросу.

Модели с принудительным оповещением основаны на регистрации контактной информации участников (например, адресов электронной почты) в центральной службе. Когда происходит событие, эти зарегистрированные участники оповещаются о нем с потенциально большим числом указателей на дополнительную информацию. Ключевым элементом проекта архитектуры в данной модели является то, что центральный орган определяет вопрос о том, должна ли распространяться данная информация, и что это повлечет за собой. Сильной стороной данной модели является то, что в ней решается вопрос о выполнении работы, связанной с мониторингом событий, и, таким образом, пользователи имеют возможность продолжать выполнять свои обычные обязанности и не заниматься мониторингом потенциальных бедствий и чрезвычайных ситуаций.

Модель с принудительным оповещением представляет собой механизм распространения от "одного" ко "многим", и она может быть реализована как в страте обслуживания, так и в страте транспортирования (например, многоадресная передача).

Отличие модели с оповещением по запросу от модели с принудительным оповещением состоит в том, что она основана на обмене информацией по принципу запрос-ответ. В то время как обе модели основаны на регистрации со стороны отдельных участников, в модели с оповещением по запросу ответственность за мониторинг и получение информации возлагается на отдельных пользователей. Преимуществом данной системы является то, что информация предоставляется исключительно по мере необходимости или по запросу.

В заключение следует отметить, что в системах оповещения используются существующие приложения и основополагающие возможности, присущие сетям на основе протокола IP. Добавление принципов принудительного оповещения или оповещения по запросу помогает сделать эти системы более приспособленными к потребностям и ожиданиям пользователей. Применение каждого из видов систем оповещения может также осуществляться в тандеме: модели с принудительным оповещением могут осуществлять периодический автоматический мониторинг и уведомление, а модели с оповещением по запросу могут использоваться для получения конкретной информации по запросу.

Примеры моделей с принудительным оповещением и с оповещением по запросу приведены в Дополнении II.

9.2 Протокол общего оповещения (CAP)

В данном пункте описывается протокол общего оповещения (CAP), определенный в [ITU-T X.1303], который может использоваться для обеспечения приложений раннего предупреждения.

В [ITU-T X.1303] определяется общий формат для обмена оповещениями о чрезвычайной ситуации и предупреждения населения обо всех видах угроз по всем типам сетей. CAP позволяет одновременно распространять предупреждающие сообщения по многим различным системам предупреждения и таким образом повысить эффективность предупреждения, упростив при этом задачу по предупреждению. CAP также способствует обнаружению на основе местных предупреждающих сообщения различного типа такого варианта развития событий, который может указывать на скрытую угрозу или враждебное действие. CAP также обеспечивает шаблон для эффективных предупреждающих сообщений на основе передового опыта, полученного из научного исследования и реальных событий.

CAP обеспечивает открытый непатентованный формат сообщения для всех типов оповещений и уведомлений. Он не относится ни к какому конкретному приложению или методу электросвязи. Формат CAP совместим с новыми методами, например веб-службами и ускоренными веб-службами МСЭ-Т, а также с существующими форматами, включая кодирование сообщений для конкретной территории (SAME), которое используется Национальным управлением океанических и атмосферных исследований (NOAA) Соединенных Штатов Америки для системы метеорологической радиосвязи и системы оповещения о чрезвычайных ситуациях (EAS), и при этом предоставляет следующие усовершенствованные возможности:

- гибкое географическое позиционирование с использованием широтно-долготных профилей и других трехмерных геопространственных изображений;
- передачу многоязычных сообщений и сообщений, рассчитанных на многочисленную аудиторию;
- распределение и задержку эффективного времени действия и истечения времени действия;
- усовершенствованные характеристики обновления и отмены сообщений;
- поддержку шаблонов для формирования полных и эффективных предупреждающих сообщений;
- поддержку возможности цифрового шифрования и цифровой подписи; а также
- средство для передачи цифровых изображений и звука.

CAP обеспечивает снижение затрат и простоту эксплуатации путем устранения необходимости в многочисленных интерфейсах на основе заказного программного обеспечения, используемых для многих источников предупреждения и систем распространения, задействованных в предупреждении обо всех видах угроз. Формат сообщения CAP можно преобразовать в прямом и обратном направлении для "родных" форматов всех видов датчиков и методов оповещения и тем самым создать основу для независимого в технологическом отношении национального и международного "предупреждающего интернета".

Протокол CAP, определенный в [ITU-T X.1303], технически соответствует общему протоколу оповещения OASIS стандарта V1.1 и совместим с ним. В [ITU-T X.1303] представлена соответствующая спецификация ASN.1, которая допускает компактное двоичное кодирование и использование ASN.1, а также средств определения схемы XML (XSD) для создания и обработки сообщений CAP. [ITU-T X.1303] обеспечивает для существующих систем, например систем H.323, возможность более простого кодирования, транспортировки и декодирования сообщений CAP.

10 Приоритет восстановления обслуживания

В случае отказа или нарушения работы сети работа критических служб (например, экстренных служб) может быть прервана, и, возможно, для нее потребуется более высокая вероятность успешного восстановления по сравнению с другими службами. В [ITU-T Y.2172] определяется три уровня приоритета восстановления для служб СПП. Это позволяет установить такую классификацию приоритетов, используемых в сигнальных сообщениях, при которой для рассматриваемого вида обслуживания может быть предоставлено установление вызова/сеанса с желаемым приоритетом восстановления. Таким образом, критическим службам будет обеспечена более высокая вероятность успешного восстановления по сравнению с другими службами.

11 Безопасность

Сетевые элементы, системы, ресурсы, данные и службы, используемые для обеспечения электросвязи в чрезвычайных ситуациях, могут подвергаться кибератакам. Целостность, конфиденциальность и

доступность электросвязи в чрезвычайных ситуациях, особенно в случае атаки, будет зависеть от сетевых средств защиты и практических мер безопасности, реализованных в СПП, а также от возможностей в области обеспечения безопасности (например, функций аутентификации и авторизации), которые выполняются в рамках прикладной услуги для электросвязи в чрезвычайных ситуациях. Общие руководящие указания для рассмотрения вопросов планирования безопасности в области электросвязи в чрезвычайных ситуациях включают, помимо прочего, следующее:

- Все аспекты электросвязи в чрезвычайных ситуациях, включая сигнализацию и контроль, канал передачи/среду, а также данные и информацию, касающиеся управления (например, информация о профиле пользователя) требуется защищать от угроз безопасности. Угрозы безопасности электросвязи в чрезвычайных ситуациях могут возникать на разных уровнях (например, транспорт, управление обслуживанием, обеспечение обслуживания) и в различных сетевых сегментах (например, доступ, базовая сеть и межсетевые интерфейсы).
- Установление и обеспечение выполнения стратегии и практики в области безопасности, характерных для услуг электросвязи в чрезвычайных ситуациях. Следует определить и реализовать возможности ослабления влияния для обеспечения защиты от различных угроз безопасности. Конкретно, для услуг электросвязи в чрезвычайных ситуациях следует определить и реализовать возможности ослабления влияния и практические меры безопасности, помимо тех, которые требуются для общих прикладных услуг. К ним относятся стратегия безопасности для защиты данных управления и накопленной информации (например, информации о профиле пользователя), относящихся к электросвязи в чрезвычайных ситуациях.
- Реализация и применение процедур для аутентификации и авторизации пользователей, устройств, с тем чтобы обеспечить защиту от неавторизованного доступа к услугам, ресурсам и информации (например, информации пользователей в серверах аутентификации и системах управления), относящимся к электросвязи в чрезвычайных ситуациях. Например, следует реализовать функции аутентификации и авторизации, чтобы не допустить использования неавторизованными пользователями ресурсов, выделенных для электросвязи в чрезвычайных ситуациях, и предотвратить атаки типа отказ в обслуживании (DoS) и другие виды атак.
- Ответственность в рамках каждой сети за безопасность сообщений в пределах своего домена, которые пересекают множество доменов поставщиков сетевых услуг, для того чтобы можно было обеспечить безопасность сквозной передачи. В связи с тем что при электросвязи в чрезвычайных ситуациях могут использоваться сообщения, которые пересекают различные домены поставщиков сетевых услуг на национальных и международных сетях (т. е. страны/администрации), требуется установить и реализовать стратегию безопасности, доверительные отношения, методы и процедуры идентификации трафика электросвязи в чрезвычайных ситуациях, управление идентичностью и аутентификацию пользователей и сетей в пределах многих доменов административного управления сетью.

При планировании безопасности электросвязи в чрезвычайных ситуациях следует учитывать рекомендации по безопасности СПП, содержащиеся в [ITU-T Y.2701]. Кроме того, следует также учитывать концепцию безопасности, в основе которой лежат следующие сферы деятельности в области безопасности, которые определены в [ITU-T X.805]:

- управление доступом;
- аутентификация;
- неотказуемость;
- конфиденциальность данных;
- безопасность связи;
- целостность данных;
- готовность;
- секретность.

Дополнение I

Категории электросвязи в чрезвычайных ситуациях

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Электросвязь в чрезвычайных ситуациях между отдельным лицом и органом власти

Инициатором электросвязи между отдельным лицом и органом власти выступает отдельное лицо, использующее обычные возможностей электросвязи в чрезвычайных ситуациях, с целью получения экстренной помощи во время отдельной (относящейся лично к нему) чрезвычайной ситуации либо даже ограниченной чрезвычайной ситуации. Например, вызов от отдельного лица к органу власти может осуществляться с использованием короткого набираемого номера (например, 112, 911 и т. д.), который обеспечивает соединение отдельного пользователя с центром обработки экстренных вызовов. Центр может передать сообщение соответствующей организации-исполнителю (полиции, пожарной службе, службе скорой медицинской помощи) от имени вызывающего абонента. В центр обслуживания вызовов может автоматически передаваться дополнительная информация, например о местонахождении вызывающего абонента. Такая информация может облегчить и даже обеспечить более быстрое реагирование, поскольку иногда вызывающие абоненты не могут либо не имеют времени или возможности предоставить эту информацию самостоятельно. Такой вид связи обычно подразумевает соединение по принципу от одного к одному, при котором инициатор взаимодействует главным образом с ведомством назначения. Подавляющее большинство таких вызовов электросвязи касается небольших по масштабу чрезвычайных ситуаций (например, пожар в отдельном доме), возникших преимущественно вследствие несвязанных событий, в то время как крупномасштабные события (например, землетрясения) могут привести ко многим одновременно связанным последствиям. (Выражение "отдельный" используется в широком смысле и должен распространяться на любое лицо, которому требуется экстренная помощь, включая, например, граждан, приезжих и других, живущих в конкретном месте). Стороны, участвующие в электросвязи в чрезвычайных ситуациях, могут общаться друг с другом с помощью многих видов средств, включая передачу голоса, изображения, текста в реальном времени и мгновенной передачи сообщений.

I.2 Электросвязь в чрезвычайных ситуациях между отдельными лицами

Инициаторами категории электросвязи в чрезвычайных ситуациях между отдельными лицами становятся и отдельные лица (или устройства) из числа граждан, и организации. Например, сразу после того как происходит чрезвычайная ситуация, потребность граждан в общении друг с другом становится высокой. Следовательно, возникает повышенный спрос на электросвязь между отдельными лицами. В то же время ресурсы электросвязи могут быть ограничены в результате повреждений, причиненных чрезвычайными событиями. С учетом всех этих факторов сети электросвязи могут оказаться перегруженными.

I.3 Электросвязь в чрезвычайных ситуациях между органами власти

Электросвязь в чрезвычайных ситуациях между органами власти обычно осуществляется с участием авторизованного пользователя электросвязи в чрезвычайных ситуациях (или его организации), который инициирует взаимодействие с другим авторизованным пользователем, с тем чтобы:

1) содействовать проведению восстановительных работ (например, путем создания центров управления в чрезвычайных ситуациях и соответствующих органов административного управления для получения от правительства и/или других организаций помощи в виде ресурсов);

2) восстановить основную коммунальную инфраструктуру (например, необходимое водоснабжение, подачу электроэнергии и т. д.); и

3) приступить к выполнению мер по обеспечению долгосрочного полного восстановления (например, восстановления дорог, мостов, зданий и т. д.).

Исторически сложилось, что электросвязь в чрезвычайных ситуациях между органами власти (иногда называемая электросвязью в целях общественной безопасности) с одновременным задействованием сетей общего пользования осуществлялась в случае, когда ресурсы электросвязи оказывались перегруженными в связи с увеличением использования электросвязи между отдельными пользователями.

Учитывая огромные возможности электросвязи в чрезвычайных ситуациях между органами власти для содействия восстановлению нормального состояния и недопущения дальнейших угроз гражданам или имуществу, данной категории электросвязи в чрезвычайных ситуациях может быть предоставлен приоритетный статус над другими категориями электросвязи в чрезвычайных ситуациях во время объявленных чрезвычайных ситуаций или при их обострении.

I.4 Электросвязь в чрезвычайных ситуациях между органом власти и отдельным лицом

В заключение рассмотрим электросвязь в чрезвычайных ситуациях между органом власти и отдельным лицом (относимую иногда к категории систем раннего предупреждения), обычно предполагающую передачу информации, которая предназначена для населения и которая поступает из авторизованного источника. Содержание может нести информацию, которая предназначена для общин, пострадавших в результате бедствия, например меры безопасности, инструкции, руководящие указания, советы и т. д. Обычно инициатором конкретного вызова электросвязи выступает один авторизованный пользователь, при этом получателями информации являются многие отдельные лица.

Связь любого с любым: пример ETS из любого места/от любого устройства для вхождения в контакт с любым другим пользователем (ETS или гражданами) с помощью некоторых мер обеспечения предпочтительного режима со стороны инфраструктуры связи. Хорошим примером является служба GETS в КТСОП, в случае если предпочтительное обслуживание не является повсеместно распространенным и не ограничено выборочным набором оконечных устройств и адресатов.

Связь одного с одним: применительно к электросвязи в чрезвычайных ситуациях данный вид связи является разновидностью случая связи любого с любым. В данном случае число участников ограничено любыми двумя пользователями ETS.

Связь многих с одним: одним из вариантов реализации данной модели является архитектура клиент-сервер для услуги на базе веб, при которой любой из пользователей имеет доступ к одному хорошо известному месту размещения информации. В КТСОП данная модель реализуется с помощью систем 911, 112 и т. д., при которых сеансы в пределах района передаются в один пункт общего доступа к услуге (PSAP).

Связь одного со многими: в данной модели информация передается из одного источника группе приемников (конечных пользователей), избранных для участия в распространении данных. В случае вещательной среды передачи, прекрасными примерами являются телевидение и радио, поскольку приемники лишь получают информацию по выбранному ими каналу. В модели с передачей данных можно провести различие между связью одного со многими и широковещательной передачей, поскольку широковещательная передача подразумевает, что сообщение получают все узлы, независимо от того, выбраны они или нет, в то время как при связи каждого с каждым предполагается непосредственное участие в группе.

Дополнение II

Пример случаев использования систем оповещения для раннего предупреждения

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

II.1 Модель с принудительным оповещением

Системы оповещения на основе модели с принудительным оповещением предлагаются как частным, так и государственным секторами. Однако в настоящей Рекомендации рассматривается только пример государственного сектора. Примером модели с принудительным оповещением для государственного сектора является центр информации о чрезвычайных ситуациях (http://alert.dc.gov/eic/site/default.asp), открытый местными органами властями г. Вашингтон (округ Колумбия). пользователи указывают при регистрации контактную информацию, включающую адрес электронной почты, номер пейджера или мобильного телефона (либо текстовое сообщение, либо автоматизированная передача голосовых сообщений). Автоматизированная передача голосовых сообщений эквивалентна передаче сообщений "inverse-911", и все жители округа Колумбия, подключенные с соответствующими станциями проводной телефонной связи, автоматически зарегистрированы в этой службе. Поскольку услуга оповещения предоставляется по электронной почте и пейджеру, она не ограничена только для жителей г. Вашингтон.

II.2 Модель с оповещением по запросу

Наилучшим примером модели по запросу, работающей через Интернет, является японский проект I-AM-Alive (http://www.isoc.org/inet2000/cdproceedings/8l/8l_3.htm, http://www.iaa-alliance.net/en/). Деятельность в рамках проекта I-AM-Alive началась после землетрясения в г. Кобе в 1995 году с целью предоставить населению возможность определения состояния и возможного места нахождения своих близких, пострадавших в результате землетрясения. Эта система работает как центр сбора информации для служб экстренного реагирования и хранит информацию, которую эти службы получили. И наоборот, эта система работает также как центр распространения информации, в котором друзья и родственники могут узнать, не пострадали ли знакомые им люди в результате бедствия.

В системе I-AM-Alive используется сочетание входных данных, получаемых по факсу, по телефону и из веб-сети, для накопления информации, размещенной отдельными лицами или службами экстренного реагирования. Последующее распространение информации осуществляется, в основном, в виде веб-страниц, однако некоторую информацию можно получить по хорошо известным телефонным номерам, относящимся к этой системе.

Библиография

[b-3GPP TS 22.153] 3GPP TS 22.153 (06/2008), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Priority Service (Release 9).* <http://www.3gpp.org/FTP/Specs/html-info/22153.htm>

[b-3GPP2 S.R0117-0-v1.0] 3GPP2 S.R0117-0-v1.0 (06/2006), *3rd Generation Partnership Project 2; Multimedia Priority Service (MMPS) for MMD-based Networks – Stage 1 Requirements.* <http://www.3gpp2.org/Public_html/specs/S.R0117-0%20v1.0_060714.pdf>

[b-IETF RFC 2750] IETF RFC 2750 (2000), *RSVP Extensions for Policy Control.* <http://www.ietf.org/rfc/rfc2750.txt?number=2750>

[b-IETF RFC 3265] IETF RFC 3265 (2002), (*SIP)-Specific Event Notification.* <http://www.ietf.org/rfc/rfc3265.txt?number=3265>

[b-IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP).* <http://www.ietf.org/rfc/rfc3853.txt?number=3853>

[b-IETF RFC 3936] IETF RFC 3936 (2004), *Procedures for Modifying the Resource reSerVation Protocol (RSVP).* <http://www.ietf.org/rfc/rfc3936.txt?number=3936>

[b-IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework.* <http://www.ietf.org/rfc/rfc4032.txt?number=4032>

[b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony.* <http://www.ietf.org/rfc/rfc4190.txt?number=4190>

[b-IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction.* <http://www.ietf.org/rfc/rfc4320.txt?number=4320>

[b-IETF RFC 4495] IETF RFC 4495 (2006), *A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow.* <http://www.ietf.org/rfc/rfc4495.txt?number=4495>

[b-IETF RFC 4916] IETF RFC 4916 (2007), *Connected Identity in Session Initiation Protocol.* <http://www.ietf.org/rfc/rfc4916.txt?number=4916>

[b-IETF RFC 5027] IETF RFC 5027 (2007), *Security Preconditions for Session Description Protocol (SDP) Media Streams.* <http://www.ietf.org/rfc/rfc5027.txt?number=5027>

[b-IETF RFC DSCP] draft-ietf-tsvwg-admitted-realtime-dscp-00, *DSCP for Capacity-Admitted Traffic*.

[b-IETF RFC RSVP] draft-ietf-tsvwg-emergency-rsvp, *Resource ReSerVation Protocol (RSVP) Extensions for Emergency Services*.

[b-UN Global Survey] United Nations/International Strategy for Disaster Reduction, *Final Report on a "Global Survey of Early Warning Systems",* September 2006. (Reference: <http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf)>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	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	Качество телефонной передачи, телефонные установки, сети местных линий
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

Отпечатано в Швейцарии
Женева, 2010 г.