Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2705

(03/2013)

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

Сети последующих поколений – Безопасность

Минимальные требования по безопасности при присоединении службы электросвязи в чрезвычайных ситуациях (ETS)

Рекомендация МСЭ-Т Y.2705

ITU-T

Международный союз электросвязи

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: 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
Будущие 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 Y.2705

Минимальные требования по безопасности при присоединении службы электросвязи в чрезвычайных ситуациях (ETS)

Резюме

Служба электросвязи в чрезвычайных ситуациях (ETS) – это национальная служба, предоставляющая приоритетные услуги связи санкционированным пользователям ETS в периоды бедствий и чрезвычайных ситуаций. В Рекомендации МСЭ-Т Y.2705 представлены минимальные требования по безопасности для межсетевых соединений ETS. Это позволит обеспечить необходимый уровень безопасности при присоединении ETS к различным национальным сетям стран, заключивших двусторонние и/или многосторонние соглашения, в периоды бедствий и чрезвычайных ситуаций.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2705	01.03.2013 г.	13-я

Ключевые слова

Служба электросвязи в чрезвычайных ситуациях (ETS), безопасность СПП, приоритетные услуги и функциональные возможности.

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

Служба электросвязи в чрезвычайных ситуациях (ETS) – это национальная служба, предоставляющая приоритетные услуги связи санкционированным пользователям ETS в периоды бедствий и чрезвычайных ситуаций. Вопросы введения в действие службы ETS решаются на национальном уровне. Однако масштабы бедствий и чрезвычайных ситуаций могут выходить за пределы географических границ, и, следовательно, существует потенциальная возможность для стран/администраций вступать в двусторонние и/или многосторонние соглашения для подключения своих соответствующих систем ETS. Это позволит обеспечить поддержку приоритетных услуг связи (например, голосовую связь, передачу сообщений, видеосвязь и передачу данных) под эгидой ETS между различными национальными сетями стран, заключивших двусторонние или многосторонние соглашения в периоды бедствий или чрезвычайных ситуаций.

Целостность, конфиденциальность и готовность службы ETS между присоединенными национальными сетями будет зависеть от безопасности каждой национальной сети, входящей в состав сквозной системы связи. Для обеспечения сетевой безопасности сквозной ETS между различными национальными сетями (т. е. странами/администрациями) необходимо определить требования по безопасности при присоединении службы ETS.

Рекомендация МСЭ-Т Y.2705

Минимальные требования по безопасности при присоединении службы электросвязи в чрезвычайных ситуациях (ETS)

1 Сфера применения

В настоящей Рекомендации приводятся минимальные требования по безопасности для межсетевого присоединения ETS. Сфера применения требований по безопасности включает защиту целостности, конфиденциальности и готовности линий связи ETS через границы сетей (т. е. между различными национальными сетями).

Целью настоящей Рекомендации является предоставление минимального набора требований по безопасности, которые могут быть использованы для обеспечения поддержки ETS в сетях, присоединенных прямым или косвенным образом.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы 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 справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. 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 M.3342] Рекомендация МСЭ-Т M.3342 (2006 г.), *Указания по определению шаблонов представления SLA*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

[ITU-T Y.2205] Рекомендация МСЭ-Т Y.2205 (2011 г.), *Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 авторизация (authorization) [b-ITU-T X.800]: Предоставление прав, которые включают предоставление доступа на основании прав доступа.

3.1.2 готовность (availability) [b-ITU-T X.800]: Свойство быть доступным и годным к эксплуатации по запросу уполномоченного объекта.

3.1.3 конфиденциальность (confidentiality) [b-ITU-T X.800]: Свойство, которое предотвращает раскрытие информации отдельными лицами, объектами или процессами, не имеющими разрешения на это.

3.1.4 целостность данных (data integrity) [b-ITU-T X.800]: Показатель того, что данные не были изменены или разрушены несанкционированным образом.

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

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин:

3.2.1 Поставщик услуг: Поставщик услуг (с большой буквы) – поставщик услуг электросвязи общего пользования, уполномоченный оказывать услуги службы электросвязи в чрезвычайных ситуациях (ETS).

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ANI	Application Network Interface	Интерфейс "приложение-сеть"
CVE	Common Vulnerabilities and Exposures	Общеизвестные уязвимости и незащищенности
CVE	Common Vulnerability and Exposure	Общеизвестная уязвимость и незащищенность
CVSS	Common Vulnerability Scoring System	Система оценки общеизвестных уязвимостей
CWE	Common Weakness Enumeration	Перечень общеизвестных слабых мест
CYBEX	Cybersecurity Information Exchange	Обмен информацией о кибербезопасности
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DNS	Domain Name Server	Сервер наименований доменов
DoS	Denial of Service	Отказ в обслуживании
DSCP	Diffserv Code Point	Кодовая точка Diffserv
ETS	Emergency Telecommunications Service	Служба электросвязи в чрезвычайных ситуациях
IDS	Intrusion Detection System	Система обнаружения вторжений
IEPS	International Emergency Preference Scheme	Международная схема приоритетов в случае чрезвычайных ситуаций
IP	Internet Protocol	Интернет-протокол
IPS	Intrusion Prevention System	Система предотвращения вторжений
IPsec	IP Security	Безопасность IP
LAN	Local Area Network	ЛВС Локальная вычислительная сеть
NE	Network Element	Элемент сети
NGN	Next Generation Network	СПП Сети последующих поколений
NNI	Network-Network Interface	Интерфейс "сеть-сеть"
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PSTN	Public Switch Telephone Network	КТСОП Коммутируемая телефонная сеть общего пользования
QoS	Quality of Service	Качество обслуживания
SLA	Service Level Agreement	Соглашение об уровне обслуживания
SNI	Service Network Interface	Интерфейс "служба-сеть"
UNI	User Network Interface	Интерфейс "пользователь-сеть"

5 Соглашения

В настоящей Рекомендации:

Выражение "Поставщик услуг" начинается с прописной буквы в этой Рекомендации в том случае, если оно относится к поставщику услуг электросвязи общего пользования, который уполномочен оказывать услуги ETS (см. пункт 3.2.1).

Ключевые слова "требуется, для того чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии данному документу.

Ключевое слово "рекомендуется" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии данному документу это требование не является обязательным.

Ключевое слово "запрещается" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии данному документу.

Ключевые слова "может предоставляться дополнительно" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Этот термин не означает, что система, предоставляемая для реализации поставщиком, должна обеспечивать выполнение данной функции и что эта функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может дополнительно предоставить данную функцию, по-прежнему заявляя о соответствующей конкретной спецификации.

В тексте настоящей Рекомендации и ее приложениях иногда встречаются слова "должен", "не должен", "следует" и "может". В этом случае их следует соответственно понимать как "требуется, для того чтобы", "запрещается", "рекомендуется" и "может предоставляться дополнительно". Появление таких фраз или ключевых слов в дополнении или материалах, явным образом помеченных как информативные, должно пониматься, как не несущее нормативного смысла.

6 Угрозы безопасности и риски

Линии связи ETS могут становиться объектами кибератак в силу уязвимого характера линий связи. Определения и конкретная информация по ETS приведены в [ITU-T E.107], [ITU-T Y.2205] и [b-ITU-T Q-Sup.57]. Угрозы или злонамеренные действия, направленные на разрушение, неправильное применение, использование в корыстных целях или нанесение вреда ETS другими способами, могут исходить из множества источников, включая присоединенные сети. В качестве примера, кибератаки в отношении ETS могут проводиться в следующих целях:

- дезорганизация нормальной работы персонала, выполняющего восстановительные работы при бедствиях, в плане осуществления связи;
- получение секретной информации путем перехвата вызовов сеансов связи службы ETS.

Угроза в данном случае рассматривается в качестве слабой стороны или потенциальной уязвимости системы безопасности, способной, в случае если ею воспользуются, отрицательно повлиять на готовность, целостность или конфиденциальность линий связи ETS.

Настоящая Рекомендация в основном посвящена угрозам, источником которых является присоединение ETS к различным сетям. Примеры угроз, относящихся к сетевым соединениям, включают, в том числе:

- основную угрозу сетевым соединениям: слабые места систем безопасности или потенциальные уязвимости, связанные с подключением сетей (например, СПП) к другим управляемым и неуправляемым сетям, таким как интернет общего пользования;
- угрозу при разработке и введение в действие: слабые места систем безопасности или потенциальные уязвимости в разработках архитектуры сетевых соединений и введении в действие готовых проектов;
- угрозы, возникающие при управлении, эксплуатации и воздействии внутренних нарушителей: слабые места систем безопасности или потенциальные уязвимости в органах руководства и управления служб ETS и их подчиненных инфраструктурах;

- угрозы для транспортировки данных и для оборудования: слабые места систем безопасности или потенциальные уязвимости, связанные с используемой транспортной сетью (например, маршрутизация, дублирование сети, разветвленность, отказоустойчивость), системами обеспечения (например, электропитание, внешняя среда) и физической защитой сетевого оборудования.

7 Эталонная архитектура для безопасности присоединения службы ETS

Настоящая Рекомендация опирается на функциональную архитектуру и модель сетевых соединений, определенные в [ITU-T Y.2012].

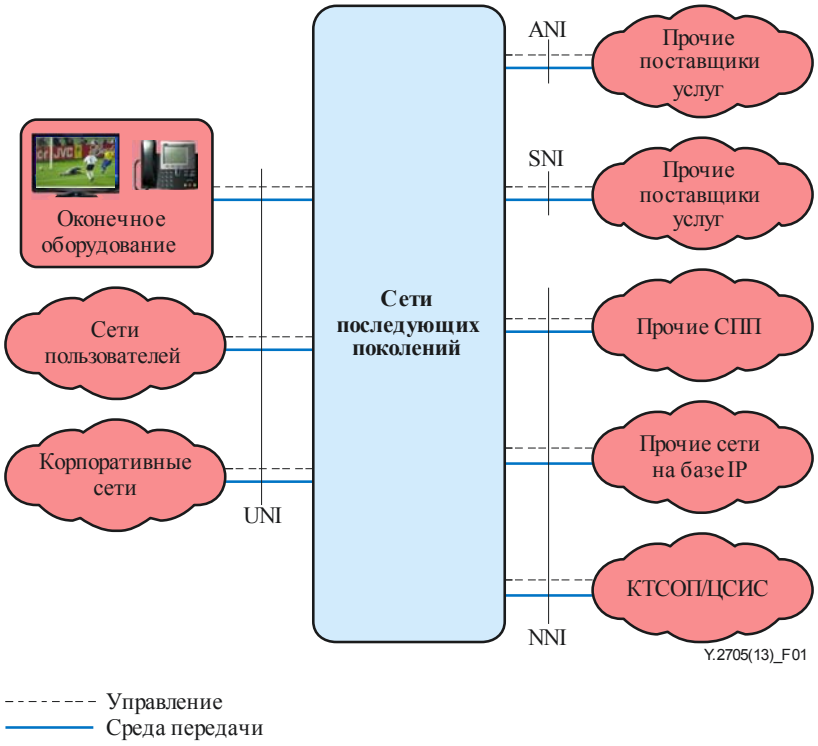


Рисунок 1 – Подключение к СПП [ITU-T Y.2012]

Интерфейсы, относящиеся к сетевым присоединениям:

- интерфейс "приложение-сеть" (ANI);
- интерфейс "служба-сеть" (SNI);
- интерфейс "сеть-сеть" (NNI).

Описания интерфейсов ANI, SNI и NNI приведены в [ITU-T Y.2012].

Для того чтобы различные сети могли поддерживать связь по линиям ETS через границы сетей, необходимы особые меры безопасности для защиты целостности, конфиденциальности и готовности линий связи ETS в рамках каждой национальной сети и по всей структуре соединений между национальными сетями.

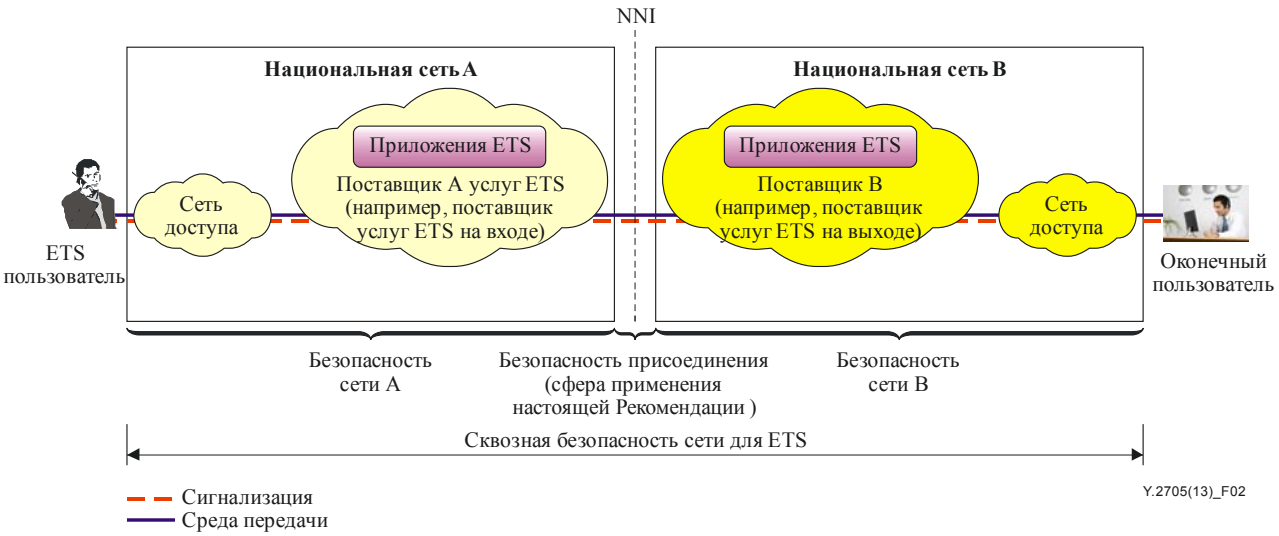


Рисунок 2 – Сквозная безопасность сети для приложений ETS

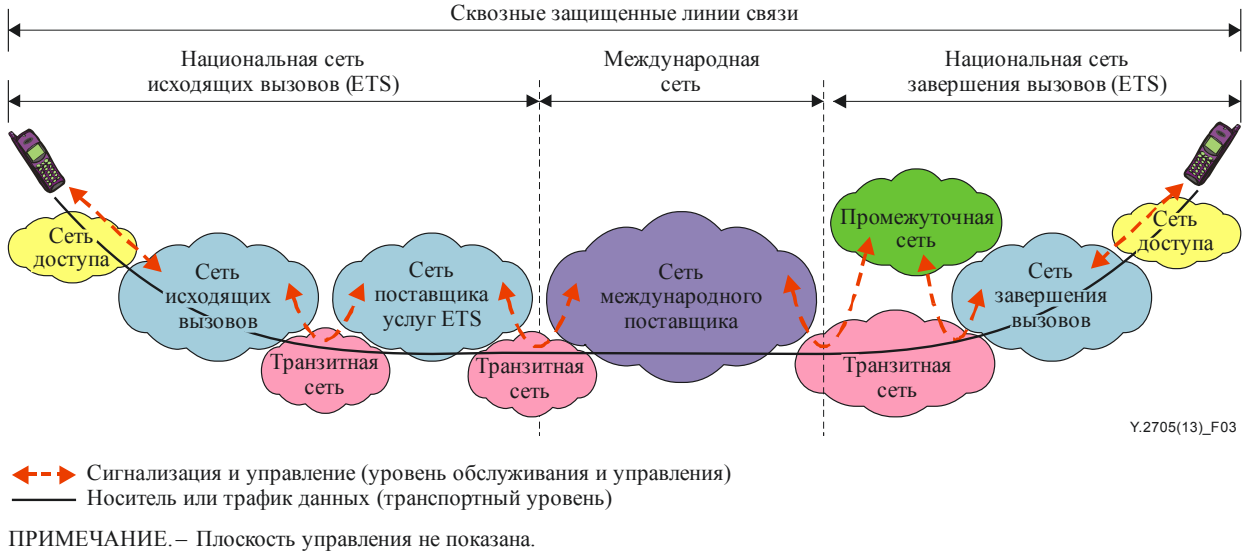
На рисунке 2 показано, что сквозная безопасность обходных многоканальных сетей связи ETS (национальные сети A и B) будет зависеть от мер безопасности, принятых в отдельных сетях, и обеспечения безопасности присоединения между двумя сетями.

На рисунке 2 показано, что настоящая Рекомендация посвящена вопросам безопасного присоединения ETS.

8 Задачи и руководящие принципы обеспечения безопасности в случае присоединения ETS

8.1 Основные задачи

Основной задачей является обеспечение сетевой безопасности сквозных линий связи ETS, которые могут проходить по доменам различных поставщиков сетевых услуг национальных и международных сетей (т. е. стран/администраций), где каждая сеть отвечает за безопасность в пределах своего домена по принципу "от сегмента к сегменту".



ПРИМЕЧАНИЕ. – Плоскость управления не показана.

Рисунок 3 – Пример сквозной связи через различные системы ETS, реализованные на национальном уровне

На рисунке 3 показаны сквозные линии связи для ETS (например, приоритетные линии голосовой связи, видеосвязи, передачи данных или сообщений), начинающиеся и заканчивающиеся в двух различных национальных сетях. Данный пример показывает, что сквозная приоритетная линия связи для ETS может проходить по нескольким сегментам сети и административным доменам (например, сеть доступа, сеть исходящих вызовов, сеть поставщика услуг ETS, сеть международного поставщика, промежуточная сеть и сеть завершения вызовов). Основной задачей является обеспечение для каждой из присоединенных сетей вдоль трассы сквозной линии связи ETS необходимой степени безопасности в пределах домена данной сети, включая присоединение к смежной сети таким образом, чтобы не были нарушены целостность, конфиденциальность и готовность сквозной линии связи ETS.

8.2 Основные руководящие принципы

В отношении присоединенных сетей для ETS должны быть сформированы и внедрены структурный подход и соответствующая методика с использованием Соглашений об уровне обслуживания (SLA). При этом должны быть учтены следующие пункты:

1 Оценка риска безопасности: оценка риска для ресурсов системы ETS, анализ угроз и уязвимости при присоединении ETS. Важнейшее значение имеет регулярность проведения оценки риска безопасности. Кроме того, оценка должна проводиться в случае внесения каких-либо изменений, а также введения в действие новых технологий, услуг или приложений.

2 Архитектура и решения по безопасности: формирование политики безопасности, разработка архитектуры безопасности и спецификация решений, направленных на минимизацию известных угроз для ETS. Данный пункт содержит также заключение необходимых двусторонних или многосторонних соглашений SLA по вопросам безопасности ETS (см. в [ITU-T M.3342] и [b-TMF GB917] информацию по соглашениям SLA). Рассматриваемые области включают политику безопасности, требования, разработку архитектуры, средства криминалистики и информирования о ситуации, а также безопасность инфраструктуры, что должно быть включено в соглашения SLA по присоединениям.

3 Внедрение систем безопасности: внедрение и развертывание архитектуры и решений по безопасности, базирующихся на двусторонних или многосторонних соглашениях SLA, как наиболее подходящих для обеспечения безопасности присоединения ETS.

4 Мероприятия по обеспечению безопасности: оперативные меры по управлению решениями по безопасности для присоединения ETS должны быть четко определены и реализованы. Например, защита от внутренних угроз, управление конфигурируемыми параметрами и значениями по умолчанию, операции по обеспечению отказоустойчивости и восстановлению после сбоя, тестирование системы безопасности ETS, регистрация и аудиторская проверка событий, относящихся к безопасности ETS.

8.3 Общие задачи и требования

В данном пункте представлены общие требования и задачи.

R-1 При прохождении потока трафика ETS через домен Поставщика услуг данный Поставщик услуг, в соответствии с передовым опытом эксплуатации коммерческих систем безопасности, должен обеспечить защиту линий связи ETS от несанкционированных вмешательств (например, прослушивания, захвата и повторного воспроизведения), которые могут нарушить аутентичность, целостность, конфиденциальность и готовность ETS.

В приведенном выше требовании слово "домен" означает физический или логический "сегмент сети", находящийся под полным административным и оперативным контролем и управлением Поставщика услуг. Поставщик услуг осуществляет также техническое обслуживание данного сегмента и обеспечивает его безопасность.

Предполагается, что Поставщики услуг будут поддерживать и использовать широкий спектр средств и функциональных возможностей обеспечения безопасности для защиты как системы ETS, так и всей сети, а также поддерживаемых приложений. Необходимо принять соответствующие меры, гарантирующие, что использование этих возможностей обеспечения безопасности не будет оказывать отрицательного влияния на эксплуатационные характеристики ETS или создавать непреднамеренные помехи работе систем безопасности ETS.

R-2 Использование Поставщиком услуг механизмов безопасности (например, системы обнаружения вторжений и системы предотвращения вторжений [IDS/IPS], а также шифрования) не должно создавать помех механизмам приоритетной обработки, используемым для поддержки ETS (определение и описание механизмов приоритетной обработки см. в [ITU-T Y.2205]).

O-1 Желательно, чтобы применение Поставщиком услуг средств и функциональных возможностей обеспечения безопасности включало соответствующие меры по минимизации отрицательных воздействий на качество обслуживания (QoS) ETS (например, путем создания ненужных задержек).

8.4 Аутентификация, авторизация и контроль доступа в системе ETS

В данный пункт включены следующие пункты:

- аутентификация и авторизация пользователей ETS;
- аутентификация пользователей ETS и авторизация поставщиков услуг ETS;
- аутентификация источников данных для ETS;
- взаимная аутентификация и авторизация поставщиков услуг ETS.

8.4.1 Взаимная аутентификация

Аутентификация – это процесс проверки заявлений идентификационной информации от стороны, участвующей в каком-либо процессе связи. Аутентификация подтверждает подлинность заявленной идентификационной информации объектов, участвующих в сеансе связи (например, человека, устройства, службы или приложения), и предоставляет гарантии, чтобы объект не пытался выдать себя за кого-либо другого или произвести несанкционированное повторное воспроизведение предыдущего сеанса связи.

Сквозная линия для связи ETS может включать несколько сетевых сегментов и административных доменов (например, сеть доступа исходящего трафика, сеть Поставщика услуг ETS, промежуточная сеть, сеть доступа завершения трафика). В процессе приема трафика ETS Поставщик услуг должен проверять подлинность и авторизацию источника принимаемого трафика (например, сети). В процессе отправки трафика ETS Поставщик услуг должен проверять подлинность и авторизацию объекта, которому отправляется трафик СПП (например, сети). В настоящее время доверительные взаимоотношения в плане безопасности для присоединения могут быть доступны для проверки только через прямое физическое присоединение между двумя присоединенными сетями.

R-3 Поставщики услуг должны проводить взаимную аутентификацию для обмена (т. е. отправки или приема) трафиком ETS. Данный пункт включает любые виды обмена трафиком сигнализации или передачи данных между двумя Поставщиками услуг через интерфейсы NNI, ANI или SNI.

Данное условие может быть выполнено с помощью верификации прямых физических присоединений и Соглашений об уровне обслуживания (SLA).

ПРИМЕЧАНИЕ. − В данном случае речь не идет об аутентификации, действующей только в течение одного вызова или сеанса связи. Целью является формирование понятия о механизмах выполнения аутентификации по мере необходимости или на периодичной основе.

8.4.2 Контроль доступа

Меры контроля доступа необходимы для защиты от несанкционированного использования ресурсов сети, включая использование ресурсов несанкционированным образом. Контроль доступа гарантирует, что доступ к элементам сети, хранимой информации, информационным потокам, службам и приложениям имеют только авторизованные пользователи или устройства.

Контроль доступа в интерфейсе NNI означает способность принимающей сети получать или отклонять определенный трафик, приходящий из соседней сети, и ограничивать доступ объектов, находящихся вне сети, к сетевым ресурсам.

R-4 Поставщик услуг должен установить правила и усилить меры по контролю доступа для защиты от попыток несанкционированной связи ETS по интерфейсам NNI. В частности, Поставщики услуг должны разрешать связь через интерфейс NNI между элементами сети (NE) только объектам, прошедшим идентификацию и предварительную авторизацию (например, с помощью соглашений SLA).

R-5 При приеме трафика сигнализации ETS от другого поставщика услуг Поставщик услуг должен проверить доверительные взаимоотношения с поставщиком, от которого он принимает трафик.

R-6 При приеме трафика передачи данных ETS от другого поставщика услуг Поставщик услуг должен проверить доверительные взаимоотношения с поставщиком услуг, от которого он принимает трафик ETS.

R-7 При отправке трафика сигнализации ETS другому поставщику услуг Поставщик услуг должен проверить доверительные взаимоотношения с поставщиком услуг, которому он отправляет трафик ETS.

R-8 При отправке трафика передачи данных ETS другому поставщику услуг Поставщик услуг должен проверить доверительные взаимоотношения с поставщиком услуг, которому он отправляет трафик ETS.

ПРИМЕЧАНИЕ. − В приведенных выше требованиях речь не идет о проведении верификации в течение одного вызова или сеанса связи.

Авторизация – это делегирование полномочий, которое включает делегирование доступа, основанное на полномочиях доступа. Объект получает авторизацию после подтверждения в процессе аутентификации и контроля доступа.

R-9 Поставщик услуг должен обеспечить безопасность в целях предотвращения несанкционированного доступа к ETS.

Средства, с помощью которых может быть выполнено требование R-9, включают, в том числе, следующие (по необходимости):

- аутентификацию и авторизацию конечных пользователей и устройств ETS;
- аутентификацию и авторизацию источников данных для линий связи ETS (например, источников сообщений или источников данных);
- функциональные возможности систем безопасности для защиты от несанкционированного доступа к информации и ресурсам ETS (например, к информации пользователей на серверах аутентификации и в системах управления).

Системный контроль доступа включает меры безопасности для предотвращения несанкционированного доступа к элементам сети и системам и связанным с ними точкам доступа. Существуют угрозы, связанные с несанкционированным доступом к элементам сети и системам, поддерживающим ETS. Поэтому должны быть установлены и усилены соответствующие меры контроля доступа для предотвращения несанкционированного доступа.

R-10 Поставщики услуг должны установить правила и усилить меры системного контроля доступа для предотвращения несанкционированного доступа к элементам сети и системам, поддерживающим ETS. Данные меры включают обеспечение безопасности как для логического, так и для физического доступа.

R-11 Поставщик услуг должен обеспечить защиту от несанкционированного доступа к данным и ресурсам ETS (т. е. Поставщик услуг должен предоставлять доступ к данным и ресурсам ETS (например, файлам, наборам команд, программному обеспечению), расположенным в элементах сети и системах, поддерживающих ETS, только авторизованным администраторам).

8.5 Целостность ETS

В данный пункт включены следующие пункты:

- защита целостности системы сигнализации ETS;
- защита целостности среды передачи данных ETS.

8.5.1 Целостность системы сигнализации

Межсетевая система сигнализации ETS должна быть защищена от перехвата, повреждений и манипуляций (например, удаления, создания новых сигналов или повторного воспроизведения).

R-12 Поставщики услуг должны обеспечивать защиту целостности всего трафика межсетевой сигнальной информации ETS, проходящего через интерфейсы NNI, ANI или SNI.

Действия, которые могли бы обеспечить защиту целостности трафика сигнализации ETS, включают, в том числе:

a) меры физической безопасности (например, физическую защиту элементов сети, среды и средств передачи, а также обеспечение выполнения соответствующих мер по управлению доступом);

b) криптографическую защиту;

c) разработку и обеспечение выполнения соответствующих требований и задач по защите целостности, определенных в Соглашениях об уровне обслуживания;

d) контроль целостности конфигураций интерфейсов NNI.

8.5.2 Целостность среды передачи данных

Среда передачи данных, относящаяся к межсетевой связи ETS, должна быть защищена от перехвата, повреждений и манипуляций (например, стирания, создания новых сигналов или повторного воспроизведения).

R-13 Поставщик услуг должен обеспечивать защиту целостности всего трафика межсетевой среды передачи данных ETS, проходящего через интерфейсы NNI или SNI.

Действия, которые могли бы обеспечить защиту целостности трафика среды передачи данных ETS, включают, в том числе:

a) меры физической безопасности (например, физическую защиту элементов сети, среды и средств передачи, а также обеспечение выполнения соответствующих мер по контролю доступа);

b) криптографическую защиту;

c) разработку и обеспечение выполнения соответствующих требований и задач по защите целостности, определенных в Соглашениях об уровне обслуживания;

d) контроль целостности конфигураций интерфейсов NNI.

8.6 Конфиденциальность линий связи ETS и защита PII

Линии связи ETS, проходящие через интерфейсы NNI, ANI и SNI, должны обеспечиваться защитой конфиденциальности, с тем чтобы предотвратить получение секретной информации неавторизованными объектами. Данный пункт включает защиту конфиденциальности:

- системы сигнализации и управления ETS;
- трафика носителей информации ETS (например, голосовой связи, видеосигналов или данных);
- информации, позволяющей установить личность (PII).

8.6.1 Конфиденциальность системы сигнализации

Поставщики услуг должны обеспечивать защиту межсетевой сигнальной информации, передаваемой через интерфейсы NNI, ANI или SNI, от несанкционированного доступа. Информация системы сигнализации должна быть защищена от перехвата для уменьшения вероятности потенциального ущерба, который может быть причинен в случае раскрытия секретной информации (например, шаблонов набора номера, информации о местоположении и идентификационных данных пользователей) путем анализа трафика сигнализации.

R-14 Поставщик услуг должен обеспечивать защиту конфиденциальности всей межсетевой сигнальной информации ETS, проходящей через интерфейсы NNI, ANI или SNI.

Действия, которые могли бы обеспечить защиту конфиденциальности трафика сигнализации ETS, включают, в том числе:

a) меры физической безопасности (например, физическую защиту элементов сети, среды и средств передачи, а также обеспечение выполнения соответствующих мер по контролю доступа);

b) криптографическую защиту;

c) разработку и обеспечение выполнения соответствующих требований и задач по защите целостности, определенных в Соглашениях об уровне обслуживания.

Поскольку защита конфиденциальности зачастую связана с криптографическими механизмами, содержащееся в данном пункте требование по обеспечению защиты конфиденциальности межсетевой системы сигнализации не подразумевает, что криптографические методы должны использоваться во всех сценариях или для всех сквозных потоков сигнальной информации. Цель данного требования заключается в том, чтобы Поставщики услуг обеспечивали и внедряли необходимые меры для гарантированной защиты от перехвата сигнальной информации, проходящей через интерфейсы NNI, ANI и SNI. Это означает, что каждое присоединение должно быть изучено с целью выявления наиболее подходящих механизмов, используемых для обеспечения защиты конфиденциальности в соответствии с заявленной политикой обеспечения безопасности. Например, возможно было бы обеспечить защиту конфиденциальности путем использования физических и связанных с ними действий, в зависимости от архитектурных и физических конфигураций IP-межсетевых соединений (например, сценарий с выделенной физической линией).

8.6.2 Конфиденциальность среды передачи данных

Потоки данных (например, голосовая связь, видеосвязь и передача данных) должны быть защищены от несанкционированного доступа, так как при перехвате потоков данных ETS может быть раскрыта секретная информация, относящаяся к безопасности (т. е. передаваемая по линии данных).

R-15 Поставщик услуг должен обеспечить защиту конфиденциальности всего межсетевого трафика среды передачи данных, проходящего через интерфейсы NNI или SNI.

Действия, которые могли бы обеспечить защиту конфиденциальности трафика сигнализации и среды передачи данных ETS, включают, в том числе:

a) меры физической безопасности (например, физическую защиту элементов сети, среды и средств передачи, а также обеспечения выполнения соответствующих мер по управлению доступом);

b) криптографическую защиту;

c) разработку и обеспечение выполнения соответствующих требований и задач по защите целостности, определенных в Соглашениях об уровне обслуживания.

8.6.3 Защита PII

Связанная с ETS информация, позволяющая установить личность (PII), должна быть защищена от несанкционированного просмотра или раскрытия (например, идентификационные данные конечных пользователей ETS, идентификационные данные объектов связи, абонентские данные ETS и местоположение конечных пользователей).

R-16 Поставщик услуг должен обеспечивать возможность анонимного доступа к услугам ETS для избранных пользователей ETS.

R-17 Поставщик услуг должен обеспечивать защиту конфиденциальности идентификационных данных избранных пользователей ETS.

R-18 Поставщик услуг должен обеспечивать защиту конфиденциальности местоположения избранных пользователей ETS.

Необходимо обеспечить защиту от несанкционированного просмотра информации, касающейся использования ETS (например, параметров использования, таких как объем трафика ETS, местоположения, время, частота и т. д.). Данный пункт включает поддержку и использование функциональных возможностей систем безопасности для защиты секретной информации, полученной при просмотре сетевой активности, включая веб-сайты, посещенные конечным пользователем, географическое местоположение конечного пользователя, а также IP-адреса и имена устройств сервера наименования доменов (DNS) в сети поставщика услуг.

О-2 Ожидается, что Поставщик услуг будет обеспечивать защиту от несанкционированного просмотра или раскрытия информации об использовании ETS (например, просмотра сетевой активности, включая веб-сайты, посещенные пользователями ETS, IP-адреса пользователей ETS или параметры использования, такие как объем трафика ETS, местоположения, время, частота).

8.7 Межсетевой IP-транспорт

8.7.1 Общие положения

Взаимное соединение IP-IP между двумя Поставщиками услуг будет иметь архитектурные и физические особенности подключений с различными вариантами реализации систем безопасности.

Целостность и готовность взаимного соединения IP-IP между двумя Поставщиками услуг будет зависеть от таких факторов, как архитектура, физическая возможность соединения и соглашения об уровне обслуживания.

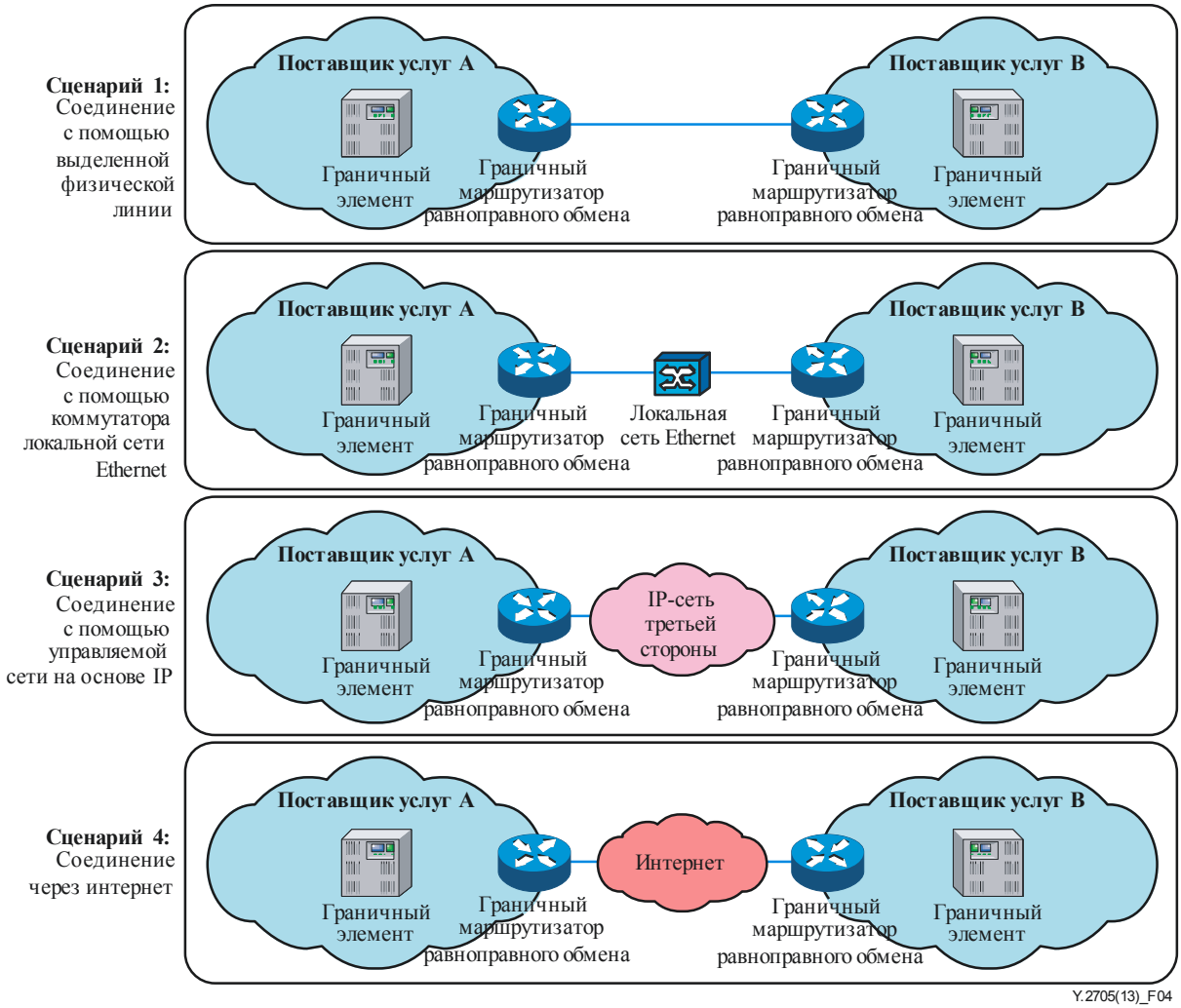


Рисунок 4 – Конфигурации взаимного соединения IP-IP

На рисунке 4 показан набор возможных конфигураций взаимных соединений IP-IP:

1 Соединение с помощью выделенной физической линии: В данной конфигурации выделенная физическая линия используется для подключения граничного маршрутизатора равноправного обмена Поставщика услуг A к граничному маршрутизатору равноправного обмена Поставщика услуг B.

2 Соединение через Ethernet-коммутатор: В данной конфигурации граничный маршрутизатор равноправного обмена Поставщика услуг A и граничный маршрутизатор равноправного обмена Поставщика услуг B физически соединены через Ethernet-коммутатор локальной сети (LAN).

3 Присоединение через управляемую IP-сеть: В данной конфигурации IP-соединение между Поставщиком услуг A и Поставщиком услуг B выполняется через управляемую IP-сеть. Это может быть управляемая IP-сеть поставщика третьей стороны.

4 Соединение через интернет: В данной конфигурации IP-соединение между Поставщиком услуг A и Поставщиком услуг B выполняется общедоступным путем – через интернет.

Существуют различные варианты реализации систем безопасности ETS для каждого из сценариев, показанные на рисунке 4.

Настоящий документ не содержит оговорок или ограничений относительно IP-соединения, используемого для присоединения Поставщика услуг. Главной задачей является возложение на Поставщика услуг обязанностей по поддержке и внедрению, на основе конкретной конфигурации IP-IP, соответствующих мер безопасности для защиты присоединения и предотвращения воздействий на услуги, возникающих вследствие нарушений работы IP-соединения.

R-19 Поставщик услуг, в соответствии с передовым опытом эксплуатации коммерческих систем безопасности, должен обеспечить защиту транспортной IP-сети между двумя присоединенными сетями Поставщика услуг от вмешательств (например, прослушивания, захвата и повторного воспроизведения), которые могут нарушить аутентичность, целостность, конфиденциальность и готовность ETS.

Для соблюдения данного требования Поставщик услуг должен разработать и обеспечить выполнение правил для защиты транспортной IP-сети между присоединенными сетями Поставщика услуг, а также закрепить эти правила документально в соглашениях SLA.

R-20 Поставщик услуг должен обеспечивать защиту целостности приоритетных механизмов, функциональных возможностей и сопроводительных данных протокола (например, кодовых точек Diffserv) IP-трафика, используемых для поддержки работы ETS через сетевое IP-соединение между Поставщиками услуг.

ПРИМЕЧАНИЕ. − Данное требование включает защиту целостности любых связанных с ETS данных или параметров с заданной конфигурацией, относящихся к IP-соединению, а также любого, применяемого в данном случае преобразования (например, преобразования кодовых точек Diffserv, основанное на схеме, используемой в индивидуальном присоединении Поставщика услуг).

CR-1 Если сигнальная информация ETS проходит по ненадежному сегменту транспортной сети IP (например, IP-транспорт третьей стороны), Поставщик услуг должен использовать шифрование (например, IPsec) для защиты целостности и конфиденциальности.

CR-2 Если данные ETS передаются по ненадежному сегменту транспортной сети IP (например, IP-транспорт третьей стороны), Поставщик услуг должен использовать шифрование (например, IPsec) для защиты целостности и конфиденциальности.

8.7.2 Использование шифрования

Использование механизмов безопасности (например, шифрования) не должно создавать помех или скрывать информацию для механизмов приоритетной обработки.

Следующее требование применяется при использовании туннелей IPsec для межсетевого трафика ETS, (т. е. проходящего через интерфейсы NNI, ANI и SNI):

R-21 Поставщик услуг должен разработать и обеспечить выполнение правил для размещения и защиты целостности приоритетной информации (например, значений DSCP) при использовании туннелей IPsec для межсетевого трафика ETS. В частности, правила размещения значений кодовой точки Diffserv (DSCP) из внутреннего заголовка в туннельном заголовке IPsec в точке входа IPsec должны быть разработаны в соглашениях SLA и введены в действие для обеспечения приоритетной обработки между точками входа и выхода IPsec.

8.8 Готовность ETS

8.8.1 Основная задача

Для обеспечения более высокого уровня готовности ETS необходимо, чтобы количество отказов каждой системы обслуживания (поддерживающей ETS) было небольшим, а восстановление работы службы (при возникновении перебоев или отказов) производилось в срочном порядке. Отказы как результаты нарушения требований безопасности должны учитываться при общем планировании готовности и в процессе разработки ETS. Ниже приводится основная задача для уровня готовности ETS в контексте обеспечения безопасности.

O-3 Желательно, чтобы Поставщики услуг принимали во внимание потенциальные отказы или нарушения обслуживания из-за сбоев в системе безопасности, влияющих на межсетевые соединения, при общем планировании и проектировании показателей готовности сквозных услуг ETS (т. е. вызовов или сеансов связи ETS, проходящих по нескольким сетям Поставщика услуг). Данный пункт включает меры быстрого восстановления после отказов, вызванных нарушениями безопасности.

8.8.2 Защита уровня готовности

Система ETS должна быть защищена от отказов в обслуживании (DoS), распределенных отказов в обслуживании (DDoS) и других типов атак, которые могут повлиять на готовность ETS. Данный пункт включает защиту от атак, влияющих на уровень готовности ETS для индивидуальных пользователей ETS, групп пользователей ETS, пользователей ETS в особых местах или расположениях (например, узлы сетей правительственных учреждений), пользователей ETS в планируемой географической или региональной области или системы ETS в целом.

R-22 Поставщик услуг должен обеспечивать защиту уровня готовности ETS (например, защиту от DoS, DDoS и других типов атак, влияющих на уровень готовность ETS) в соответствии с передовым опытом эксплуатации коммерческих систем безопасности. Данный пункт включает защиту от DoS, DDoS и других типов атак, влияющих на уровень готовности ETS для индивидуальных пользователей ETS, групп пользователей ETS, пользователей ETS в особых местах или расположениях (например, узлы сетей правительственных учреждений), пользователей ETS в планируемой географической или региональной области или системы ETS в целом.

Действия, которые могли бы обеспечить защиту уровня готовности ETS, включают, в том числе:

a) использование управления доступом к соединениям и механизмам регулирования;

b) использование инструментов и функций для противодействия DoS- и DDoS-атакам;

c) использование систем обнаружения вторжений и систем предотвращения вторжений (IDS/IPS);

d) использование средств контроля безопасности;

e) использование средств информированности о ситуации.

R-23 Использование Поставщиками услуг инструментов и функциональных возможностей для защиты уровня готовности ETS (например, механизмов противодействия DoS- и DDoS-атакам) должно включать соответствующие меры для предотвращения непреднамеренных отказов в проведении легальных вызовов или сеансов связи ETS (например, блокирование или предотвращение проведения легального вызова или сеанса связи ETS либо исключение легальных пакетов данных ETS).

8.9 Безопасность управления и эксплуатации

В данный пункт включены некоторые темы, касающиеся:

- безопасности операций по управлению (например, конфигурируемые и заданные по умолчанию параметры, относящиеся к введению в эксплуатацию присоединения ETS);
- регистрации событий, имеющих отношение к безопасности ETS;
- сигналов предупреждения и тревоги при возможном или произошедшем нарушении требований безопасности.

8.9.1 Целостность данных ETS

Целостность хранящихся данных ETS должна быть обеспечена защитой, направленной на предотвращение любых повреждений или манипуляций данных, влияющих на целостность или готовность ETS.

R-24 Поставщик услуг должен обеспечивать защиту целостности данных, предоставленных ETS. Данный пункт включает любые конкретные данные ETS, например абонентские данные, об абонентских подключениях, которые обслуживаются системой.

8.9.2 Конфигурируемые параметры и значения по умолчанию

Существует множество угроз безопасности, относящихся к управлению конфигурируемыми параметрами и значениями по умолчанию, установленными производителями и поставщиками оборудования. Например, значения по умолчанию различных конфигурируемых параметров, заданные производителем, должны быть настроены в соответствии с требованиями Поставщика услуг. Конфигурируемые параметры должны быть заданы правильным образом и регулярно обновляться для обеспечения удовлетворительного функционирования. Административное лицо должно иметь соответствующую авторизацию для осуществления административных действий по обеспечению безопасности.

R-25 Поставщик услуг должен разработать и обеспечить выполнение правил администрирования конфигурируемых параметров и значений по умолчанию в контексте поддержки ETS. Меры по управлению доступом должны быть разработаны и реализованы таким образом, чтобы доступ к выполнению данных функций имел только авторизованный администратор (т. е. все остальные пользователи не должны иметь соответствующего разрешения).

8.9.3 Защита от внутренних угроз

Частное лицо (например, сотрудник, контрактный служащий или другой работник) может получить несанкционированный доступ к управлению или ненадлежащим образом использовать данный ему доступ к управлению элементами сети и системами, поддерживающими ETS. Следовательно, существует необходимость минимизации угроз, исходящих от внутренних сотрудников.

R-26 Поставщик услуг должен разработать и ввести в действие процессы обеспечения безопасности для минимизации угроз ETS, исходящих от внутренних сотрудников.

Примеры методов противодействия, которые стоит принять к сведению, включают:

- средства управления аутентификацией, делегирование полномочий на ролевой основе, разделение функциональных обязанностей, а также методы безопасного доступа, касающиеся дистанционного, пультового, передвижного и автоматизированного доступа к системе;
- регистрацию событий безопасности, имеющих отношение к управляющим действиям;
- классификацию информации, приложений и доступа к совместно используемым системам и приложениям ETS;
- аудиторскую проверку сконфигурированных данных в сетевых элементах и базах данных (например, абонентские профили) для регистрации и выявления несанкционированных изменений.

8.9.4 Совместная деятельность по обмену информацией, касающейся кибербезопасности

Поставщики услуг должны установить взаимодействие с партнерами для реализации общего доступа к информации о событиях кибербезопасности (включая обмен информацией в реальном времени во время кибератак). Обмен информацией о происшествиях, касающихся кибербезопасности, может принести партнерам обоюдную выгоду, а также использоваться для предупреждения угроз ETS, которые вынуждают Поставщика услуг применять эффективные меры противодействия.

O-4 Желательно, чтобы Поставщики услуг разработали и ввели в действие процедуры управления и оперативных действий, достаточные для обеспечения партнерских взаимоотношений с целью обеспечения совместного доступа и обмена информацией о событиях кибербезопасности. При разработке данных процедур следует учитывать функции анализа, с тем чтобы информация могла использоваться в качестве вводных данных для действий по обеспечению безопасности и мер противодействия для защиты ETS.

Сведения по обмену информацией, касающейся кибербезопасности, приведены в следующих Рекомендациях МСЭ-Т:

- [b-ITU-T X.1500];
- [b-ITU-T X.1500.1];
- [b-ITU-T X.1520];
- [b-ITU-T X.1521];
- [b-ITU-T X.1524];
- [b-ITU-T X.1570].

8.9.5 Управление реагированием на происшествия и восстановлением после событий нарушения требований безопасности

Уровень готовности ETS зависит от рабочих процедур, применяемых для восстановления и возобновления обслуживания после событий нарушения требований безопасности. Крайне важно, чтобы данные процедуры были четко определены, документированы и реализованы. Этот пункт включает необходимые принципы и практические действия по восстановлению и возобновлению обслуживания в пределах домена Поставщика услуг и в доменах присоединенных и межсетевых служб. Необходима защита документации и внедрения рабочих процедур от действий злоумышленников и внутренних угроз.

R-27 Поставщик услуг должен иметь документированный план реагирования на происшествия и восстановления, описывающий принципы, методы управления, пошаговые действия, процессы и процедуры для восстановления и возобновления обслуживания после событий нарушения требований безопасности. Данный пункт включает необходимые принципы и практические действия для восстановления и возобновления услуг в пределах домена Поставщика услуг и в доменах присоединенных и межсетевых служб.

Библиография

[b-ITU-T Q-Sup.57] ITU-T Q-series Recommendations – Supplement 57 (2008), *Signalling requirements to support the emergency telecommunications service (ETS) in IP networks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1500] Рекомендация МСЭ-Т X.1500 (2011 г.), *Методы обмена информацией о кибербезопасности*.

[b-ITU-T X.1500.1] Рекомендация МСЭ-Т X.1500.1 (2012 г.), *Процедуры регистрации дуг в рамках дуги идентификатора объекта для обмена информацией о кибербезопасности*.

[b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2011 г.), *Общеизвестные уязвимости и незащищенность*.

[b-ITU-T X.1521] Рекомендация МСЭ-Т X.1521 (2011 г.), *Система оценки общеизвестных уязвимостей*.

[b-ITU-T X.1524] Рекомендация МСЭ-Т X.1524 (2012 г.), *Перечень общеизвестных слабых мест*.

[b-ITU-T X.1570] Рекомендация МСЭ-Т X.1570 (2011 г.), *Механизмы обнаружения, используемые при обмене информацией о кибербезопасности*.

[b-TMF GB917] GB917 (2012), *SLA Management Handbook*, Release 3.1, TM Forum.

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	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

Отпечатано в Швейцарии
Женева, 2013 г.