МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.2701

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2007)

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

Сети последующих поколений – Безопасность

Требования к безопасности для сетей последующих поколений версии 1

Рекомендация МСЭ-Т Y.2701

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.2701

Требования к безопасности для сетей последующих поколений версии 1

Резюме

В Рекомендации МСЭ-Т Y.2701 представлены требования к безопасности для сетей последующих поколений (СПП) и их интерфейсов, например UNI, NNI и ANI, путем применения принципов Рекомендации МСЭ-Т X.805 *Архитектура безопа**с**ности для систем, обеспечивающих связь между оконечными устройствами,* к Рекомендациям МСЭ-Т Y.2201 *Требования к СПП версии 1* и МСЭ-Т Y.2012 *Функциональные требования и архитектура СПП версии 1*.

Требования должны обеспечивать основанную на сети безопасность соединений конечных пользователей через административные домены множества сетей. Безопасность активов пользователя и информации в домене пользователя, например, в сети пользователя, а также использование возможностей одноранговых приложений в оборудовании клиента, выходят за рамки настоящей Рекомендации.

В данной Рекомендации используется модель доверия, основанная на элементах сети (физических объектах). Поставщики услуг СПП будут использовать элементы сети, которые поддерживают функциональные объекты, определенные в Рекомендации МСЭ-Т Y.2012. Привязка этих функциональных объектов к заданному элементу сети будет меняться в зависимости от поставщика. Таким образом, в данной Рекомендации не будут делаться попытки указать строгую и фиксированную привязку логических функциональных объектов к физическим элементам сети.

Требования, представленные в данной Рекомендации, следует рассматривать как минимальный набор требований к безопасности, и поставщикам СПП рекомендуется принимать дополнительные меры, помимо тех, что определены в Рекомендациях по безопасности СПП.

Источник

Рекомендация МСЭ-Т Y.2701 утверждена 27 апреля 2007 года 13-й Исследовательской комиссией МСЭ-Т (2005-2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

ПРЕДИСЛОВИЕ

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

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

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 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 носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т Y.2701

Требования к безопасности для сетей последующих поколений версии 1

1 Сфера применения

В данной Рекомендации представлены требования к безопасности для сетей последующих поколений (СПП) с целью противостояния угрозам безопасности. Они сформированы за счет применения принципов Рекомендации МСЭ-Т X.805 *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами* к Рекомендациям МСЭ-Т Y.2201 *Требования к СПП версии 1* и Y.2012, *Функциональные требования и архитектура СПП версии 1*.

Эти требования в условиях множества сетей должны защищать следующее:

- сеть и инфраструктуру поставщика услуг, и его активы, например, активы и ресурсы СПП, такие как элементы сети, системы, компоненты, интерфейсы, а также данные и информацию, его ресурсы, его связь, т. е. сигнализацию, управление и трафик данных/канала передачи, и ее услуги;
- услуги и возможности СПП, например, голосовые услуги, услуги передачи видео и данных;
- соединения и информацию оконечного пользователя, например, личную информацию.

Требования должны обеспечивать основанную на сети безопасность соединений конечных пользователей через административные домены множества сетей. Безопасность активов пользователя и информации в домене пользователя, например, в сети пользователя, а также использование возможностей одноранговых приложений в оборудовании клиента, выходят за рамки настоящей Рекомендации.

Требования, определенные в данной Рекомендации, применимы к СПП, включая интерфейсы пользователь-сеть (UNI), интерфейсы сеть-сеть (NNI) и интерфейсы приложение-сеть (ANI) в условиях множества сетей.

Поставщики услуг СПП будут использовать элементы сети, которые поддерживают функциональные объекты, определенные в Рекомендации МСЭ-Т Y.2012. Привязка этих функциональных объектов к заданному элементу сети будет меняться в зависимости от поставщика. Таким образом, в данной Рекомендации не делается попытки указать строгую и фиксированную привязку логических функциональных объектов к физическим элементам сети.

Требования, представленные в данной Рекомендации, следует рассматривать как минимальный набор требований к безопасности для СПП, не являющийся исчерпывающим. В связи с этим поставщикам СПП может потребоваться принимать дополнительные меры, помимо тех, что определены в Рекомендациях по безопасности СПП.

Кроме того, требования в данной Рекомендации охватывают некоторые технические аспекты того, что обычно известно как IdM (управление идентичностью). Рабочее определение IdM заключается в следующем "управление со стороны поставщиков СПП доверенными атрибутами таких объектов, как абонент, устройство или поставщик". Оно не предназначено для обозначения положительных результатов проверки подлинности личности.

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

1.1 Принципы X.805

В рекомендации МСЭ-Т X.805 определены следующие аспекты безопасности:

контроль доступа;
аутентификация;
сохранность данных;
конфиденциальность данных;
безопасность связи;
целостность данных;

доступность;
секретность.

В ней также определены следующие угрозы безопасности.

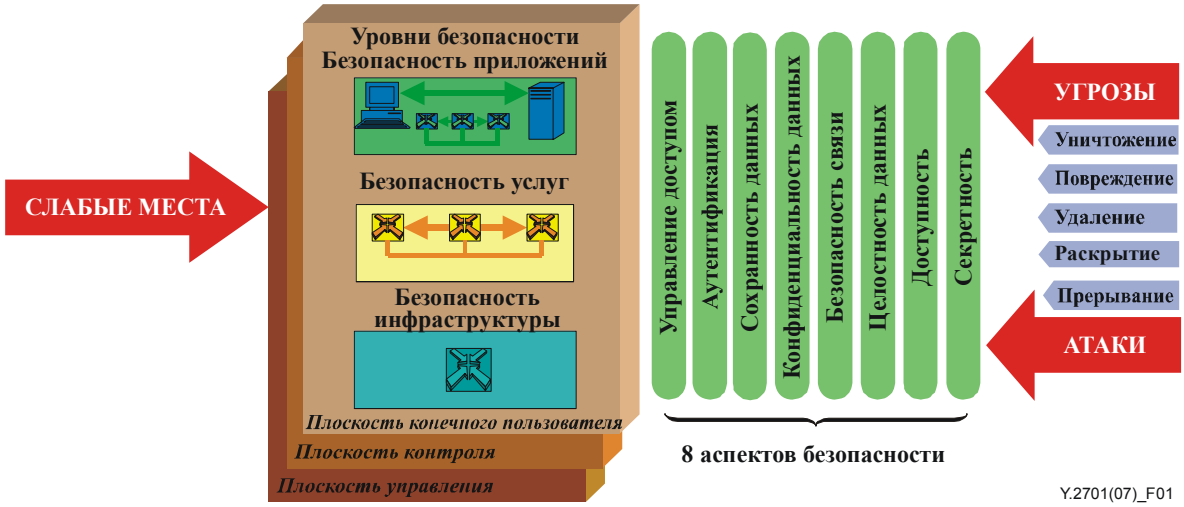

Рисунок 1 – Архитектура безопасности X.805 (Рисунок 3/X.805)

Данные аспекты безопасности и угрозы безопасности, изложенные выше, положены в основу данной Рекомендации.

В данной Рекомендации не уточняется определение и не различается использование уровней защиты X.805 (приложения, службы или инфраструктура), и соответствие данному стандарту не требует такого различия. Данная Рекомендация не определяет различий между трафиком плоскостей администрирования, управления и пользователя, но предупреждает читателя, что использование этого деления различается в зависимости от уровня в стеке рассматриваемого протокола. Следовательно, для определения совместимости с такими различиями будут нужны ссылки на дополнительные стандарты. В данном стандарте приводятся рекомендации, касающиеся применения аспектов защиты, но он не претендует на завершенность, и не может использоваться для оценки защищенности сетей СПП.

1.2 Допущения

Данная Рекомендация основана на следующих допущениях:

1) Привязка функциональных объектов, как определено в [Y.2012], к данному элементу сети будет изменяться в зависимости от поставщика.

2) Каждый поставщик СПП имеет определенные обязанности по безопасности в пределах своего домена. Например, реализация применимых услуг и технологий безопасности в целях:

   a) собственной защиты;

   b) обеспечения того, что сквозная безопасность не подвергается риску в пределах его сети, и

   c) обеспечения высокой доступности соединений СПП.

3) Каждый домен сети будет устанавливать и реализовывать правила формирования соглашений об уровне обслуживания (SLA) для обеспечения безопасности своего домена и безопасности сетевых соединений. Предполагается, что соглашения SLA будут определять услуги безопасности, механизмы и действия, которые должны быть выполнены для защиты взаимосвязанных сетей и соединений (трафик сигнализации/управления, трафик канала передачи и трафик администрирования) через интерфейсы UNI, ANI и NNI.

4) В данной Рекомендации рассматриваются вопросы безопасности сети, которая имеет многоуровневую архитектуру, состоящую из периметра защиты для доверенных доменов, физической защиты оборудования поставщика и возможно использования шифрования.

1.3 Обзор

Данная Рекомендация организована следующим образом:

- Раздел 2 (Справочные документы) – В данном разделе представлены нормативные справочные документы.
- Раздел 3 (Определения и сокращения) – В данном разделе представлены определения и сокращения, использованные в настоящей Рекомендации.
- Раздел 4 (Угрозы безопасности и риски) – В данном разделе рассмотрены угрозы безопасности и риски, предполагаемые в среде СПП. Предполагаемые угрозы безопасности и риски используются в качестве руководства при разработке требований к безопасности, а также при определении возможностей и процедур безопасности, которые должны поддерживаться.
- Раздел 5 (Модель доверия безопасности) – В данном разделе описана модель доверия для безопасности СПП. Модель доверия может использоваться при построении отношений доверия для связи между интерфейсами UNI, ANI и NNI, и при разработке архитектуры безопасности.
- Раздел 6 (Архитектура безопасности) – В данном разделе описаны взаимоотношения между функциональной архитектурой СПП, определенной в [Y.2012], и сложными архитектурами безопасности.
- Раздел 7 (Задачи и требования) – В данном разделе описаны задачи безопасности и общие требования для сетей СПП, которые должны использоваться в качестве основы при определении требований к безопасности СПП.
- Раздел 8 (Особые требования к безопасности) – В данном разделе представлены особые требования к безопасности, как определено в Разделе 7.
- Дополнение I – Задачи безопасности и руководящие принципы для служб электросвязи в чрезвычайных ситуациях (ETS).
- Список литературы.

Данная Рекомендация должна стать основой для безопасности СПП. В будущем должны быть разработаны различные сопутствующие Рекомендации для конкретных областей безопасности, например, аутентификации и авторизации, управления сертификатами, управления идентичностью и другие.

2 Справочные документы

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

[ITU-T M.3016.0] Рекомендация МСЭ-Т M.3016.0 (2005 г.), *Безопасность для плоскости управления. Обзор*.

[ITU-T M.3016.1] Рекомендация МСЭ-Т M.3016.1 (2005 г.), *Безопасность для плоскости управления. Требования по безопасности*.

[ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимодействия открытых систем для приложений МККТТ*.

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

[ITU-T Y.2012] Рекомендация МСЭ-Т Y.2012 (2006 г.), *Функциональные требования и архитектура сетей СПП версии 1*.

[ITU-T Y.2201] Рекомендация МСЭ-Т Y.2201 (2007 г.), *Требования сетей СПП версии 1*.

3 Определения и сокращения

3.1 Термины, определенные в других документах

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

3.1.1 Служба электросвязи в чрезвычайных ситуациях (emergency telecommunications service (ETS)). Национальная служба, предоставляющая санкционированную приоритетную связь для содействия тем, кто проводит аварийно-спасательные работы в период бедствий. (Рекомендация МСЭ-Т E.107.)

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

3.2 Термины, определенные в настоящей Рекомендации

В данной Рекомендации определяются следующие термины.

3.2.1 Активы (asset). Все, что имеет ценность для организации, ее бизнеса, ее функционирования и ее целостности.

3.2.2 Пограничный элемент (border element). Элемент сети, выполняющий функции соединения различных доменов безопасности и административных доменов.

3.2.3 Корпоративная сеть (corporate network). Частная сеть, которая поддерживает множество пользователей и которая может располагаться во многих местах, например, на предприятии, в университетском городке.

3.2.4 Пограничный элемент домена (domain border element). Пограничный элемент под единоличным контролем поставщика, обеспечивающий выполнение функций безопасности с другими доменами сети.

3.2.5 Пограничный элемент сети (network border element). Пограничный элемент под единоличным контролем поставщика, обеспечивающий выполнение функций безопасности связи с оконечным оборудованием.

3.2.6 Домен безопасности (security domain). Совокупность элементов, политика безопасности, орган безопасности и совокупность действий по обеспечению безопасности, в которых управление элементами осуществляется в соответствии с политикой безопасности. Эта политика будет проводиться органом безопасности. Данный домен безопасности может простираться на несколько зон безопасности.

3.2.7 Зона безопасности (security zone). В данной Рекомендации определены 3 зоны безопасности:

1) доверенная;
2) доверенная, но уязвимая; и
3) недоверенная.

Зона безопасности определяется оперативным управлением, местоположением и возможностью соединения с другими устройствами/элементами сети.

3.2.8 Пограничный элемент оконечного оборудования (terminal equipment border element). Пограничный элемент, обеспечивающий функции безопасности связи между оборудованием в помещении абонента и сетью поставщика услуг.

3.2.9 Доверие (trust). Говорят, что объект X доверяет объекту Y относительно некоторой совокупности действий, если и только если объект X надеется, что в отношении данных действий объект Y будет вести себя определенным образом.

3.2.10 Доверенная, но уязвимая зона (trusted but vulnerable zone). С точки зрения поставщика СПП, зона безопасности – это зона, в которой работают (предоставлены и обслуживаются) элементы сети/устройства поставщика СПП. Оборудование может управляться либо пользователем/абонентом, либо поставщиком СПП. Кроме того, оборудование может размещаться как в пределах домена поставщика СПП, так и за его границами. Оно связывается как с элементами доверенной зоны, так и с элементами в недоверенной зоне, именно поэтому оно является "уязвимым". Главной функцией безопасности является такая защита элементов сети (NE) от атак безопасности, инициируемых в недоверенной зоне, при которой не возникает неисправностей.

3.2.11 Доверенная зона (trusted zone). С точки зрения поставщика СПП, доверенная зонам – это домен безопасности, в котором находятся элементы сети и системы поставщика СПП, которые никогда не связываются непосредственно с абонентским оборудованием. Общие характеристики элементов сети СПП в этом домене заключаются в том, что данные элементы полностью контролируются соответствующим поставщиком СПП, находятся в собственности поставщика СПП, что гарантирует физическую безопасность, и они связаны только с элементами в "доверенной" зоне и с элементами в "доверенной, но уязвимой" зоне.

3.2.12 Недоверенная зона (un-trusted zone). С точки зрения поставщика СПП, недоверенная зона – это зона, в которую включены все элементы сети сетей пользователей или возможно одноранговых сетей, или зоны других поставщиков СПП за пределами исходного домена, которые соединяются с пограничными элементами данного поставщика СПП.

3.2.13 Сеть пользователя (user network). Частная сеть, состоящая из оконечного оборудования, в которой может быть множество пользователей.

3.3 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения и акронимы.

3G	3rd Generation	Третье поколение
AGW	Access Gateway	Шлюз доступа
ANI	Application-to-Network Interface	Интерфейс "Приложение-Сеть"
B2BUA	Back-to-Back User Agent	Двусторонний пользовательский агент
BE	Border Element	Пограничный элемент
CSC-FE	Call Session Control Functional Entity	Функциональный объект управления сеансом связи
DBE	Domain Border Element	Пограничный элемент домена
DNS	Domain Name System	Система доменных имен
ETS	Emergency Telecommunications Service	Служба электросвязи в чрезвычайных ситуациях
FE	Functional Entity	Функциональный объект
GW	Gateway	Шлюз
I-CSC-FE	Interrogating Call Session Control Functional Entity	Запрашивающий функциональный объект управления сеансом связи
IMS	IP Multimedia Subsystem	Мультимедийная подсистема IP
IP	Internet Protocol	Интернет-протокол
ISDN	Integrated Services Digital Network	ЦСИС, цифровая сеть с интеграцией служб
LAN	Local Area Network	Локальная сеть (ЛС)
MPLS	Multi Protocol Label Switching	Многопротокольная коммутация по меткам
MRP-FE	Media Resource Processing Functional Entity	Функциональный объект обработки источника информационных данных
NAC-FE	Network Access Control Functional Entity	Функциональный объект управления доступом в сеть
NAPT	Network Address and Port Translation	Трансляция сетевых адресов и портов
NAT	Network Address Translation	Трансляция сетевого адреса

NBE	Network Border Element	Сетевой пограничный элемент
NE	Network Element	Элемент сети
NGN	Next Generation Network	Сеть последующего поколения (СПП)
NNI	Network-to-Network Interface	Интерфейс "Сеть-Сеть"
OAMP	Operations, Administration, Maintenance and Provisioning	Эксплуатация, администрирование, техническое обслуживание и снабжение
P-CSC-FE	Proxy Call Session Control Functional Entity	Функциональный объект управления вызовом сеанса связи с прокси-элементом
POTS	Plain Old Telephone Service	Обычная аналоговая телефонная служба
PSTN	Public Switched Telephone Network	Телефонная сеть общего пользования с коммутацией каналов (ТфОП)
QoS	Quality of Service	Качество обслуживания
RAC-FE	Resource and Admission Control Functional Entity	Функциональный объект управления ресурсами и установлением соединений
RAN	Radio Access Network	Сеть с радиодоступом
RTSP	Real Time Streaming Protocol	Потоковый протокол реального времени
SAA-FE	Service Authentication and Authorization Functional Entity	Функциональный объект аутентификации и авторизации услуги
S-CSC-FE	Serving Call Session Control Functional Entity	Обслуживающий функциональный объект управления сеансом связи
SIM	Subscriber Identity Module	Модуль идентификации абонента
SIP	Session Initiation Protocol	Протокол инициации сеанса связи
SLA	Service Level Agreement	Соглашение об уровне обслуживания
SL-FE	Subscription Locator Functional Entity	Функциональный объект обнаружения данных о правах подписки
TAA-FE	Transport Authentication and Authorization Functional Entity	Функциональный объект аутентификации и авторизации транспортировки
TE	Terminal Equipment	Оконечное оборудование
TE-BE	Terminal Equipment Border Element	Пограничный элемент оконечного оборудования
TMN	Telecommunication Management Network	Сеть управления электросвязью (СУЭ)
UA	User Agent	Агент пользователя
UICC	Universal Integrated Circuit Card	Универсальная встроенная монтажная плата
UNI	User-to-Network Interface	Интерфейс "Пользователь-Сеть"
VLAN	Virtual LAN	Виртуальная локальная сеть доступа
W-CDMA	Wideband Code Division Multiple Access	Широкополосный многостанционный доступ с кодовым разделением каналов
WLAN	Wireless LAN	Беспроводная локальная сеть доступа
xDSL	x Digital Subscriber Line	Любая цифровая абонентская линия

4 Угрозы безопасности и риски

В данной Рекомендации предполагается, что системы, компоненты, интерфейсы, информация, ресурсы связь, т. е. сигнализация, управление и трафик данных/канал передачи, и услуги, которые составляют СПП, будут испытывать различные угрозы безопасности и подвергаться различным рискам. Эти угрозы и риски будут зависеть от различных факторов. Кроме того, конечные пользователи также будут подвергаться некоторым угрозам, например, несанкционированного доступа к секретной информации.

Угрозы для СПП:

- неавторизованная разведка, например, дистанционный анализ системы для определения слабых точек, она может включать в себя сканирование, развертку, запрос порта, таблицу маршрутизации и др.;
- захват/взлом устройства, приводящий к потере управления устройством, аномалиям и ошибкам при проверке конфигурации;
- уничтожение информации и/или других источников;
- повреждение или изменение информации;
- кража, удаление, или потеря информации и/или других источников;
- раскрытие информации; и
- прерывание обслуживания и отказ в обслуживании.

Далее ясно, что сети СПП будут работать в условиях, отличающихся от условий работы сетей ТфОП и, следовательно, могут подвергаться различным видам угроз и атак изнутри или снаружи. Сети СПП будут непосредственно или косвенно связаны с недоверенными или доверенными сетями и оконечным оборудованием, и поэтому будут подвержены рискам и угрозам безопасности, связанным с возможностью соединения с небезопасными сетями и принадлежащим пользователю оборудованием. Например, сеть поставщика СПП может иметь возможность непосредственного или косвенного, т.е. через другую сеть, соединения со следующими объектами, как показано на Рисунке 2:

- другими поставщиками услуг и их приложениями;
- другими сетями СПП;
- другими IP-сетями;
- телефонной сетью общего пользования с коммутацией каналов (ТфОП);
- корпоративными сетями;
- сетями пользователя;
- оконечным оборудованием;
- другими транспортными доменами СПП.

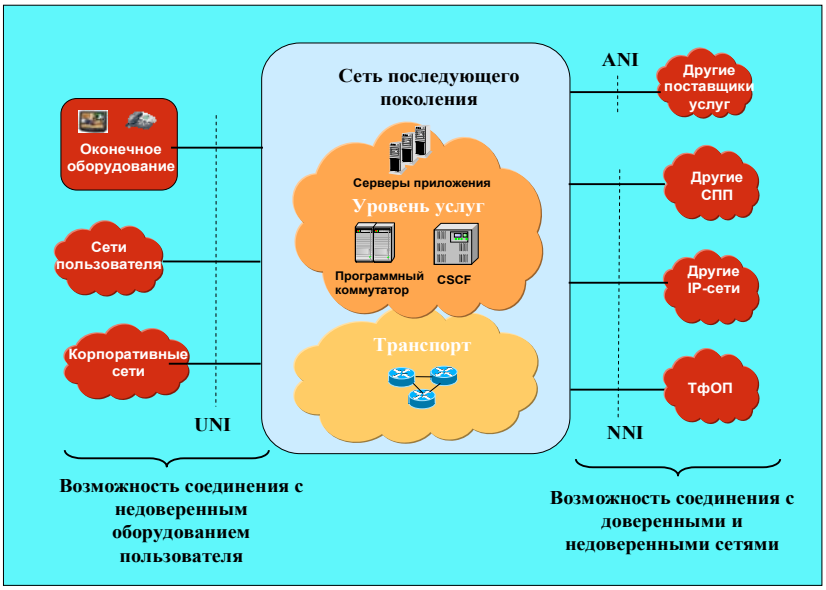

Рисунок 2 – Возможность соединения с сетями и пользователями

В условиях развивающихся технологий безопасность во многих сетевых доменах поставщиков основана на объединении всего того, что все поставщики решают предпринять для обеспечения безопасности собственных сетей. Несанкционированный доступ в сеть какого-либо поставщика может легко привести к использованию связанной с ней сети и связанных с ней услуг. Это является примером использования самого слабого звена, которое может угрожать целостности сети поставщика и бесперебойности обслуживания в условиях атак различных типов.

Каждый поставщик СПП несет ответственность за безопасность в пределах своего домена. Каждый поставщик СПП несет ответственность за разработку и внедрение решений безопасности с использованием определенной политики сети для отношений доверия (раздел 5), для того чтобы удовлетворять потребности собственной сети и поддерживать достижение целей глобальной сквозной безопасности в многочисленных сетевых доменах поставщиков.

5 Модель доверия безопасности

В данном разделе определяется модель доверия безопасности СПП.

В функциональной эталонной архитектуре СПП определяются функциональные объекты (FE). Тем не менее, так как аспекты безопасности сети значительно зависят от способа, при помощи которого объекты FE связываются вместе, архитектура безопасности СПП основывается на физических элементах сети (NE), т.е. материальных модулях, содержащих один или несколько FE. Способ связывания данных объектов FE и объединения их в элементы NE будет зависеть от поставщика.

5.1 Единая сетевая модель доверия

В данном подразделе определяются три зоны безопасности:

1) доверенная;
2) доверенная, но уязвимая;
3) недоверенная,

которые зависят от эксплуатационного управления, местоположения и возможности соединения с другими устройствами/элементами сети. Эти три зоны представлены в модели доверия безопасности, показанной на Рисунке 3.

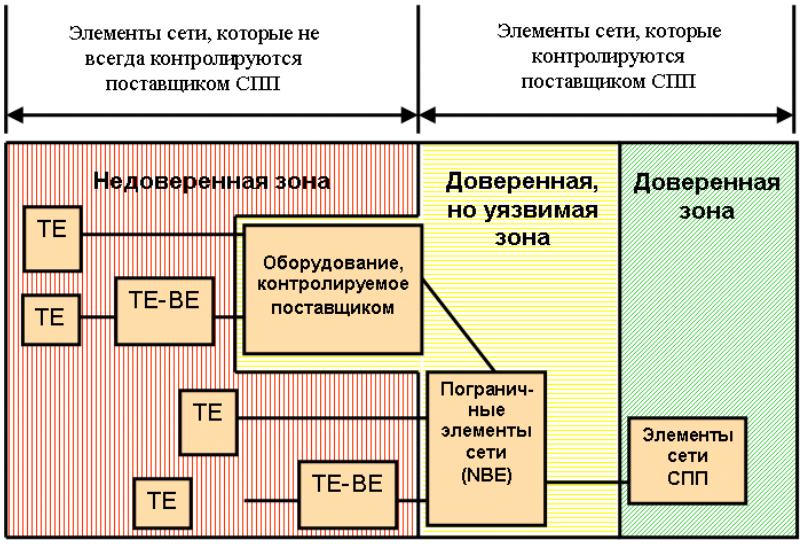

Рисунок 3 – Модель доверия безопасности

"Доверенная зона безопасности сети", или для краткости, "доверенная зона" – это область, где расположены элементы сети и системы поставщика СПП, которые никогда не связываются напрямую с оборудованием пользователя или другими доменами. Общие характеристики элементов сети СПП в данной области заключаются в том, что они полностью управляются поставщиком СПП, расположены в домене поставщика СПП и связываются только с элементами в "доверенной" зоне и

с элементами в "доверенной но уязвимой зоне". Следует заметить, что поскольку речь идет о доверенной области, она безопасна *сама по себе*.

"Доверенная" область будет защищаться сочетанием различных методов. В качестве примера можно привести физическую безопасность элементов сети СПП, общее укрепление систем, использование безопасной сигнализации, безопасность для сообщений OAMP отдельной сети VPN в пределах сети MPLS/IP для связи в пределах "доверенной" зоны и с элементами сети СПП в "доверенной, но уязвимой" зоне. Подробности приводятся в разделе 8.

"Доверенная, но уязвимая зона безопасности сети", или, для краткости, "доверенная, но уязвимая зона" представляет собой зону, в которой работают (предоставлены и обслуживаются) элементы сети/устройства поставщика СПП. Оборудование может находиться под управлением либо пользователя/абонента, либо поставщика СПП. Кроме того, оборудование может находиться, как на объектах поставщика СПП, так и в других местах. Оно связывается с элементами, как в доверенной зоне, так и в недоверенной зоне, и поэтому оно является "уязвимым". Его главная функция безопасности заключается в защите элементов NE в доверенной зоне от атак безопасности, инициированных в недоверенной зоне.

Элементы, располагающиеся в домене поставщика СПП, имеющие возможность соединения с элементами, находящимися вне доверенной зоны, называются пограничными элементами сети (NBE). Например, такими элементами являются:

- Пограничные элементы сети (NBE) на интерфейсе UNI, который служит средством связи с управлением службой или транспортными элементами поставщика СПП в доверенной зоне для обеспечения доступа пользователю/абоненту к сети поставщика СПП с целью получения услуг и/или транспортировки данных.
- Пограничный элемент домена (DBE), который являются тем же видом оборудования, что и пограничный элемент сети, за исключением того, что он находится на границе доменов.
- Пограничный элемент сети (NBE) конфигурации устройств и начальной загрузки (DCB-NBE), служит средством связи с системой конфигурации устройства поставщика СПП в доверенной зоне и позволяет конфигурировать устройство пользователя/абонента и оборудование поставщика СПП, находящееся вне помещений поставщика.
- Пограничный элемент сети (NBE) OAMP-NBE служит средством связи с системами OAMP поставщика СПП в доверенной зоне и служит для обслуживания и поддержки устройств пользователя/абонента и оборудования поставщика СПП, находящегося вне помещений поставщика.
- Пограничный элемент сети (NBE) сервера приложения/веб-сервера (AS/WS-NBE), который служит средством связи с AS/WS-NBE поставщика СПП в доверенной зоне и служит для предоставления пользователю/абоненту доступа к веб-услугам.

К примерам устройств/элементов, которые управляются поставщиком СПП, но не располагаются в помещении поставщика СПП, и могут принадлежать или не принадлежать поставщику СПП, относятся:

- оборудование наружной установки сети/технологии доступа;
- маршрутизатор базовой станции (BSR) – элемент сети, объединяющий базовую станцию, контроллер радиосети и функциональные возможности маршрутизатора;
- оптические блоки (ONU) в пределах местонахождения пользователя/абонента.

Защита "доверенной, но уязвимой зоны", состоящей из NBE, будет осуществлена при помощи сочетания различных методов. Некоторыми примерами являются физическая защита элементов сети СПП, общее укрепление систем, присвоение каждому элементу сети СПП уникального сертификата, использование безопасной сигнализации для всех сообщений сигнализации, отправляемых элементам сети СПП в "доверенной" зоне, безопасность для сообщений OAMP, а также по необходимости модульные фильтры пакетов и брандмауэры. Более подробная информация содержится в разделе 8.

"Недоверенная зона" включает в себя все элементы сети абонентских сетей или возможно одноранговых сетей, или доменов других поставщиков СПП, находящихся за пределами исходного домена, которые связаны с пограничными элементами поставщика СПП. Поставщики СПП могут не иметь возможности управлять оконечным оборудованием пользователя, расположенным в "недоверенной зоне", и не иметь возможности навязать пользователю политику безопасности поставщика. Тем не

менее, желательно принимать некоторые меры безопасности, и с этой целью рекомендуется, чтобы сигнализация, среда передачи и OAM&P были бы защищены и чтобы был бы укреплен TE-BE, расположенный в "недоверенной" зоне. Однако, из-за недостаточной физической защиты, данные меры не могут считаться абсолютно безопасными. Более подробная информация содержится в разделе 8.

5.2 Одноранговая сетевая модель доверия

Когда сеть СПП соединена с другой сетью, доверие зависит от:

- физического соединения, причем соединение может варьироваться от непосредственной связи в защищенном здании до связи через совместно используемые устройства;
- одноранговой модели, в которой обмен трафиком может происходить непосредственно между двумя поставщиками услуг СПП или через одного или нескольких поставщиков транспортных сетей СПП;
- деловых отношений, к которым могут относиться пункты о штрафах в соглашениях SLA и/или доверие к политике безопасности другого поставщика СПП;
- как правило, поставщики СПП должны считать других поставщиков недоверенными.

На Рисунке 4 приведен пример, когда сеть соединения считается недоверенной.

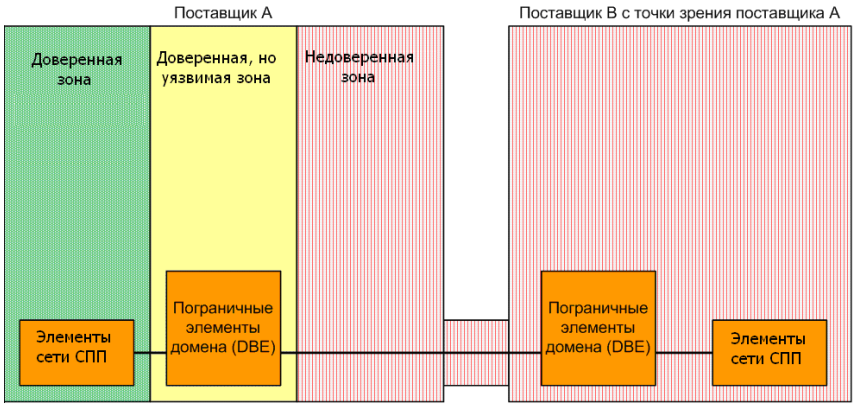

Рисунок 4 – Одноранговая сетевая модель доверия

6 Архитектура безопасности

6.1 Эталон функциональной архитектуры СПП

Архитектура СПП, которая реализует [МСЭ-Т Y.2201] *Требования сетей СПП варианта 1*, определяется в [МСЭ-Т Y.2012] *Функциональные требования и архитектура сетей СПП версии 1.*

На Рисунке 5 показан функциональный вид архитектуры СПП.

Рисунок 5 – Обзор архитектуры СПП (Рисунок 1/Y.2012)

В СПП имеется эталонная точка связи с функциями конечного пользователя, называемая интерфейсом пользователь-сеть (UNI), а также точка связи с другими сетями, которая называется интерфейсом сеть-сеть (NNI). В ней также имеется эталонная точка связи с функциональной группой приложений, которая называется интерфейсом приложение-сеть (ANI) и позволяет использовать возможности СПП для создания и предоставления приложений пользователям СПП.

Транспортный уровень сетей СПП версии 1 предоставляет пользователям СПП услуги IP-соединения управляемые функциями управления транспортировкой, включая функции управления присоединением сети (NACF) и функции управления ресурсами и установлением соединений (RACF).

Уровень обслуживания доставляет услуги и приложения конечному пользователю с помощью функций поддержки приложений, функций поддержки услуг и соответствующих функций управления.

Функции конечного пользователя – это функции, связанные с сетями доступа СПП, и никаких предположений не делалось относительно интерфейсов для различных конечных пользователей и сетей конечного пользователя.

Функции управления обеспечивают возможность управлять сетями СПП для предоставления услуг СПП с ожидаемыми показателями качества, безопасности и надежности.

Более подробная информация содержится в [МСЭ-Т Y.2012].

6.2 Отображение в функциональную архитектуру СПП

В данной Рекомендации описывается метод достижения безопасности с помощью доверенной модели, показанной в разделе 5, то есть сети СПП, состоящей из доверенного домена (зеленая зона), недоверенного домена (красная зона) и доверенного, но уязвимого домена (желтая зона) между ними.

Одним из главных способов достижения безопасности с данной моделью является метод передачи сигнализации, мультимедийной информации и трафика OAMP из недоверенного домена в доверенный домен. Существуют различные методы для достижения этого, и поставщик СПП выбирает метод с учетом своих правил. Ниже приведены примеры данных методов.

a) Установить элемент NE для завершения трафика (например, B2B-UA для сигнализации SIP) между зеленой зоной и красной зоной. Он принимает пакет из красной зоны, изучает его, в случае несоответствия отбрасывает его, а в случае соответствия копирует необходимую часть для восстановления пакета, подходящего для зеленой зоны. В этом случае элементы NE для завершения трафика становятся элементами NE желтой зоны.

b) Управлять трафиком на уровне среды передачи, например, путем открывания и закрывания определенного порта (микроканала) в брандмауэре, этот метод гарантирует, что на оборудование в зеленой зоне могут передавать трафик только авторизованные элементы NE (и пользователи). В данном случае элементы NE, которые управляют трафиком, становятся элементами NE желтой зоны.

c) Сквозное кодирование между отправителем и получателем.

В функциональной архитектуре, показанной в [МСЭ-Т Y.2012] (Рисунок 6 данной Рекомендации), сигнализация SIP, выполняемая функцией конечного пользователя, она обычно является недоверенной, так как поставщик СПП не может подтвердить, что функция не фальшивая, передается на протокол S-2, P-CSC-FE. Следовательно, элементы NE, содержащие объект P-CSC-FE, считаются элементами NE желтой зоны или зеленой зоны, благодаря функциям брандмауэра. Если элементы NE, содержащие S-1 (S-CSC-FE), отделены от элементов NE, содержащих P-CSC-FE, они считаются элементами NE зеленой зоны.

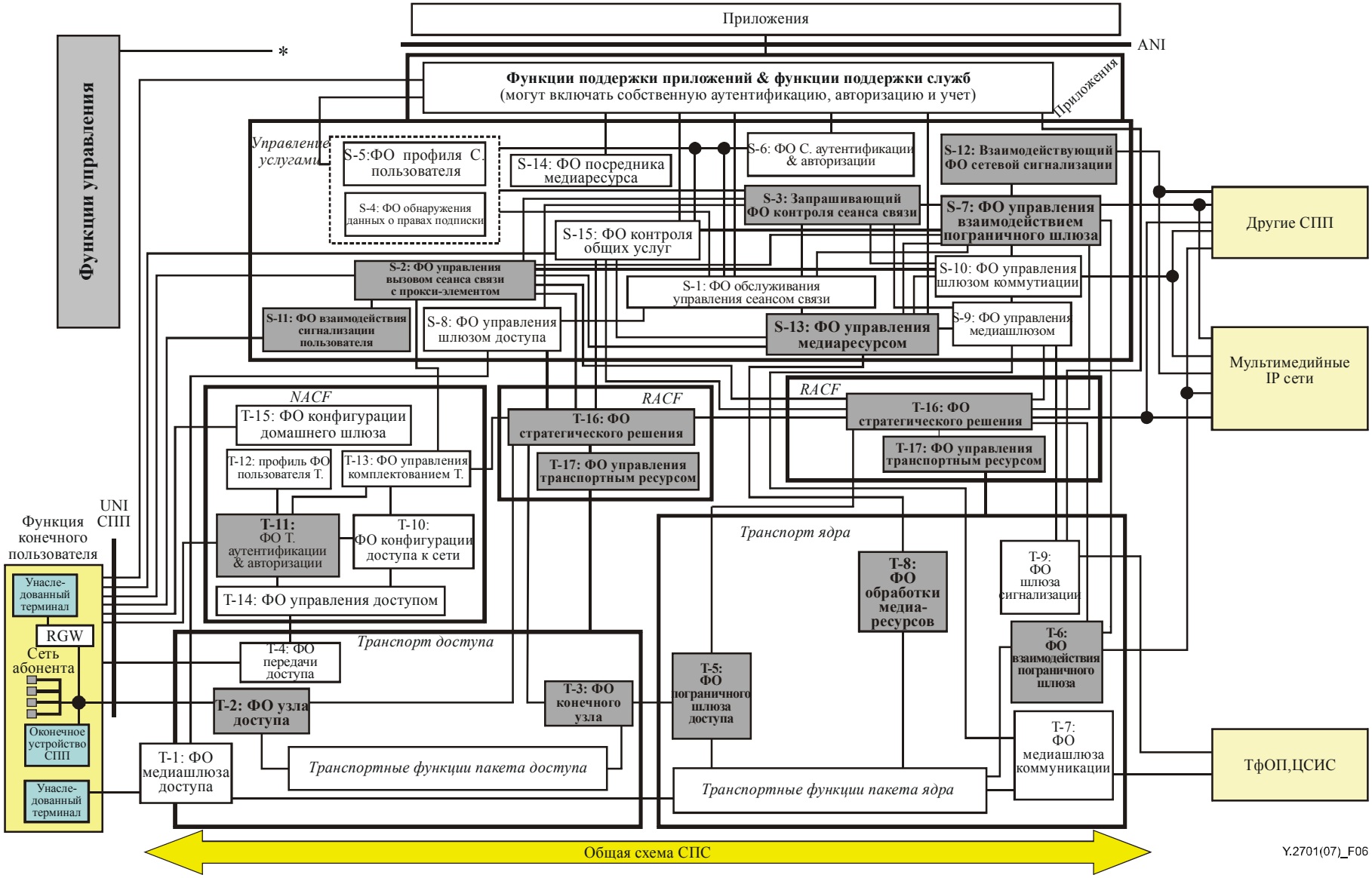

Рисунок 6 – Обобщенная функциональная архитектура (Рисунок 3/Y.2012)

6.3 Идентификация ресурсов СПП для обеспечения безопасности

Каждый поставщик сети должен определить внутри своей сети активы, ресурсы, информацию и интерфейсы, которые должны быть защищены, и угрозы, которые должны быть уменьшены. Например, элементы сети, интерфейсы (UNI, ANI и NNI), системы управления и сигнализации, управление и передача информационных файлов/каналов связи. При определении ресурсов СПП для обеспечения безопасности от угроз, теоретическая многоуровневая архитектура, определенная в [МСЭ-Т Y.2012], должна быть рассмотрена вместе с практической реализацией функциональных объектов.

В последующих таблицах приведены примеры активов, ресурсов и интерфейсов сетей СПП для гарантии безопасности от угроз, организованные следующим образом:

- Таблица 1 – Пример активов, ресурсов и информации, связанных с UNI.
- Таблица 2 – Пример активов, ресурсов, информации и интерфейсов, связанных с транспортным уровнем.
- Таблица 3 – Пример активов, ресурсов, информации и интерфейсов, связанных с уровнем обслуживания.
- Таблица 4 – Пример активов, ресурсов, информации и интерфейсов, связанных с администрированием.

Примеры в Таблицах 1–4 не являются полностью исчерпывающими.

Таблица 1 – Пример активов, ресурсов и информации, связанных с UNI

Примеры	Цели и задачи
Ресурсы конечного пользователя: • Устройства пользователя • Шлюзы сети пользователя • Шлюзы корпоративной сети	a) Защищать оборудование конечного пользователя, соединенного с сетью, например, оконечные устройства, шлюзы сети пользователя и корпоративной сети, от атак, исходящих от сети, например, атак с целью уничтожения, повреждения, изменения оборудования пользователя. b) Защищать от прерывания услуг, например, запрет атак отказа в обслуживании, и гарантия доступности услуг. c) Защищать сети от несанкционированного доступа, например, несанкционированных пользователей и устройств пользователя.
Информация конечного пользователя: • Информация о подписке • Информация идентичности • Информация о местонахождении	a) Защищать от повреждения или изменения информации. b) Защищать от кражи, удаления или потери, например, от кражи идентичности. c) Защищать от раскрытия, например, от несанкционированного доступа к данным о местонахождении.
Информация поставщика СПП • Информация идентичности	a) Защищать от повреждения или изменения информации. b) Защищать от кражи, удаления или потери, например, от кражи идентичности. c) Защищать от раскрытия, например, от несанкционированного доступа к данным о местонахождении.
Интерфейсы UNI	a) Транспортный уровень – обеспечивать защиту трафика/канала передачи на интерфейсах UNI. b) Служебный уровень (управление услугами) – обеспечивать защиту сигнализации и управления на интерфейсах UNI, например, SIP, HTTP, ISDN, и H.248. c) Служебный уровень (поддержка приложений и услуг) – обеспечивать защиту функций управления приложениями и услугами в интерфейсах UNI, например, внутриполосной сигнализацией.

Таблица 2 – Пример активов, ресурсов, информации и интерфейсов, связанных с транспортным уровнем

Примеры	Цели и задачи
Ресурсы транспортного уровня: • Элементы транспортной сети, например, IP маршрутизаторы, узлы MPLS • Линии передачи • Маршрутная информация, например, серверы DNS • Информация о профиле пользователя транспорта, например, транспортные базы данных и хранилище данных	a) Защищать все элементы, компоненты и функции транспортной сети от несанкционированного доступа. b) Защищать целостность элементов, компонентов и функций транспортной сети. c) Защищать доступность элементов, компонентов и функций транспортной сети. Защищать от прерывания обслуживания, т.е. от атак типа "отказ в обслуживании". d) Защищать от раскрытия любой личной информации пользователя или сети.
Внутрисистемные связи на транспортном уровне (связь в пределах сети поставщика сетевых услуг)	a) Обеспечивать безопасность трафика/канала передачи между системами в пределах сети поставщика. b) Обеспечивать безопасность сигнализации, контроль и управление транспортом, например, OSPF, в сети поставщика. c) Обеспечивать безопасность сигнализации между системами на уровне обслуживания, например, между серверами приложений, и системами на транспортном уровне, например, IP-маршрутизаторами.
Транспортные интерфейсы и связи	a) Обеспечивать защиту безопасности трафика/канала передачи между транспортными интерфейсами UNI, NNI и ANI. b) Обеспечивать защиту безопасности сигнализации управления транспортировкой, например OSPF, и управления на транспортных интерфейсах UNI, NNI и ANI.

Таблица 3 – Пример активов, ресурсов, информации и интерфейсов, связанных с уровнем обслуживания

	Примеры	Цели и задачи
Уровень обслуживания – Управление обслуживанием	Уровень обслуживания – Ресурсы управления обслуживанием • Элементы сети управления обслуживанием, например, элементы CSC-FE, SL-FE, MRP-FE, шлюзы, S/BC	a) Защищать все элементы сети, компоненты и функции управления обслуживанием от несанкционированного доступа b) Защищать целостность элементов сети, компонентов и функций управления обслуживанием, включая защиту от повреждения или изменения информации. c) Защищать доступность элементов сети, компонентов и функций управления обслуживанием. Защищать от прерывания в обслуживании, т. е. от атак типа "отказ в обслуживании".
	Уровень обслуживания – Информация управления обслуживанием • Информация абонентов, например, базы данных и хранилища данных, содержащие профили пользователей и профили услуг • Сетевая информация, например, базы данных и хранилища данных, содержащие информацию о маршрутизации, нумерации и адресации информации	a) Защищать от повреждения или изменения данных и информации b) Защищать от кражи, удаления или потери, например, от кражи идентичности c) Защищать от раскрытия, например, от несанкционированного доступа к частной информации пользователя и сети.
	Уровень обслуживания – Межсистемные связи для управления обслуживанием	Обеспечивать защиту безопасности межсистемной сигнализации, например, протоколов SIP, RADIUS, Диаметр, в сети поставщика сетевых услуг, например, защиту передачи сигнализации от CSCF к HSS.
	Интерфейсы и связь	Обеспечивать защиту безопасности сигнализации и управления на интерфейсах UNI, NNI и ANI.

Таблица 3 – Пример активов, ресурсов, информации и интерфейсов, связанных с уровнем обслуживания

	Примеры	Цели и задачи
Уровень обслуживания – Поддержка приложений и обслуживания	Уровень обслуживания – Ресурсы поддержки приложений и обслуживания: • Элементы сети и платформы поддержки приложений и обслуживания, например, сервера приложений, базы данных, интернет-порталы	a) Защищать все элементы сети, компоненты и функции поддержки обслуживания от несанкционированного доступа b) Защищать целостность элементов сети, компонентов и функций поддержки обслуживания, включая защиту от повреждения или изменения информации. c) Защищать доступность элементов сети, компонентов и функций поддержки обслуживания. d) Защищать от прерывания в обслуживании, т. е. от атак типа "отказ в обслуживании".
	Уровень обслуживания – Информация поддержки приложений и обслуживания: • Информация приложений и обслуживания • Информация о подписке	a) Защищать от повреждения или изменения данных и информации. b) Защищать от кражи, удаления или потери, например, кражи идентичности. c) Защищать от раскрытия, например, от несанкционированного доступа к частной информации пользователя и сети.
	Интерфейсы	a) Обеспечивать защиту безопасности элементов сети и ресурсов для доступа другого поставщика приложений, например, шлюзы Parlay и Открытого мобильного альянса (OMA) b) Обеспечивать защиту безопасности интерфейсов UNI, NNI и ANI c) Обеспечивать защиту безопасности передачи трафика сигнализации и управления через интерфейсы ANI.

Таблица 4 – Пример активов, ресурсов, информации и интерфейсов, связанных с управлением

Пример	Цели и задачи
Ресурсы управления • Системы управления транспортного уровня, например, системы управления элементами сети, управления сетями и управления обслуживанием • Системы управления уровня обслуживания, например, системы управления элементами сети, управления сетями и управления обслуживанием	a) Защищать все элементы сети, компоненты, функции и интерфейсы управления от несанкционированного доступа. b) Защищать целостность элементов сети, компонентов, функций и интерфейсов управления. Включает в себя защиту от повреждения или изменения информации. c) Защищать доступность элементов сети, компонентов, функций и интерфейсов управления. Защищать от прерывания в обслуживании, т. е. от атак типа "отказ в обслуживании".
Межсистемные связи в пределах сети поставщика сетевых услуг	a) Обеспечивать защиту безопасности трафика управления между системами управления, в пределах сети, например, на уровне обслуживания. b) Обеспечивать защиту безопасности трафика управления между сетью пользователя, транспортным уровнем поставщика сети и уровнем обслуживания
Интерфейсы и межсистемные связи	a) Обеспечивать защиту безопасности внутренних интерфейсов управления сети и любых интерфейсов управления UNI, NNI и ANI. b) Обеспечивать защиту безопасности передачи трафика управления через интерфейсы UNI, ANI, NNI.

7 Задачи и требования

7.1 Общие задачи безопасности

Ниже представлен список основных задач безопасности, используемый для руководства требованиями в данной Рекомендации.

- Функции безопасности СПП должны быть расширяемыми и достаточно гибкими для удовлетворения различных нужд.
- Требования безопасности должны учитывать качественные показатели, удобство в эксплуатации, расширяемость и стоимость СПП.
- При возможности методы безопасности должны основываться на существующих и хорошо понятных стандартах безопасности.
- Архитектура безопасности СПП должна быть универсально масштабируема в пределах домена поставщика сети, в доменах нескольких поставщиков сети, при предоставлении услуг безопасности.
- Архитектура безопасности СПП должна учитывать логическое или физическое разделение трафика сигнализации и контроля, трафика пользователя и трафика управления.
- Безопасность сетей СПП должна безопасно обеспечиваться и безопасно управляться.
- Сеть СПП должна обеспечивать безопасность со всех точек зрения: службы, поставщика сети и абонента.
- Методы безопасности не должны влиять на качество предоставляемых услуг.
- Безопасность должна обеспечивать абонентам и поставщикам возможность простой, безопасной работы и конфигурации (включи и работай).
- Соответствующие уровни защиты должны поддерживаться даже, если используется функция многоадресной связи.

- Функции обнаружения услуги должны иметь множество критериев обзора, например, местонахождение, стоимость и пр., для обеспечения необходимого масштабирования с необходимыми механизмами для обеспечения безопасности и секретности.
- Система распознавания адреса должна быть особой системой, которая используется только данной сетью и требует применения определенных мер безопасности. Данная система может использовать базы данных, находящиеся в пределах или вне домена.
- Должны соблюдаться принципы и общие задачи безопасности для безопасного управления СУЭ в том виде, как они приведены в разделе 7 [МСЭ-Т M.3016.0].

7.2 Задачи безопасности, охватывающие домены нескольких поставщиков сетевых услуг

Главной задачей является обеспечение безопасности на основе сети для сквозных систем связи в условиях существования множества доменов поставщиков. Это достигается с помощью обеспечения сквозной безопасности системы связи, основанной на возможности ретрансляции через домены различных поставщиков. На Рисунке 7 показана основная концепция сети, обеспечивающая связь между оконечными пользователями. Каждый участок сети несет ответственность за безопасность в пределах своей области безопасности для облегчения безопасности и доступности систем связи СПП в условиях множества сетей.

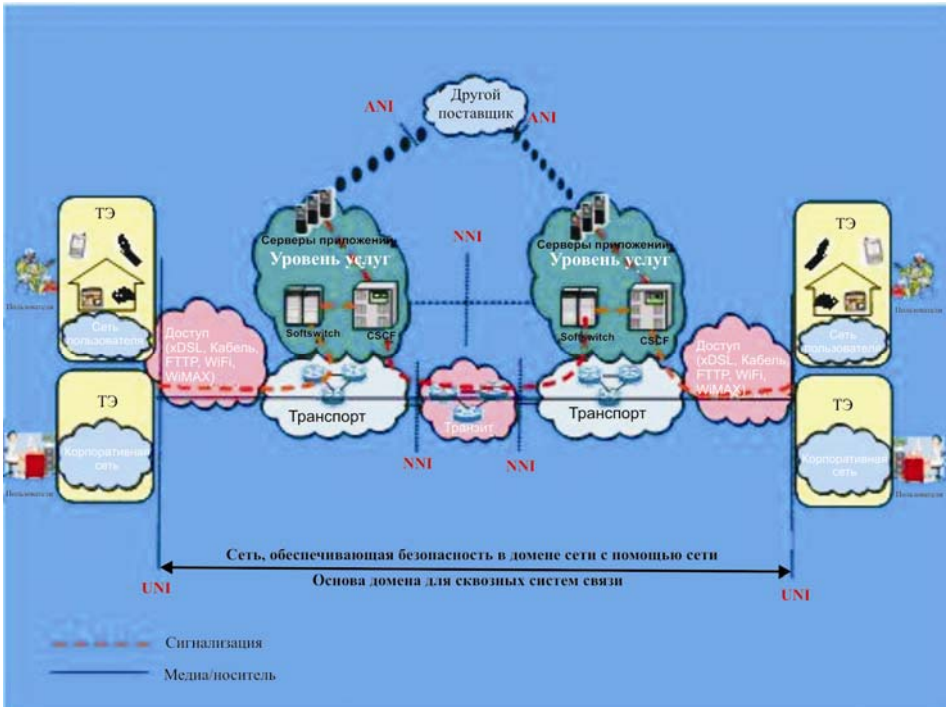

Рисунок 7 – Безопасность систем связи в условиях множества сетей

Как описывается в разделе 5.2, доверенная модель между взаимосвязанными сетями СПП зависит от нескольких аспектов, таких как физическая взаимосвязь, модели одноранговых сетей и деловое сотрудничество.

7.3 Задачи, характерные для аспектов безопасности

Задачи, описанные в данном пункте, являются характерными для определенных аспектов безопасности, таких как аутентификация. Они являются общими для всех интерфейсов.

7.3.1 Контроль доступа

Поставщики СПП должны предоставлять доступ только авторизованным абонентам. Авторизация может даваться поставщиком, предоставляющим доступ, или другими поставщиками после выполнения процессов аутентификации и управления доступом.

Сеть СПП должна предотвращать несанкционированный доступ, например, нарушителей, маскирующихся под авторизованных пользователей.

7.3.2 Аутентификация

Поставщики СПП должны поддерживать возможность аутентификации абонентов, оборудования, элементов сети и других поставщиков. Это включает в себя, но не ограничивается, поддержкой следующего:

1) Возможностей аутентифицировать пользователей для доступа в транспортную сеть, например, аутентификация и авторизация устройства конечного пользователя, шлюза пользовательской сети или шлюза корпоративной сети для получения доступа или присоединения к доступу в транспортную сеть.
2) Возможностей аутентифицировать пользователей для доступа к услугам в начале и во время доставки услуги, например, аутентификация пользователя, устройства или комбинации пользователь/устройство, когда аутентификация применятся к доступу к службам/приложениям СПП.
3) Возможностей для абонента аутентифицировать поставщика СПП на каждом уровне, например, аутентификация пользователем идентичности поставщика подключенной сети СПП или поставщика услуг, если это требуется политикой безопасности.
4) Возможностей, позволяющих пользователю аутентифицировать равноправные с ним объекты, например, вызываемого пользователя, объект, инициирующий вызов, или источник данных, в качестве услуг или возможностей сети.
5) Возможностей, позволяющих двустороннюю аутентификацию между двумя поставщиками СПП на каждом уровне для обмена трафиком сигнализации, управления и информации/канала передачи, например, аутентификация сетей, соединенных непосредственно или косвенно через интерфейсы NNI.
6) Возможности аутентификации других поставщиков услуг через интерфейсы ANI. Должны поддерживаться методы на основе SIM или не на основе SIM.

ПРИМЕЧАНИЕ. – Аутентификация объекта не означает положительного подтверждения физического лица.

7.3.3 Сохранность информации

В данной Рекомендации не определяются никакие требования безопасности для сохранности информации.

7.3.4 Конфиденциальность данных

Поставщики СПП должны защищать конфиденциальность трафика абонента с помощью криптографии или другими способами.

Поставщики СПП должны защищать конфиденциальность сообщений контроля с помощью криптографии или другими способами, если этого требует политика безопасности.

Поставщики СПП должны защищать конфиденциальность трафика управления с помощью криптографии или другими способами.

7.3.5 Безопасность связи

Поставщики СПП должны иметь возможность предоставлять механизмы обеспечения того, что информация не подвергается незаконному перенаправлению или перехвату.

7.3.6 Целостность данных

Поставщики СПП должны защищать целостность трафика абонента с помощью криптографии или другими способами.

Поставщики СПП должны защищать целостность сообщений контроля с помощью криптографии или другими способами, если этого требует политика безопасности.

Поставщики СПП должны защищать целостность трафика управления с помощью криптографии или другими способами.

7.3.7 Доступность

Для подавления атак отказа в обслуживании (DoS), распространения вирусов или червей, а также других атак, поставщики СПП должны иметь возможность поддерживать предоставление мер безопасности для предотвращения или завершения соединений с несоответствующим оборудованием конечного пользователя. Действие данных возможностей может приостанавливаться для обеспечения связи в чрезвычайных ситуациях. Элементы внешней сети СПП также могут быть восприимчивы к вирусам, червям и другим атакам. Также требуются аналогичные меры для карантина сетевых компонентов.

Сеть СПП должна предоставить возможности обеспечения безопасности, для того чтобы поставщик СПП мог отфильтровывать пакеты и трафик, считающиеся вредными с точки зрения политики безопасности.

Сеть СПП должна предоставить возможности для поддержки функций и процедур восстановления после бедствий. Эти особые требования не входят в сферу применения данной Рекомендации.

7.3.8 Секретность

Сеть СПП должна обеспечивать возможности защиты личной информации абонента, например, о местонахождении данных, идентичностях, телефонных номерах, сетевых адресах или данных учета вызовов, согласно национальным правилам и законам. Эти особые требования не входят в сферу применения данной Рекомендации.

8 Особые требования к безопасности

В данном разделе определяются особые требования безопасности для каждого элемента сети в пределах инфраструктуры СПП. Однако, поскольку многие потребности безопасности будут одинаковыми для разных типов элементов сети, сначала определяются типовые требования безопасности в разделе 8.1.

Пограничные элементы могут объединяться или разделяться в зависимости от реализации.

8.1 Типовые требования к безопасности для элементов сети СПП

Данные требования применяются к элементам сети СПП в доверенной области и в доверенной, но уязвимой области. Желательно, чтобы данным требованиям соответствовали и устройства в недоверенной зоне.

Ниже приведен список общих требований к безопасности.

Взаимодействие должно поддерживаться различными элементами сети СПП, в частности, между различными механизмами безопасности СПП. Минимальные стандартизованные возможности безопасности должны быть доступны во всем мире.

Необходимо, чтобы аутентификация и авторизация (пользователь-сеть, сеть-пользователь, сеть-сеть) применялись на транспортном уровне и уровне обслуживания. Аутентификация должна быть возможной также и при обратной трансляции NAPT.

Элемент сети СПП должен принимать меры безопасности против несанкционированного доступа к сетевым ресурсам, устройствам, услугам и данным абонента (профилю), например, путем блокирования неавторизованного трафика.

Сетевая инфраструктура СПП должна позволять поставщикам обеспечивать видимость топологии и ресурсов сети только авторизованным объектам.

Необходимо, чтобы инфраструктура СПП поддерживала множественные области безопасности. С целью обеспечения безопасности может потребоваться изоляция между разными зонами безопасности.

Необходимо, чтобы инфраструктура СПП гарантировала конфиденциальность и целостность передаваемых через нее потоков сигнализации/контроля и потоков управления.

Инфраструктура СПП должна гарантировать конфиденциальность, целостность передаваемых через нее потоков информации.

СПП должна точно гарантировать безопасность элементов сети, связанных с ресурсами управления (OSS, базы данных и пр.) и ресурсов услуг.

Требования безопасности для безопасного управления СУЭ соответствуют требованиям, приведенным в п.10.1 [МСЭ-Т M.3016.0] и более подробно описанным в п. 6 [МСЭ-Т M.3016.1].

Необходимо, чтобы функциональные возможности безопасности применялись для пограничных элементов сети (NBE или TE-BE, т.е. для элементов NE в доверенной, но уязвимой области). Они включают в себя такие функции, как контроль доступа к пакетам данных и информации сигнализации в соответствии с определенными правилами, например, отказ передавать трафик от определенных приложений или пользователей.

Чувствительные элементы СПП, особенно пограничные элементы сети, могут осуществлять логическое и/или физическое разделение транспортных путей в соответствии с применяемой политикой безопасности, например, отделение потоков контроля и/или управления от информационных потоков, используя логически различные интерфейсы или разные адресные планы, и при помощи физически различных реальных или виртуальных транспортных сетей (например, виртуальные сети VPN и VLAN).

Необходимо, чтобы СПП обеспечивала безопасное хранение данных о безопасности, например, об идентичности и полномочиях. Необходимо, чтобы такое хранение осуществлялось отдельно от общего хранилища данных, содержащего информацию, относящуюся к услугам для абонентов. Необходимо, чтобы в СПП обеспечивалась политика безопасности, включающая набор правил, определяющих, какой трафик должен быть защищен на основе, например, контрактов, какой вид защиты используется, как часто меняются ключи сеансов связи, и правила, определяющие соответствие безопасности устройства.

Необходимо, чтобы СПП поддерживала возможность мониторинга сетевого трафика и определяла базовые данные того, что должно считаться обычными событиями сети.

Необходимо, чтобы СПП имела возможность обнаруживать случаи анормальных событий сети, сообщать о них и противостоять им.

8.1.1 Политика безопасности

Политика безопасности – это набор правил, определенных органом безопасности, который управляет использованием и предоставлением услуг и возможностей безопасности. Поставщики СПП должны подготовить соответствующую политику безопасности и должны нести ответственность за ее применение ко всем элементам NE и устройствам, находящимся под их контролем.

8.1.2 Укрепление и лишение права на обслуживание

Все элементы сети СПП должны иметь способность к конфигурированию для минимальных услуг, необходимых для поддержки инфраструктуры СПП поставщика СПП. Во всех системах и элементах сети необходимо отключить любой порт уровня обслуживания или транспортировки, которые не требуются для правильной работы элементов СПП. Кроме того, необходимо, чтобы приложения работали с минимальными привилегиями, например, на платформах "UNIX/Linux" приложения не должны запускаться как корневые, если им не нужны корневые привилегии. Необходимо, чтобы операционная система (OS), поддерживающая любой элемент СПП, могла быть сконфигурирована специальным образом для обеспечения безопасности и соответственно укреплена. Недопустимы никакие "черные ходы" (доступ для программного обеспечения, которое может обойти обычные механизмы контроля доступа) к любому элементу СПП.

Помимо укрепления, для реализации наилучших практических методов в промышленности должны применяться физические и логические схемы управления доступом.

8.1.3 Журнал регистрации событий, перехват событий и регистрация событий

Все элементы СПП должны иметь возможность создания и ведения журнала регистрации событий, который содержит реестр событий, связанных с безопасностью, в соответствии с политикой безопасности поставщика СПП. Необходимы механизмы для предотвращения его несанкционированного или неопределяемого изменения.

Должна существовать возможность управления журналом регистрации событий, а также возможность перемещения старых данных из журнала регистрации событий на другие носители информации, например, сменные носители для долгосрочного хранения. Данный интерфейс должен позволять авторизованным администраторам перемещать старые данные из журнала регистрации событий на сменные носители. Необходимо, чтобы данная возможность требовала специальной авторизации для управления и была защищена с помощью определенной авторизации для управления журналом регистрации событий.

В п. 10.1.2.6.3 [МСЭ-Т M.3016.0] и пп. 6.6, 6.7 [МСЭ-Т M.3016.1] содержится более подробная информация о требованиях безопасности для безопасной регистрации и учета.

8.1.4 Нанесение меток времени и датчик времени

Необходимо, чтобы элементы СПП поддерживали использование доверенных датчиков времени для системных часов и записей в журнале регистрации. Доверенный источник времени в данном случае означает источник времени, который может быть проверен на предмет устойчивости к несанкционированному изменению. Переходное доверие также приемлемо, т. е. источник времени, полагающийся на доверенный источник времени, сам является доверенным источником времени.

8.1.5 Распределение ресурсов и обработка исключительных ситуаций

Необходимо, чтобы каждый элемент СПП имел возможность ограничивать количество своих важных ресурсов, например, распределение памяти запросам на обслуживание. Эти ограничения могут уменьшить негативные последствия атак "отказ в обслуживании". Запросы на обслуживание, конкурируют в системе с другими запросами на ресурсы. Кроме того, каждое отдельное приложение СПП должно иметь возможность ограничивать использование у себя важных ресурсов, выделенных для выполнения запросов.

Целью данного требования является ограничение воздействия вспышек активности так, чтобы они не влияли на другие запросы на обслуживание. Это также даст/оставит приложению (и OS) возможность сообщать системе мониторинга о том, что приложение и/или его платформа могут испытывать атаку DoS. Необходимо, чтобы элемент СПП обеспечивал интерфейс для наблюдения за использованием ресурсов.

Элемент СПП должен безмолвно отклонять любые пакеты, которые не соответствуют ожидаемому протоколу или формату, и, основываясь на политике безопасности, должен иметь возможность создавать в журнале запись для каждого подобного события. "Безмолвное отклонение" означает перехват и регистрацию принятого пакета, а также отбрасывание принятого пакета, без уведомления об отбрасывании, например, без передачи сообщения об ошибке.

Цель состоит в том, чтобы ограничить возможные атаки со стороны вредоносных или неправильных пакетов. Однако, что если использование действий регистрации так велико, что оно пересекается с другими действиями элемента, очевидным решением будет прекращение регистрации до тех пор, пока использование ресурсов не вернется на приемлемый уровень.

ПРИМЕЧАНИЕ. – Это часть управления внешними ресурсами, как упоминалось ранее.

8.1.6 Мониторинг и целостность кода и системы

Элемент сети должен иметь основанные на политике безопасности возможность мониторинга 1) своей конфигурации и программного обеспечения и 2) любых изменений для обнаружения несанкционированных изменений. Любые несанкционированные изменения должны приводить к созданию записи в журнале регистрации и генерированию сигнала тревоги. Элемент должен периодически сканировать свои ресурсы и программное обеспечение на предмет вредоносного программного обеспечения, например, вируса. Элемент должен генерировать сигнал тревоги, если в процессе сканирования обнаруживается вредоносное программное обеспечение.

Необходимо, чтобы управление мониторингом велось таким образом, чтобы оно не влияло на передачи в реальном времени, которые чувствительны к задержкам связи, или чтобы соединения не разрывались без необходимости.

В Рекомендации [M.3016.0] (пункт 10.1.2.6.4) содержаться подробное описание требований к безопасности для целостности системы.

8.1.7 Поправки, текущие исправления и добавочный код

Для того чтобы доверять сигналам, создаваемым элементами СПП поставщика СПП внутри недоверенных сетей, например, терминалами, требуется, чтобы программное обеспечение системы не подвергалось опасности. Это дает гарантии того, что "Троянские кони[1]" (которые звонят своему создателю), "черви" (которые создают бесполезный трафик или превращают систему в "зомби") и

[1] Многие троянские кони действуют для хакера, отправляющего их, как программное обеспечение дистанционного управления. Когда они благополучно установлены на целевой системе, они инициируют обратное соединение к хакерской системе для информирования его/ее о готовности к работе.

другие вирусы не будут загружены в элементы СПП или в базовую операционную систему. Такие вирусы могут повредить целостность, конфиденциальность и/или доступность данных системы.

Необходимо, чтобы элементы и системы поставщика СПП обеспечивали возможность подтверждения и проверки всего их программного обеспечения. Результаты проверки должны быть доступны OSS. Это позволит анализировать состояние безопасности инфраструктуры СПП поставщика СПП и сообщать администраторам и поставщикам о том, когда необходимо подавление.

Поправки безопасности должны быть получены от производителей оборудования и своевременно установлены, после того как их сертифицирует поставщик СПП.

В разделе I.5.2 Рекомендации [МСЭ-Т M.3016.1] приводится дальнейшее рассмотрение процесса поправок, а в разделе I.5.3.9 Рекомендации [МСЭ-Т M.3016.1] представлено рассмотрение предположение безопасности операционной системы.

8.1.8 Доступ к функциям OAMP в устройствах

Для обеспечения безопасности инфраструктуры OAMP каждый внутренний элемент сети СПП должен управляться через отдельный IP-адрес, назначенный ему из отдельного блока адресов. Каждый внутренний элемент сети СПП должен иметь физически или логически отдельный интерфейс для исключительного использования данного трафика OAMP. При использовании отдельного интерфейса элемент сети СПП должен по умолчанию отбрасывать все пакеты, полученные по интерфейсу OAMP с адресом источника, отличающимся от адреса OAMP. Элемент сети должен по умолчанию отбрасывать все пакеты, полученные по не OAMP интерфейсу с адресом источника, назначенным трафику OAMP.

Необходимо, чтобы доступ к функциям OAMP мог управляться посредством аутентификации. После того как пользователь аутентифицирован системой, внутренний элемент СПП должен отслеживать все сделанные изменения и обеспечивать возможность их отмены.

Необходимо, чтобы всякое относящееся к безопасности использование авторизации регистрировалось в журнале регистрации в определенное время. Например, необходимо, чтобы в журнале регистрации отмечались все попытки доступа к элементу, успешные или нет.

Конфиденциальность трафика OAMP должна быть защищена. Если трафик OAMP (включая SNMP и NTP) проходит через недоверенную сеть, то его конфиденциальность должна быть защищена, например, с помощью протоколов IPSec или MPLS.

8.2 Требования к безопасности для элементов сети СПП в доверенной зоне

Элементу сети СПП версии 1 в "доверенной" области должен быть присвоен IP-адрес в блоке, предназначенном для внутренних элементов СПП. Необходимо, чтобы этот адрес использовался для всей сигнализации. Кроме того, необходимо, чтобы элементу СПП версии 1 был присвоен IP-адрес в блоке, предназначенном для OAMP, и все OAMP должны использовать данный адрес.

Для того чтобы сохранить конфиденциальность и целостность связи, трафик сигнализации и передачи информации пользователя должен быть защищен либо с помощью криптографии транспортировки, либо за счет гарантии того, что, трафик будет передаваться только в защищенном домене.

8.3 Требования к пограничным элементам сети СПП в "доверенной, но уязвимой" зоне

Пограничные элементы сети являются главной защитой от внешних атак, т.е. атак от элементов сети/устройств в недоверенной зоне. Весь трафик от элементов сети/устройств в недоверенной зоне передается сначала на пограничный элемент сети, где он проверяется перед передачей в пункт назначения в "доверенной" зоне. Возможность обеспечения физического/логического разделения сети используется для того, чтобы запретить трафику от элементов сети/устройств в недоверенной зоне попадать на любой элемент в "доверенной" зоне.

Пограничные элементы сети (NBE) являются главной защитой от атак на трафик сигнализации. Весь трафик сигнализации от TE или TE-BE в недоверенной зоне обрабатывается в приписанном к нему

NBE, который перенаправляет сигнализацию сетевому оборудованию в доверенной зоне. Возможность обеспечения физического/логического разделения сетей в элементе NBE используется для того, чтобы запретить трафику от TE/TE-BE в недоверенной зоне попадать на любой элемент в доверенной зоне, за исключением приписанного(ых) к нему элемента(ов) NBE.

Как и в случае сигнализации, пограничные элементы сети (NBE) являются главной защитой от атак на информационные потоки. Весь информационный трафик от TE/TE-BE обрабатывается в NBE, и элемент NBE передает информацию далее. Элемент NBE направляет информационные пакеты к пункту назначения и через доверенный домен, только если информационный пакет связан с работающим авторизованным сеансом связи. Информационные пакеты, которые не связаны с запросом сеанса связи, являются недействительными, они не имеют пункта назначения и отбрасываются. Более того, элемент NBE проверяет источник информационного потока и проверяет, соответствует ли скорость пакетов установленному сеансу связи. Информация передается в пределах оборудования поставщика СПП либо к шлюзу ТфОП (для соединения ТфОП) или к другому элементу NBE. На втором элементе NBE информация обрабатывается и перенаправляется к пункту назначения TE.

ПРИМЕЧАНИЕ. – Термин "сеанс связи" используется для обозначения типа информационного потока, не зависящего от соглашения, использованного для установления сеанса.

Необходимо, чтобы пограничный элемент сети поддерживал множество IP-адресов или множество сетевых интерфейсов. Один IP-адрес ("внутренний" адрес) должен быть присвоен из блока, предназначенного для внутренних элементов СПП версии 1. Этот адрес (или этот интерфейс) должны использовать все потоки сигнализации и все информационные потоки к внутренним элементам СПП версии 1 и от них. Должен быть присвоен один IP-адрес ("внешний" адрес); он должен быть доступен для оборудования TE. Этот адрес (или этот интерфейс) должны использовать все потоки сигнализации и все информационные потоки к TE и от него. Один IP-адрес ("OAMP адрес") должен быть присвоен из блока, предназначенного для OAMP, который доступен для серверов OAMP.

Для того чтобы защитить конфиденциальность связи пользователя от перехвата трафика сигнализации, необходимо, чтобы транспортировка всех сообщений сигнализации передавалась по элементам СПП в "доверенной" и в "доверенной, но уязвимой" зонах. Все соединения, созданные элементами NBE и используемые для передачи информации сигнализации таким элементам СПП, должны устанавливаться при помощи безопасных каналов с аутентификацией. Все сообщения сигнализации, полученные элементами NBE на их "внутренний" адрес СПП по недоверенным каналам должны безмолвно отбрасываться.

Информационные потоки должны быть защищены либо с помощью кодирования транспортировки, либо с помощью гарантии того, что трафик будет передаваться только по защищенной сети. Кроме того, гарантия адреса источника на границе сети гарантирует, что пакеты извне не будут приниматься за пакеты от внутреннего адресного блока СПП.

Пакеты информации, принятые элементом NBE на его внешний адрес, должны быть проверены на принадлежность активному сеансу, на основе данных, полученных в ходе обмена сигнализацией, и на соответствие адреса ожидаемого источника, на основе описания сеанса, полученного в ходе обмена сигнализацией. Элемент NBE должен безмолвно отбрасывать любые пакеты информации, которые не соответствуют активному сеансу связи. Также NBE должен удостовериться, что скорость пакетов соответствует согласованным параметрам сеанса связи. NBE может удостовериться, что размер пакета соответствует установленному сеансу связи. Пакеты информации, полученные от IP-адреса источника, который не является действительным источником информации для данного элемента NBE, должны быть безмолвно отброшены.

Элемент NBE должен аутентифицировать все запросы, если этого требует соглашение о предоставлении услуг с пользователем. Если запрос получен по незашифрованному соединению, каждый отдельный запрос должен быть аутентифицирован. Если запрос получен по зашифрованному соединению, которое было создано без аутентификации клиента, должен быть аутентифицирован первый запрос соединения. Если запрос получен по зашифрованному соединению, которое было создано с аутентификацией, то дальнейшая аутентификация не требуется. Следует заметить, что запросы, переданные через элемент TE-BE, не будут запрашивать аутентификацию устройства, так как элемент TE-BE использует зашифрованное соединение с элементом NBE. Если запрос приходит от источника, IP-адреса которого является недействительным источником запросов к данному NBE, то он должен быть безмолвно отброшен. Запрос на создание безопасного канала от источника, IP-адреса которого является недействительным источником запросов к данному NBE, должен быть также безмолвно отброшен.

8.4 Требования к пограничным элементам CPE в "недоверенной" зоне

Обеспечение физической безопасности оборудования на стороне пользователя является сложной задачей. В конце концов, необходимо признать, что безопасность данных устройств в значительной степени зависит от пользователя. Это говорит о том, что в отношении каждого устройства необходимо принимать разумные меры предосторожности для защиты от атак, рассекречивания или иных повреждений. С целью сохранения конфиденциальности связи абонента в случае перехвата трафика сигнализации, сообщения сигнализации должны использовать безопасное соединение сигнализации между элементами TE-BE и NBE. Элемент TE-BE может выполнять функцию транзита информации.

8.4.1 Функции OAMP

Все функции OAMP между элементом TE-BE и поставщиком СПП должны быть защищены от преднамеренного перехвата. Поскольку OAMP может работать как внутри диапазона, так и вне его, эти два случая рассматриваются отдельно.

8.5 Рекомендации по безопасности для оконечного оборудования, расположенного в помещении клиента в "недоверенной" зоне

Реальные функциональные возможности безопасности пограничных элементов поставщика СПП требуют дальнейших исследований.

Информационный трафик должен быть защищен от перехвата или изменения.

Дополнение I

Задачи безопасности и руководящие принципы для присоединения служб электросвязи в чрезвычайных ситуациях

(Данное приложение не является неотъемлемой частью настоящей Рекомендации)

I.1 Исходные данные

Служба электросвязи в чрезвычайных ситуациях (ETS) является национальной службой, обеспечивающей приоритетное предоставление услуг электросвязи авторизованным пользователям ETS во время бедствий и чрезвычайных ситуаций. Выбор модели службы ETS является внутренним делом каждой страны. Однако бедствия/чрезвычайные ситуации могут выходить за географические границы, и потому существует возможность того, что страны/администрации могут заключить двусторонние и/или многосторонние соглашения по соединению своих соответствующих систем ETS. Это сделает возможной поддержку предоставления во время бедствий и чрезвычайных ситуаций приоритетных услуг электросвязи (например, голос, сообщения, видео и данные) в рамках ETS между различными государственными сетями, имеющими двусторонние и/или многосторонние соглашения.

Услуги электросвязи ETS между различными национальными сетями, т.е. странами/администрациями, должны быть защищены от угроз безопасности. Чтобы дать возможность сети обеспечивать безопасность сквозных услуг электросвязи ETS между различными национальными сетями, т.е. странами/администрациями, необходимы рекомендации и общие задачи и требования безопасности. Безопасность и доступность услуг электросвязи ETS будут зависеть от безопасности каждой сети, участвующей в создании сквозной связи.

I.2 Сфера применения/цель

В данном приложении представлены общие задачи и требования безопасности и даются рекомендации, позволяющие поддерживать безопасность на основе сети для служб электросвязи ETS при работе в различных видах реализации национальных сетей (т.е. стран/администраций) ETS.

В область применения данного Дополнения не включена одноранговая функция безопасности пользователя с использованием особых функций безопасности оборудования пользователя. Область применения данного Дополнения ограничена безопасностью, обеспечиваемой сетью для услуг электросвязи ETS через несколько сетей на основе отдельных сегментов. Тем не менее, СПП должна иметь возможность прозрачной поддержки таких одноранговых функций.

В данном приложении не ставится задача определить условия для национальных моделей ETS. Основной задачей является обеспечить безопасность услуг, предоставляемых сетью, т.е. безопасной и приоритетной передачи голоса, видео, данных и сообщений.

I.3 Основные задачи

Основная задача заключается в том, чтобы дать сетям возможность обеспечить безопасность услуг электросвязи ETS, например, безопасной и приоритетной передачи голоса, видео, данных и сообщений, через различные национальные сети, т. е. страны/администрации, и защиты доступности ETS. Она включает в себя безопасность сквозных соединений, которые могут проходить через домены различных поставщиков сетевых услуг в национальных и международных сетях, т. е. странах/администрациях, где каждая сеть несет ответственность за безопасность в пределах своего домена.

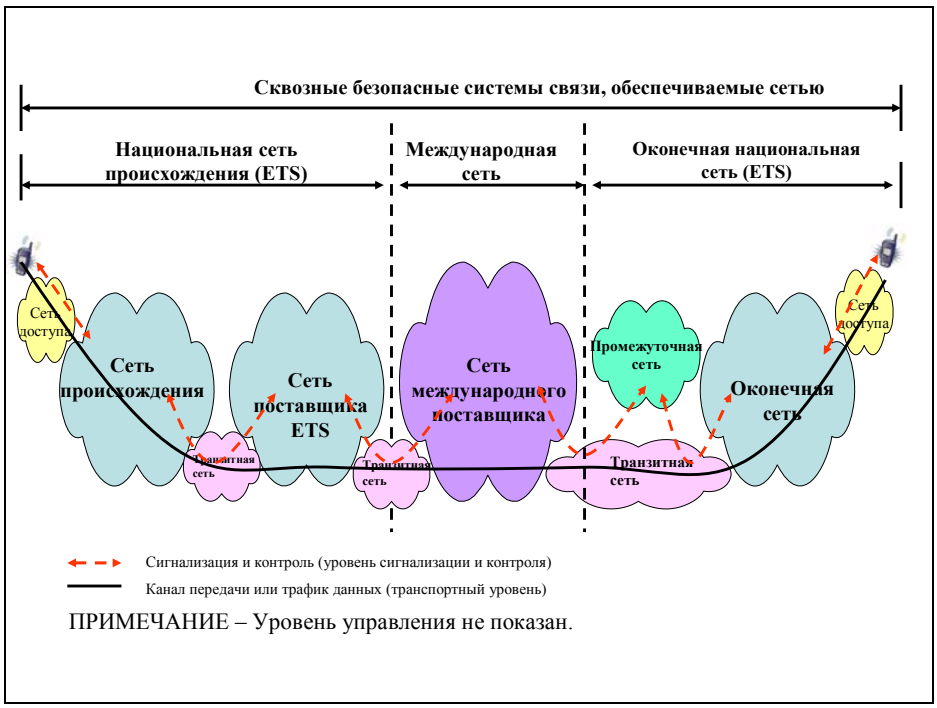

Рисунок I.1 – Пример сквозной связи через различные национальные сети ETS

На Рисунке I.1 показаны сквозные услуги электросвязи ETS, например, системы приоритетной передачи голоса, видео или сообщений, между двумя разными национальными сетями. Пример показывает, что сквозные приоритетные системы связи для ETS могут состоять из многих сетевых сегментов и административных доменов, например, сеть доступа, сеть происхождения, сеть поставщика ETS, сеть международного поставщика, промежуточная сеть и оконечная сеть.

Каждый сегмент сети будет нести определенную ответственность за безопасность в пределах своего домена для обеспечения сквозной безопасности и доступности услуг электросвязи ETS.

Ниже приведен минимальный набор основных руководств и планов безопасности для защиты сигнализации, канала передачи и данных, а также данных и информации, связанной с управлением ETS, например, информации о профиле пользователя:

- Каждый домен сети должен устанавливать и применять стратегии безопасности, а также реализовывать возможности подавления атак для ETS в пределах своего домена. В частности, рекомендуется, чтобы для приоритетных соединений ETS определялись и применялись возможности подавления атак и практические применения по безопасности помимо тех, которые необходимы для служб общего пользования. Например, должны разрабатываться данные возможности и практические применения для предотвращения использования ресурсов ETS неавторизованными пользователями, а также для предотвращения атак типа "отказ в обслуживании" и атак других типов.
- Каждый домен сети должен устанавливать отношения доверия, методики и процедуры для определения услуг электросвязи ETS, а также для управления идентичностью и аутентификации конечных пользователей и сетей через множество сетевых доменов администраций. Например, соглашения об уровне обслуживания (SLA) должны устанавливать политику безопасности для аутентификации каждого домена при обработке и получении услуг электросвязи ETS
- Каждый административный домен сети должен устанавливать и применять стратегии безопасности для защиты данных и информации, связанных с управлением ETS, например, информации о профиле пользователя.

I.4 Основные функции безопасности

Рекомендуется, чтобы для ETS выполнялись следующие основные требования к безопасности:

- Возможности безопасности по защите сквозных услуг электросвязи ETS при передаче через домены множества сетей.
- Возможности безопасности по защите доступности услуг электросвязи ETS при передаче через домены множества сетей.
- Возможности безопасности по обеспечению управления идентичностью и аутентификацией пользователей и сетей при передаче через домены множества администраций. Весьма желательно, чтобы пользователь взаимодействовал со службой ETS только один раз, а полномочия конечного пользователя передавались от одного административного домена к другому посредством механизмов безопасности.

I.5 Аутентификация, авторизация и контроль доступа

Рекомендуется, чтобы для ETS поддерживался следующий минимальный набор возможностей аутентификации, авторизации и управления доступом:

- Возможности безопасности по защите механизмов, используемых при аутентификации и авторизации конечных пользователей и устройств ETS.
- Возможности безопасности по защите механизмов, используемых при связывании конечного пользователя ETS с соответствующими устройствами.
- Возможности безопасности по защите механизмов, используемых при совместном использовании информации аутентификации, например, подтверждение того, что пользователь был аутентифицирован, при передаче через домены множества сетей.
- Возможности безопасности по защите механизмов, используемых при двусторонней аутентификации пользователя и объектов. Включает в себя механизмы для пользователя ETS по аутентификации вызываемой стороны или взаимодействующих объектов, например, интернет-сайта, сервера контента и т. п.
- Возможности безопасности по защите механизмов, используемых одной сетью при аутентификации другой сети. Включает в себя механизмы, используемые при аутентификации сети, обрабатывающей услуги электросвязи ETS, например, сети происхождения вызова, и аутентификации сети, получающей услуги электросвязи ETS, например, промежуточной или оконечной сетей.
- Возможности безопасности по защите от несанкционированного доступа к информации и ресурсам ETS, например, информации пользователей на серверах аутентификации и в системах управления.

I.6 Конфиденциальность и секретность

Рекомендуется, чтобы поддерживался следующий минимальный набор возможностей конфиденциальности:

- Возможности безопасности по обеспечению защиты конфиденциальности для сигнализации и управления ETS.
- Возможности безопасности по обеспечению защиты конфиденциальности канала передачи и данных трафика ETS, например, голоса, видео или данных.
- Возможности безопасности по обеспечению защиты конфиденциальности конечного пользователя ETS и идентичности взаимодействующих объектов, а также информации об условиях подписки.
- Возможности безопасности по обеспечению защиты конфиденциальности местоположения конечного пользователя ETS.

Рекомендуется, чтобы поддерживался следующий минимальный набор возможностей секретности:

- Возможности безопасности по обеспечению защиты секретности информации ETS, например, информации, получаемой из наблюдений за деятельностью сети, такой как интернет-сайты, которые посетил конечный пользователь, географическое положение конечного пользователя, IP-адреса и имена DNS устройств в сети поставщика сетевых услуг.

- Возможности безопасности по обеспечению защиты секретности от несанкционированного наблюдения за информацией использования ETS, например, таких особенностей использования, как объем трафика ETS, местоположения, время, частота и т. п.

I.7 Целостность данных

Рекомендуется, чтобы поддерживался следующий минимальный набор возможностей обеспечения целостности данных:

- Механизмы безопасности по обеспечению защиты целостности услуг электросвязи ETS, например, защита от несанкционированного изменения, удаления, создания или замещения. Включает в себя механизмы предоставления уведомлений о фальсификации или изменении информации.
- Механизмы безопасности по обеспечению защиты целостности информации ETS, например, обозначение приоритета, голос, данные и видео.
- Механизмы безопасности по обеспечению защиты целостности особых данных по конфигурации ETS, например, информации о приоритетах, хранящейся в функциях стратегических решений, уровень приоритета пользователя и т. п.

I.8 Связь

Рекомендуется, чтобы поддерживался следующая минимальная возможность.

- Механизмы безопасности по защите услуг электросвязи ETS от вторжений против авторизованных конечных пользователей ETS, например, механизмы для предотвращения перехвата, захвата или замещения сигнализации или канала передачи/трафика данных ETS.

I.9 Доступность

Рекомендуется, чтобы поддерживался следующий минимальный набор возможностей.

- Механизмы безопасности по защите доступности услуг электросвязи ETS, например, защита сигнализации и контроля ETS, а также канала передачи/трафика данных от атак типа "отказ в обслуживании" (DoS) и атак другого типа.
- Механизмы безопасности по защите доступности особых ресурсов и информации ETS, например, баз данных аутентификации/авторизации, информации о приоритетах, хранящейся в функции стратегических решений, а также специальных сетевых ресурсов от атак типа "отказ в обслуживании" (DoS) и атак другого типа.

Список литературы

Рекомендации МСЭ-Т

[b-ITU-T E.106] Рекомендация МСЭ-Т E.106 (2003), *Международная схема аварийных приоритетов (IEPS) для операций по ликвидации последствий чрезвычайных ситуаций*.

[b-ITU-T E.107] Рекомендация МСЭ-Т E.107 (2007), *Служба электросвязи в чрезвычайных ситуациях (ETS) и основа для взаимодействия реализованных на национальном уровне ETS.*

[b-ITU-T E.115] Рекомендация МСЭ-Т E.115 (2007), *Компьютеризированное справочное обслуживание.*

[b-ITU-T M.3016.2] Рекомендация МСЭ-Т M.3016.2 (2005), *Безопасность для плоскости администрирования: Услуги безопасности*.

[b-ITU-T M.3016.3] Рекомендация МСЭ-Т M.3016.3 (2005), *Безопасность для плоскости администрирования: Механизм безопасности*.

[b-ITU-T M.3016.4] Рекомендация МСЭ-Т M.3016.4 (2005), *Безопасность для плоскости администрирования: Платформа профиля*.

[b-ITU-T M.3060] Рекомендация МСЭ-Т M.3060/Y.2401 (2006), *Принципы управления сетями последующих поколений.*

[b-ITU-T X.1121] Рекомендация МСЭ-Т X.1121 (2004*), Структура технологий безопасности для сквозной подвижной передачи данных.*

[b-ITU-T X.1122] Рекомендация МСЭ-Т X.1122 (2004), *Руководящие указания по созданию защищенных систем подвижной связи на основе инфраструктуры открытого ключа (PKI)*

[b-ITU-T Y.1271] Рекомендация МСЭ-Т Y.1271 (2004), *Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов*.

[b-ITU-T Y.2000-Sup.1] Дополнение 1 к Рекомендациям МСЭ-Т серии Y.2000 (2006), *СПП версии 1 . Сфера применения*.

[b-ITU-T Y.2111] Рекомендация МСЭ-Т Y.2111 (2006), *Функции управления ресурсами и установлением соединений в сетях последующих поколений*

Документы ETSI TISPAN

[b-ETSI TR 187.002] ETSI TR 187 002 V.1.1.1 (2006), *Объединенные услуги электросвязи и интернет-услуги для новейших сетей (TISPAN); Безопасность СПП TISPAN (NGN_SEC); Анализ угроз и рисков*.

[b-ETSI TS 187.001] ETSI TS 187 001 V.1.1.1 (2006), *Объединенные услуги электросвязи и интернет-услуги для новейших сетей (TISPAN); Безопасность СПП (SEC); Требования*.

[b-ETSI TS 187.003] ETSI TS 187 003 V.1.1.1 (2006), *Объединенные услуги электросвязи и интернет-услуги для новейших сетей (TISPAN); Безопасность СПП; Архитектура безопасности*.

Документы ETSI/3GPP

[b-3GPP TS 33.102] 3GPP TS 33.102 (2007), *Безопасность сетей 3G; Архитектура безопасности*.

[b-3GPP TS 33.103] 3GPP TS 33.103 (2001), *Безопасность сетей 3G; Руководство по объединению*.

[b-3GPP TS 33.110] 3GPP TS 33.110 (2007), *Определение ключей между UICC и терминалом*.

[b-3GPP TS 33.120] 3GPP TS 33.120 (2001), *Задачи и принципы безопасности*.

[b-3GPP TS 33.200] 3GPP TS 33.200 (2004), *Безопасность сетей 3G; Безопасность сетевого домена (NDS); Безопасность на стороне уровня мобильного приложения (MAP)*.

[b-3GPP TS 33.203] 3GPP TS 33.203 (2007), *Безопасность сетей 3G; Безопасность доступа к услугам на базе IP*.

[b-3GPP TS 33.204] 3GPP TS 33.204 (2007), *Безопасность сетей 3G; Безопасность сетевого домена (NDS); Безопасность пользователя TCAP*.

[b-3GPP TS 33.210] 3GPP TS 33.210 (2007), *Безопасность сетей 3G; Безопасность сетевого домена; Безопасность уровня IP сети*.

[b-3GPP TS 33.220] 3GPP TS 33.220 (2007), *Общая архитектура аутентификации (GAA); Общая архитектура начальной загрузки*.

[b-3GPP TS 33.310] 3GPP TS 33.310 (2007), *Безопасность сетевого домена (DNS); Концепция аутентификации (AF)*.

[b-3GPP TR 33.901] 3GPP TR 33.901 (2001), *Критерии для процесса разработки криптографического алгоритма*.

[b-3GPP TR 33.902] 3GPP TR 33.902 (2001), *Формальный анализ протокола аутентификации 3G*.

[b-3GPP TR 33.908] 3GPP TR 33.908 (2001), *Безопасность сетей 3G; Общий отчет о проекте, спецификации и оценка стандартных алгоритмов конфиденциальности целостности 3GPP*.

[b-3GPP TR 33.909] 3GPP TR 33.909 (2001), *Безопасность сетей 3G; Отчет о проекте и оценка набора алгоритмов MILENAGE; Отчет 5: Примерный алгоритм для функций аутентификации 3GPP и генерации ключей*.

[b-3GPP TR 33.918] 3GPP TR 33.918 (2007), *Общая архитектура аутентификации (GAA); Ранняя реализация протокола передачи гипертекста по соединению с защищенным протоколом передачи гипертекста (HTTPS) между универсальной смарт-картой (UICC) и прикладной функцией сети (NAF)*.

[b-3GPP TR 33.919] 3GPP TR 33.919 (2007), *Безопасность сетей 3G; Общая архитектура аутентификации (GAA); Описание системы*.

[b-3GPP TR 33.920] 3GPP TR 33.920 (2007), *Общая архитектура начальной загрузки (GBA) на основе SIM-карты; Возможность ранней реализации*.

[b-3GPP TR 33.980] 3GPP TR 33.980 (2007), *Безопасное взаимодействия Альянса Liberty Alliance и партнерства 3GPP; Концепция взаимодействия Федерации идентичности Альянса Liberty Alliance (ID-FF), Концепции веб-услуг идентичности (ID-WSF) и общая архитектуры аутентификации (GAA)*.

[b-ETSI TR 133.901] ETSI TR 133.901 V4.0.0 (2001), *Универсальная система подвижной связи (UMTS); Безопасность сетей 3G – Критерии для процесса разработки криптографического алгоритма*.

[b-ETSI TR 133.902] ETSI TR 133.902 V4.0.0 (2001), *Универсальная система подвижной связи (UMTS); Формальный анализ протокола аутентификации 3G*.

[b-ETSI TR 133.908] ETSI TR 133.908 (2001), *Универсальная система подвижной связи (UMTS); Группа экспертов по алгоритмам защиты информации (SAGE); Общий отчет о проекте, спецификации и оценка стандартных алгоритмов конфиденциальности целостности 3GPP*.

[b-ETSI TR 133.909] ETSI TR 133.909 (2001), *Универсальная система подвижной связи (UMTS); Безопасность сетей 3G; Безопасность сетей 3G; Отчет о проекте и оценка набора алгоритмов MILENAGE; Отчет 5: Примерный алгоритм для функций аутентификации 3GPP и генерации ключей*.

[b-ETSI TR 133.919] ETSI TR 133.919 V6.2.0 (2005), *Универсальная система подвижной связи (UMTS); Общая архитектура аутентификации (GAA); Описание системы*.

[b-ETSI TS 133.102] ETSI TS 133 102 V7.1.0 (2006), *Универсальная система подвижной связи (UMTS); Безопасность сетей 3G; Архитектура безопасности*.

[b-ETSI TS 133.103] ETSI TS 133 103 V4.2.0 (2001), *Универсальная система подвижной связи (UMTS); Безопасность сетей 3G; Руководство по объединению*.

[b-ETSI TS 133.120] ETSI TS 133 120 V4.0.0 (2001), *Универсальная система подвижной связи (UMTS); Безопасность сетей 3G; Задачи и принципы безопасности*

[b-ETSI TS 133.200] ETSI TS 133 200 V6.1.0 (2005), *Универсальная система подвижной связи (UMTS); Безопасность сетей 3G; Безопасность сетевого домена (NDS); Безопасность на стороне уровня мобильного приложения (MAP)*.

[b-ETSI TS 133.203] ETSI TS 133 203 V6.10.0 (2006), *Цифровая сотовая система электросвязи (Фаза 2+); Универсальная система подвижной связи (UMTS); Безопасность сетей 3G; Безопасность доступа к услугам на базе IP*.

[b-ETSI TS 133.210] ETSI TS 133 210 V7.2.0 (2006), *Цифровая сотовая система электросвязи (Фаза 2+); Универсальная система подвижной связи (UMTS); Безопасность сетей 3G; Безопасность сетевого домена (NDS)*.

[b-GPP TS 133.220] ETSI TS 133 220 V7.8.0 (2007), *Цифровая сотовая система электросвязи; (Фаза 2+); Универсальная система подвижной связи (UMTS); Общая архитектура аутентификации (GAA); Общая архитектура начальной загрузки*.

[b-ETSI TS 133.310] ETSI TS 133 310 V7.1.0 (2006), *Универсальная система подвижной связи (UMTS); Безопасность сетевого домена; Концепция аутентификации (NDS/AF)*.

Документы ATIS/3GPP2

[b-GPP2 S.S0086] 3GPP2 S.S0086 (2004), *Концепция безопасности IMS.*

Документы IETF RFC, касающиеся IPsec

[b-IETF RFC 2085] IETF RFC 2085 (1997), *HMAC-MD5 IP Аутентификация с предотвращением повтора*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *Использование HMAC-MD5-96 в рамках ESP и AH*.

[b-IETF RFC 2404] IETF RFC 2404 (1998), *Использование HMAC-SHA-1-96 в рамках ESP и AH*.

[b-IETF RFC 2405] IETF RFC 2405 (1998), *Алгоритм шифрования ESP DES-CBC с явным IV*.

[b-IETF RFC 2410] IETF RFC 2410 (1998), *Криптографический алгоритм NULL и его применение с IPsec*.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *Путеводитель по документации по безопасности IP*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *Алгоритмы шифрования ESP CBC-Mode*.

[b-IETF RFC 2709] IETF RFC 2709 (1999), *Модель безопасности с режимом туннелирования IPsec для доменов NAT*.

[b-IETF RFC 2857] IETF RFC 2857 (2000), *Применение HMAC-RIPEMD-160-96 в рамках ESP и AH*.

[b-IETF RFC 3526] IETF RFC 3526 (2003), *Дополнительные экспоненциальные группы (MODP) Диффи-Хельмана для обмена ключами в интернете (IKE)*.

[b-IETF RFC 3602] IETF RFC 3602 (2003), *Алгоритм шифрования AES-CBC и его применение с IPsec*.

[b-IETF RFC 3664] IETF RFC 3664 (2004), *Алгоритм AES-XCBC-PRF-128 для протокола обмена ключами в интернете (IKE)*.

[b-IETF RFC 4109] IETF RFC 4109 (2005), *Алгоритмы для обмена ключами в интернете - версия 1 (IKEv1)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Архитектура безопасности для интернет-протокола*.

[b-IETF RFC 4302] IETF RFC 4302 (2005), *Заголовок аутентификации IP*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *Заголовок, шифрующий содержимое IP-пакета. (ESP).*

[b-IETF RFC 4304] IETF RFC 4304 (2005), *Расширенный порядковый номер (ESN) Дополнение в область интерполяции IPsec (DOI) для ассоциации безопасности интернета и протокола управления ключами (ISAKMP)*.

[b-IETF RFC 4305] IETF RFC 4305 (2005), Требования к реализации *Криптографического алгоритма для заголовка, шифрующего содержимое IP-пакета (ESP), и заголовка аутентификации (AH)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Протокол обмена ключами в интернете (IKEv2)*.

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Криптографические алгоритмы для использования в протоколе обмена ключами в интернете – версия 2 (IKEv2)*.

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Криптографические правила для IPsec*.

[b-IETF RFC 4309] IETF RFC 4309 (2005), *Использование режима CCM усовершенствованного стандарта шифрования (AES) с заголовком, шифрующим содержимое IP-пакета (ESP).*

[b-IETF RFC 4312] IETF RFC 4312 (2005), *Алгоритм шифрования Camellia и его использование с IPsec*.

Документы IETF RFC, касающиеся S/MIME

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME версия 2. Спецификация сообщений*.

[b-IETF RFC 2312] IETF RFC 2312 (1998), *S/MIME версия 2. Обработка сертификата*.

[b-IETF RFC 3565] IETF RFC 3565 (2003), *Использование криптографического алгоритма усовершенствованного стандарта шифрования (AES) в синтаксисе криптографического сообщения (CMS)*.

[b-IETF RFC 3657] IETF RFC 3657 (2004), *Использование криптографического алгоритма Camellia в синтаксисе криптографического сообщения (CMS)*.

[b-IETF RFC 3850] IETF RFC 3850 (2004), *Безопасные/Многоцелевые расширения электронной почты в Интернет (S/MIME) Версия 3.1 Обработка сертификата*.

[b-IETF RFC 3851] IETF RFC 3851 (2004), *Безопасные/Многоцелевые расширения электронной почты в Интернет (S/MIME) Версия 3.1 Спецификация сообщений*.

[b-IETF RFC 3852] IETF RFC 3852 (2004), *Синтаксис криптографического сообщения*.

[b-IETFB RFC 4134] IETF RFC 4134 (2005), *Примеры сообщений S/MIME*.

Документы IETF RFC, относящиеся к безопасности транспортного уровня (TLS)

[b-IETF RFC 2246] IETF RFC 2246 (1999), *Протокол TLS версия 1.0*.

[b-IETF RFC 2817] IETF RFC 2817 (2000), *Обновление TLS в рамках HTTP/1.1*.

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP через TLS*.

[b-IETF RFC 3268] IETF RFC 3268 (2002), *Таблицы шифров усовершенствованного стандарта шифрования (AES) для безопасности транспортного уровня (TLS)*.

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Расширения для безопасности транспортного уровня (TLS)*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Добавление таблиц шифра Camellia к безопасности транспортного уровня (TLS)*.

Отдельные документы RFC IETF, относящиеся к безопасности

[b-IETF i-d.SIPUAP] Неоконченная работа по проекту IETF, draft-ietf-sipping-config-framework-08.txt (6 марта 2006 г.), *Концепция доставки профиля агента пользователя протокола инициации сеанса связи*.

[b-IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Простое преобразование протокола дейтаграмм пользователя (UDP) при помощи трансляторов сетевых адресов (NAT)*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *Безопасный протокол транспортировки в реальном времени (SRTP)*.

[b-IETF RFC 3715] IETF RFC 3715 (2004), *Требования к совместимости протокола IPsec и трансляции сетевых адресов (NAT)*.

[b-IETF RFC 3847] IETF RFC 3847 (2004), *Повтор сигнализации для отрезка от промежуточной системы к промежуточной системе (IS-IS)*.

[b-IETF RFC 3948] IETF RFC 3948 (2005), *UDP инкапсуляция пакетов ESP протокола IPsec*.

Документы IETF RFC, относящиеся к DNS

[b-IETF RFC 4033] IETF RFC 4033 (2005), *Введение и требования к безопасности DNS*.

[b-IETF RFC 4034] IETF RFC 4034 (2005), *Регистрация ресурсов для расширений безопасности DNS*.

[b-IETF RFC 4035] IETF RFC 4035 (2005), *Изменения протокола для расширений безопасности DNS*.

Документы TIA

[b-TIA-683-D] Стандарт TIA-683-D (2006), *Предоставление по радиоканалу услуг для подвижных станций в системах с расширением спектра*.

[b-TIA-1053] Стандарт TIA-1053 (2005), *Концепция безопасности радиовещательной/ многоадресной передачи*.

[b-TIA-1091] Стандарт TIA-1091 (2006), *Концепция безопасности IMS*

Документы ARIB

[b-ARIB-SS0078] ARIB STD-T64 S.S0078-0 v1.0 (2002), *Общие алгоритмы безопасности*.

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 интернет-протокола и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2008 г.