Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1032

(12/2010)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Безопасность информации и сетей – Безопасность сетей

Архитектура внешних взаимосвязей для системы безопасности сети электросвязи на базе IP

Рекомендация МСЭ-Т X.1032

ITU-T

ITU Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	**X.1030–X.1049**
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589

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

Рекомендация МСЭ-Т X.1032

Архитектура внешних взаимосвязей для системы безопасности сети электросвязи на базе IP

Резюме

В настоящей Рекомендации предлагаются четыре модели, которые позволяют рассмотреть взаимосвязи системы безопасности сети электросвязи на базе IP (TNSS) и разных групп внешних объектов. Каждый объект рассматривается в аспекте его основных функций и возможного воздействия данного объекта на принципы конструирования и функционирования TNSS. Настоящая Рекомендация служит основой для разработки подробных Рекомендаций по безопасности сетей с учетом воздействия внешних объектов.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1032	17.12.2010 г.	17-я

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1032

Архитектура внешних взаимосвязей для системы безопасности сети электросвязи на базе IP

1 Сфера применения

1.1 При исследовании любого объекта необходимо принимать во внимание не только взаимосвязанность различных компонентов внутри объекта, но и внешние взаимосвязи объекта. При помощи внешних взаимосвязей объект осуществляет свои функции в составе комплексной системы. Однако эти взаимосвязи могут представлять риск вследствие различных угроз, способных нарушить функционирование объекта.

Исследование этих объектов особенно важно для системы безопасности сети электросвязи на базе IP (TNSS), которая необходима для защиты сети электросвязи на базе IP в основном от внешних угроз (см. рисунок 1).

В Дополнении I представлен возможный состав технических компонентов сети электросвязи на базе IP.

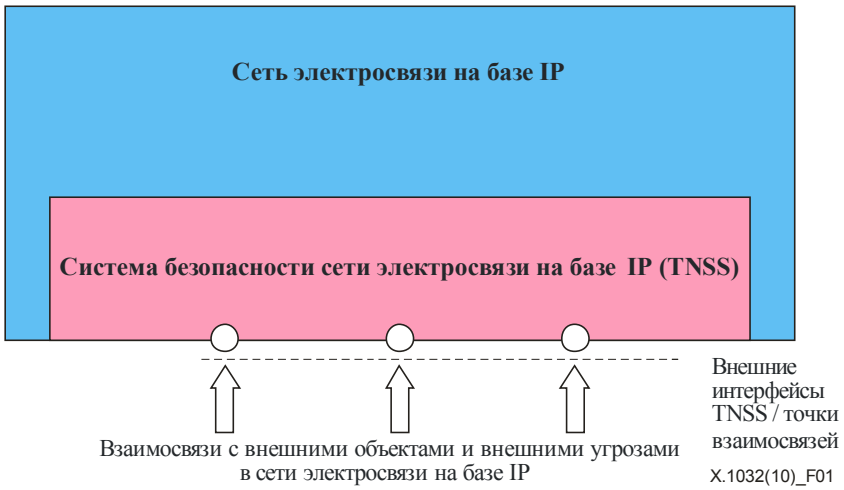

Рисунок 1 – Взаимосвязи между системой безопасности сети электросвязи на базе IP и внешними объектами

1.2 Система TNSS не функционирует как отдельная система; она работает в тесном взаимодействии с множеством внешних систем.

Эти внешние системы, прежде всего, включают в себя саму сеть электросвязи на базе IP, которую защищает система TNSS. Принципы конструирования транспортной среды и платформ услуг напрямую определяют требования к TNSS и, следовательно, принципы конструирования TNSS.

Во-вторых, эти внешние системы включают пользователей сети электросвязи на базе IP, чьи потребности должны удовлетворяться при помощи сети электросвязи на базе IP и ее TNSS.

Некоторые внешние организации также могут влиять на принципы конструирования TNSS. К этим организациям относятся:

– национальные регуляторные органы;

– третьи доверенные стороны, предоставляющие услуги для систем безопасности (по принципу внешнего исполнения работ);

– организации, использующие службы сети электросвязи на базе IP для создания информационных сетей.

В итоге, основными задачами TNSS являются защита сети электросвязи на базе IP и информации, передаваемой через эту сеть, от различных внешних угроз безопасности в среде функционирования TNSS.

В приведенном выше перечне указано, что TNSS имеет взаимосвязи с множеством внешних объектов, которые можно разделить на несколько групп.

1.3 Взаимосвязи TNSS с внешними объектами могут прямо или косвенно воздействовать на требования к TNSS и принципам конструирования и функционирования TNSS. Поэтому при разработке TNSS эти взаимосвязи следует принимать во внимание. Существуют Рекомендации МСЭ-Т, в которых рассмотрены определенные аспекты данной проблемы. Например, в Рекомендациях [ITU-T X.842] и [ITU-T X.843] рассматриваются взаимосвязи с третьей доверенной стороной. Тем не менее большое число аспектов взаимосвязей TNSS с внешними объектами пока еще не рассматривались.

1.4 В настоящей Рекомендации охватывается общая архитектура взаимосвязей TNSS с внешними объектами. Эта архитектура может применяться к разным типам сетей электросвязи на базе IP и различным системам безопасности электросвязи. В настоящей Рекомендации представлен обзор всех внешних взаимосвязей TNSS. Эта Рекомендация может служить основой для разработки более подробных Рекомендаций по безопасности сетей с учетом воздействия внешних объектов.

2 Справочные документы

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

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

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

[ITU-T X.842] Recommendation ITU-T X.842 (2000) | ISO/IEC TR14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.

[ITU-T X.843] Recommendation ITU-T X.843 (2000) | ISO/IEC 15945:2002, *Information technology – Security techniques – Specification of TTP services to support the application of digital signatures*.

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 система безопасности (security system): Множество взаимосвязанных элементов (определенных принципов, организационных и технических мер для обеспечения безопасности), которые уменьшают уязвимость активов и ресурсов.

3.2.2 система безопасности сети электросвязи на базе IP (TNSS) (telecommunication IP-based network security system): Система безопасности, применяемая в сети электросвязи на базе IP.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ICT	Information and Communication Technologies	ИКТ	Информационно-коммуникационные технологии
TNSS	Telecommunication IP-based Network Security System		Система безопасности сети электросвязи на базе IP

5 Условные обозначения

Отсутствуют.

6 Общие положения

6.1 Рассмотрение взаимосвязей TNSS с внешними объектами является сложной задачей вследствие большого числа этих объектов и разных типов связей и интерфейсов. Поэтому главной проблемой является возможность декомпозиции (разделения) набора взаимосвязей. В настоящей Рекомендации предложено четыре типа внешних взаимосвязей:

– взаимосвязи TNSS с системами безопасности, которые перекрывают инфраструктурные информационные системы и информационные структуры;

– взаимосвязи TNSS с объектами системы электросвязи;

– взаимосвязи TNSS с другими объектами, например внешними организациями;

– взаимосвязи TNSS с угрозами безопасности в форме либо упоминавшихся выше объектов, либо новых объектов.

Эти типы взаимосвязей рассматриваются ниже в пунктах 7, 8, 9 и 10, соответственно.

6.2 Кроме того, в пунктах 7, 8, 9 и 10 использован принцип декомпозиции. Сначала модель взаимосвязей определяется в графической форме. Эта модель содержит внешние объекты и их взаимосвязи с TNSS. Затем описываются функции каждого внешнего объекта. Наконец, на основе этих функций делаются краткие оценки, касающиеся:

– возможного воздействия внешних объектов на систему TNSS (например, воздействие на требования к TNSS, принципы конструирования и функционирования TNSS);

– возможных типов взаимосвязи (например, электрический интерфейс, организационные требования, влияние окружающей среды.

7 Взаимосвязи TNSS с системами безопасности информационных систем и информационной структуры

7.1 Модель взаимосвязей

На рисунке 2 показаны взаимосвязи TNSS с системами безопасности, которые перекрывают инфраструктурные информационные системы, которые, в свою очередь, имеют интерфейсы с системами безопасности информационной структуры.

7.2 Функции внешних объектов и их воздействие на TNSS

7.2.1 В информационных системах применяются разные типы информационных технологий, использующих электросвязь. Функции информационных систем включают в себя, например, сбор, хранение и запрос информации, организацию баз данных и сайтов пользователей, техническую поддержку редактирования, преобразования и других типов обработки информации. Информационные системы могут осуществлять функции удаленной передачи и распределения информации при помощи служб электросвязи, т. е. создание сетей информации-электросвязи. Одним из примеров сети информации-электросвязи общего пользования является интернет.

Традиционные типы связи (например, телефонная связь и факсимильная связь) могут осуществляться как с использованием сети информации-электросвязи, так и без нее.

Системы безопасности информационных систем служат для защиты технических процессов этих систем и информации, хранящейся и передающейся в этих системах. Системы безопасности информационных систем могут воздействовать на TNSS следующим способом, например:

– дополнять одна другую в процессе защиты от некоторых угроз, например от раскрытия информации; и

– вводить ограничения для протоколов безопасности, используемых в TNSS.

Внешние взаимосвязи TNSS с системами безопасности информационных систем могут иметь форму:

– интерфейсов аппаратного или программного обеспечения; или

– договорных соглашений.

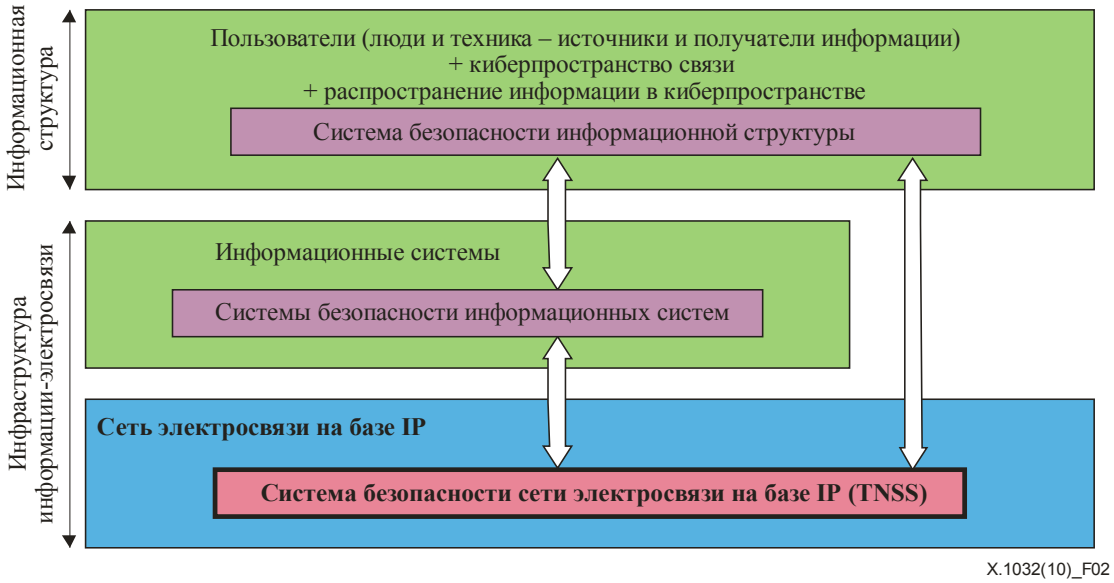

Рисунок 2 – Модель взаимосвязей TNSS с системами безопасности информационных систем и информационной структуры

7.2.2 Информационная структура обеспечивает использование информации во всех сферах человеческого деятельности. Система безопасности информационной структуры служит для защиты пользователей киберпространства (авторов, владельцев, источников, получателей и покупателей информации) от проникновений в киберпространство, которые могут уничтожить работу пользователей. К пользователям киберпространства относятся как люди, так и техника (датчики, исполнительные механизмы, автоматика и т. д.). Примерами нежелательного проникновения являются вирусы, "черви", спам, различное вредоносное программное обеспечение, существующие в киберпространстве. Нежелательное проникновение может также включать отказ в обслуживании в информационно-коммуникационной инфраструктуре.

Система безопасности информационной структуры может воздействовать на TNSS напрямую или через системы безопасности информационной сети. Например, она может вводить требования к TNSS, такие как защита в киберпространстве при помощи технических средств, которые могут поддерживать внедрение в системе безопасности информационной структуры правовых, административных и организационных мер. Такой тип технических средств включает средства противодействия вирусам и спаму.

Внешняя взаимосвязь TNSS с системой безопасности информационной структуры может иметь форму договорного соглашения.

8 Взаимосвязи TNSS с объектами систем электросвязи

8.1 Модель взаимосвязей TNSS

На рисунке 3 показаны взаимосвязи TNSS с объектами ее собственной сети электросвязи и с системами безопасности объектов других систем безопасности, т. е. с системами безопасности оконечного оборудования пользователя и соседних сетей электросвязи.

8.2 Функции внешних объектов и их воздействие на TNSS

8.2.1 Внутренние объекты сети электросвязи (транспортная страта и страта обслуживания) определяют как номенклатуру представляемых услуг электросвязи, так и качественные и количественные характеристики этих услуг. Эти объекты напрямую воздействуют на TNSS, в частности, они определяют:

– перечень услуг, которые следует защищать;

– возможности сети, относящиеся к реализации механизмов безопасности.

Внешние взаимосвязи TNSS с транспортной стратой и стратой обслуживания могут иметь форму:

– интерфейсов аппаратного или программного обеспечения; или

– контрактных соглашений.

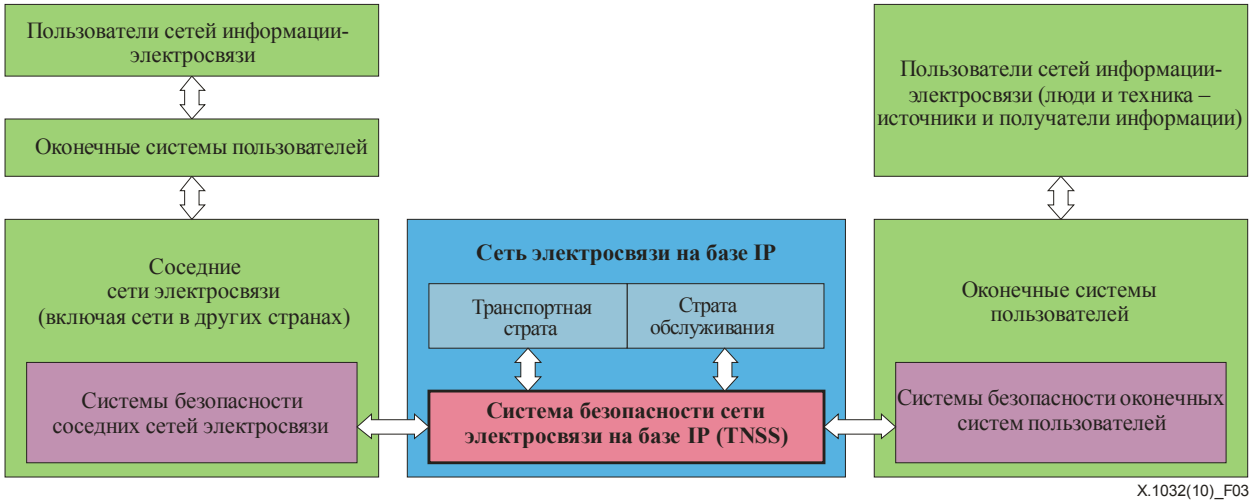

Рисунок 3 – Модель взаимосвязей TNSS с объектами системы электросвязи

8.2.2 Оконечные системы пользователя состоят из нескольких оконечных устройств (телефонные аппараты, телевизоры, компьютеры и другие виды терминалов) и соответствующих соединений домашней/корпоративной сети (подробно см. в Дополнении I). Системы безопасности оконечных систем пользователей выполняют функции защиты для оконечных устройств и домашних/корпоративных сетей от угроз безопасности. Эти угрозы могут исходить или от самой сети электросвязи, или от внутренних источников (например, оконечных систем пользователей). Кроме того, в системах безопасности оконечных систем пользователей используются механизмы защиты информации пользователя, передаваемой в сеть электросвязи.

Системы безопасности оконечных систем пользователей могут воздействовать на систему TNSS, в частности они могут:

– поддерживать одна другую в процессе защиты информации пользователя от некоторых угроз, например, кодируя передаваемые данные;

– определять требования для желательного(ых) уровня(ей) безопасности, который(е) должна обеспечить система TNSS.

Внешние взаимосвязи TNSS с системами безопасности могут иметь форму:

– электрического интерфейса; или

– организационных требований и ограничений.

8.2.3 Соседние сети электросвязи (включая сети других стран) осуществляют обмен трафиком с рассматриваемой сетью электросвязи. Системы безопасности соседних сетей электросвязи выполняют функции защиты этих сетей и информации, передаваемой в этих сетях, от угроз безопасности. Эти системы могут воздействовать на систему TNSS, в частности они могут:

– дополнять одна другую в процессе защиты информации пользователя от некоторых угроз, например от повреждения или искажения информации;

– вводить ограничения на применение определенных механизмов безопасности TNSS или режимов функционирования этих механизмов.

Внешние взаимосвязи TNSS с системами безопасности соседних сетей электросвязи могут иметь форму:

– электрического интерфейса; или

– согласованных на двусторонней основе организационных положений.

9 Взаимосвязи TNSS с внешними организациями

9.1 Модель взаимосвязей

На рисунке 4 показаны взаимосвязи TNSS с разными организациями, являющимися внешними для сети электросвязи, включая:

– регуляторные органы;

– доверенные третьи стороны;

– правоохранительные органы; и

– поставщиков технических средств (аппаратного и программного обеспечения).

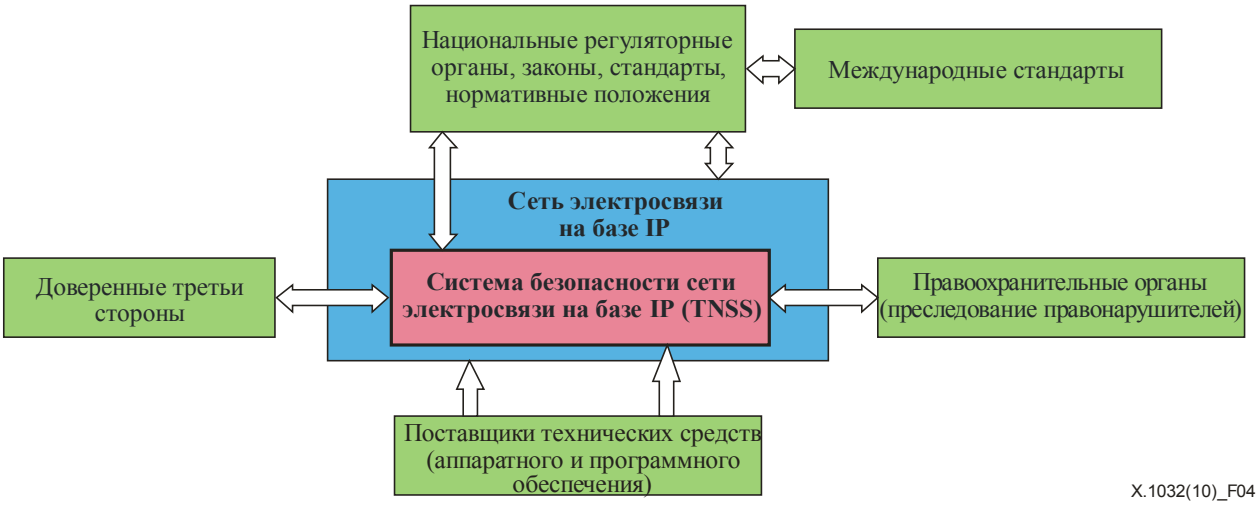

Рисунок 4 – Модель взаимосвязей системы TNSS с внешними организациями

9.2 Функции внешних организаций и их воздействие на TNSS

9.2.1 Регуляторные органы определяют общую политику в области электросвязи. В частности, они поддерживают разработку и применение международных стандартов, нормативных положений и законов, поддерживая также разработку национальных стандартов.

9.2.2 В соответствии с двусторонними соглашениями с оператором сети электросвязи третьи стороны могут выполнять определенные функции для обеспечения функционирования TNSS.

Перечень этих функций и принципов взаимодействия третьих сторон и TNSS определяется оператором инфраструктуры, в которую включена данная TNSS.

Внешние взаимосвязи TNSS с третьей стороной могут иметь форму:

– интерфейсов аппаратного или программного обеспечения; или

– договорных соглашений.

9.2.3 Правоохранительные органы (преследование правонарушителей) должны реагировать на случаи нарушения национального законодательства в области информационных сетей и сетей электросвязи. В частности, они должны осуществлять задержание правонарушителей, ответственных за такие нарушений. Работа правоохранительных органов и функционирование TNSS являются взаимодополняющими, что повышает уровень безопасности электросвязи.

Учитывая важность информационно-коммуникационных технологий (ИКТ) во всех сферах человеческого общества при продвижении к информационному обществу, разработка законов является и останется весьма важным фактором. В конечном счете эта тенденция будет усиливать роль соответствующих правоохранительных органов.

Для выполнения вышеуказанных функций правоохранительные органы должны регулярно получать данные от операторов сетей электросвязи о случаях нарушения безопасности, являющихся нарушением закона. TNSS должна выполнять сбор, хранение и анализ информации, что позволит формировать соответствующие сообщения и передавать их в правоохранительные органы. Возможность передавать информацию о случаях нарушения безопасности от организаций электросвязи в правоохранительные органы в качестве примера указана в [b-ITU-T E.409], [b-ITU-T X.1051] и [b-ITU-T X.1056].

Внешние взаимосвязи TNSS с правоохранительными органами могут иметь форму:

– электрического интерфейса или других услуг электросвязи или почтовых услуг; и

– организационных положений, согласованных на двусторонней основе.

10 Взаимосвязи TNSS с источниками угроз безопасности

10.1 Модель взаимосвязей

На рисунке 5 показана модель взаимосвязей TNSS с различными источниками угроз безопасности, к которым относятся:

– пользователи и их оконечные системы, подключенные к рассматриваемой сети электросвязи;

– посторонние лица (не пользователи) и внешняя среда;

– объекты и персонал данной сети электросвязи;

– соседние сети электросвязи, включая соответствующих пользователей и оконечные системы пользователей;

– подключенные информационные системы;

– доверенные третьи стороны; и

– поставщики технических средств.

10.2 Функции внешних объектов и их воздействие на систему TNSS

Источники угроз безопасности могут совершать атаки на сети электросвязи. Для предотвращения, обнаружения и нейтрализации таких атак применяется система безопасности сети электросвязи на базе IP (TNSS). Поэтому можно с уверенностью сказать, что угрозы безопасности напрямую связаны с TNSS, как показано на рисунке 5.

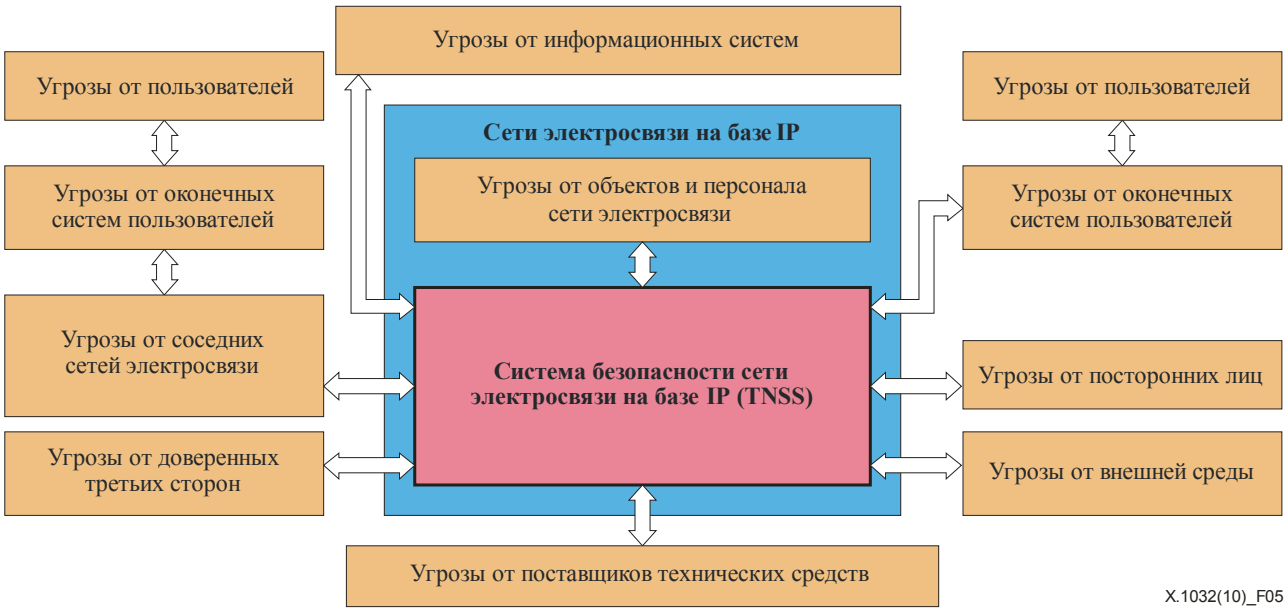

Рисунок 5 – Модель взаимосвязей TNSS с источниками угроз безопасности

Угрозы классифицируются по пяти типам, как указано в [ITU-T X.800] и [ITU-T X.805]:

– разрушение информации и других источников;
– повреждение или искажение информации;
– кража, удаление или потеря информации и других источников;
– раскрытие информации; и
– прерывание обслуживания.

Политика безопасности в сети электросвязи может применяться либо для противодействия всем угрозам, либо для противодействия некоторым из этих угроз. Соответственно, необходимые измерения безопасности выбираются в процессе разработки TNSS. Соответствие угроз безопасности измерениям безопасности приведено в таблице 1 [ITU-T X.805].

Внешние взаимосвязи системы TNSS с источниками угроз безопасности могут иметь форму:

– электрических интерфейсов;
– действий людей;
– атак с использованием технических средств через сеть электросвязи и внешних технических средств;
– воздействия окружающей среды;
– технических мер противодействия атакам; и
– организационных мер противодействия атакам.

Дополнение I

Возможный состав технического оборудования сети электросвязи на базе IP

(Данное Дополнение не составляет неотъемлемой части настоящей Рекомендации.)

I.1 В настоящей Рекомендации термин "сеть электросвязи" используется для охвата следующего оборудования операторов электросвязи:

– оборудование поставщиков инфраструктуры (т. е. сетевые узлы, их схемы соединений, сети доступа и т. д.);

– оборудование поставщиков услуг (т. е. серверы услуг и т. д.); роль поставщика услуг может выполнять поставщик инфраструктуры; в противном случае поставщик услуг может работать в сети независимо;

– оборудование поставщиков приложений (т. е. серверы приложений и т. д.); роль поставщика приложений может выполнять поставщик услуг; в противном случае поставщик приложений может работать в сети независимо;

– линии связи, соединяющие пользователя с оператором электросвязи (т. е. линии связи с поставщиками инфраструктуры/услуг/приложений); и

– информации, передающейся и хранящейся с использованием оборудования, обслуживаемого поставщиками инфраструктуры/услуг/приложений.

I.2 Сеть электросвязи не включает в себя термин "оконечные системы пользователей". Такие системы образуют:

– терминал(ы) абонента электросвязи (вместе с его программным обеспечением для осуществления функций пользователя инфраструктуры, пользователя услуг и пользователя приложений, включая выполнение определенных локальных функций, например, подготовку и редактирование сообщений);

– сервер(ы) приложений, если пользователь выполняет функции поставщика услуг приложений, не входящих в структуру сети;

– корпоративная/локальная/домашняя сеть (если таковая имеется);

– брандмауэр/шлюз (если таковые имеются); и

– информация пользователя – переданная, полученная и хранящаяся.

Библиография

[b-ITU-T E.409] Рекомендация МСЭ-Т E.409 (2004 г.), *Организация реагирования на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи*.

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[b-ITU-T X.1056] Recommendation ITU-T X.1056 (2009), *Security incident management guidelines for telecommunications organizations*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2012 г.