Международный союз электросвязи

Безопасность в электросвязи и информационных технологиях

Обзор содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи

МСЭ-Т

Сектор стандартизации электросвязи МСЭ

2012 г.

МСЭ-Т

Безопасность в электросвязи и информационных технологиях

Обзор содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи

Январь, 2012 г.

Предисловие

Малколм Джонсон
Директор
Бюро стандартизации электросвязи МСЭ

Еще сравнительно недавно проблема безопасности в информационно-коммуникационных технологиях (ИКТ) относилась в основном к таким специальным областям, как банковская деятельность, авиакосмические и военные приложения. Однако по мере стремительного роста и широкого распространения средств передачи данных, особенно интернета, безопасность в настоящее время касается практически каждого человека.

Возросшее внимание к проблеме безопасности ИКТ можно отчасти объяснить получившими широкую огласку инцидентами, например вирусами, проникновением хакеров и угрозами для неприкосновенности личной жизни. Однако реальность состоит в том, что поскольку в настоящее время вычислительная техника и сети стали важной частью повседневной жизни, возникает настоятельная необходимость в принятии эффективных мер безопасности для защиты систем ИКТ органов государственной власти, промышленности, торговли, ключевых инфраструктур и индивидуальных потребителей. Кроме того, во многих странах ныне существует законодательство о защите данных, которое требует соблюдения признанных стандартов в отношении такой защиты.

Для того чтобы безопасность была действительно эффективной, ее необходимо учитывать на всех этапах существования системы от планирования и проектирования до реализации, развертывания и, наконец, отключения. Ошибки адекватного учета безопасности на любом из этих этапов могут привести к появлению угроз для систем или передаваемых данных. Комитеты по стандартам играют весьма значимую роль, обеспечивая осведомленность в вопросах безопасности ИКТ, заботясь о том, чтобы аспекты безопасности стали одним из главных элементов технических спецификаций, и снабжая конструкторов и пользователей техническими стандартами и руководящими указаниями в отношении того, как сделать системы и услуги связи достаточно надежными, чтобы они могли противостоять кибератакам.

В течение длительного времени Сектор МСЭ-Т активно занимался проблемами безопасности в ИКТ, но объем работы значительно вырос в ответ на новые и эволюционирующие угрозы и потребности Членов Сектора в стандартах, помогающих бороться с этими угрозами. Настоящее Руководство представляет собой обзор некоторых ключевых элементов такой работы и является введением ко множеству ресурсов, доступных в МСЭ-Т для оказания содействия пользователям в решении стоящих перед нами проблем безопасности ИКТ.

Стандартизация – это ключевой строительный элемент для создания глобальной культуры кибербезопасности. Мы можем выиграть, и мы выиграем войну против киберугроз. Мы сделаем это, опираясь на работу тысяч увлеченных людей из государственных администраций, частного сектора или научных институтов, которые объединяются в организациях типа МСЭ для разработки стандартов безопасности и руководящих указаний по наилучшему их использованию. Эта работа не имеет блеска или высокого статуса, но тем не менее она чрезвычайно важна для защиты нашего цифрового будущего. Я хотел бы выразить свою признательность инженерам Бюро стандартизации электросвязи МСЭ, которые совместно с экспертами, представляющими членов МСЭ, работали и продолжают неустанно работать над разработкой этих стандартов и руководящих указаний.

Надеюсь, что данное Руководство окажется полезным для тех, кто желает лучше понимать вопросы безопасности ИКТ и деятельность МСЭ-Т в этой области, и я буду благодарен читателям за предложения в отношении следующих изданий.

Малколм Джонсон
Директор
Бюро стандартизации электросвязи МСЭ

Благодарности

В подготовку настоящего Руководства внесли вклад многие авторы, которые участвовали либо в разработке соответствующих Рекомендаций МСЭ-Т, либо в работе собраний Исследовательских комиссий, конференциях и семинарах МСЭ-Т. Особой благодарности заслуживают Докладчики, редакторы и координаторы Исследовательских комиссий МСЭ по вопросам безопасности, Мартин Ойхнер – советник ИК17 и Джордж Себек – бывший советник ИК17, и, в частности, Герберт Бертайн – бывший председатель ведущей Исследовательской комиссии МСЭ-Т по безопасности электросвязи и Майкл Хэрроп – бывший Докладчик по проекту безопасности и главный редактор настоящего Руководства.

Резюме

В настоящем Руководстве представлено обширное введение в работу МСЭ-Т в области безопасности ИКТ, и, более конкретно, в нем приводятся сводные данные о том, каким образом МСЭ-Т реагирует на глобальные вызовы в области кибербезопасности посредством соответствующих Рекомендаций, методических документов и разъяснительных инициатив. Оно в основном предназначено для тех, кто интересуется проблемами безопасности информации и электросвязи и соответствующими стандартами или отвечает за эту сферу деятельности, и для тех, кому нужно просто лучше понимать вопросы безопасности ИКТ.

В зависимости от организации, роли и потребностей пользователей настоящее Руководство может использоваться различными способами. Во вводных главах представлен обзор текущих ключевых областей деятельности МСЭ-Т в сфере безопасности, а также обсуждаются основные требования по защите приложений, услуг и информации ИКТ. Разъясняются угрозы и уязвимости, которые обусловливают требования безопасности, и рассматривается роль стандартов в удовлетворении таких требований. Обсуждаются некоторые функции, необходимые для защиты различных организаций, участвующих в предоставлении, поддержке и использовании информационно-коммуникационных технологий и услуг. Кроме того, разъясняется важное значение стандартов безопасности ИКТ и приводятся примеры развития деятельности МСЭ-Т по удовлетворению требований безопасности.

Затем вводятся общие архитектуры безопасности для открытых систем и для связи между конечными пунктами вместе с некоторыми видами архитектуры, определяемыми приложениями. Каждая из этих архитектур устанавливает рамки, в которых определенным образом могут применяться различные методы обеспечения безопасности. Они также стандартизируют лежащие в их основе концепции услуг и механизмы обеспечения безопасности и содержат стандартизированный словарь терминов и базовые концепции безопасности ИКТ. Общие принципы, вводимые в этих архитектурах, формируют основу для множества других стандартов по услугам, механизмам и протоколам безопасности, причем некоторые из них рассматриваются далее в тексте.

Тема управления безопасностью охватывает многие действия, связанные с регулированием и защитой доступа к системе и сетевым ресурсам, контроль событий и отчетность, правила и аудит, а также управление информацией, связанной с этими функциями и действиями. В одном из разделов обращается внимание на темы управления информационной безопасностью, управления рисками и управления ресурсами. Действия по управлению безопасностью, связанные с защитой сетевой инфраструктуры, обсуждаются далее в тексте раздела, который охватывает вопрос о необходимости защиты данных, используемых для контроля и управления сетью электросвязи, а также темы, относящиеся к управлению сетью и общим услугам управления безопасностью.

Каталог и его роль в поддержке услуг аутентификации и других услуг безопасности рассматриваются вместе с некоторыми ключевыми областями, зависящими от услуг каталога. Эти важные области включают управление определением идентичности, инфраструктуру открытых ключей, телебиометрию (т. е. персональную идентификацию и аутентификацию с использованием биометрических устройств в сфере электросвязи), а также защиту персональных данных. Обсуждается также важность защиты информационной базы каталога.

Описываются некоторые конкретные примеры и подходы к безопасности сети. Они включают требования к безопасности для сетей последующих поколений и сетей подвижной связи, которые находятся на этапе перехода от мобильности, основанной на отдельной технологии (например, CDMA или GSM), к мобильности на гетерогенных платформах с использованием межсетевого протокола. В этот раздел также включено рассмотрение положений безопасности для домашних сетей, кабельного телевидения и повсеместных сетей датчиков.

В настоящее издание Руководства добавлен новый раздел по кибербезопасности и реагированию на инциденты. Эффективное реагирование на кибератаки зависит от наличия информации об источнике и характере конкретной атаки и от обмена информацией с контролирующими органами. В данном разделе обсуждаются вопросы разработки структуры для совместного использования информации, относящейся к кибербезопасности, а также требования к обнаружению кибератак, защите от них, смягчению последствий и восстановлению работоспособности после таких атак.

Потребности обеспечения безопасности для ряда прикладных областей рассматриваются с особым акцентом на функции безопасности, которые определены в Рекомендациях МСЭ-Т. Обсуждаемые темы включают передачу голоса по межсетевому протоколу (VoIP), телевидения по межсетевому протоколу (IPTV) и веб-услуги. В этот раздел включена также тема идентификационных маркеров (включая маркеры RFID), которые широко применяются и в то же время являются предметом растущей обеспокоенности из-за риска нарушения неприкосновенности частной жизни.

Описываются технические меры для противодействия некоторым общим угрозам в сети, таким как спам, вредоносный код и шпионские программы, и рассматривается важность своевременных уведомлений и распространения обновлений программного обеспечения, а также необходимость в организации и последовательности при обработке инцидентов в сфере безопасности.

В заключение приводится краткий раздел о вероятных будущих направлениях стандартизации безопасности ИКТ.

В конце текста включен обзор источников дополнительной информации, а также добавлены приложения, содержащие определения и сокращения, используемые в данном Руководстве, сводный список Исследовательских комиссий, занимающихся проблемами безопасности, и полный список Рекомендаций, упомянутых в этом Руководстве. В электронной версии документа по всему тексту приведены ссылки на некоторые ключевые ресурсы МСЭ-Т по проблемам безопасности и разъяснительная информация.

Введение в 5-е издание

С того времени, когда в 2003 году было опубликовано первое издание Руководства, Сектор МСЭ-Т включил в свою деятельность множество новых сфер, и было завершено и опубликовано огромное количество новых Рекомендаций. Кроме того, сами Исследовательские комиссии были реструктурированы после Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) в 2008 году.

После опубликования четвертого издания данного Руководства работа по расширению объема деятельности была продолжена, в результате чего в ответ на непрерывные требования относительно стандартизации решений в целях противодействия растущим угрозам безопасности ИКТ возросло количество подготовленных Рекомендаций, касающихся сферы безопасности. И в очередной раз редакторы столкнулись с проблемой представления характерного профиля работы в ограниченном объеме документа. Структура и содержание четвертого издания данного Руководства были значительно пересмотрены и для его текста были установлены некоторые руководящие принципы. Эти руководящие принципы соблюдаются также и в настоящем издании, а структура и формат, разработанные для четвертого издания, остались в основном неизмененными.

Руководящие принципы, которые были разработаны после консультаций с членами МСЭ-Т, приведены ниже:

- публикация должна быть адресована широкой аудитории, и в ней следует избегать сложной терминологии и терминов, которые, вероятно, будут понятны только в специализированных отраслях;
- документ должен дополнять, а не дублировать существующие материалы, доступные в другой форме (например, Рекомендации);
- она должна быть написана так, чтобы ее можно было использовать как отдельный печатный документ и как электронный документ;
- текст должен содержать максимально возможное число гиперссылок на Рекомендации и другие источники общедоступных материалов. Подробная информация, сверх той, что необходима для выполнения основных целей, должна быть указана в виде гиперссылок; и
- текст, насколько это возможно, должен фокусироваться на работе, которая завершена и опубликована, а не на той, которая запланирована или выполняется.

В соответствии с этими целями Руководство не стремится охватить всю деятельность МСЭ-Т в области безопасности, которая либо была завершена, либо проводится. Вместо этого оно сфокусировано на ключевых отобранных темах и содержит гиперссылки на дополнительную информацию.

Руководство публикуется как в бумажном виде, так и в электронном формате. Для читателей, использующих электронную версию текста, приводятся прямые гиперссылки на перечисленные Рекомендации и другую онлайновую документацию. Для читателей, использующих бумажную копию текста, все упомянутые Рекомендации перечислены в Приложении D. Они могут быть доступны в электронном виде по адресу: www.itu.int/rec/T-REC/en.

ПРИМЕЧАНИЕ. – Настоящее Руководство является чисто иллюстративным. Оно не носит нормативного характера и не заменяет собой упомянутые в нем Рекомендации МСЭ-Т.

Содержание

Стр.

1. Как пользоваться данным Руководством по безопасности

1 Как пользоваться данным Руководством по безопасности

Настоящее Руководство разработано для того, чтобы ознакомить с работой МСЭ-Т в области безопасности руководителей и менеджеров, ответственных или интересующихся проблемами безопасности ИКТ и соответствующими стандартами. Кроме того, это Руководство будет интересно и для тех, кто желает лучше понимать вопросы безопасности ИКТ и соответствующие Рекомендации МСЭ-Т, в которых они рассматриваются.

Данное Руководство содержит обзор безопасности электросвязи и информационных технологий, рассматривает некоторые соответствующие практические вопросы и показывает, как в ходе работ МСЭ-Т по стандартизации рассматриваются различные аспекты безопасности ИКТ. Руководство содержит учебные материалы, а также ссылки на более подробные руководящие указания и дополнительные справочные материалы. В частности, оно содержит прямые ссылки на Рекомендации МСЭ-Т и на соответствующие справочные материалы и разъяснительные документы. Оно объединяет выбранные материалы по безопасности из Рекомендаций МСЭ-Т в одну публикацию и разъясняет взаимосвязи различных аспектов работы. Включены также результаты, достигнутые в стандартизации МСЭ-Т в сфере безопасности со времени четвертого издания. В большей части Руководство сфокусировано на работе, которая уже завершена. Результаты работы, которая в настоящий момент ведется, будут рассмотрены в будущих изданиях этого Руководства.

В дополнение к работе МСЭ-Т работа в области безопасности выполняется также Генеральным секретариатом и некоторыми другими Секторами МСЭ. Примеры включают следующие работы: *Understanding cybercrime: Phenomena, challenges and legal response*; *ITU national cybersecurity strategy guide*; работу МСЭ-R по безопасности международной подвижной связи и спутниковых служб; а также работу в рамках МСЭ-D по определению передового опыта для национального подхода к проблемам кибербезопасности.

Данное Руководство задумано как широкомасштабный высокоуровневый обзор видов деятельности МСЭ-Т в области стандартизации безопасности. Для тех, кому необходима более подробная информация об опубликованных Рекомендациях и связанных с ними документах, приводятся прямые ссылки на электронную версию текста. Руководство может использоваться различными способами. В таблице 1 показано, как оно может использоваться для удовлетворения потребностей различных групп читателей.

Таблица 1 – Как данное Руководство удовлетворяет потребности различных групп читателей

Организация	Конкретная аудитория	Потребности	Как в Руководстве могут рассматриваться потребности
Поставщики услуг электросвязи	Руководители/ менеджеры	Широкий обзор сферы приложения усилий по стандартизации в области безопасности ИКТ Высокоуровневая дорожная карта к соответствующим стандартам в области безопасности ИКТ	В Руководстве непосредственно рассматриваются эти потребности
	Инженеры разработчики и инженеры по внедрению	Дорожная карта к соответствующим стандартам в области безопасности ИКТ и технические подробности для определенных областей	Руководство предоставляет дорожную карту и ссылки на подробный разъяснительный текст Рекомендации предоставляют технические подробности
Продавцы услуг электросвязи	Руководители/ менеджеры	Широкий обзор сферы приложения усилий по стандартизации в области безопасности ИКТ Высокоуровневая дорожная карта к соответствующим стандартам в области безопасности ИКТ	В Руководстве непосредственно рассматриваются эти потребности
	Менеджеры продукции	Дорожная карта к соответствующим стандартам	В Руководстве предоставляется дорожная карта и ссылки на подробный разъяснительный текст
	Дизайнеры продукции	Технические подробности для определенных областей	Руководство предоставляет ссылки на подробный разъяснительный текст для определенных областей Рекомендации предоставляют технические подробности
Конечные пользователи	Технические	Могут интересоваться техническими подробностями в определенных областях	Руководство предоставляет ссылки на подробный разъяснительный текст для определенных областей
	Нетехнические	Могут интересоваться широким обзором сферы приложения усилий по стандартизации в области безопасности ИКТ	В Руководстве непосредственно рассматриваются эти потребности
Академические институты	Студенты/ преподаватели	Дорожная карта к соответствующим стандартам Технические подробности в определенных областях Осведомленность о новых и будущих усилиях по стандартизации в области безопасности ИКТ	В Руководстве предоставляются дорожная карта и ссылки на подробный разъяснительный текст для определенных областей
Правительство	Руководители и менеджеры Регуляторы Политики	Широкий обзор сферы приложения усилий по стандартизации в области безопасности ИКТ Высокоуровневая дорожная карта к соответствующим стандартам в области безопасности ИКТ	В Руководстве непосредственно рассматриваются эти потребности
Неправительственные организации	Руководители/ менеджеры	Широкий обзор сферы приложения усилий по стандартизации в области безопасности ИКТ Высокоуровневая дорожная карта к соответствующим стандартам в области безопасности ИКТ	В Руководстве непосредственно рассматриваются эти потребности
	Развитие и создание человеческого потенциала	Дорожная карта к соответствующим стандартам в области безопасности ИКТ Технические подробности в определенных областях	Руководство предоставляет ссылки на подробный разъяснительный текст для определенных областей Рекомендации предоставляют технические подробности

2. Обзор видов деятельности МСЭ-Т в области безопасности

2 Обзор видов деятельности МСЭ-Т в области безопасности

Работа МСЭ-Т в области безопасности ИКТ выполняется уже более трех десятилетий, в течение этого времени несколько Исследовательских комиссий разработали Рекомендации и руководящие указания во множестве ключевых областей. 17-я Исследовательская комиссия (ИК17) сегодня несет основную ответственность за работу МСЭ-Т в области безопасности ИКТ и назначена ведущей Исследовательской комиссией по безопасности. Однако аспекты безопасности простираются на большую часть областей работы МСЭ-Т, и большинство Исследовательских комиссий ведут работу в области безопасности, связанную с их собственной областью ответственности.

Как часть своих обязанностей ведущей Исследовательской комиссии по безопасности, ИК17 разработала множество справочных и информационных публикаций. Эти публикации, в которые входит и данное Руководство, содействуют усилиям по внутренней координации работ МСЭ-Т в области безопасности, а также помогают продвигать эту работу для более широкого сообщества и стимулировать применение Рекомендаций.

Данный раздел предлагает читателям краткое введение к основным темам по безопасности наряду с примерами некоторых Рекомендаций, относящихся к безопасности. В нем также приводятся ссылки на источники дополнительной информации по разъяснительным публикациям и выполняемым в настоящее время работам.

2.1 Справочные и информационные документы

МСЭ-Т поддерживает множество публикаций на веб-сайтах, из которых можно получить более подробную информацию о Рекомендациях и о работе МСЭ-Т в области безопасности.

Веб-сайт ИК17 websi предлагает перечень обязанностей и видов деятельности ИК17. На этом сайте также имеются краткие описания и ссылки на документацию и информационные материалы, информация о проведенных семинарах, презентациях и информационных мероприятиях, а также ссылки на руководящие указания по безопасности ИКТ, включая учебное пособие по написанию программ защиты и безопасности.

Более подробная информация о различных аспектах работы в области безопасности вместе с прямыми ссылками на дополнительную информацию содержится в разделе 13.

2.2 Обзор основных тем и Рекомендаций по безопасности

В таблице 2 даются оперативные ссылки на некоторые главные темы и соответствующие Рекомендации, рассмотренные в этом Руководстве. Для тех читателей, которые пользуются электронной версией текста, предоставлены прямые гиперссылки на текст каждой темы и подтемы к перечисленным Рекомендациям. Приложение D содержит полный список Рекомендаций, указанных в этом Руководстве. Гиперссылки включены в Приложение D, так что те, кто читает электронную версию текста, смогут перейти прямо к загрузке Рекомендаций.

Таблица 2 – Обзор некоторых ключевых тем и выбранных Рекомендаций (Часть 1 из 3)

Тема	Подтема	Примеры соответствующих Рекомендаций и публикаций	
Требования к безопасности	Угрозы, риски и уязвимости (3.2) Требования к персональной и физической безопасности (3.6) Сети последующих поколений (8.1) Требования к безопасности для IPCablecom (8.4) IPTV (IP-телевидение) (10.2)	МСЭ-Т E.408	*Требования к безопасности сетей электросвязи*
		МСЭ-Т X.1051	*Руководство по управлению информационной безопасностью для организаций электросвязи, основанное на ИСО/МЭК 27002*
		МСЭ-Т Y.2701	*Требования к безопасности для сетей последующих поколений версии 1*
		МСЭ-Т Y.2740	*Требования к безопасности мобильных дистанционных финансовых транзакций в сетях последующих поколений*
		МСЭ-Т J.170	*Спецификация обеспечения безопасности IPCablecom*
		МСЭ-Т X.1191	*Функциональные требования и архитектура аспектов безопасности IPTV*
Архитектуры безопасности	Архитектура безопасности открытых систем (4.1) Услуги безопасности (4.2) Архитектура безопасности для систем, обеспечивающих связь между конечными пунктами (4.3) Доступность сети и ее компонентов (4.3.2) Архитектуры, зависящие от приложений (4.5) Архитектуры безопасности одноранговой связи (4.6) Защита сообщений (4.5.2) Архитектура управления сетью (7.2) Архитектура IPCablecom (8.4.1) IPTV (10.2)	МСЭ-Т X.800	*Архтектура обеспечения безопасности в среде взаимодействия открытых систем для приложений МККТТ*
		МСЭ-Т X.810	*Инфраструктура обеспечения безопасности открытых систем: Обзор*
		МСЭ-Т X.805	*Архитектура безопасности для систем связи между конечными пунктами*
		МСЭ-Т G.827	*Параметры и цели функции готовности для сквозных международных цифровых трактов с постоянной скоростью передачи*
		МСЭ-Т X.1162	*Архитектура безопасности и работы для одноранговых сетей*
		МСЭ-Т X.1161	*Концепция защиты одноранговой связи*
		МСЭ-Т X.1143	*Архитектура безопасности для защиты сообщений в подвижных веб-услугах*
		МСЭ-Т M.3010	*Принципы для сети управления электросвязью*
		МСЭ-Т J.160	*Архитектура структуры для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов*
		МСЭ-Т X.1191	*Функциональные требования и архитектура аспектов безопасности IPTV*
Управление безопасностью	Управление информационной безопасностью (5.1) Управление рисками (5.2) Обработка инцидентов (5.3) Управление ресурсами (5.4)	МСЭ-Т X.1051	*Руководство по управлению информационной безопасностью для организаций электросвязи, основанное на ИСО/МЭК 27002*
		МСЭ-Т X.1052	*Information security management framework*
		МСЭ-Т X.1055	*Управление рисками и руководство по профилям рисков для организаций электросвязи*
		МСЭ-Т E.409	*Организация и безопасная обработка инцидентов: руководство для организаций электросвязи*
		МСЭ-Т X.1057	*Asset management guidelines in telecommunication organizations*

Таблица 2 – Обзор некоторых ключевых тем и выбранных Рекомендаций (Часть 2 из 3)

Тема	Подтема	Примеры соответствующих Рекомендаций и публикаций	
Управление аутентификацией, каталогом и идентичностью	Концепции каталога (6) Защита информации каталога (6.1) Механизмы безопасности с открытым ключом (6.2) Защита персональных данных (6.1.4) Управление определением идентичности (6.4) Терминология управления идентичностью (6.4.2) Телебиометрическая аутентификация (6.5.1) Аспекты защиты и безопасности телебиометрии (6.5.3)	МСЭ-Т X.500	*Каталог: Обзор концепций, моделей и услуг*
		МСЭ-Т X.509	*Каталог: Концепции открытого ключа и сертификата атрибута*
		МСЭ-Т X.1171	*Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров*
		МСЭ-Т X.1250	*Базовые возможности для улучшенного доверия и функциональной совместимости при глобальном управлении определением идентичности*
		МСЭ-Т X.1251	*Структура осуществляемого пользователем управления в отношении цифровой идентичности*
		МСЭ-Т X.1253	*Руководящие указания по обеспечению безопасности для систем управления определением идентичности*
		МСЭ-Т Y.2720	*Концепция управления идентичностью в СПП*
		МСЭ-Т Y.2722	*Механизмы управления определением идентичности в СПП*
		МСЭ-Т X.1252	*Базовые термины и определения в области управления определением идентичности*
		МСЭ-Т X.1084	*Механизм телебиометрической системы – Часть 1: Общий протокол биометрической аутентификации и профили модели системы для систем электросвязи*
		МСЭ-Т X.1089	*Инфраструктура телебиометрической аутентификации*
		МСЭ-Т X.1081	*Телебиометрическая мультимодальная модель – Концепция для спецификации аспектов защиты и безопасности телебиометрии*
Защита сетевой инфраструктуры	Сеть управления электросвязью (7.1) Защита действий по контролю и управлению (7.4) Защита действий по эксплуатации сети и приложений по управлению (7.5) Общие услуги управления безопасностью (7.6) Услуги безопасности CORBA (7.6.4)	МСЭ Т M.3010	*Принципы для сети управления электросвязью*
		МСЭ-Т M.3016.0	*Безопасность для плоскости административного управления: обзор*
		МСЭ-Т M.3210.1	*Услуги управления СУЭ для управления обеспечением безопасности сетей IMT-2000*
		МСЭ-Т X.790	*Функция исправления неполадок для приложений МСЭ-Т*
		МСЭ-Т X.711	*Общий протокол управления информацией*
		МСЭ-Т X.736	*Управление системами: функция оповещения о нарушении безопасности*
		МСЭ-Т X.740	*Управление системами: Функция предоставления данных проверки безопасности*
		МСЭ-Т X.780	*Руководства СУЭ для определения объектов, управляемых CORBA*
Некоторые конкретные подходы к безопасности сети	Безопасность сетей последующих поколений (СПП) (8.1) Безопасность подвижной связи (8.2) Безопасность для домашних сетей (8.3) Безопасность для повсеместных сетей датчиков (8.6)	МСЭ-Т Y.2001	*Общий обзор СПП*
		ITU-T Y.2701	*Security requirements for NGN release 1*
		МСЭ-Т X.1121	*Структура технологий безопасности для подвижной передачи данных от конца до конца*
		МСЭ-Т X.1111	*Концепция технологий безопасности для домашней сети*
		МСЭ-Т X.1311	*Security framework for ubiquitous sensor networks*

Таблица 2 – Обзор некоторых ключевых тем и выбранных Рекомендаций (Часть 3 из 3)

Тема	Подтема	Примеры соответствующих Рекомендаций и публикаций	
Кибербезопасность и реагирование на инциденты	Обмен информацией о кибербезопасности (9.1) Обмен информацией об уязвимостях (9.1.3) Обнаружение информации о кибербезопасности (9.1.5) Обработка инцидентов (9.2)	МСЭ-Т X.1205	*Обзор кибербезопасности*
		МСЭ-Т X.1500	*Методы обмена информацией о кибербезопасности*
		МСЭ-Т X.1520	*Общеизвестные уязвимости и незащищенность*
		МСЭ-Т X.1570	*Механизмы обнаружения, используемые при обмене информацией о кибербезопасности*
		МСЭ-Т E.409	*Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи*
		МСЭ-Т X.1056	*Руководящие указания для организаций электросвязи по управлению инцидентами в области безопасности*
Безопасность приложения	Передача голоса (VoIP) и мультимедиа по IP-протоколу (10.1) IPTV (10.2) Защищенная факсимильная передача (10.3) Веб-услуги (10.4) Услуги на основе маркеров (10.5)	МСЭ-Т H.235	*Защита H.323: Инфраструктура защиты в мультимедийных системах серии H (H.323 и других, основанных на H.245)*
		МСЭ-Т X.1195	*Service and content protection interoperability scheme*
		МСЭ-Т T.36	*T.36: Возможности безопасности для использования с факсимильными терминалами Группы 3*
		МСЭ-Т X.1141	*Язык разметки, предусматривающий защиту данных (SAML 2.0)*
		МСЭ-Т X.1142	*Расширяемый язык разметки контроля доступа (XACML 2.0)*
		МСЭ-Т X.1171	*Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров*
Противостояние общим сетевым угрозам	Спам (11.1) Вредоносный код, шпионское и заведомо ложное программное обеспечение (11.2) Уведомление и распространение обновлений программного обеспечения (11.3)	МСЭ-Т X.1231	*Технические стратегии в деле противостояния спаму*
		МСЭ-Т X.1241	*Техническая основа противодействия спаму, рассылаемому по электронной почте*
		МСЭ-Т X.1244	*Общие аспекты противостояния спаму в мультимедийных IP-приложениях*
		МСЭ-Т X.1207	*Руководство для поставщиков услуг электросвязи по оценке рисков шпионских программ и потенциально нежелательного программного обеспечения*
		МСЭ-Т X.1206	*Независимая от поставщика концепция автоматического уведомления об информации по безопасности и распространение обновлений*

В данной таблице указаны *некоторые* из тем и Рекомендаций, рассматриваемые в настоящей публикации. Таблица не предназначалась быть источником исчерпывающей информации. Полный перечень Рекомендаций по безопасности, упомянутых в тексте, содержится в Приложении D. Полный набор Рекомендаций МСЭ-Т по безопасности представлен по адресу: http://www.itu.int/ITU-T/recommendations/.

Номера в скобках, указанные после подтем, относятся к соответствующим темам в основной части текста.

3. Требования к безопасности

3 Требования к безопасности

При разработке структуры безопасности любого вида очень важно иметь четкое представление о требованиях. Всеобъемлющий обзор требований к безопасности должен учитывать: вовлеченные стороны; ресурсы, которые нуждаются в защите; угрозы, от которых необходимо защитить эти ресурсы; уязвимости, связанные с этими ресурсами; и общие риски, которым эти угрозы и уязвимости подвергают ресурсы.

В этом разделе представлены основные требования по защите приложений ИКТ, услуг и информации, точки зрения на угрозы и уязвимости, которые обусловливают требования, рассматривается роль стандартов в удовлетворении требований, и определяются некоторые особенности, которые необходимы для защиты различных сторон, участвующих в применении и работе со средствами ИКТ.

Требования к безопасности являются как общими, так и зависят от конкретных условий. Кроме того, некоторые требования являются общепринятыми, в то время как другие продолжают развиваться совместно с новыми приложениями и изменяют среду, содержащую угрозы. По большей части дискуссия в этом разделе носит общий характер. Требования для конкретных приложений и сред рассматриваются в следующих разделах.

3.1 Угрозы, риски и уязвимости

В целом в отношении ИКТ может потребоваться защита ресурсов для следующих сторон:

- *потребители*/*абоненты*, которым необходимо испытывать доверие к сети и предлагаемым услугам, включая готовность услуг (особенно экстренного обслуживания);
- *общественность*/*органы власти*, которые требуют закрепления мер защиты в директивах и/или законодательстве, с тем чтобы обеспечить готовность услуг, добросовестную конкуренцию и защиту персональных данных; и
- *операторы сетей* и поставщики услуг, которые нуждаются в обеспечении безопасности для защиты своих эксплуатационных и коммерческих интересов и для выполнения своих обязательств перед клиентами, деловыми партнерами и населением.

Ресурсы, которые должны быть защищены, включают:

- услуги в области связи и компьютерных операций;
- информацию и данные, включая программное обеспечение и данные, относящиеся к услугам обеспечения безопасности;
- персонал; и
- оборудование и средства.

Угроза безопасности – это потенциальное нарушение безопасности. Примерами угроз являются:

- несанкционированное раскрытие информации;
- несанкционированное разрушение или изменение данных, оборудования или других ресурсов;
- кража, удаление или потеря информации или других ресурсов;
- прерывание обслуживания или отказ в обслуживании; и
- выдача себя за допущенный объект.

Угрозы бывают *случайными* (иногда их также называют *неумышленными*) или *умышленными* и могут быть *активными* или *пассивными*. Случайная угроза – это угроза без какого-либо преднамеренного умысла, как, например, ошибка в системе или программе или физический сбой оборудования. Умышленная угроза – это угроза, которая реализуется неким объектом, совершающим преднамеренное действие. К умышленным угрозам относятся угрозы от простого просмотра с использованием легко доступных инструментов слежения до изощренных попыток нарушения защиты с использованием специальных знаний о системе. Если реализуется

умышленная угроза, она называется *атакой*. Активная угроза – это угроза, которая приводит к некоторому изменению состояния или работы системы, таких как изменение данных или разрушение оборудования. Пассивная угроза не приводит к изменению состояния. Примером пассивной угрозы является перехват информации (подслушивание).

Уязвимость защиты представляет собой результат ошибки или дефекта, которыми можно воспользоваться с целью нарушения системы или содержащейся в ней информации. Существование уязвимости означает возможность реализации угрозы при отсутствии эффективных мер противодействия.

Рекомендации МСЭ-Т различают четыре вида уязвимостей:

- уязвимость, зависящая от модели угроз, обусловлена сложностью прогнозирования будущих угроз;
- уязвимость, обусловленная проектом и техническими характеристиками, является следствием ошибок и упущений при разработке системы или протокола, которые делают их уязвимыми по определению;
- уязвимость реализации представляет собой уязвимость, возникающую в результате ошибок в процессе реализации системы или протокола; и
- уязвимость эксплуатации и конфигурации возникает в результате ненадлежащего использования вариантов при реализации или неправильной политики и практики внедрения (например, неприменение шифрования в беспроводной сети).

Риск нарушения безопасности представляет собой показатель негативных последствий, которые могут наступить, если воспользоваться уязвимостью защиты, т. е. если будет реализована угроза. Хотя риск невозможно полностью устранить, одной из целей защиты является уменьшение риска до приемлемого уровня. Для выполнения этой задачи необходимо иметь представление о существующих угрозах и уязвимостях и применять соответствующие меры противодействия. Как правило, существуют услуги и механизмы обеспечения безопасности, которые могут быть дополнены нетехническими мерами, такими как физическая и персональная безопасность.

Хотя угрозы и факторы угроз меняются, уязвимости защиты будут существовать на протяжении всего срока эксплуатации системы или протокола, если не принять конкретных мер по устранению уязвимостей. Любые уязвимости, обусловленные свойствами протокола, в случае широкого применения стандартизованных протоколов, могут привести к весьма серьезным последствиям и быть глобальными по масштабу. Поэтому важно понять и выявить уязвимости протоколов и принять меры по устранению уязвимых элементов при их обнаружении.

Организации по стандартизации несут не только ответственность, но и имеют уникальную возможность для решения проблемы уязвимости защиты, которая может быть заложена в технических характеристиках, таких как архитектуры, структуры и протоколы. Даже при надлежащей осведомленности относительно угроз, рисков и уязвимостей, связанных с обработкой информации и сетями связи, невозможно обеспечить адекватную защиту без систематического применения защиты в соответствии с установленной политикой безопасности. Политика безопасности должна периодически пересматриваться и обновляться. Также следует надлежащим образом обеспечить управление мерами безопасности и реагирование на инциденты. Это включает установление ответственности и конкретных действий, которые должны способствовать предупреждению, обнаружению, расследованию и реагированию на любой инцидент в области безопасности.

Услуги и механизмы обеспечения безопасности должны защищать сети электросвязи от преднамеренных атак, таких как отказ в обслуживании, подслушивание, спуфинг, искажение сообщений (изменение, задержка, удаление, вставка, повторная передача перехваченного сообщения, перемаршрутизация, неправильная маршрутизация или изменение порядка поступления сообщений), отрицание факта получения или отправления или фальсификация. Защита включает в себя предупреждение, обнаружение и восстановление после атаки, а также управление информацией, касающейся безопасности. Защита должна включать меры по предотвращению прерываний в обслуживании вследствие природных явлений (таких как штормы и землетрясения) и

злонамеренных атак (умышленных или насильственных действий). Следует также предусмотреть возможность перехвата и наблюдения надлежащим образом уполномоченными правоохранительными органами.

Безопасность сетей электросвязи также требует широкого сотрудничества поставщиков услуг. В Рекомендации МСЭ-Т E.408 содержится обзор требований к безопасности и структуре, которая опознает угрозы безопасности в сетях электросвязи в общем виде (как для фиксированной, так и для подвижной связи, для голосовой связи и передачи данных), а также приводится руководство по планированию мер противодействия, которые могут быть приняты для уменьшения рисков, создаваемых угрозами. Выполнение требований Рекомендации МСЭ-Т E.408 будет способствовать международному сотрудничеству в следующих областях, связанных с безопасностью сетей электросвязи:

- совместное использование и распространение информации;
- координация при инциденте и ответные действия при кризисе;
- набор и обучение специалистов в области безопасности;
- координация в области правоприменения;
- защита ключевой инфраструктуры и основных услуг; и
- разработка соответствующего законодательства.

Однако для успешного осуществления такого сотрудничества крайне важно, чтобы на национальном уровне указанные требования выполнялись в отношении национальных компонентов сети.

В Рекомендации МСЭ-Т X.1205 представлена классификация угроз безопасности с организационной точки зрения наряду с обсуждением угроз на различных уровнях сети.

3.2 Общие задачи безопасности для сетей ИКТ

Задачи безопасности для сетей электросвязи состоят в следующем.

a) Доступ к сетям и услугам электросвязи и возможность их использования должны иметь только санкционированные пользователи.

b) Санкционированные пользователи должны обладать доступом и возможностью работать с ресурсами, к которым им предоставлен доступ.

c) Сети электросвязи должны обеспечивать секретность на уровне, определенном политикой безопасности в данной сети.

d) Все объекты сети должны нести ответственность за свои, и только свои действия в сетях электросвязи.

e) Сети электросвязи должны быть защищены от непредусмотренного доступа или воздействия.

f) Информация, связанная с безопасностью, должна быть доступна в сетях электросвязи, но только для санкционированных пользователей.

g) Следует принять планы в отношении рассмотрения вопроса о том, каким образом должны обрабатываться инциденты в области безопасности.

h) При обнаружении взлома защиты необходимо принять соответствующие процедуры для восстановления нормальных условий работы.

i) Архитектура сетей электросвязи должна обеспечивать поддержку разных стратегий безопасности и механизмов защиты различной эффективности.

Для выполнения этих задач необходимо обращать особое внимание на вопросы безопасности в процессе планирования, реализации и эксплуатации сетей. Должны быть разработаны стратегии обеспечения

безопасности, должны использоваться соответствующие услуги безопасности, а риски должны управляться последовательно и постоянно.

3.3 Обоснование стандартов безопасности

Использование согласованных на международном уровне стандартов в качестве основы сетевой безопасности способствует общности подходов и взаимопомощи, а также будет более эффективным с экономической точки зрения, чем разработка индивидуальных подходов для каждой сферы полномочий.

В некоторых случаях предоставление и использование услуг и механизмов безопасности может быть довольно дорогим по отношению к стоимости защищаемых ресурсов, так что важно иметь возможность адаптировать услуги и механизмы безопасности для удовлетворения местных потребностей. Однако возможность адаптации безопасности к требованиям пользователя также может отразиться на количестве возможных сочетаний функций обеспечения безопасности. Поэтому желательно иметь *профили безопасности*, охватывающие широкий диапазон сетевых услуг электросвязи, для обеспечения выравнивания возможностей в различных реализациях. Стандартизация и использование стандартизированных профилей облегчает функциональную совместимость и повторное использование решений и продуктов, а это означает, что безопасность может быть введена быстрее и с меньшими затратами.

Преимуществами применения стандартных решений в области сетевой безопасности, как для продавцов, так и для поставщиков услуг, являются экономия за счет масштаба при разработке продуктов и взаимодействие компонентов в сетях электросвязи.

3.4 Эволюция стандартов безопасности МСЭ-Т

Работа МСЭ-Т в области безопасности продолжает расширяться в ответ на требования, предъявляемые членами МСЭ-Т. Здесь рассматриваются некоторые ключевые аспекты этого развития, особенно те их них, которые связаны с требованиями по обеспечению безопасности. Некоторые из отдельных Рекомендаций рассматриваются более подробно.

Как правило, требования к безопасности ИКТ определяются в понятиях угроз для сети и/или системы, внутренней уязвимости сети и/или системы и шагов, которые необходимо предпринять для противостояния угрозам и снижения уязвимостей. Требования по защите распространяются на сеть и на ее компоненты. Основные понятия безопасности, включая угрозы, уязвимости и меры противодействия в области безопасности, были определены в Рекомендации МСЭ-Т X.800, которая была опубликована в 1991 году. Вышеупомянутая Рекомендация МСЭ-Т E.408, которая была опубликована в 2004 году, основывается на принципах и терминологии Рекомендации МСЭ-Т X.800. Рекомендация МСЭ-Т E.408 носит общий характер и не рассматривает требования для конкретных сетей, а также не определяет новые услуги безопасности. Вместо этого данная Рекомендация была сфокусирована на применении существующих услуг безопасности, определенных в других Рекомендациях МСЭ-Т и соответствующих стандартах других органов.

Необходимость борьбы с растущим числом и разнообразием угроз кибербезопасности (вирусы, черви, "троянские кони", спуфинг, кража идентичности, спам и другие формы кибератак) была отражена в 2008 году в Рекомендации МСЭ-Т X.1205. Эта Рекомендация направлена на создание основ знаний, которые помогут защитить будущие сети и рассматривает различные технологии, которые можно применить для устранения угроз, включая: маршрутизаторы, брандмауэры, антивирусную защиту, системы обнаружения вторжения, системы защиты от вторжения, безопасную компьютерную обработку данных, а также аудит и мониторинг. Также она рассматривает такие принципы защиты сетей, как углубленная защита и управление доступом. Рассматриваются технологии и стратегии управления рисками, включая значимость профессионального

обучения и образования, связанных с вопросом защиты сетей. Также представлены примеры защиты различных сетей на основе обсуждаемых технологий.

Рекомендация МСЭ-Т X.1205 определяет кибербезопасность как "набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональную подготовку, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя". Указанные ресурсы включают подсоединенные компьютерные устройства, пользователей компьютерами, приложения/услуги, системы связи, мультимедийные соединения и всю совокупность передаваемой и/или сохраняемой информации в киберсреде. В соответствии с этим определением кибербезопасность обеспечивает достижение и сохранение свойств безопасности ресурсов организаций (включая готовность системы, целостность и конфиденциальность) и защиту ресурсов пользователей от соответствующих угроз безопасности в киберсреде.

В современном деловом окружении концепция периметра исчезает. Границы между внутренними и внешними сетями становятся более размытыми. Приложения выполняются на верхнем уровне сетей, с использованием уровневого подхода. Безопасность должна обеспечиваться в пределах каждого из уровней и между уровнями. Уровневый подход к проблеме безопасности дает организациям возможность создания множества уровней защиты, направленных против угроз.

Технологии кибербезопасности могут использоваться для гарантирования готовности систем, целостности, аутентичности, конфиденциальности и неотказуемости, а также для гарантий соблюдения личной тайны пользователя. Технологии кибербезопасности также могут использоваться для установления достоверности пользователя. Наиболее важные современные методы обеспечения кибербезопасности включают:

– криптографию, которая поддерживает ряд услуг безопасности, включая обеспечение конфиденциальности данных при передаче и во время хранения, и электронную подпись;

– управление доступом, цель которого состоит в предотвращении несанкционированного доступа к информации или ее использования;

– целостность системы и данных, цель которой состоит в обеспечении того, чтобы система и ее данные не были изменены или искажены неуполномоченными сторонами или несанкционированным образом;

– аудит, регистрацию и мониторинг, которые предоставляют информацию для оказания помощи при оценке эффективности стратегии безопасности и применяемых методов;

– управление безопасностью, которое включает конфигурацию и устройства управления безопасностью, управление рисками, обработку инцидентов и управление информацией о безопасности.

Организации должны разработать всесторонний план обеспечения безопасности в каждом отдельном случае. Безопасность не может подходить "на все случаи жизни". Безопасность следует рассматривать как непрерывный процесс, который охватывает защиту систем, данных, сетей, приложений и ресурсов. Также безопасность должна быть всесторонней на всех уровнях сетей. Принятие уровневого подхода к проблеме безопасности, который в союзе с сильным управлением на основе заданных правил и обеспечения их выполнения предоставит профессионалам по безопасности выбор решения по этому вопросу, который будет модульным, гибким и масштабируемым.

3.5 Требования к персональной и физической безопасности

По большей части Рекомендации МСЭ-Т, связанные с безопасностью, сосредоточены на технических аспектах систем и сетей. Некоторые аспекты персональной безопасности определены в Рекомендации МСЭ-Т X.1051. Физическая безопасность также является очень важным аспектом защиты, но она в значительной степени выходит за рамки большинства работ МСЭ-Т. Вместе с тем основные требования к физической безопасности

определены в Рекомендации МСЭ-Т X.1051, а физическая безопасность линейно-кабельных сооружений рассматривается в двух документах, указанных ниже.

Требования к физической безопасности линейно-кабельных сооружений включают в себя необходимость убедиться в устойчивой работе оборудования в случае пожара, стихийного бедствия и намеренных или случайных повреждений. Методы обеспечения защиты компонентов систем, кабельных линий, соединительных муфт, шкафов и пр. рассматриваются в *Справочнике МСЭ-Т по технологиям внешних установок для сетей общего пользования* и в *Справочнике МСЭ-Т по применению компьютеров и микропроцессоров для создания, установки и защиты кабелей электросвязи*. В этих документах также рассматривается мониторинг систем в целях предотвращения повреждений и предлагаются способы реагирования на проблемы, а также функционального восстановления систем самым оперативным образом.

4. Архитектуры безопасности

4 Архитектуры безопасности

Архитектуры безопасности и связанные с ними модели и концепции формируют структуру и контекст, в которых соответствующие технические стандарты могут согласованно разрабатываться. В начале 1980-х годов была признана необходимость в разработке концепции, в которой безопасность могла использоваться в многоуровневой архитектуре связи. Это привело к разработке Рекомендации МСЭ-Т X.800. Этот стандарт был первым из набора архитектурных стандартов для услуг и механизмов обеспечения безопасности. В результате этой работы, основная часть которой была проведена совместно с ИСО, разработаны последующие стандарты, в том числе для моделей и структур безопасности, в которых указано, какие конкретные виды защиты можно применять в конкретных ситуациях.

Позднее была признана необходимость в разработке как общей архитектуры безопасности, так и архитектуры безопасности, определяемой приложением. Это привело к разработке Рекомендации МСЭ-Т X.805, а также целого ряда определяемых приложением архитектур для рассмотрения таких областей, как управление сетью, одноранговая связь и подвижные веб-серверы. Описанная далее в данном разделе Рекомендация МСЭ-Т X.805 дополняет другие Рекомендации МСЭ-Т серии X.800, предлагая решения в области защиты, нацеленные на обеспечение сквозной защиты сети.

4.1 Архитектура безопасности для открытых систем и относящиеся к ней стандарты

Первая из архитектур безопасности связи, которая была стандартизирована, была архитектурой защиты для взаимосвязи открытых систем согласно Рекомендации МСЭ-Т X.800. В этой Рекомендации определяются общие архитектурные элементы, связанные с безопасностью, которые могут применяться в соответствии с обстоятельствами, требующими защиты. В частности этот документ содержит общее описание услуг обеспечения безопасности и соответствующих механизмов, которые могут использоваться для оказания таких услуг. Кроме того, в нем для базовой эталонной модели взаимосвязи открытых систем (OSI) с семью уровнями определяется наиболее подходящее расположение (т. е. уровень, на котором следует реализовывать услуги обеспечения безопасности.

Рекомендация МСЭ-Т X.800 касается только тех видимых аспектов канала связи, которые позволяют оконечным системам добиться безопасной передачи информации между ними. В ней не делается попыток дать спецификацию по реализации систем и она не служит основой для оценки соответствия варианта реализации тому или иному стандарту безопасности. В ней также не указаны сколь-нибудь подробно дополнительные меры защиты, которые могут потребоваться в оконечных системах для обеспечения заданных параметров защиты связи.

Хотя Рекомендация МСЭ-Т X.800 была разработана специально для архитектуры безопасности OSI, практика показала, что базовые концепции в данном документе имеют намного более широкое применение и признание. Этот стандарт имеет особое значение, поскольку он представляет собой впервые согласованные на международном уровне определения базовых услуг по обеспечению безопасности (*аутентификация*, *управление доступом*, *конфиденциальность данных*, *целостность данных* и *неотказуемость*) наряду с более общими (всеобъемлющими) услугами, такими как *проверенные функциональные возможности*, *обнаружение событий*, а также *проверка безопасности* и *восстановление защиты.* До принятия Рекомендации МСЭ-Т X.800 существовал широкий круг представлений о том, какие базовые услуги безопасности необходимы и в чем именно должна заключаться каждая услуга. Ценность и общая применимость Рекомендации МСЭ-Т X.800 основана на том, что она отражает достигнутый важный консенсус в отношении значения терминов,

употребляемых для описания параметров защиты, набора услуг обеспечения безопасности, которые необходимы для защиты передачи данных, а также характера этих услуг безопасности.

В процессе разработки Рекомендации МСЭ-Т X.800 была выявлена необходимость в дополнительных стандартах, связанных с безопасностью связи. В результате началась работа по созданию ряда вспомогательных стандартов и дополнительных Рекомендаций в области архитектуры. Ниже рассматриваются некоторые из этих Рекомендаций.

4.2 Услуги безопасности

Структуры безопасности были разработаны с целью обеспечить всеобъемлющее и согласованное описание каждой из услуг обеспечения безопасности, определенных в Рекомендации МСЭ-Т X.800. Эти стандарты предназначены для решения всех аспектов вопроса о том, как могут быть применены услуги обеспечения безопасности в контексте конкретной архитектуры защиты, включая возможные будущие архитектуры безопасности. Структуры нацелены на обеспечение защиты систем, объектов внутри систем и на взаимодействие между системами. Они не предусматривают методику построения систем или механизмов. **В** Рекомендации МСЭ-Т X.810 представлены другие структуры и описаны общие понятия, включая домены безопасности, ответственный объект и политику защиты, которые используются во всех структурах. В ней также описан формат общих данных, который может быть использован для безопасной передачи информации как в целях аутентификации, так и для управления доступом.

Аутентификация – это обеспечение гарантии заявленной подлинности объекта. Объектами могут быть не только физические лица, но и устройства, услуги и приложения. Аутентификация может также гарантировать, что объект не пытается выдать себя за другой объект или несанкционированным образом воспроизвести предыдущее сообщение. В Рекомендации МСЭ-Т X.800 определены два вида аутентификации: *аутентификация отправителя данных* (т. е. удостоверение того, что источником полученных данных является заявленный источник) и *аутентификация равноправного объекта* (т. е. удостоверение того, что равноправным объектом в ассоциации защиты является заявленный объект). В Рекомендации МСЭ-Т X.811 определяются основные понятия аутентификации, устанавливаются возможные классы механизма аутентификации, определяются услуги для этих классов механизма, устанавливаются функциональные требования для протоколов поддержки этих классов механизма и устанавливаются требования по общему управлению аутентификацией.

Управление доступом – это предотвращение несанкционированного использования ресурса, включая предотвращение использования ресурса несанкционированным образом. Контроль за доступом гарантирует, что доступ к элементам сети, хранимой информации, информационным потокам, услугам и приложениям имеет только уполномоченный персонал или допущенные устройств. Структура контроля за доступом (Рекомендация МСЭ-Т X.812) описывает модель, которая включает все аспекты контроля за доступом в открытых системах, взаимосвязи с другими функциями обеспечения безопасности, например аутентификацию и проверку, а также эксплуатационные требования в отношении контроля за доступом.

Неотказуемость – это способность не допустить, чтобы объекты впоследствии отказались от того, что они выполнили те или иные действия. Неотказуемость связана с установлением доказательств, которые впоследствии могут быть использованы для опровержения ложных утверждений. В Рекомендации МСЭ-Т X.800 описываются две формы услуги по неотказуемости – *неотказуемость с доказательством доставки*, которое используется для опровержения ложного отказа получателя признать, что данные были получены, и *неотказуемость с доказательством происхождения*, которое используется для опровержения ложного отказа отправителя признать, что данные были отправлены. Однако в более широком смысле понятие неотказуемости может применяться во многих других контекстах, включая неотказуемость создания,

представления, хранения, передачи и получения данных. Рекомендация МСЭ-Т X.813 расширяет понятия услуг по обеспечению неотказуемости как они описаны в Рекомендации МСЭ-Т X.800, и предусматривает основу для развития таких услуг. Она также устанавливает возможные механизмы поддержки этих услуг и общие требования к управлению в отношении неотказуемости.

Конфиденциальность – это характеристика, которая делает информацию недоступной или нераскрываемой для неуполномоченных лиц, объектов или процессов. Цель услуги обеспечения конфиденциальности состоит в том, чтобы защитить информацию от несанкционированного раскрытия. Рекомендация МСЭ-Т X.814 рассматривает конфиденциальность путем определения основных понятий конфиденциальности, возможных классов конфиденциальности и средства, необходимого для каждого класса механизма конфиденциальности. Она также устанавливает процесс управления и необходимые вспомогательные услуги, а также взаимодействие с другими услугами и механизмами обеспечения безопасности.

Целостность данных – это характеристика, которая свидетельствует о том, что данные не были изменены несанкционированным образом. В общем смысле услуга по обеспечению целостности состоит в необходимости гарантировать, что данные не были искажены или что в случае искажения пользователь узнает об этом. Рекомендация МСЭ-Т X.815 рассматривает целостность данных при поиске и передаче информации, а также управлении ею. Она определяет основные понятия целостности, устанавливает возможные классы механизма обеспечения целостности и средства, требования к управлению и соответствующие услуги, необходимые для поддержки этого класса механизмов. Следует отметить, что хотя стандарты архитектуры безопасности концентрируются главным образом на целостности данных, другие аспекты целостности, например целостность системы, также имеют большое значение для безопасности.

4.3 Архитектура безопасности для систем, обеспечивающих связь между оконечными пунктами

В 2003 году после более углубленного рассмотрения архитектуры безопасности для сетей была утверждена Рекомендация МСЭ-Т X.805. Эта архитектура, которая строится на базе некоторых концепций Рекомендации МСЭ-Т X.800 и рассмотренных выше концепций безопасности и расширяет их, может применяться к различным видам сетей и является технологически нейтральной.

4.3.1 Элементы архитектуры согласно Рекомендации МСЭ-Т X.805

Архитектура согласно Рекомендации МСЭ-Т X.805 определяется исходя их трех основных концепций: уровней безопасности, плоскостей и аспектов безопасности для сети между оконечными пунктами. При распределении требований к безопасности по слоям и плоскостям применяется иерархический подход, так что сквозная безопасность обеспечивается за счет разработки в каждом аспекте мер безопасности для борьбы с конкретными угрозами. На рисунке 1 показаны элементы этой архитектуры.

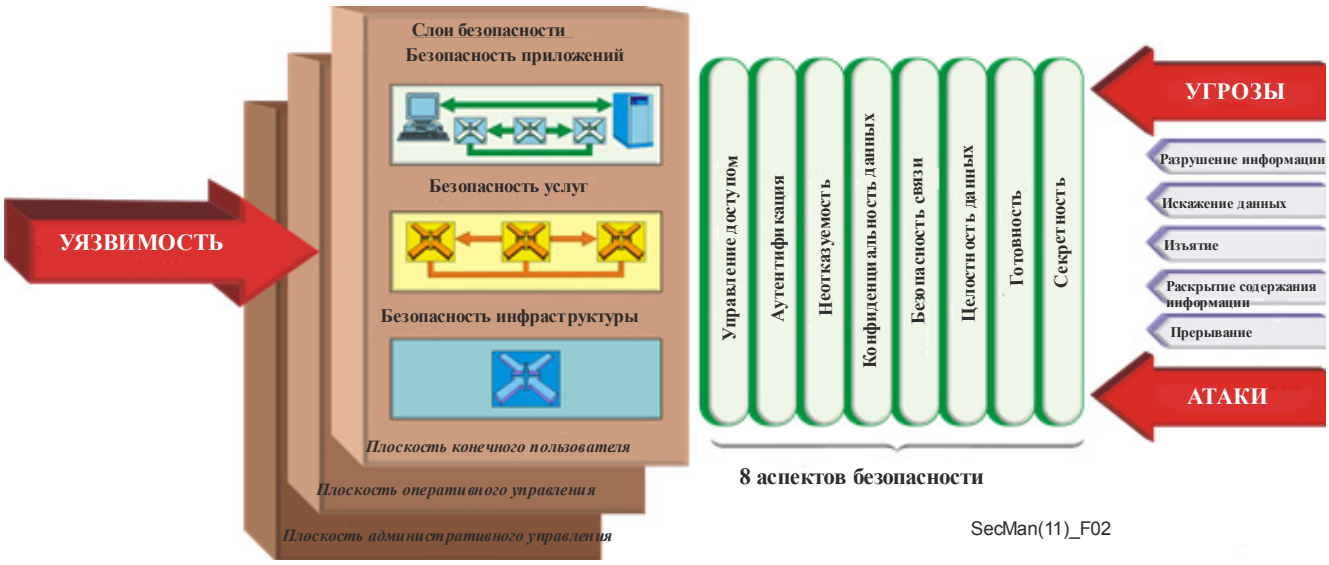


Рисунок 1 – Элементы архитектуры безопасности согласно Рекомендации МСЭ-Т X.805

Аспектом безопасности называется набор мер безопасности, разработанных для конкретного аспекта безопасности сети. Основные услуги безопасности согласно Рекомендации МСЭ-Т X.800 (*управление доступом, аутентификация, конфиденциальность данных, целостность данных* и *неотказуемость)* отражаются в функциональных возможностях соответствующих *аспектов безопасности* Рекомендации МСЭ-Т X.805 (как показано на рисунке 1). Кроме того, Рекомендация МСЭ-Т X.805 вводит три аспекта (*безопасность связи, готовность* и *секретность)*, которых нет в Рекомендации МСЭ-Т X.800:

- аспект *безопасность связи,* который гарантирует, что информация передается только между уполномоченными оконечными точками, т. е. информация не изменяет направления и не перехватывается при передаче между этими оконечными точками;
- аспект *готовность,* который обеспечивает, что вследствие влияющих на сеть событий не возникнет отказа в санкционированном доступе к элементам сети, хранимой информации, потокам данных, услугам и приложениям; и
- аспект *секретность* обеспечивает защиту информации, которая может быть получена в результате наблюдения за действиями сети. Примерами могут служить веб-сайты, которые посещает пользователь, географическое положение пользователя и IP-адреса и имена DNS-устройств в сети поставщика услуг.

Указанные аспекты предусматривают дополнительную защиту сети и защищают от всех основных угроз безопасности. Эти аспекты не ограничиваются рамками сети, а распространяются на приложения и на информацию конечного пользователя. Аспекты безопасности распространяются также на поставщиков услуг или предприятия, предлагающие своим клиентам услуги безопасности.

Для того чтобы обеспечить сквозное решение по обеспечению безопасности, аспекты безопасности должны применяться к иерархии сетевого оборудования и группам установок, которые называются *слоями безопасности*. *Плоскость безопасности* представляет собой определенный тип действий сети, защищаемых аспектами безопасности. Каждая плоскость безопасности представляет собой защищаемый тип действий сети.

Слои безопасности касаются требований, которые применимы к сетевым элементам, системам, к услугам и приложениям, ассоциированным с этими элементами. Одним из преимуществ подхода, основанного на определении слоев, является возможность его многократного применения по различным приложениям для обеспечения сквозной защиты. Уязвимости в каждом слое различны, и поэтому должны быть определены меры противодействия для удовлетворения потребности каждого слоя. Это три следующих слоя:

- *слой инфраструктуры*, который представляет основные структурные элементы сети, их услуги и приложения. Примерами элементов, относящихся к этому слою, являются отдельные сетевые элементы, такие как маршрутизаторы, коммутаторы и серверы, а также каналы связи между ними;
- *слой услуг*, который относится к безопасности предлагаемых потребителям сетевых услуг. Эти услуги лежат в широком диапазоне – от услуг базового подключения, таких как услуги выделенных каналов, до дополнительных услуг, таких как немедленная передача текстовых сообщений; и
- *слой приложений,* который касается требований к сетевым приложениям, используемым потребителями. Приложения могут быть простыми, как электронная почта, или сложными, как, например, групповая визуализация, когда видеоинформация высокой четкости используется, например, для ведения нефтепоисковых работ или проектирования автомобилей.

Плоскости безопасности удовлетворяют конкретные потребности в защите, которые связаны, соответственно, с административным управлением сетью, оперативным управлением сетью или действиями по сигнализации, а также операциями конечного пользователя. Сети следует разрабатывать так, чтобы события в одной плоскости безопасности были бы изолированы от других плоскостей безопасности.

Плоскостями безопасности являются:

- *плоскость административного управления,* которая связана с функциями эксплуатации, администрирования, технического обслуживания и обеспечения, такого как обеспечение пользователя или сети;
- *плоскость оперативного управления*, которая связана с действиями по сигнализации для настройки (и модификации) сквозной связи по сети независимо от среды передачи и технологии, используемой в сети; и
- *плоскость конечного пользователя*, которая рассматривает вопросы безопасности доступа и использование сети абонентами. Эта плоскость также служит для защиты потоков данных конечного пользователя.

Архитектура, предусмотренная в Рекомендации МСЭ-Т X.805, может служить руководством для разработки политики в области безопасности, технологических структур, планов реагирования на инциденты и восстановления. Эта архитектура может также быть использована как основа для анализа безопасности. После введения программы безопасности ее следует поддерживать, с тем чтобы она соответствовала постоянно меняющимся условиям угроз. Эта архитектура безопасности может помочь в поддержании программы безопасности, обеспечивая учет каждого аспекта безопасности в каждом слое и в каждой плоскости безопасности при внесении изменений в программу безопасности.

Несмотря на то что Рекомендация МСЭ-Т X.805 представляет собой архитектуру безопасности сети, некоторые ее положения могут быть распространены на устройства конечного пользователя. Эта тема рассматривается в Рекомендации МСЭ-Т X.1031.

4.3.2 Готовность сети и ее компонентов

Готовность сети – это важный аспект безопасности ИКТ. Как отмечено выше, цель аспекта безопасности *готовность* в МСЭ-Т X.805 состоит в обеспечении непрерывности обслуживания и санкционированного доступа к элементам сети, информации и приложениям. Решения для восстановления после бедствий также включены в этот аспект.

Функциональные, эксплуатационные и оперативные требования для ограничения рисков и последствий неготовности сетевых ресурсов очень многочисленны и разнообразны. Существует множество элементов, которые требуется учитывать, среди них защищенность от помех, борьба с перегрузками, сообщения об отказах и меры по исправлению. Рекомендация МСЭ-Т G.827 определяет параметры и показатели качества сети для

элементов трассы и готовности для сквозных международных цифровых трактов с постоянной скоростью передачи. Эти параметры не зависят от типа физической сети, используемой для создания сквозных трактов. В Приложении А Рекомендации МСЭ-Т G.827 содержится подробная инструкция по методикам оценки сквозной готовности и приводятся примеры топологий трактов и расчетов сквозной готовности тракта. Другие Рекомендации, которые рассматривают показатели качества сети, включают: Рекомендацию МСЭ-Т G.1000, Рекомендацию МСЭ-Т G.1030, Рекомендацию МСЭ-Т G.1050 и Рекомендацию МСЭ-Т G.1081.

4.4 Руководящие указания по реализации

Все стандарты архитектуры безопасности МСЭ-Т являются составными частями Рекомендаций МСЭ-Т по безопасности серии X.800–849. Руководящие указания по реализации приведены в Дополнении 3 к Рекомендациям МСЭ-Т серии X. В этом дополнении содержатся руководящие указания по важнейшим действиям в плане безопасности на протяжении срока жизни сети. Эти руководящие указания касаются четырех областей: политика технической безопасности; иерархическая идентификация средств; угрозы, уязвимости и меры смягчения на базе иерархии средств; а также оценка безопасности. Руководящие указания и соответствующие им шаблоны предназначены для обеспечения систематического планирования безопасности сети, ее анализа и оценки.

4.5 Некоторые виды архитектур, определяемых приложениями

В этом разделе вводятся некоторые аспекты архитектур, относящихся к конкретным приложениям.

4.5.1 Одноранговая связь

В одноранговой сети (P2P) все пользователи имеют равные права и ответственность. В отличие от модели клиент/сервер, когда в сети передаются данные или сообщения, один пользователь связывается непосредственно с другими. Так как трафик обрабатывается и распределяется для каждого пользователя, для сети P2P не требуется сверхмощных компьютеров или сверхширокополосных сетей.

Сеть P2P – это сеть, наложенная поверх сети электросвязи и интернета. Она использует разнообразные соединения между узлами, а также вычислительную мощность и память, доступную на каждом узле, а не привычные централизованные ресурсы.

Сети P2P обычно используются для связи между узлами через временные соединения. Такие сети полезны для многих целей, включая совместное использование файлов, содержащих звук, изображение, текст или другие данные в цифровом формате. Для передачи данных в реальном времени, например телефонного трафика, также используется технология P2P.

4.5.1.1 Архитектура и операции по обеспечению безопасности для одноранговых сетей

Общая архитектурная модель, связанная с безопасностью, которая может быть применена в различных сетях P2P, описывается в Рекомендации МСЭ-Т X.1162.

На рисунке 2 показана базовая архитектура услуги P2P. Информация, обрабатываемая каждым равноправным участником, передается непосредственно между пользователями. Поскольку центрального сервера для хранения информации нет, каждому участнику, прежде чем получить данные, требуется отыскать того из участников, кто имеет нужные данные. Более того, каждый равноправный участник должен разрешить другим участникам доступ, для того чтобы началась передача данных.

Рисунок 2 – Архитектура услуги P2P

В физической сети P2P пользователь может присоединиться к услугам P2P с помощью того или иного устройства. Обычно термин *равноправный участник* используется для описания пользователя или устройства, принадлежащего пользователю. Типы соединений между блоками в сети P2P можно разделить на следующие категории:

- внутридоменное соединение с равноправным участником;
- междоменное соединение с равноправным участником; и
- соединение с равноправным поставщиком услуг, расположенным в домене другой сети.

На рисунке 3 показана логическая архитектура сети P2P в виде виртуальной сети поверх транспортного уровня. Предполагается, что работа каждого участника не ограничивается физической архитектурой сети и что участник может связываться с любым другим участником вне зависимости от его местоположения (при необходимости – через вышестоящего участника). Структура одноранговой сети делится на два уровня: уровень наложения P2P и транспортный уровень. Транспортный уровень обеспечивает передачу пакетов от верхнего слоя или к нему, а уровень наложения обеспечивает предоставление услуг P2P.

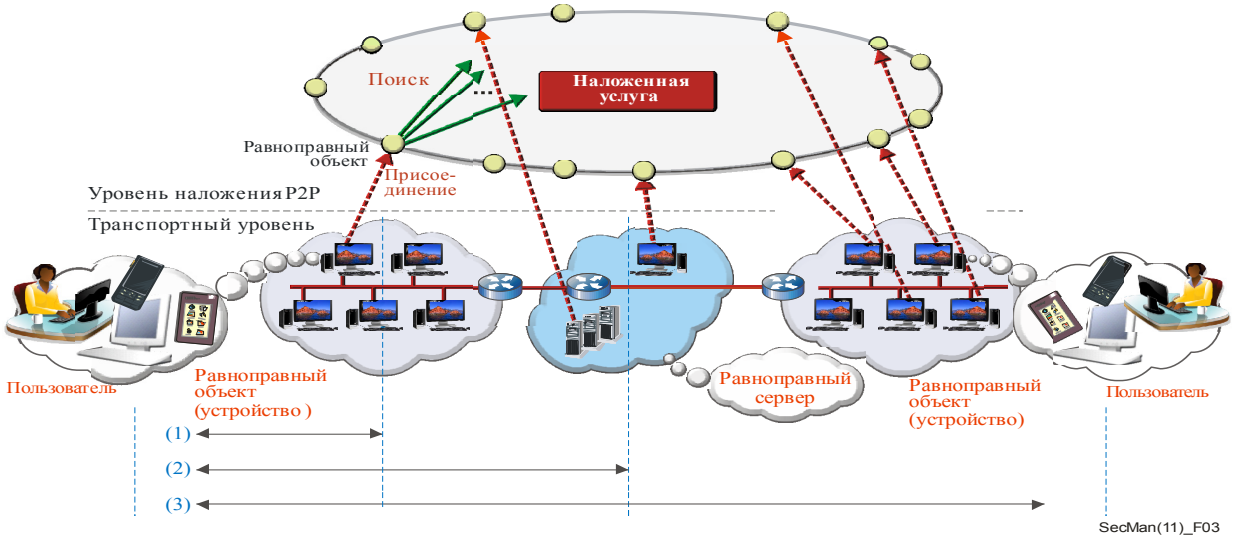


Рисунок 3 – Архитектурная эталонная модель для сети P2P

4.5.1.2 Концепция защиты одноранговой связи

Требования к безопасности для сетей P2P, а также услуги и механизмы, которые должны удовлетворять этим требованиям, определены в Рекомендации МСЭ-Т X.1161.

Угрозы соединениям P2P включают в себя подслушивание, создание помех, вторжение и внесение изменений, несанкционированный доступ, непризнание участия, активное вмешательство в соединение и атаки типа Sybil. Меры противодействия угрозам для P2P показаны в таблице 3.

Таблица 3 – Взаимосвязь между требованиями к безопасности P2P и мерами противодействия

Функции / Требования	Шифрование	Обмен ключами	Цифровая подпись	Управление доверием	Управление доступом	Механизм обеспечения целостности данных	Обмен аутентификацией	Нотариальное заверение	Защищенная маршрутизация	Механизм управления трафиком	Назначение ID
Аутентификация пользователя	X	X	X	X	X		X				X
Анонимность	X			X							X
Секретность	X				X		X				
Целостность данных	X	X	X		X	X	X				
Конфиденциальность данных	X	X			X		X				
Контроль за доступом					X		X				X
Неотказуемость			X				X	X			X
Удобство использования					X						
Готовность					X		X		X	X	
Возможность оперативного контроля			X						X		X
Управление трафиком		X								X	

4.5.2 Архитектура безопасности для защиты сообщений в подвижных веб-услугах

Архитектура безопасности и сценарии для защиты сообщений в подвижных веб-услугах описаны в Рекомендации МСЭ-Т X.1143. Этот стандарт представляет:

- архитектуру безопасности для защиты сообщений, которая опирается на соответствующие механизмы политики веб-услуг;
- механизмы сетевого взаимодействия и сценарии услуг между приложениями, которые поддерживают стеки протокола безопасности полных веб-услуг и традиционные приложения, которые не поддерживают стеки протокола безопасности полных веб-услуг;
- механизмы аутентификации сообщений, обеспечения целостности и конфиденциальности;
- механизмы фильтрации сообщений на основе содержания сообщений; и

- эталонную архитектуру безопасности сообщений и сценарии услуг безопасности.

На рисунке 4 показана архитектура безопасности согласно Рекомендации МСЭ-Т X.1143 для подвижных веб-услуг.

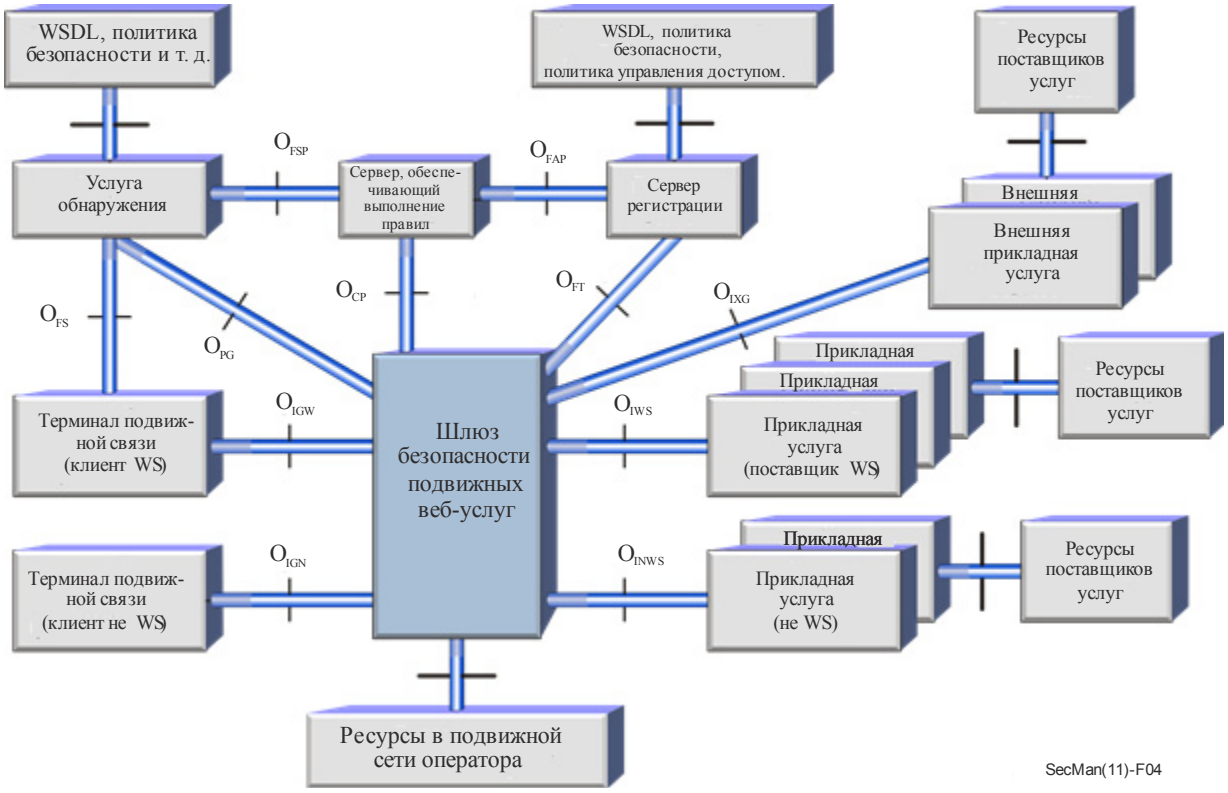


Рисунок 4 – Архитектура безопасности для подвижных веб-услуг

Архитектура безопасности для подвижных веб-услуг состоит из следующих компонентов:

- подвижных терминалов, которые являются клиентами подвижных веб-услуг;
- шлюзов безопасности подвижных веб-услуг (MWSSG). Все запросы от подвижных клиентов передаются на MWSSG, который также выполняет функции управления доступом;
- службы принятия решений, которая управляет политикой безопасности, относящейся к безопасной обработке сообщений, и политикой управления доступом для сообщений;
- службы приложений, которая предоставляет клиентам различные дополнительные услуги;
- службы обнаружения, которая хранит информацию интерфейса для служб приложений и соответствующие правила безопасности для доступа клиентов к службам приложений; и
- сервера регистрации, который находится во внутреннем домене оператора подвижной связи и управляет информацией интерфейса для служб приложений, в соответствии со связанными с ней правилами безопасности для доступа клиентов к прикладным услугам и правилами управления доступом к целевым услугам.

Инфраструктура обеспечения безопасности в режиме мобильности для транспортного уровня СПП определяется в Рекомендации МСЭ-Т Y.2760, которая рассматривает требования к безопасности, механизмы и процедуры обеспечения безопасности для управления мобильностью и контроля над этим режимом в СПП.

4.6 Архитектура для обеспечения внешних взаимосвязей

Взаимосвязи между системой обеспечения безопасности в сетях электросвязи (TNSS) на основе IP и различными группами внешних объектов рассматриваются в Рекомендации МСЭ-Т X.1032. Данный стандарт обеспечивает:

- взаимосвязи TNSS с системами обеспечения безопасности информационных систем и информационной структуры;
- взаимосвязи TNSS с объектами систем электросвязи;
- взаимосвязи TNSS с внешними организациями; и
- взаимосвязи TNSS с источниками угроз безопасности.

На рисунке 5 показаны действия внешних объектов согласно МСЭ-Т X.1032 и их влияние на TNSS.

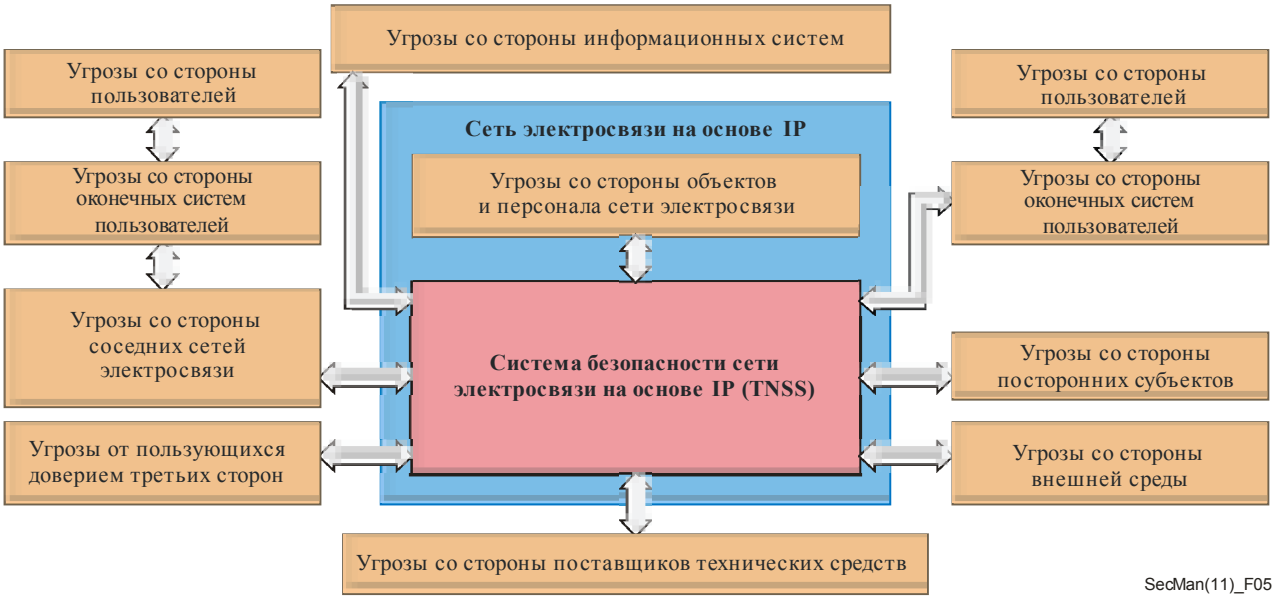


Рисунок 5 – Модель взаимосвязей TNSS с источниками угроз безопасности

Угрозы разделяются на пять типов, как указано в [МСЭ-Т X.800] и [МСЭ-Т X.805]:

- разрушение информации и других ресурсов;
- искажение или изменение информации;
- кража, удаление или потеря информации и других ресурсов;
- раскрытие информации; и
- прерывание обслуживания.

Политика обеспечения безопасности в сети электросвязи может использоваться для противодействия всем угрозам, либо некоторым из этих угроз. Соответствующим образом в ходе разработки системы TNSS выбираются необходимые аспекты безопасности. Внешнее взаимодействие TNSS с источниками угроз безопасности может быть обусловлено:

- электрическими интерфейсами;
- действиями людей;
- техническими атаками посредством сети электросвязи и внешними техническими атаками;

- воздействиями внешней среды;
- техническими мерами для противодействия атакам; и
- организационными мерами для противодействия атакам.

4.7 Архитектура и модели безопасности других сетей

Дополнительные аспекты архитектуры безопасности сетей рассматриваются далее в этом документе. В частности, обратитесь к разделам 7.2 – Архитектура управления сетью; 8.1 – Безопасность сетей последующих поколений (СПП); 8.4.1 – Архитектура IPCablecom; и 10.2 – IPTV.

5. Аспекты управления безопасностью

5 Аспекты управления безопасностью

Управление безопасностью это широкая тема, которая охватывает многие действия, связанные с управлением и защитой доступа к системе и сетевым ресурсам, контроль событий, отчетность, правила и аудит, а также управление информацией, связанной с этими функциями и действиями. В этом разделе рассматриваются некоторые общие действия по управлению безопасностью. Действия по управлению безопасностью, связанные с защитой сетевой инфраструктуры, рассматриваются в разделе 7.

5.1 Управление информационной безопасностью

Информация, как и другие активы, вносит существенный вклад в бизнес организации. Информация может быть распечатана, сохранена в электронном виде, выслана по почте, передана в электронном виде, отображена на пленке, высказана в разговоре или передана другими способами. Вне зависимости от формы или функциональности информации или средств, посредством которых происходит обмен информацией или ее хранение, информацию всегда следует защищать соответствующим образом.

Организации электросвязи, устройства которых используются абонентами для обработки информации, которая может содержать персональные данные, секретные данные и важную коммерческую информацию, должны обеспечивать соответствующий уровень защиты для предотвращения перехвата информации, т. е. им требуется создать эффективную систему управления информационной безопасностью (ISMS).

Если безопасность информации нарушена, например, за счет несанкционированного доступа к системе обработки информации какой-либо организации, эта организация может понести значительные убытки. Следовательно, для организации очень важно обеспечить эффективную защиту своей информации путем внедрения структурированного процесса управления безопасностью. Такая задача достигается путем реализации набора соответствующих мер управления. Эти меры управления, которые применяются к данным, к устройствам электросвязи, услугам и приложениям, должны быть разработаны, реализованы, их следует контролировать, проверять и непрерывно улучшать. Невозможность успешного создания эффективного управления безопасностью может привести к тому, что организация не сможет решать задачи как своей безопасности, так и бизнеса.

Наиболее широко используемой спецификацией ISMS является та, что опубликована в серии стандартов ИСО/МЭК серии 27000, в которую входят стандарты по основам ISMS, требования, кодекс применения, руководящие указания по реализации и связанные темы. МСЭ-Т и ИСО/МЭК совместно разработали Рекомендацию МСЭ-Т X.1051 | Международный стандарт ИСО/МЭК 27011, основанные на ИСО/МЭК 27002, Кодекс использования ISMS.

Рекомендация МСЭ-Т X.1051 устанавливает руководящие указания и общие принципы для инициирования, реализации, обслуживания и улучшения управления информационной безопасностью в организациях электросвязи и представляет основы по внедрению для управления информационной безопасностью, с тем чтобы гарантировать конфиденциальность, целостность и готовность устройств и услуг электросвязи. Специальные руководящие указания для сектора электросвязи включены по следующим тематикам:

- организация информационной безопасности;
- управление средствами;
- безопасность людских ресурсов;
- физическая и экологическая безопасность;
- управление связью и эксплуатацией;

- управление доступом;
- приобретение информационных систем;
- разработка и обслуживание;
- управление инцидентами; и
- управление непрерывностью бизнеса.

В дополнение к применению показателей безопасности и управления, описанных в Рекомендации МСЭ-Т X.1051, организации электросвязи также должны учитывать следующие конкретные задачи безопасности:

- информация должна быть защищена от несанкционированного раскрытия. Это предусматривает нераскрытие передаваемой информации, в том что касается ее существования, содержания, источника, получателя, даты и времени;
- установкой и использованием устройств электросвязи следует управлять для того, чтобы обеспечить аутентичность, точность и полноту информации, передаваемой, ретранслируемой или принимаемой по проводам, по радио или любыми другими способами; и
- весь доступ к информации, устройствам и среде электросвязи, используемым для предоставления услуг связи, должен быть санкционирован и предоставляться только по необходимости. В качестве расширения положений о готовности организации должны отдавать приоритет важнейшим сеансам связи в неотложных случаях и соответствовать регламентарным требованиям.

В целях снижения риска надлежащим образом реализованное управление информационной безопасностью в организациях электросвязи требуется вне зависимости от среды или режима передачи.

Организации электросвязи предоставляют свои услуги, действуя как посредник в процессе передачи данных другими юридическими и физическими пользователями. Следовательно, необходимо учитывать тот факт, что устройства обработки информации в конкретной организации доступны и могут использоваться не только ее собственными сотрудниками и подрядчиками, но также и различными пользователями вне организации.

Учитывая, что услуги и устройства электросвязи могут использоваться совместно с другими поставщиками услуг и/или соединяться с ними, управление информационной безопасностью в организациях электросвязи должно распространяться на любую область сетевой инфраструктуры и на все услуги, приложения и устройства.

5.2 Структура управления информационной безопасностью

В Рекомендации МСЭ-Т X.1051 определяются категории управления безопасностью электросвязи. Рекомендация МСЭ-Т X.1052 определяет ряд основных видов деятельности по проведению и поддержке реализации функций управления безопасностью, а также объединяет функции управления в Рекомендации МСЭ-Т X.1051 и в других Рекомендациях, которые представляют собой конкретное руководство для ряда областей управления информационной безопасностью, например Рекомендации МСЭ-Т X.1055, МСЭ-Т X.1056 и МСЭ-Т X.1057, как показано на рисунке 6.

Рисунок 6 – Взаимосвязь между Рекомендацией МСЭ-Т X.1052 и другими Рекомендациями для областей управления информационной безопасностью

Организациям электросвязи необходимо подтверждать область применения своих систем ISMS, которая должна включать ресурсы обработки информации. Такое подтверждение, наряду с созданием руководства по реализации системы управления информационной безопасностью, должно выдаваться до оценки рисков для информационных ресурсов и последующего управления рисками. Кроме того, необходимо создать структуру и определить форму организации по обеспечению информационной безопасности в качестве основы для выполнения функций управления рисками. Действия по управлению рисками этих организаций не должны отделяться от их эксплуатационной деятельности, которая, как правило, описывается с помощью ряда процедур. Действия по управлению рисками должны рассматриваться как неотъемлемая часть соответствующих процедур.

Система ISMF описывает основные действия, связанные с управлением информационной безопасностью в сетях электросвязи, с учетом трех аспектов:

a) стимулирования конкретной организации по осуществлению функций управления информационной безопасностью, включая такие сферы управления, как управление организацией и персоналом, а также управление ресурсами;

b) создания системы ISMS и постоянного ее улучшение, включая такие сферы управления, как управление рисками и управление на основе заданных правил; и

c) конкретной эксплуатационной деятельности организации, включая такие сферы управления, как управление приобретением и развитием системы, управление эксплуатацией и техническим обслуживанием, а также управление инцидентами.

5.3 Управление рисками

Управление рисками – это процесс оценки и количественного определения риска и выполнение действий для обеспечения того, чтобы остаточный риск был бы ниже заранее определенного приемлемого уровня. Эта тема была включена в Рекомендацию МСЭ-Т X.1205. Более подробные руководящие указания по управлению рисками содержатся в Рекомендации МСЭ-Т X.1055, определяющей процессы и методы, которые могут использоваться для оценки требований к безопасности электросвязи и рисков и для содействия в выборе,

реализации и обновлении соответствующих методов управления для поддержания требуемого уровня безопасности.

Существует целый ряд конкретных методик для решения проблем управления рисками. В Рекомендации МСЭ-Т X.1055 содержатся критерии по оценке и выбору соответствующих методик для организации электросвязи. Однако она не предлагает никакой специальной методики управления рисками.

Процесс управления рисками показан на рисунке 7.

Рисунок 7 – Процесс управления рисками МСЭ-Т X.1055

Профили рисков используются для регулирования всего процесса управления рисками. В частности, они используются для содействия в процессе принятия решения и для оказания помощи в определении приоритетов рисков в плане их критичности, а также для оказания помощи при выборе распределения ресурсов и мер противодействия. Они также могут служить для оказания помощи в разработке соответствующих мер и могут применяться вместе с другими инструментами, например методами анализа пробелов. В Рекомендации МСЭ-Т X.1055 содержится руководство по разработке профилей рисков, а также шаблон и примеры профилей некоторых рисков.

5.5 Управление ресурсами

Ресурсом является какой-либо компонент или объект, стоимость которого непосредственно определяется организацией. Ресурсы организации обладают своими собственными уникальными значениями стоимости с различных точек зрения: бизнеса, финансовых дел, надежности и т. д. Можно считать, что информационные и коммуникационные устройства в рамках системы ISMS обладают большей стоимостью по сравнению со стоимостью других ресурсов. Инциденты, в которых затрагиваются такие активы, могут негативно воздействовать не только на пользователей, но и на бизнес самой организации. Поэтому ресурсы должны рассматриваться в качестве активов, имеющих более высокие приоритеты защиты. Многие организации пытаются найти наилучшие методы определения ресурсов, которые обладают высокими приоритетами защиты. Целью управления ресурсами является определение и защита особо важных компонентов организации, с тем чтобы свести к минимуму риск возникающих проблем. При определении степени важности ресурсов должны рассматриваться основные службы и значимость ресурсов с точки зрения бизнеса, учитывая при этом:

- потенциальное влияние каждого ресурса на службу и на объем предоставляемых услуг;
- возможные потери прибыли и степень возможных финансовых потерь;
- потенциальное влияние на потери клиента(ов); и
- потенциальный ущерб для имиджа организации.

Организации электросвязи должны ставить перед собой особо емкие задачи для задействования своих разного рода ресурсов и управления ими для предоставления услуг клиентам и для прямой или косвенной поддержки их бизнеса. В целях защиты этих ресурсов важно обеспечить со стороны организаций электросвязи, чтобы эксплуатационная деятельность и обслуживание бизнеса не подвергались риску.

В Рекомендации МСЭ-Т X.1057 приведен обзор процессов и методик, подлежащих рассмотрению, для определения, классификации, оценки и обслуживания ресурсов, которыми обладают организации электросвязи.

В отношении управления ресурсами для обеспечения информационной безопасности смотри соответствующие меры по обработке и защите с учетом стоимости ресурсов, которая была определена организацией. Для систематического и безопасного управления различными ресурсами организации должен быть принят процесс управления ресурсами в течение их жизненного цикла, который охватывает период приобретения или создания, изменения и ликвидации или уничтожения ресурсов в соответствии с заранее определенными правилами и нормами. Процесс управления ресурсами показан на рисунке 8.

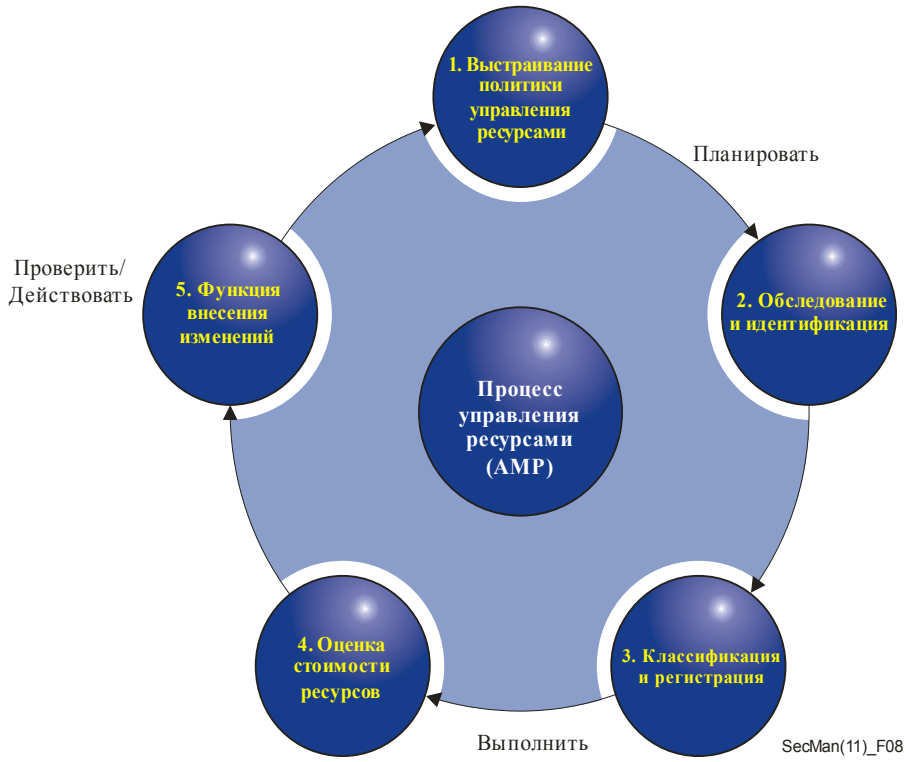


Рисунок 8 – Концепция процесса управления ресурсами

В Рекомендации МСЭ-Т X.1057 приведены руководящие указания с подробным описанием действий для каждого из процессов, которые охватывают: выстраивание политики управления ресурсами; обследование и идентификацию; классификацию и регистрацию; оценку стоимости ресурсов и функцию внесения изменений. В документе МСЭ-Т X.1057 также дается описание ресурсов, относящихся конкретно к электросвязи, с показанными в таблице 4 примерами.

Таблица 4 – Примеры ресурсов общего назначения и ресурсов, относящихся конкретно к электросвязи

Тип ресурса	Описание	Примеры	
		Конкретно для электросвязи	Общего назначения
Электронная информация	Информация, сохраняемая в электронной форме	Информация (база данных) для пользователей услуг электросвязи, журнал сеанса связи в сети и доступа к сеансу, файлы конфигурации сети, использование услуг и общие принципы доступа и т. д.	База данных (БД офиса и т. д.), файлы данных (основные принципы и руководящие указания офиса, журнал скрытого видеонаблюдения (CCTV) и т. д., файлы системы (конфигурация файлов, журналы файлов и пр.) и т. д.
Информация на бумажных носителях	Информация, сохраняемая на бумажных носителях и означающая документы или записи, подлежащие представлению и использованию при решении задач	Договоры и соглашения, включая соглашение об уровне обслуживания (SLA), схема сетевой архитектуры, список IP-адресов, схема кабельных соединений, схема системы серверов, руководства операционной системы сети и т. д.	Договоры и соглашения, документы на систему (схема конфигурации сети, руководство пользователя и пр.) и т. д.
Программное обеспечение	Программное обеспечение, разработанное на промышленной основе или для самой организации	Операционная система сети, сетевой сканер, инструментальные средства и служебные программы для раннего обнаружения и предупреждения, программное обеспечение контрольного журнала и т. д.	Прикладное программное обеспечение (офисная прикладная программа и т. д.), системное программное обеспечение (ОС, СУБД, сканер выявления уязвимостей и т. д.), инструментальные средства и служебные программы для проектирования и т. д.
Аппаратное обеспечение	Серверные и сетевые устройства, используемые для предоставления внутренних и внешних услуг или для целей бизнеса	Сервер (сервер DNS, сервер DHCP, сервер для журнала регистраций, сервер аутентификации, сервер NTP, сервер NMS, сервер контроля и т. д.), сетевое и связное оборудование (маршрутизатор базовых сетей, коммутатор, CMTS, NAS/RAS, AP, модем и т. д.), оборудование обеспечения безопасности (ESM, брандмауэр, IPS, IDS, VPN, virus wall, программа вакцинации и т. д.), подвижные системы, спутниковые системы (станции), микроволновые системы, система передачи и т. д.	Сервер (веб-сервер, сервер БД, WAS, сервер для журнала регистраций, резервный сервер, сервер хранения данных и т. д.), базовые ЭВМ, сетевое и связное оборудование (коммутатор и т. д.), оборудование обеспечения безопасности, настольные установки, рабочие станции, переносные компьютеры, портативные устройства и т. д.

Тип ресурса	Описание	Примеры	
		Конкретно для электросвязи	Общего назначения
Помещение	Место, где устанавливаются и работают системы, которое включает физические пространства и различные вспомогательные аппаратные комнаты	Помещения для разводки кабеля, помещения для управления и контроля за сетью, комната для связного оборудования, центр сбора данных интернета и т. д.	Офисное здание, серверная комната, комната для работы с бумажными носителями, помещение для электро-оборудования и т. д.
Вспомогательные поддерживающие системы и оборудование	Оборудование, используемое для работы поддерживающей информационной системы, которая включает источник электропитания, оборудование кондиционирования воздуха и т. д.	Вспомогательные системы, поддерживающие работу сетей подвижной, спутниковой и фиксированной связи (генератор, UPS и пр.) и т. д.	Электрическое оборудование, оборудование кондиционирования воздуха, противопожарное оборудование, CCTV и т. д.

6. Аутентификация и роль каталога

6 Аутентификация и роль каталога

Аутентификация – это приобретающая все большую важность услуга обеспечения безопасности, которая в значительной мере опирается на услуги каталога. В дополнение к поддержке аутентификации каталог поддерживает ряд других ключевых услуг обеспечения безопасности и некоторые механизмы, используемые для предоставления услуг, в частности услуги шифрования.

Как правило, термин "каталог" используется для указания организованного набора информация или файлов, которые могут запрашиваться для получения конкретной информации. В рамках МСЭ-Т и, в более широком смысле, в контексте стандартизации безопасности и электросвязи термин *"каталог"* обозначает хранилище информации, основанное на Рекомендациях МСЭ-Т серии X.500, которые были разработаны совместно с ИСО/МЭК. Каталог, который включен в Рекомендацию МСЭ-Т X.500 и разработан в Рекомендациях МСЭ-Т X.501, МСЭ-Т X.509 и МСЭ-Т X.519, предоставляет услуги каталога для упрощения связи и обмена информацией между объектами, людьми, терминалами, списками рассылки и т. д. В дополнение к обычным услугам каталогов, таким как назначение имен, преобразование имени в адрес и установление связи между объектами и их местоположением, каталог играет важную роль в поддержке услуг безопасности путем определения и хранения удостоверяющих данных аутентификации в форме сертификатов безопасности. В частности, в Рекомендациях МСЭ-Т серии X.500 рассматриваются два аспекта безопасности:

- защита информации каталога, определенная главным образом в Рекомендации МСЭ-Т X.501 и Рекомендации МСЭ-Т X.509; и
- базовые принципы инфраструктуры с открытым ключом (PKI) и инфраструктуры управления привилегиями (PMI), как определено в Рекомендации МСЭ-Т X.509.

Этот раздел начинается с обсуждения важности защиты самого каталога и необходимости защиты информации каталога. Затем рассматривается роль каталога в поддержании надежной аутентификации, инфраструктуры открытых ключей, управления определением идентичности и телебиометрии.

6.1 Защита информации каталога

6.1.1 Цели защиты каталога

Защита информации каталога – это главным образом вопрос секретности, т. е. защиты от несанкционированного раскрытия важных персональных данных, но она также включает обеспечение целостности данных и защиту активов, представляемых этими данными.

Каталог содержит информацию об объектах. Информация об объекте может быть важной и ее следует раскрывать только тем, кто имеет и *право* и *необходимость* знать.

Существуют три аспекта защиты информации:

- аутентификация пользователя, запрашивающего доступ к информации;
- управление доступом для защиты данных от несанкционированного доступа (ПРИМЕЧАНИЕ. – Управление доступом зависит от надлежащей аутентификации); и
- защита персональных данных, которая зависит от надлежащего управления доступом.

Функции по защите информации всегда были важнейшей частью Рекомендации МСЭ-Т X.500, которая является единственной спецификацией каталога, имеющей эти важные функции.

6.1.2 Аутентификация пользователей каталога

Каталог, соответствующий МСЭ-Т X.500, может допускать анонимный доступ к некоторой неконфиденциальной информации. Однако для получения доступа к более важным данным требуется некоторый уровень аутентификации пользователей. Рекомендация МСЭ-Т X.500 предлагает четыре уровня аутентификации, включающие:

a) только имя;

b) имя плюс незащищенный пароль, т. е. имя и пароль, который передается по соединительной схеме в виде открытого текста (который при использовании стека TCP/IP может быть зашифрован посредством TLS). Стратегия применения паролей предлагает механизмы по обеспечению того, чтобы пользователи периодически меняли свои пароли и чтобы пароли удовлетворяли требованиям качества и не могли повторно использоваться до некоторого установленного периода времени. Пользователь может быть также заблокирован после определенного количества неудачных попыток аутентификации;

c) имя и защищенный пароль, т. е. пароль, который хэшируется с какой-либо дополнительной информацией для гарантии того, что будет обнаружена любая попытка получить доступ к каталогу путем воспроизведения хэшированного значения; и

d) надежная аутентификация, при которой отправитель подписывает определенную информацию при помощи цифровой подписи. Подписанная информация включает в себя имя получателя и некоторую дополнительную информацию, которая также позволяет обнаруживать попытки повторного использования.

Для разного типа пользователей, имеющих доступ, требуются различные уровни защиты данных. Уровень аутентификации пользователя также влияет на права доступа для этого пользователя.

6.1.3 Управление доступом к каталогу

Управление доступом используется для разрешения или отказа в выполнении операций над элементами информации каталога. Рекомендация МСЭ-Т X.500 очень гибкая в том смысле, что показывает, как может подразделяться информация каталога и пользователи для целей управления доступом. Элемент информации, который должен быть защищен, называется защищаемым элементом. Защищаемые элементы можно сгруппировать по общим свойствам управления доступом. Пользователи также могут быть сгруппированы в соответствии с тем, разрешен ли им доступ или нет.

Права доступа пользователя или группы пользователей зависят от уровня аутентификации. Получение важной информации или обновление записей обычно требуют более высокого уровня аутентификации, чем получение менее важной информации.

Управление доступом также учитывает тип доступа к данным, например чтение, добавление, удаление, обновление и изменение названий. В ряде случаев пользователи могут даже не знать о существовании определенных элементов информации.

Управление доступом касается "права знать". Однако "необходимость знать" – это нечто большее, чем просто управление доступом. Обладание *правом знать* не позволяет пользователю получить информацию, если не установлена *необходимость знать*. В этом случае раскрытие информации может стать нарушением секретности.

Имеется еще несколько примеров, когда *права знать* недостаточно. Например:

– даже если у пользователя есть право получить конкретные почтовые адреса некоторых объектов, разрешить ему получение большого количества почтовых адресов может быть неправильным решением; и

– если у пользователя есть права доступа к некоторой информации, это может не относиться к конкретному приложению, для которого выполняется получение информации, в этом случае необходимость знать отсутствует, и информацию раскрывать не следует.

6.1.4 Защита персональных данных

Защита персональных данных в соответствии с Рекомендацией МСЭ-Т X.500 является уникальной и очень мощной. Защита персональных данных потенциально связана с риском, когда пользователь осуществляет поиск по каталогу, указывая общие критерии поиска, по которым может быть выдан огромный объем информации. (Такой поиск иногда называют *прочесыванием данных*.)

В Рекомендации МСЭ-Т X.500 приведена созданная в виде таблиц концепция административного управления услугой, которая помимо управления общими услугами, обеспечивает также выполнение функции защиты персональных данных. Администратор создает одну или несколько таблиц для каждой комбинации типа услуги и группы пользователей. Для того чтобы получение данных было выполнено успешно, необходимо иметь таблицу, которая точно бы совпадала с типом услуги и типом группы пользователей. Однако этого недостаточно. Эта таблица защищена управлением доступом, т. е. пользователь также должен иметь разрешение для доступа к соответствующей таблице.

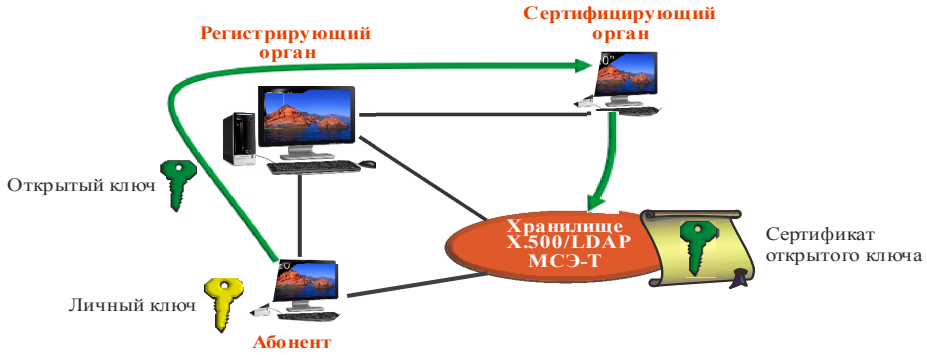
Таблица, которая также называется правилом поиска, может содержать такую информацию, как:

- требуемые критерии поиска для обеспечения того, чтобы поиск был направлен на получение информации об одном объекте или малом их числе. Это не даст возможности тому, кто ищет, запрашивать огромные массивы информации и предотвратит ее прочесывание;
- список элементов информации, относящихся к данному типу услуги; и
- управляющую информацию по отдельным объектам, представленным в каталоге. Используемая таблица взаимодействует с управляющей информацией объекта с целью ограничения объема информации, предоставляемой для этого объекта. Это позволяет отрегулировать данные по критериям защиты персональных данных для каждого отдельного объекта. Объект может иметь особые требования, например не раскрывать почтовый адрес и, по возможности, предоставлять фальшивый адрес. Другие объекты могут не желать сообщать свои электронные адреса некоторым группам пользователей.

Защита важной персональной информации представляет интерес по множеству причин. Некоторые стандарты безопасности, в частности те, что относятся к аутентификации физических лиц и управлению идентичностью, предусматривают сбор и хранение важной информации для персональной идентификации. Все большее число стран законодательно вводят требования, относящиеся к сбору и использованию такой информации. Услуги и механизмы обеспечения безопасности, многие из которых основаны на стандартах МСЭ-Т, служат механизмом для защиты информация, которая является чувствительной с точки зрения секретности. Секретность рассматривается во множестве Рекомендаций, ряд из которых непосредственно рассматривает влияние определенных технологий на секретность. Среди примеров – Рекомендация МСЭ-Т X.1171, которая более подробно рассматривается в разделе 10.5, касающемся услуг на основе маркеров, и руководство по защите информации для персональной идентификации в приложении RFID, которое в настоящее время разрабатывается в ИК17 в качества части работы IDM (см. раздел 6.4).

6.2 Надежная аутентификация: механизмы обеспечения безопасности с открытым ключом

Инфраструктура с открытым ключом (PKI) упрощает управление открытым ключом для предоставления услуг аутентификации, шифрования, целостности и неотказуемости. Фундаментальной технологией для PKI является шифрование с открытым ключом, которое описано ниже. Рекомендация МСЭ-Т X.509 является стандартом PKI для надежной аутентификации, основанной на сертификатах открытого ключа и органах по сертификации. В дополнение к определению структуры аутентификации для PKI Рекомендация МСЭ-Т X.509 также описывает инфраструктуру управления привилегиями (PMI), которая используется для проверки прав и привилегий пользователей в контексте надежной авторизации, основанной на сертификатах атрибутов и органах по присвоению атрибутов. Компоненты PKI и PMI показаны на рисунке 9.



a) Компоненты инфраструктуры с открытым ключом

b) Компоненты инфраструктуры управления привилегиями

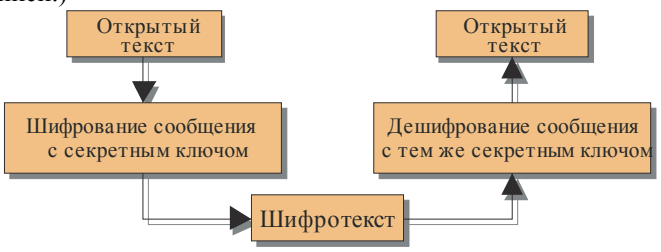
Рисунок 9 – Компоненты PKI и PMI:

6.2.1 Шифрование с секретным и с открытым ключом

Симметричным шифрованием (или шифрованием *с секретным ключом*) называется криптографическая система, в которой один и тот же ключ используется и для шифрования, и для дешифрования, как показано на рисунке 10 *a)*. В симметричной криптосистеме стороны, между которыми устанавливается связь, используют уникальный секретный ключ. Этот ключ должен быть передан участникам с обеспечением секретности, так как знание ключа шифрования означает знание ключа дешифрования, и наоборот.

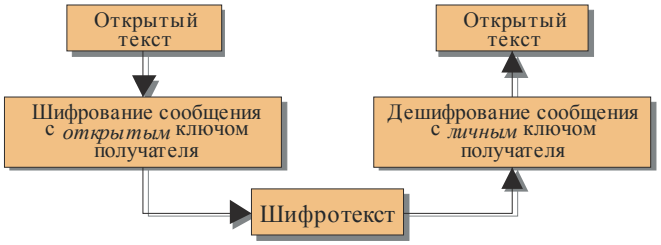
Асимметричное шифрование (или шифрование *с открытым ключом*) использует пару ключей – открытый ключ и секретный ключ, как показано на рисунке 10 *b)*. Открытые ключи могут широко распространяться, но секретные ключи должны всегда храниться в секрете. Секретный ключ обычно содержится в смарт-карте или маркере. Открытый ключ генерируется из секретного ключа и, хотя эти ключи математически связаны, не

существует выполнимого способа, для того чтобы обратным процессом получить секретный ключ из открытого ключа. Для безопасной передачи кому-либо секретных данных с использованием шифрования с открытым ключом отправитель шифрует данные при помощи открытого ключа получателя. Получатель дешифрует его при помощи своего соответствующего секретного ключа. Шифрование с открытым ключом может использоваться также для применения к данным цифровой подписи для обеспечения подтверждения того, что документ или сообщение было создано именно тем человеком, который заявляет, что он отправитель (или автор). Цифровая подпись на самом деле "выжимка" из данных, созданная с использованием секретного ключа автора и присоединенная к документу или сообщению. Получатель использует открытый ключ отправителя для проверки достоверности цифровой подписи. (ПРИМЕЧАНИЕ. – Некоторые системы с открытым ключом используют две разных пары секретных/открытых ключей – одну для шифрования/дешифрования, другую – для проверки/цифровой подписи.)



– Обе стороны пользуются единым секретным ключом.
– Проблема: сложно обеспечить обмен ключами при полной секретности, и такой обмен невозможно масштабировать, т. е. осуществить для большого числа пользователей.
– Наилучший пример : DES (стандарт шифрования данных .)

***a)* шифрование с симметричным (или секретным) ключом**



– Каждый участник имеет:
  – личный ключ, которым не владеет никто другой; и
  – открытый ключ, известный всем.
– Проблема – медленнее, чем шифрование секретным ключом.
– Наилучший пример: RSA.

***b*) шифрование с асимметричным (или открытым) ключом**

SecMan(11)_F10

Рисунок 10 – Иллюстрация процессов шифрования с секретным и открытым ключом:

При симметричном шифровании каждая пара пользователей должна иметь различные ключи и их необходимо распространять и сохранять в секрете. С другой стороны, при асимметричном шифровании, открытые ключи шифрования могут быть опубликованы в каталоге, и любой может использовать один и тот же (открытый) ключ шифрования для безопасной передачи данных конкретному пользователю. Это делает асимметричное шифрование намного более гибким, чем симметричное шифрование. Однако асимметричное шифрование требует больших затрат, в том что касается времени вычислений, поэтому при помощи асимметричного шифрования неэффективно шифровать целые сообщения. На практике асимметричное шифрование обычно используется для безопасного распределения симметричных ключей шифрования. Эти симметричные ключи затем используются для шифрования текста сообщения с применением симметричного алгоритма, который более эффективен в плане использования вычислительной техники. Если требуется цифровая подпись,

создается выжимка (или хэш) сообщения с использованием безопасной односторонней хэш-функции (например, SHA-1 или MD5). Затем этот хэш шифруется (с применением секретного ключа отправителя) и присоединяется к сообщению. Получатель может проверить достоверность цифровой подписи, дешифровав цифровую подпись с открытым ключом отправителя для получения хэша, созданного отправителем, и затем создав свой собственный хэш принятого сообщения. Если подпись достоверная, то оба хэша должны быть идентичными.

Вне зависимости от того, используется ли симметричное или асимметричное шифрование, невозможно направить сообщения получателям, если зашифровано все сообщение целиком (включая заголовки), так как промежуточные узлы не смогут определить адрес получателя. Следовательно, заголовки сообщения должны оставаться незашифрованными.

Безопасная работа системы с открытым ключом существенно зависит от достоверности открытых ключей. Обычно открытые ключи публикуются в виде цифровых сертификатов, которые хранятся в каталоге МСЭ-Т X.500. Сертификат содержит не только открытый ключ шифрования и, при необходимости ключ проверки подписи для физического лица, но еще и дополнительную информацию, включая достоверность сертификата. Сертификаты, которые были отозваны по какой-либо причине, также обычно перечислены в каталоге в списке отозванных сертификатов (CRL). Прежде чем использовать открытые ключи, их достоверность, как правило, проверяют по списку CRL.

6.2.2 Сертификаты открытого ключа

Сертификат открытого ключа (иногда называемый "цифровой сертификат") является одним из средств проверки подлинности владельца асимметричной пары ключей. Сертификат открытого ключа жестко связывает открытый ключ с именем его владельца, и пользующееся доверием учреждение, удостоверяющее эту связь, скрепляет ее цифровой подписью. Указанным пользующимся доверием учреждением является сертифицирующий орган (CA). Признанный на международном уровне стандартный формат сертификатов открытого ключа определен в Рекомендации МСЭ-Т X.509. Сертификат открытого ключа МСЭ-Т X.509 состоит из открытого ключа, идентификатора асимметричного алгоритма, с которым должен использоваться этот ключ, имени владельца пары ключей, наименования CA, удостоверившего права владения, серийного номера и срока действия сертификата, номера версии МСЭ-Т X.509, которой соответствует данный сертификат, и не имеющего обязательного характера набора полей расширения, в которых хранится информация о стратегии сертификации указанного CA. Сертификат целиком сопровождается цифровой подписью, для которой используется личный ключ CA. Сертификат МСЭ-Т X.509 может быть опубликован без ограничений, например на веб-сайте, в каталоге или в V-карте[1], присоединяемой к сообщениям электронной почты. Подпись CA гарантирует, что содержание сертификата не может быть изменено без обнаружения.

Для того чтобы дать пользователю возможность подтверждения подлинности сертификата, необходимо иметь доступ к действительному открытому ключу того CA, который выдал сертификат, с целью проверки подписи CA на сертификате. Так как открытый ключ CA может быть сертифицирован другим (вышестоящим) CA, подлинность открытых ключей может подтверждаться цепочкой сертификатов и CA. В итоге эта цепочка должна иметь некую конечную точку, где, как правило, находится сертификат CA, являющийся "корнем доверия". Открытые ключи корневого CA распространяются как подписанные им самим сертификаты (в которых корневой CA удостоверяет, что данный ключ является его собственным открытым ключом). Эта подпись позволяет убедиться в том, что ключ и наименование CA не подделывались с момента создания сертификата. Однако мы не можем безоговорочно принять наименование CA, заключенное в подписанном им самим сертификате, поскольку CA сам вставил наименование в сертификат. Таким образом, одним из

[1] V-карта является электронной карточкой стандартного формата, которыми часто обмениваются по электронной почте.

важнейших компонентов инфраструктуры открытого ключа является метод безопасного распространения открытых ключей для корневых СА, который гарантирует действительную принадлежность открытого ключа корневому СА, наименование которого указано в подписанном им самим сертификате. Без этого нельзя быть уверенным в том, что некто не маскируется под корневой СА.

6.2.3 Инфраструктуры открытых ключей

Основным назначением инфраструктуры открытых ключей является выдача сертификатов открытых ключей и управление ими, включая сертификаты корневого СА. Управление ключами включает создание пар ключей, создание сертификатов открытых ключей, аннулирование сертификатов открытых ключей (например, если личный ключ пользователя подвергся опасности), хранение и архивирование ключей и сертификатов, а также их уничтожение по истечении срока службы. Каждый СА функционирует в соответствии с набором стратегических процедур. В Рекомендации МСЭ-Т X.509 предусмотрены механизмы для распространения некоторой части информации об этой стратегии в полях расширения сертификатов МСЭ-Т X.509, выданных данным СА. Стратегические правила и процедуры, которым следует СА, обычно определяются в стратегии применения сертификатов (CP) и в заявлении о практике применения сертификатов (CPS), публикуемых этим СА. Указанные документы способствуют обеспечению общей основы для оценки того, насколько можно доверять сертификатам открытых ключей, выданным этим СА, как на международном уровне, так и на уровне секторов. Эти документы также обеспечивают правовую основу, необходимую для укрепления доверия между учреждениями, а также для определения ограничений на использование выданных сертификатов.

В ранних версиях Рекомендации МСЭ-Т X.509 (1988, 1993 и 1997 гг.) указаны основные элементы, необходимые для инфраструктуры открытых ключей, включая определение сертификатов открытого ключа. Пересмотренная Рекомендация МСЭ-Т X.509, утвержденная в 2001 году (и обновленная в 2005 и 2008 гг.), содержит существенно расширенные характеристики сертификатов атрибута и основу для инфраструктуры управления привилегиями (PMI).

6.2.4 Инфраструктура управления привилегиями

Инфраструктура управления привилегиями (PMI) управляет привилегиями в целях содействия всеобъемлющей службе авторизации с PKI. Описанные механизмы позволяют осуществлять установку привилегий пользователя в отношении доступа в среде, объединяющей оборудование различных производителей и многочисленные приложения. Концепции PMI и PKI весьма сходны, но PMI относится к авторизации, а область действия PKI – аутентификация. В таблице 5 показано сходство двух инфраструктур.

Таблица 5 – Сравнение параметров инфраструктуры управления привилегиями и инфраструктуры открытого ключа

Инфраструктура управления привилегиями	Инфраструктура открытого ключа
Источник полномочий (SoA)	Корневой сертифицирующий орган (исходная точка доверия)
Орган по присвоению атрибутов	Сертифицирующий орган
Сертификат атрибута	Сертификат открытого ключа
Список аннулирования сертификатов атрибута	Список аннулирования сертификатов
Список аннулирования полномочий для PMI	Список аннулирования полномочий для PKI

Цель присвоения пользователям привилегий заключается в том, чтобы обеспечить выполнение ими предписанной стратегии безопасности, которую установил источник полномочий. Информация, касающаяся стратегии, увязывается с именем пользователя в сертификате атрибута и состоит из ряда элементов, показанных в таблице 6.

Таблица 6 – Структура сертификатов атрибутов согласно Рекомендации МСЭ-Т X.509

Версия
Держатель
Выдавший орган
Подпись (ID алгоритма)
Серийный номер сертификата
Срок действия
Атрибуты
Уникальный ID выдавшего органа
Расширения

Сертификаты атрибутов также применяются в телебиометрии (см. раздел 6.5) для создания биометрических сертификатов для увязки пользователя с его/ее биометрической информацией. Сертификаты биометрических устройств определяют возможности и ограничения биометрических устройств. Сертификаты биометрических правил определяют взаимосвязь между уровнем безопасности и параметрами биометрических алгоритмов.

В Рекомендации МСЭ-Т X.509 описаны пять компонентов для управления PMI: заявитель привилегий, верификатор привилегий, объектный метод, политика привилегий и переменные среды (см. рисунок 11). Верификатор привилегий может управлять доступом к объектному методу с помощью заявителя привилегий в соответствии с политикой привилегий.

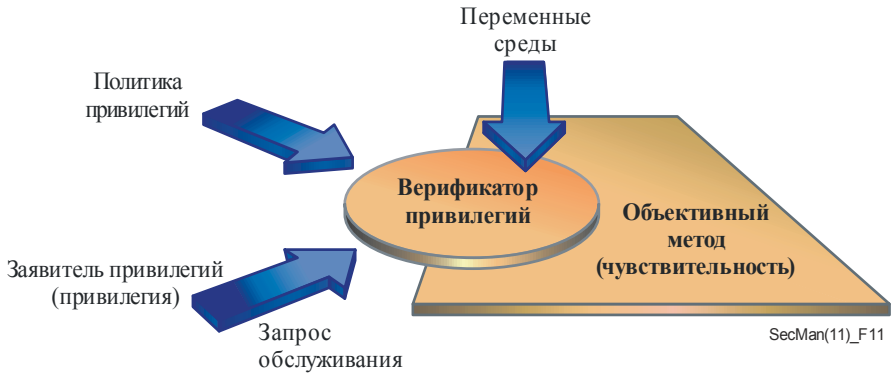


Рисунок 11 – Модель управления PMI согласно Рекомендации МСЭ-Т X.509

Если для какого-либо варианта реализации требуется делегирование привилегий, в Рекомендации МСЭ-Т X.509 рассмотрены четыре компонента модели делегирования для PMI: верификатор привилегий, источник полномочий, другие органы по присвоению атрибутов и заявитель привилегий (см. рисунок 12).

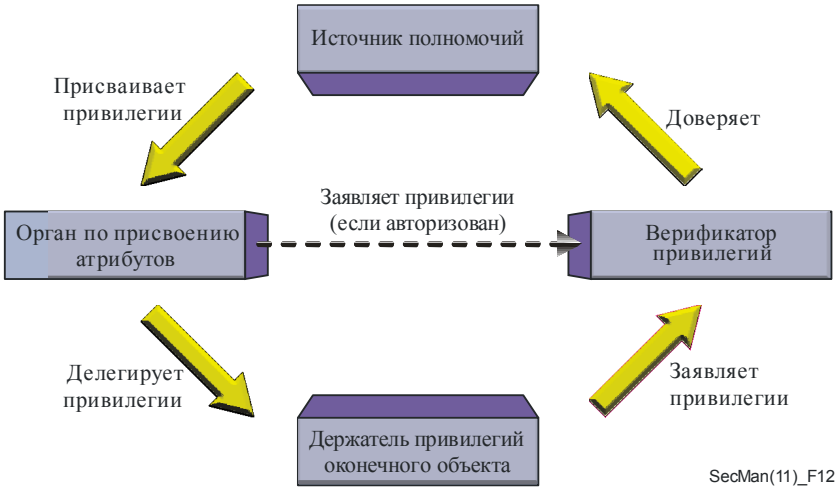


Рисунок 12 – Модель делегирования для PMI согласно Рекомендации МСЭ-Т X.509

В последних реализациях схем авторизации, которые соответствуют модели управления доступом по ролевому признаку (RBAC), предполагается, что конкретному пользователю присваивается некая роль. Стратегия авторизации связывает набор разрешений и роль. При доступе к ресурсу роль, которая присвоена пользователю, сверяется с правилами стратегии для получения разрешения на выполнение каких-либо последующих действий.

6.3 Руководящие указания по аутентификации

Для работы с некоторыми аспектами аутентификации было разработано несколько руководящих указаний. Они описаны ниже.

6.3.1 Протокол аутентификации на базе секретного пароля с обменом ключами

Протокол аутентификации на базе секретного пароля с обменом ключами (SPAK) является простым протоколом аутентификации, в котором применение запоминаемого человеком пароля между клиентом и сервером приводит к взаимной аутентификации и секрету группы лиц, который может использоваться в качестве ключей для следующего сеанса.

В Рекомендации МСЭ-Т X.1151 указаны требования для протокола SPAK наряду с руководящими указаниями по выбору наиболее подходящих протоколов SPAK из различных протоколов аутентификации с безопасным паролем. Этот протокол очень прост. Его легко реализовать и использовать и для него, в отличие от PKI, не требуется никакой другой инфраструктуры. Ожидается, что в будущем он будет более широко использоваться для многих приложений. SPAK обеспечивает как аутентификацию пользователя, так и надежный обмен ключами с простым паролем, так что последующий сеанс связи может иметь защиту при помощи секрета, которым владеет группа лиц во время процедуры аутентификации (см. рисунок 13).

Рисунок 13 – Типовая работа протокола SPAK

6.3.2 Расширяемый протокол аутентификации

Расширяемый протокол аутентификации (EAP) поддерживает в сети передачи данных множество механизмов аутентификации между запрашивающим устройством и сервером аутентификации. EAP может использоваться как основной инструмент, позволяющий провести аутентификацию пользователя и распределяющий сеансовые ключи. Он может осуществлять аутентификацию устройств для создания безопасного соединения между оконечными пунктами и предотвращения доступа для неавторизованного устройства.

В Рекомендации МСЭ-Т X.1034 описывается структура для аутентификации на основе EAP и управление ключами для защиты нижних уровней в сети связи. Она содержит руководящие указания для выбора методов EAP и описывает механизм управления ключами для нижних уровней сети передачи данных. Эта инфраструктура применима как к беспроводным сетям доступа, так и к проводным сетям доступа с совместно используемой средой передачи.

Для аутентификации и управления ключами необходимы три объекта: запрашивающий объект (или равноправный объект), аутентификатор и сервер аутентификации, как показано на рисунке 14. Запрашивающий объект действует в качестве конечного пользователя, входя в сеть со станции конечного пользователя. Аутентификатор действует в качестве точки обязательного выполнения стратегических решений, распределяя сообщения EAP между запрашивающим объектом и сервером аутентификации. Сервер аутентификации аутентифицирует запрашивающий объект и, возможно, использует на совместной основе секретную информацию, которая может использоваться для создания ключей шифрования, отправляет результаты аутентификации конечного пользователя аутентификатору и переправляет секрет группы лиц аутентификатору. Эта секретная информация группы лиц может использоваться для создания ключей шифрования между аутентифактором и запрашивающим объектом для гарантий конфиденциальности и целостности и возможности аутентификации сообщений.

Процесс аутентификации и управления ключами в целом состоит из четырех рабочих этапов: обнаружение возможностей обеспечения безопасности, аутентификация EAP, распределение ключей и управление ключами (см. рисунок 15). На этапе возможностей обеспечения безопасности запрашивающий объект согласует возможности обеспечения безопасности с различными параметрами протокола, который должен использоваться с аутентификатором. На этапе EAP сервер аутентификации аутентифицирует запрашивающий объект и выводит главные секретные данные, используемые совместно с запрашивающим объектом. На этапе распределения ключей сервер аутентификации передает основную секретную информацию аутентификатору, с тем чтобы позволить во время аутентификации создание разных ключей шифрования для последующего сеанса связи между запрашивающим объектом и аутентификатором (в каждом сеансе связи должны использоваться

новые ключи шифрования). Наконец, на этапе управления ключами аутентификатор обменивается случайными числами с запрашивающим объектом для получения нового ключа шифрования, что обеспечивает безупречную упреждающую секретность.

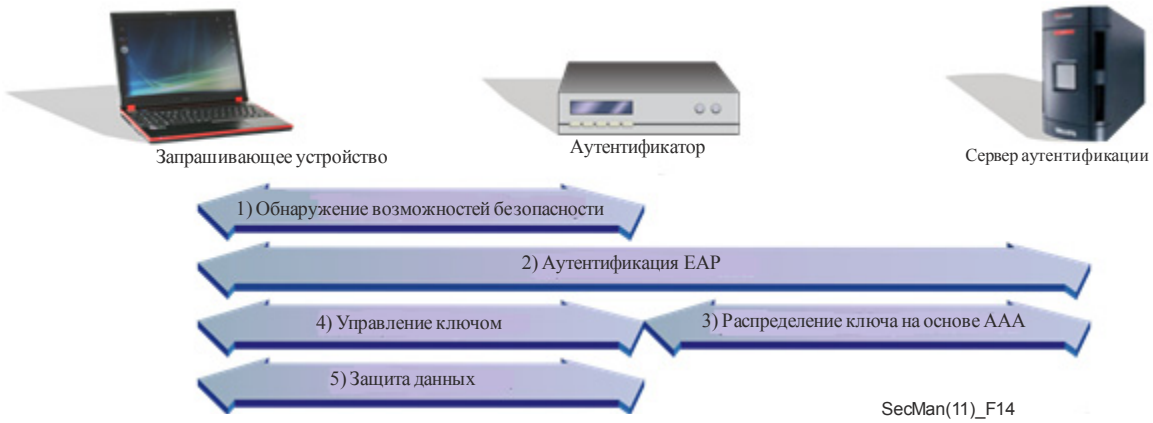


Рисунок 14 – Четыре рабочих этапа для аутентификации и управления ключами на нижнем уровне

6.3.3 Аутентификация одноразового пароля

Применение одноразового пароля (OTP) повышает уровень безопасности, предотвращая риск возможного угадывания и повторного использования пароля. Аутентификация на основе OTP может использоваться наряду с другими механизмами аутентификации (например, PKI, статический пароль) для поддержки многофакторной аутентификации. В Рекомендации МСЭ-Т X.1153 определяется структура управления для аутентификации на основе одноразового пароля и предлагается совместимая структура управления, позволяющая совместно использовать единый одноразовый парольный маркер между различными поставщиками услуг.

6.4 Управление определением идентичности

6.4.1 Обзор управления определением идентичности

Управление определением идентичности (IdM) представляет собой процесс безопасного управления и контроля информации об идентичности (например, полномочиями, идентификаторами, атрибутами и репутацией), который используется для представления объектов (например, поставщиков услуг, организаций конечного пользователя, людей, сетевых устройств, приложений программного обеспечения и услуг) в процессе связи. Один объект может иметь несколько цифровых идентичностей, с тем чтобы иметь доступ к различных услугам с разными требованиями, и они могут существовать во многих местах. IdM поддерживает аутентификацию объекта. Для целей МСЭ-Т идентичность, заявленная объектом, отражает уникальность этого объекта в определенном контексте.

Процесс IdM является ключевым компонентом кибербезопасности, так как он включает возможность создания и поддержки заслуживающих доверия сеансов связи между объектами и позволяет иметь кочевой доступ по запросу к сетям и электронным услугам. Также он позволяет проводить авторизацию ряда привилегий (вместо привилегий "все или ничего") и упрощает процесс изменения привилегий в случае изменения роли объекта. IdM улучшает способность организации применять ее стратегии безопасности, так как позволяет контролировать и проверять действия объекта в сети, и может также облегчать доступ к объектам как внутри, так и вне организации.

IdM обеспечивает достоверность информации об идентичности таким образом, что это поддерживает безопасное, заслуживающее доверия управление доступом. Эта возможность достигается за счет единой регистрации/единого выхода из всей сети путем однократного ввода пароля, контроля пользователем информации, подлежащей личной идентификации, и возможности выбора пользователем поставщика идентичности, который может предложить функции подтверждения и делегирования функций от его имени, в отличие от предоставления полномочий каждому поставщику услуг. IdM также поддерживает множество услуг на основе идентичности, включая целевую рекламу, персонализированные услуги на основе географического местоположения и интереса и аутентифицированные услуги для уменьшения случаев мошенничества и кражи идентичности.

IdM является комплексной технологией, включающей:

- создание, изменение, приостановку, архивацию и уничтожение информации об идентичности;
- распознавание отдельных видов идентичности, которые представляют объекты в определенном контексте или роли;
- создание и оценка доверия между объектами; и
- определение местонахождения информации об идентичности объекта (например, посредством авторитетного поставщика идентичности, который является юридически ответственным за поддержку идентификаторов, полномочий и некоторых или всех атрибутов объекта).

В Дополнении 7 к подсерии Рекомендаций МСЭ-Т серии X представлено краткое введение в вопрос управления определением идентичности.

6.4.2 Работы МСЭ-Т по управлению определением идентичности

Работа по IdM сконцентрирована в основном в двух Исследовательских комиссиях, как это описывается ниже.

17-я Исследовательская комиссия, ведущая ИК по IdM, отвечает за проведение исследований, относящихся к созданию общей модели управления определением идентичности, которая не зависит от сетевых технологий и помогает осуществлять между объектами безопасный обмен информацией об идентичности. Эта работа также включает: исследование процесса обнаружения авторитетных источников информации об идентичности; общие механизмы запараллеливания/взаимодействия различных наборов форматов информации об идентичности; угрозы управления определением идентичности и механизмы противостояния им; защиту информации, подлежащей личной идентификации (PII); и создание механизмов, гарантирующих, что доступ к PII разрешен, только когда это уместно. Утвержденные к настоящему времени Рекомендации по управлению определением идентичности включают Рекомендации МСЭ-Т X.1250, МСЭ-Т X.1251, МСЭ-Т X.1253 и ITU-T X.1275. Кроме того, в Рекомендации МСЭ-Т X.1252 *Базовые термины и определения в области управления определением идентичности* приводится набор связанных с IdM определений, с тем чтобы помочь гарантировать единообразную и согласующуюся терминологию в стандартах IdM МСЭ-Т. Близятся к завершению работы по расширенной структуре подтверждения подлинности сертификатов и по созданию совместной структуры ИСО/МСЭ-Т для обеспечения достоверности при аутентификации объекта.

13-я Исследовательская комиссия (Будущие сети, включая сети подвижной связи и СПП) отвечает за особую для СПП функциональную архитектуру IdM, которая поддерживает услуги идентичности добавленной стоимости, безопасный обмен информацией об идентичности и применение запараллеливания/взаимодействия между различными наборами форматов информации об идентичности. ИК13 также отвечает за идентификацию любых угроз управлению определением идентичности в пределах СПП и механизмы противостояния им. В Рекомендации МСЭ-Т Y.2720 описывается структурный подход к разработке, определению и реализации решений IdM и облегчению взаимодействия в гетерогенных условиях. ИК13 разработала две дополнительные Рекомендации по вопросам IdM – Рекомендацию МСЭ-Т Y.2721, в которой описываются задачи и требования к

IdM, а также приводится анализ примеров случаев применения, и Рекомендацию МСЭ-Т Y.2722, в которой определяются механизмы, которые могут использоваться для удовлетворения требований, связанных с IdM, и потребностей, обусловленных развертыванием СПП.

С 2007 года начала работу Совместная группа по координации деятельности для управления определением идентичности (JCA-IdM). Цель Группы JCA-IdM – координировать работу по вопросам IdM в рамках МСЭ-Т и с внешними организациями. JCA создала веб-страницу информационного ресурса по IdM, на которой указываются документы МСЭ-Т и других организаций по разработке стандартов, относящиеся к управлению определением идентичности и сгруппированные по категориям, организациям и статусу их работы. На веб-странице ведущей Исследовательской комиссии по IdM представлена расширенная информация по деятельности IdM, утвержденным и разрабатываемым Рекомендациям IdM, а также другая информация, связанная с работой по тематике IdM. Эта "панорама" деятельности по вопросам IdM доступна по адресу: http://groups.itu.int/itu-t/StudyGroups/SG17/IdmRoadmap.aspx.

6.5 Телебиометрия

Телебиометрия занимается персональной идентификацией и аутентификацией с использованием биометрических устройств в области электросвязи. В частности, она занимается тем, как можно улучшить идентификацию и аутентификацию пользователей при помощи безопасных и защищенных телебиометрических методов. Работа МСЭ-Т по этому вопросу велась в тесном сотрудничестве с другими организациями по разработке стандартов и охватывает вопросы, включающие: взаимодействие человека и окружающей среды; биометрические цифровые ключи; биометрические расширения сертификатов МСЭ-Т X.509; и биометрическую аутентификацию в открытой сети.

6.5.1 Телебиометрическая аутентификация

Биометрия может поддерживать услуги аутентификации с высокой степенью защиты, но стандартизация биометрической аутентификации в открытой сети сталкивается с рядом проблем:

- у поставщиков услуг может не быть никакой информации, относящейся к тому, какие биометрические устройства используются в среде конечного пользователя, об уровне/настройке безопасности таких устройств или как они работают;
- у разных биометрических продуктов различается точность (определяемая коэффициентом ложной идентификации или отказов в доступе законному пользователю). Поэтому поставщик услуг не может требовать поддержания единообразного уровня точности; и
- точность биометрического подтверждения может ухудшаться как из-за факторов окружающей среды (например, освещенность и погодные условия), так и из-за человеческих факторов (поза, косметика, характеристики глазного хрусталика и старение).

Общие протоколы и профили биометрической аутентификации для систем электросвязи в открытых сетях определены в Рекомендации МСЭ-Т X.1084.

На рисунке 15 показана аутентификация конечного пользователя при помощи открытой сети неличного общения.

Рисунок 15 – Телебиометрическая аутентификация конечного пользователя

6.5.2 Генерация и защита телебиометрического ключа

Структура создания и защиты цифрового биометрического ключа определена в Рекомендации МСЭ-Т X.1088. Эта структура определяет защиту при помощи биометрического шаблона с сертификатом открытого ключа и биометрического сертификата, с тем чтобы обеспечить криптографически безопасную аутентификацию и безопасную связь в открытых сетях. Также определены требования к безопасности для создания и защиты биометрического цифрового ключа. Эта структура может применяться к биометрическому шифрованию и цифровой подписи. Предлагаются два метода:

- генерация биометрического ключа, при которой ключ создается из биометрического шаблона (рисунок 16); и
- привязка/восстановление биометрического ключа, когда ключ хранится в базе данных и может быть извлечен при помощи биометрической аутентификации (рисунок 17).

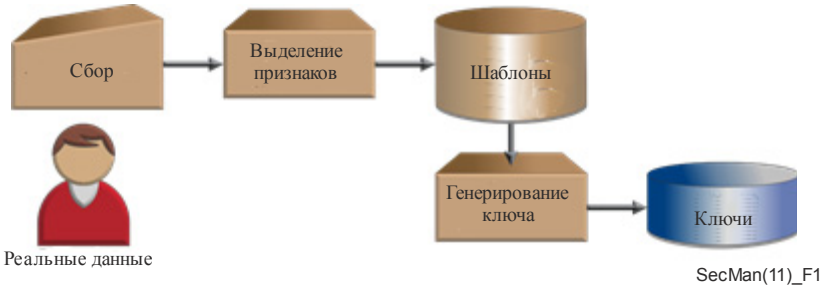


Рисунок 16 – Создание биометрического ключа

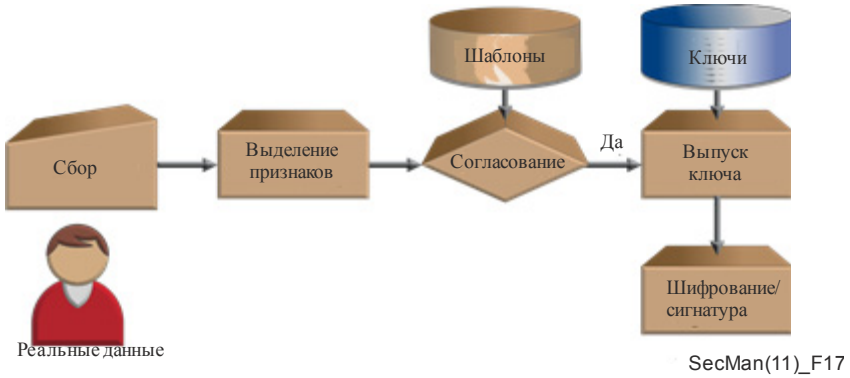


Рисунок 17 – Привязка/восстановление биометрического ключа

6.5.3 Аспекты защиты и безопасности телебиометрии

Структура для аспектов защиты и безопасности телебиометрии определена в многомодальной модели телебиометрии (Рекомендация МСЭ-Т X.1081), где определяется взаимодействие человека и окружающей среды, а также значения и оборудование, которые использовались для измерения этого взаимодействия. Многомодальная модель телебиометрии не ограничивается рассмотрением чистых физических взаимодействий, но еще и узнает поведенческое взаимодействие, не имеющее в настоящее время определения посредством стандартного оборудования.

В Рекомендации МСЭ-Т X.1086 не только определяются уязвимости и угрозы, связанные с работой телебиометрических систем, но также описываются меры противодействия для защиты биометрических устройств на этапах их установки, демонтажа и поставок. Указанные меры противодействия включают схемы технической защиты биометрической системы в рамках эксплуатационных процедур, а также роли и ответственность персонала, наделенного полномочиями по контролю за работой системы.

6.5.4 Телебиометрия, связанная с психологией человека

Аспекты защиты и безопасности телебиометрии также рассмотрены в Рекомендации МСЭ-Т X.1082, где определены значения и оборудование для физиологических, биологических или поведенческих характеристик, которые могут обеспечить входные или выходные данные для систем телебиометрической идентификации или подтверждения (системы распознавания), включая все известные пороги распознавания или безопасности. Она содержит имена, определения и символы для значений и оборудования для телебиометрии, связанной с психологией человека (т. е. характеристики и излучения человека, которые можно определить при помощи датчика). Также она включает значения и оборудование, имеющие отношение к воздействию на человека, вызванному использованием устройств телебиометрии.

6.5.5 Одноразовый телебиометрический шаблон

Применение структуры аутентификации пользователя для биометрических одноразовых шаблонов рассмотрено в Рекомендации МСЭ-Т X.1090. Эта структура обеспечивает безопасные механизмы защиты и аутентификации пользователя для биометрических шаблонов, передаваемых по открытым сетям, посредством генерации нового одноразового шаблона для каждого случая аутентификации.

6.5.6 Другие разработки в сфере стандартов телебиометрии

Для создания биометрических сертификатов были разработаны расширения сертификатов МСЭ-Т X.509, используемых в инфраструктурах открытых ключей или инфраструктурах управления привилегиями. Они указаны в Рекомендации МСЭ-Т X.1089. В Рекомендации МСЭ-Т X.1083 определяется синтаксис (использующий ASN.1), семантика и кодирование сообщений, которые позволяют приложению, совместимому с BioAPI, запросить у биометрических поставщиков услуг, совместимых с BioAPI (BSP), выполнение биометрических операций с пересечением узла или границ обработки, а также позволяет им получить извещение о событиях, происходящих у этих удаленных BSP.

Другой важный аспект этой работы связан с обобщенными протоколами, которые обеспечивают защиту, безопасность, защиту персональных данных и согласие на манипулирование биометрическими данными при любом применении телебиометрии, например электронное здравоохранение, телемедицина и телездравоохранение. В Рекомендации МСЭ-Т X.1080.1 определяется обобщенный протокол электросвязи, поддерживающий взаимодействие между пациентом местного медицинского пункта и удаленным медицинским центром, который может предложить более квалифицированное заключение.

7. Защита сетевой инфраструктуры

7 Защита сетевой инфраструктуры

Данные, используемые для контроля и управления сети электросвязи, часто передаются по отдельной сети, по которой передается только трафик управления сетью (т. е. не трафик пользователей). Такая сеть обычно называется сетью управления электросвязью (СУЭ), которая описана в Рекомендации МСЭ-Т М.3010. Этот трафик обязательно должен быть защищен. Обычно категории трафика управления определяются в зависимости от информации, необходимой для выполнения функций управления обработкой отказов, конфигурацией, характеристиками, функциями расчетов и управления безопасностью. Область управления безопасностью сети охватывает как настройку сети безопасного управления, так и управление безопасностью информации, которая связана с тремя плоскостями архитектуры безопасности МСЭ-Т Х.805.

Действия по управлению, связанные с элементами инфраструктуры сети, всегда должны выполняться в безопасном режиме. Например, любые действия в сети должны осуществляться только авторизованным пользователем. Для обеспечения безопасной структуры между оконечными пунктами все меры безопасности (например, управление доступом, аутентификация) должны применяться к каждому типу выполняемых в сети процессов в отношении инфраструктуры сети, сетевых услуг и сетевых приложений. Существует ряд Рекомендаций МСЭ-Т, специально посвященных аспекту безопасности в плоскости управления для сетевых элементов и систем управления, которые являются частями сетевой инфраструктуры.

Другие приложения управления сетью включают приложения, связанные со средой, в которой должны взаимодействовать различные поставщики услуг, с тем чтобы обеспечивалось сквозное предоставление услуги между оконечными пунктами. Среди примеров таких услуг – средства связи, предоставляемые регламентарным органам или правительственным учреждениям в условиях ликвидации последствий чрезвычайных ситуаций, и ситуации, когда для абонентов, пересекающих географические границы, предоставляются выделенные линии.

7.1 Сеть управления электросвязью (СУЭ)

СУЭ является отдельной сетью, изолированной от инфраструктуры сети общего пользования, поэтому какие-либо перерывы связи, возникающие вследствие угроз безопасности в плоскости конечного пользователя в сети общего пользования, на СУЭ не распространяются. Благодаря такому разделению обеспечить защиту трафика сети управления относительно просто, поскольку доступ к этой плоскости ограничен полномочными администраторами сети, а трафик ограничен разрешенными процессами управления. С появлением сетей последующего поколения трафик приложений конечных пользователей иногда может совмещаться с трафиком управления. Хотя такой подход минимизирует затраты за счет создания только инфраструктуры единой интегрированной сети, он создает множество новых проблем, связанных с обеспечением безопасности. Угрозы в плоскости конечного пользователя становятся при таком подходе угрозами для плоскостей управления и контроля, поскольку плоскость управления становится доступной для огромного числа конечных пользователей, и возникает возможность осуществления множества самых разнообразных злонамеренных действий, которым необходимо противодействовать.

7.2 Архитектура управления сетью

Архитектура для обеспечения сетевого управления сетью электросвязи описана в Рекомендации МСЭ-Т М.3010. На рисунке 18 показана взаимосвязь между СУЭ и сетью электросвязи. Архитектура управления сетью устанавливает интерфейсы, которые определяют процессы обмена, необходимые для выполнения функций эксплуатации, управления, технического обслуживания и предоставления услуг.

ПРИМЕЧАНИЕ. – Граница СУЭ, представленная пунктирной линией, может расширяться и управлять услугами и оборудованием потребителя/пользователя.

Рисунок 18 – Взаимосвязь между СУЭ и сетью электросвязи

В Рекомендации МСЭ-Т M.3016.0 приводятся обзор и структура, которая определяет угрозы безопасности для СУЭ. В рамках Рекомендаций МСЭ-Т серии M.3016 Рекомендация МСЭ-Т M.3016.1 устанавливает конкретные требования, Рекомендация МСЭ-Т M.3016.2 описывает услуги обеспечения безопасности, а Рекомендация МСЭ-Т M.3016.3 определяет механизмы, которые могут противодействовать угрозам в контексте функциональной архитектуры СУЭ, определенной в Рекомендации МСЭ-Т M.3010. Поскольку не все требования нуждаются в поддержке со стороны различных организаций, Рекомендация МСЭ-Т M.3016.4 предусматривает образец для создания профилей, основанных на требованиях, услугах и механизмах обеспечения безопасности. Эта позволяет разрабатывать профили в соответствии со специфической политикой организации в области безопасности.

При анализе управления безопасностью сети следует рассматривать два его аспекта. Первый относится к плоскости управления для сквозных действий пользователя между оконечными точками (например, услуги VoIP), причем административное управление работой пользователей должно быть защищено. Это называется *безопасностью управляющей информации*, которая передается по сети для обеспечения функционирования приложений между оконечными точками. Вторым аспектом является *управление информацией безопасности*, которое применяется независимо от типа приложения. Например, составление донесения о неисправностях между двумя поставщиками услуг должно осуществляться в условиях безопасности. Это может потребовать шифрования передач, в таком случае должны обеспечиваться меры безопасности для управления ключами шифрования.

Для определенной в Рекомендации МСЭ-Т X.805 архитектуры существует несколько рекомендаций, посвященных функциям управления безопасностью для трех уровней плоскости управления (см. рисунок 1). Кроме того, как сказано в последующих подразделах, существуют другие Рекомендации, которые определяют общие или широкоиспользуемые услуги, такие как отчеты об аварийных ситуациях при нарушении безопасности, функции аудита, а также информационные модели, определяющие уровни защиты для различных целей.

7.3 Защита элементов сетевой инфраструктуры

Возможность взаимодействия между оконечными пунктами может рассматриваться в понятиях сетей(и) доступа и базовой(ых) сети(ей). Эти сети могут быть построены с применением различных технологий. Для сетей доступа и базовых сетей разработаны специальные Рекомендации. В качестве примера здесь используется пассивная оптическая сеть для широкополосного доступа. Административное управление привилегиями пользователей для такой сети доступа определяется с применением унифицированной методологии моделирования согласно Рекомендации МСЭ-Т Q.834.3. Обмен управляющей информацией с применением обобщенной архитектуры посредника объектных запросов (CORBA) определяется согласно Рекомендации МСЭ-Т Q.834.4. Описываемый в указанных Рекомендациях интерфейс применяется между системой управления элементами и системой управления сетью. Первая используется для управления отдельными сетевыми элементами и вследствие этого располагает информацией о внутренних параметрах аппаратной и программной архитектуры элементов одного или нескольких поставщиков, вторая же функционирует на сквозном сетевом уровне между оконечными точками и охватывает системы управления разных поставщиков. На рисунке 19 показаны различные объекты, используемые для создания, удаления, распределения и применения информации по управлению доступом для пользователей системы управления элементами. В списке полномочий пользователя каждого авторизованного пользователя содержится перечень разрешенных функций управления. Диспетчер по управлению доступом проверяет идентификатор и пароль пользователя управляющих функций и предоставляет доступ к функциональным возможностям, разрешенным в списке полномочий.

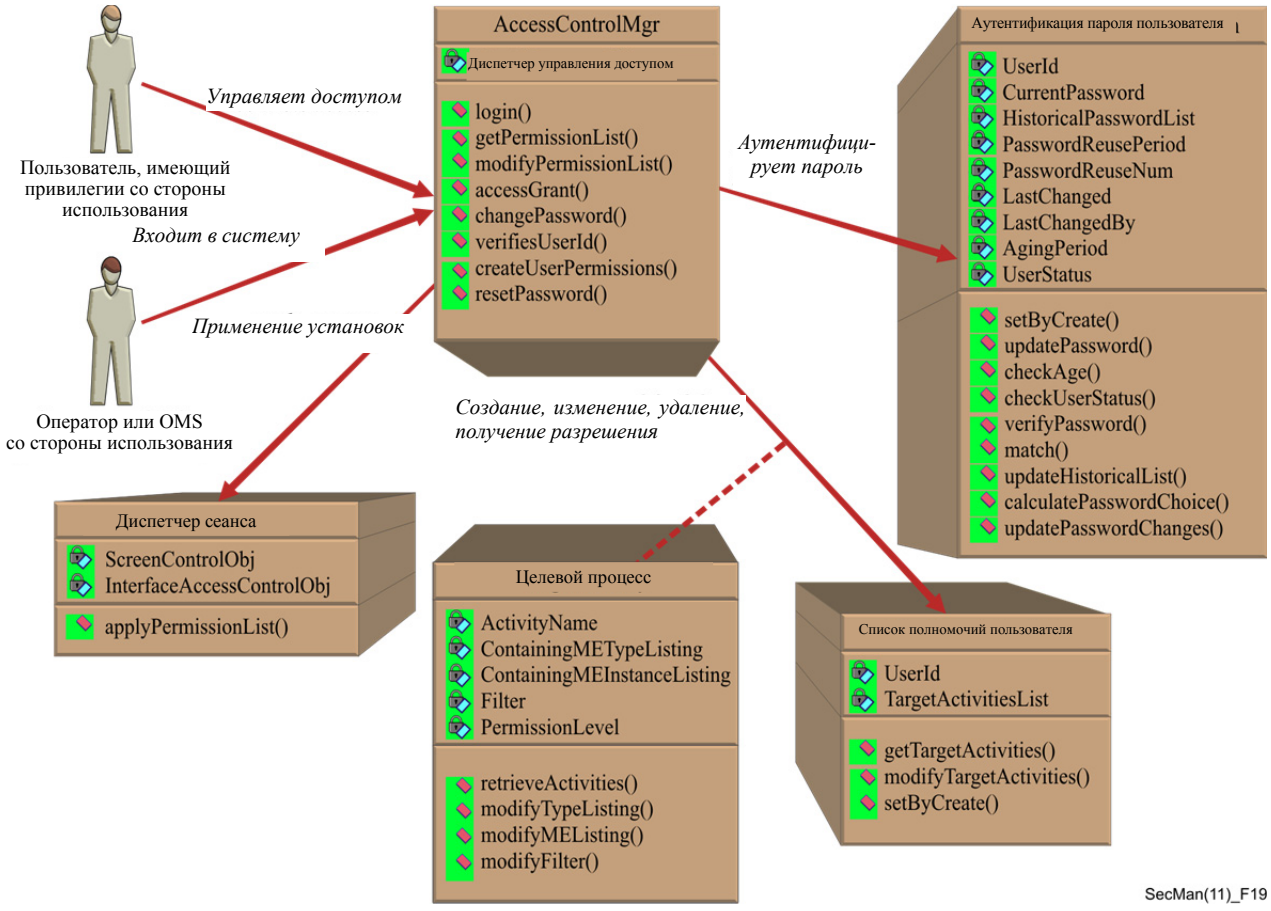


Рисунок 19 – Администрирование привилегий пользователя по МСЭ-Т Q.834.3

7.4 Защита действий по управлению и мониторингу

В пересечении плоскости управления и слоя услуг важны два аспекта безопасности. Один аспект заключается в обеспечении надлежащих мер безопасности для услуг, предоставляемых по данной сети. Примером может служить обеспечение такого положения дел, при котором разрешение на выполнение операций, связанных с инициализацией услуги, имеют только авторизованные пользователи. Вторым аспектом является определение того, какая передача административной информации и управляющей информации является достоверной, с тем чтобы помочь в обнаружении нарушений безопасности.

Рекомендация МСЭ-Т M.3208.2 посвящена первому аспекту – функциям управления услугами. Эта услуга управления соединениями позволяет абоненту создавать/активировать, изменять и удалять выделенные линии связи в пределах заранее предоставленных ресурсов. Учитывая, что пользователь задает параметры соединения между пунктами, необходимо обеспечить, чтобы выполнение таких операций было разрешено только имеющим полномочия пользователям. Параметрами безопасности МСЭ-Т X.805, которые связаны с данной услугой, являются: аутентификация одноранговых объектов; контроль целостности данных (для предотвращения неразрешенного изменения данных в процессе их транзита); и управление доступом (для обеспечения того, чтобы какой-либо абонент не мог получить, злонамеренно или случайно, доступа к данным другого абонента).

Рекомендация МСЭ-Т M.3210.1, которая определяет административные функции, связанные с плоскостью управления для услуг беспроводной связи, является примером стандарта, посвященного второму аспекту. В беспроводной сети пользователи при перемещении из своей домашней сети в посещаемую сеть могут пересекать различные административные домены. В услугах, которые определены в МСЭ-Т M.3210.1, описывается, как домен управления по борьбе с мошенничеством в домашней сети собирает соответствующую информацию об абоненте, зарегистрировавшемся в посещаемой сети. В сценариях *a)* и *b)* на рисунке 20 показано инициирование мониторинга процесса управления домашней сетью или посещаемой сетью. Система обнаружения мошенничества в домашней сети запрашивает информацию о действиях с момента, когда абонент регистрируется в посещаемой сети и остается активным до того момента, когда абонент завершает регистрацию в сети и уходит из нее. Затем можно разработать профили, относящиеся к использованию на основе анализа записей вызовов на уровне услуги или абонента. Система обнаружения мошенничества может проанализировать обнаруженное мошенническое поведение и инициировать соответствующие аварийные сигналы.

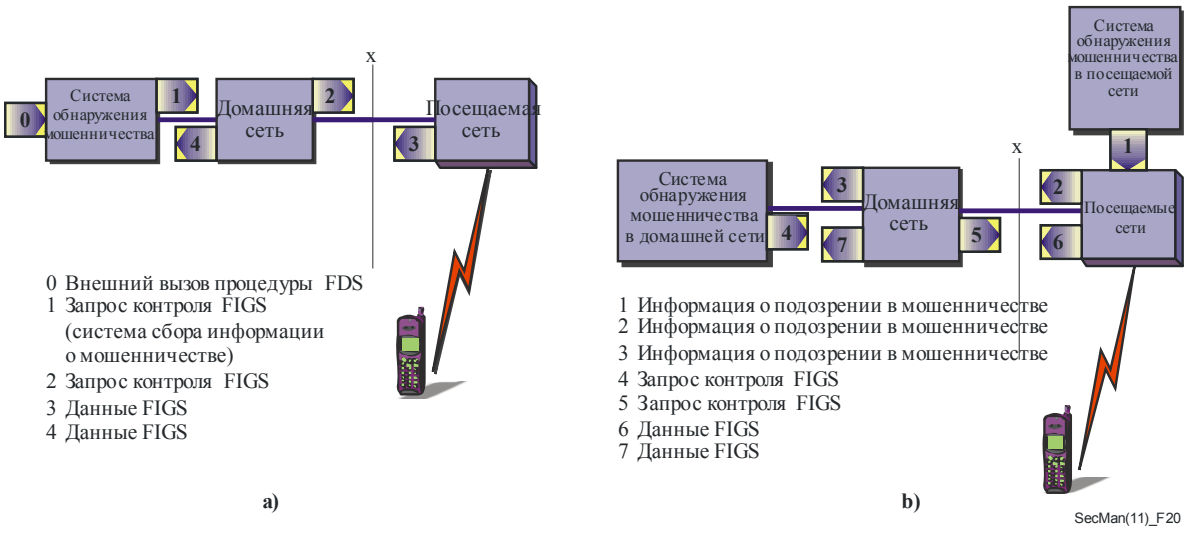


Рисунок 20 – Обнаружение мошенничества для беспроводных служб

7.5 Обеспечение безопасности при эксплуатации сети и защита приложений, связанных с управлением

Пересечение плоскости управления и слоя приложений в МСЭ-Т X.805 связано с обеспечением безопасности сетевых приложений конечного пользователя. Это включает в себя такие приложения, как передача сообщений и работа с директориями. Другой класс приложений, в которых необходимо обеспечивать защиту управляющих процессов, образуют сами приложения управления. Это лучше пояснить на конкретных примерах. Конечным пользователем таких приложений является персонал поставщика услуг, осуществляющий управление (эксплуатацию). Рассмотрим случай, когда один поставщик услуг для предоставления своих услуг по установлению сквозного соединения между оконечными пунктами пользуется услугами предоставления соединения другого поставщика услуг. В зависимости от регуляторной или рыночной среды некоторые поставщики услуг могут предлагать услуги доступа, а другие, называемые *компаниями, предоставляющими услуги связи*, могут предлагать установление соединения для междугородной связи. Для установления сквозного соединения между географически разнесенными точками предоставляющие услуги связи компании арендуют услуги доступа у местных поставщиков услуг. В случае прерывания обслуживания включается приложение, называемое *административной службой составления отчета о неисправности*. Пользователю таких систем, а также и самому приложению для составления донесения о неисправностях в процессе предоставления услуг необходима авторизация. Имеющие полномочия системы и пользователи должны выполнить необходимые действия для поиска статуса неисправностей, вошедших в донесение. На рисунке 21 показаны виды взаимодействия, которые должны быть защищены. Осуществляется администрирование привилегий доступа, с тем чтобы исключить несанкционированный доступ к донесениям о неисправностях. Поставщик услуг имеет разрешение на составление отчета о неисправностях только в отношении тех услуг, которые он арендует, но не услуг, арендуемых другим поставщиком.

Рисунок 21 – Составление отчета о неисправности

В Рекомендации МСЭ-Т X.790 содержится описание такого приложения по управлению и приводятся механизмы, такие как списки управления доступом и двусторонняя аутентификация, для защиты процессов.

7.6 Общие услуги управления безопасностью

Существует несколько общих услуг, которые рассматриваются в качестве деятельности в плоскости управления МСЭ-Т X.805. Обычно они применяются, когда используется *Общий протокол управляющей информации*

(CMIP) (Рекомендация МСЭ-Т X.711). Ниже приведено краткое описание услуг, включенных в эти Рекомендации.

7.6.1 Функция аварийной сигнализации системы безопасности

Передача аварийных сигналов является одной из ключевых функций в интерфейсе управления. Если обнаруживается сбой в результате неисправности (например, сбой в работе оборудования или нарушение режима безопасности), в систему управления поступает аварийный сигнал. В аварийном сообщении содержится ряд параметров, с тем чтобы система управления могла установить причину сбоя и осуществить правильные действия. Параметры по любому событию включают поле обязательного ввода, называемое *типом события*, и набор других полей, называемых *информацией о событии*. Последняя состоит из такой информации, как серьезность аварийного сигнала, возможные причины аварийного сигнала и детектор нарушения безопасности. Причины аварийного сигнала связаны с типами событий, как показано в таблице 7.

Таблица 7 – Причины аварийного сигнала

Тип события	Причины аварийного сигнала
Нарушение целостности	Дублированная информация Пропавшая информация Обнаруженное изменение информации Нарушение последовательности информации Неожиданная информация
Функциональное нарушение	Отказ в обслуживании Перерыв по техническим причинам Процедурная ошибка Неустановленная причина
Физическое нарушение	Повреждение кабеля Обнаружение вторжения Неустановленная причина
Нарушение службы или механизма безопасности	Отказ в обеспечении аутентификации Нарушение конфиденциальности Неудача в получении информации по неотказуемости Попытка несанкционированного доступа Неустановленная причина
Нарушение во временной области	Задержанная информация Ключ с истекшим сроком действия Действия в нерабочее время

Эти причины аварийного сигнала более подробно объясняются в Рекомендации МСЭ-Т X.736.

7.6.2 Функции отслеживания проверки безопасности

Данные проверки обеспечения безопасности используются для создания записи о событиях, относящихся к безопасности, и, в частности, нарушениях безопасности. События, относящиеся к безопасности, могут включать соединения, разрывы соединения, применение механизмов обеспечения безопасности, действия по управлению и отчетность по использованию. *Функции отслеживания проверки безопасности* определены в Рекомендации МСЭ-Т X.740.

7.6.3 Управление доступом для управляемых объектов

Модель, связанная с передачей функции управления доступом различным управляемым объектам, очень подробно описана в Рекомендации МСЭ-Т X.741. Требования, удовлетворяемые этой Рекомендацией, включают защиту информации об управлении от несанкционированного введения, удаления и изменения; разрешенные операции соответствуют правам доступа для инициаторов операций и предотвращают передачу информации об управлении не имеющим доступа получателям. С целью удовлетворения этих требований описаны различные уровни управления доступом. В отношении операций по управлению может применяться ограничение доступа на множественных уровнях. Политика управления доступом может применять одну или несколько определенных схем (например, списки управления доступом, управление доступом на основе функциональных возможностей, меток и контекста). В модели МСЭ-Т X.741 решение о том, разрешить или не разрешить доступ, принимается на основе политики управления доступом и информации об управлении доступом (ACI). Например, ACI включает правила, идентификацию инициатора, идентификацию целей, к которым запрашивается доступ, и информацию, касающуюся аутентификации инициатора.

7.6.4 Услуги безопасности на основе CORBA

Хотя многие Рекомендации МСЭ-Т серии X.700 предполагают использование CMIP как протокола интерфейса управления, существуют и другие тенденции, которые теперь отражены в этих Рекомендациях. Они включают использование протоколов, услуг и моделей объектов на основе Обобщенной архитектуры посредника объектных запросов (CORBA) для интерфейсов управления. Особого внимания заслуживают Рекомендации МСЭ-Т X.780, МСЭ-Т X.780.1, МСЭ-Т X.780.2, *TMN* и Рекомендация МСЭ-Т X.781. Кроме того, в Рекомендации МСЭ-Т Q.816 определяется структура использования этих услуг в контексте интерфейсов управления. В целях поддержки требований к безопасности для этих интерфейсов Рекомендация МСЭ-Т Q.816 ссылается на спецификацию группы управления объектами (OMG) для общих услуг безопасности.

8. Некоторые особые подходы к безопасности сети

8 Некоторые особые подходы к безопасности сети

В данном разделе пересмотрены подходы к защите различных типов сетей. Этот раздел начинается со взгляда на требования к безопасности для сетей последующих поколений. Затем следует обзор сетей подвижной связи, которые находятся в переходном состоянии от подвижности, основанной на одной технологии (такие как CDMA или GSM), к подвижности в пределах гетерогенных платформ с использованием межсетевого протокола (IP). Далее рассматривается обеспечение безопасности для домашних сетей и кабельного телевидения. И наконец, представлены проблемы безопасности в повсеместных сетях датчиков.

8.1 Безопасность сетей последующих поколений (СПП)

Сеть последующих поколений (СПП) является сетью на основе коммутации пакетов, которая имеет возможность предоставлять услуги связи пользователям и которая позволяет использовать технологии многоканальной широкополосной передачи информации с данным качеством обслуживания (QoS). Кроме того, функции, связанные с услугами, не зависят от основных технологий, связанных с транспортным протоколом. СПП предоставляет пользователям неограниченный доступ к сетям и конкурирующим поставщикам услуг и услугам. Она поддерживает обобщенную подвижность, которая позволит последовательно и повсеместно предоставлять услуги пользователям. Дополнительные подробности об общих характеристиках СПП приведены в Рекомендации МСЭ-Т Y.2001.

8.1.1 Задачи и требования к безопасности СПП

Признавая, что безопасность является одной из определяющих функций СПП, необходимо ввести в действие ряд стандартов, которые будут гарантировать, что безопасность СПП будет достигнута в максимально возможной степени. С развитием СПП появляются новые уязвимости безопасности, для которых нет заранее известных автоматических средств, такие уязвимости должны быть надлежащим образом задокументированы, с тем чтобы администраторы сети и конечные пользователи могли смягчить последствия их влияния.

Рекомендация МСЭ-Т Y.2701, которая основана на принципах Рекомендации МСЭ-Т X.805, определяет требования к безопасности для защиты СПП от угроз безопасности и охватывает некоторые технические аспекты управления идентичностью.

В среде, где работает несколько сетей, должны быть защищены следующие элементы:

- инфраструктура сети и поставщика услуг, а также средства инфраструктуры (например, средства и ресурсы СПП, такие как элементы сети, системы, компоненты, интерфейсы, данные и информация), ее ресурсы, ее соединения (т. е. сигнализация, управление и трафик данных/носителей) и ее услуги;
- услуги и возможности СПП, например услуги передачи голоса, видео и данных; и
- связь с конечным пользователем и информация о нем (например, личная информация).

Эти требования должны обеспечить безопасность на основе сети для соединений конечных пользователей, находящихся в пределах административных доменов нескольких сетей, как показано на рисунке 22.

Требования, определенные в МСЭ-Т Y.2701, рассматриваются, как минимальный набор требований. Поставщику СПП, возможно, потребуется принять дополнительные меры, помимо указанных.

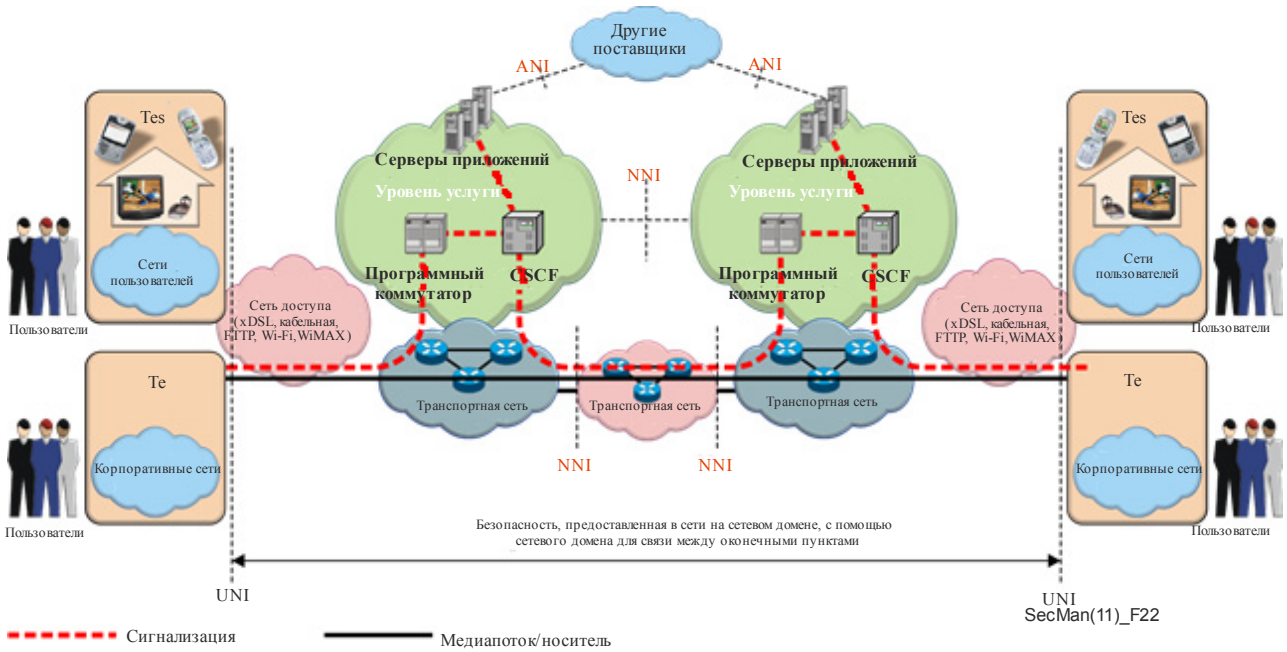


Рисунок 22 – Безопасность связи в пределах многоканальных сетей

В дополнение к требованиям, указанным в Рекомендации МСЭ-Т Y.2701, в Рекомендации МСЭ-Т Y.2702 представлены подробные требования к аутентификации и авторизации в СПП, а в Рекомендации МСЭ-Т Y.2704 определены механизмы обеспечения безопасности, в которых учитываются требования Рекомендации МСЭ-Т Y.2701 и Рекомендации МСЭ-Т Y.2702.

В Рекомендации МСЭ-Т Y.2740 определены конкретные требования для поддержки СПП, касающиеся мобильных дистанционных финансовых транзакций.

8.2 Безопасность подвижной связи

Подвижная связь представляет собой эволюцию от подвижности, которая ограничена особой технологией, например GSM или CDMA, до подвижности в пределах гетерогенных сетей (например, GSM, Wi-Fi, КТСОП) с использованием IP. Иными словами, будущие сети будут представлять собой интеграцию проводных и беспроводных сетей, предоставляющих широкий диапазон новых услуг, которые не могут быть предоставлены одной существующей сетью.

С появлением настоящей конвергенции фиксированной и подвижной связи (FMC) пользователь подвижной связи получает возможность перемещаться между гетерогенными сетями, такими как GSM, беспроводная ЛВС и Bluetooth. Требования к безопасности для каждого типа доступа должны выполняться разными способами, но все требования к безопасности должны соблюдаться, чтобы защитить пользователей, сети и приложения при наличии доступа.

Вопросы безопасности можно в целом классифицировать как:

- вопросы, связанные с использованием IP в подвижных беспроводных сетях связи; и
- вопросы, связанные с использованием многоканальных сетей с несколькими технологиями.

Интернет-атаки и уязвимости будут угрожать беспроводным подвижным сетям, которые используют IP в качестве своего транспортного протокола. Кроме того, новые угрозы будут появляться исходя из подлинного характера самих беспроводных сетей, т. е. их мобильности. Механизмы безопасности, уже разработанные для сетей IP, не могут удовлетворить все потребности в безопасности беспроводных систем на основе IP и,

следовательно, предстоит разработать новые или усовершенствованные меры безопасности IP. Кроме того, безопасность должна разрабатываться не только для радиоинтерфейса, но и для полномасштабных услуг между оконечными пунктами, а также политика безопасности должна быть достаточно гибкой, для того чтобы предоставить различные уровни безопасности в соответствии с предоставляемой услугой/приложением. Участие многоканальных сетей увеличивает возможность для угроз, таких как незаконный перехват профилей пользователей, содержания (например, голоса или передачи данных), а также информации аутентификации. С развертыванием подвижных услуг и приложений IP необходимо вводить дополнительные меры безопасности для защиты пользователя, оператора и поставщика услуг.

Международная подвижная электросвязь-2000 (IMT-2000) является всемирным стандартом для беспроводной связи третьего поколения (3G). Она определяется рядом взаимосвязанных Рекомендаций МСЭ. IMT-2000 обеспечивает основу для беспроводного доступа во всем мире путем соединения различных систем на основе наземной и/или спутниковой сетей. Она будет использовать потенциальное взаимодействие между технологиями цифровой подвижной электросвязи и системами для фиксированных и подвижных систем беспроводного доступа.

Деятельность МСЭ по IMT-2000 охватывает международную стандартизацию, включая радиочастотный спектр и технические спецификации для радиочастотных и сетевых составляющих, тарифы и начисление платы, техническую помощь и изучение регуляторных и стратегических вопросов.

Общие требования к безопасности в сетях IMT-2000 описаны в Рекомендациях МСЭ-Т Q.1701, МСЭ-Т Q.1702 и МСЭ-Т Q.1703.

Кроме того, спецификации 3G, содержащиеся в Рекомендациях МСЭ-Т серии Q.1741.x (для 3GPP) и МСЭ-Т серии Q.1742.x (для 3GPP2), содержат оценку предполагаемых угроз и перечень требований к безопасности для устранения этих угроз. Эти Рекомендации также содержат цели и принципы обеспечения безопасности для подвижной связи, определенную архитектуру безопасности, требования к криптографическим алгоритмам, требования к законному перехвату, архитектуру и функции законного перехвата.

8.2.1 Безопасная подвижная передача данных между оконечными пунктами

В настоящее время широко доступны и применяются для все большего количества приложений терминалы подвижной связи с возможностью передачи данных (например, мобильные телефоны с возможностями подключения к сетям Wi-Fi и GSM, ноутбуки, планшеты, электронные читающие устройства и КПК). С учетом самого характера беспроводной сети и уязвимостей, присущих технологиям беспроводной связи, для защиты как приложений, так и данных эффективная безопасность крайне необходима.

Сети подвижной связи являются особенно уязвимыми. Безопасность должна рассматриваться с точки зрения оператора подвижной сети, поставщика прикладных услуг и конечного пользователя. Безопасность между терминалом подвижной связи и сервером приложений имеет особенно большое значение. Для целей установления подвижной связи между оконечными пунктами МСЭ-Т разработал полный набор решений по безопасности, причем некоторые из них обсуждаются ниже.

8.2.1.1 Структура обеспечения безопасной подвижной передачи данных между оконечными пунктами

В Рекомендации МСЭ-Т X.1121 описаны две модели подвижной передачи данных между пользователем подвижной связи и поставщиком прикладных услуг (ASP) – общая модель и модель со шлюзом, как показано на рисунках 23 и 24. Услуга предоставляется пользователям подвижной связи через сервер приложений. В модели со шлюзом шлюз безопасности ретранслирует пакеты от терминалов подвижной связи на сервер приложений и преобразует протокол связи на основе подвижной сети в протокол связи на основе открытой

сети, и наоборот. На рисунке 25 описаны угрозы в сети подвижной передачи данных между оконечными пунктами. На рисунке 26 показаны те места, где для каждого объекта запрашиваются функции безопасности и отношения между объектами.

Рисунок 23 – Общая модель передачи данных между оконечными пунктами – пользователем и ASP

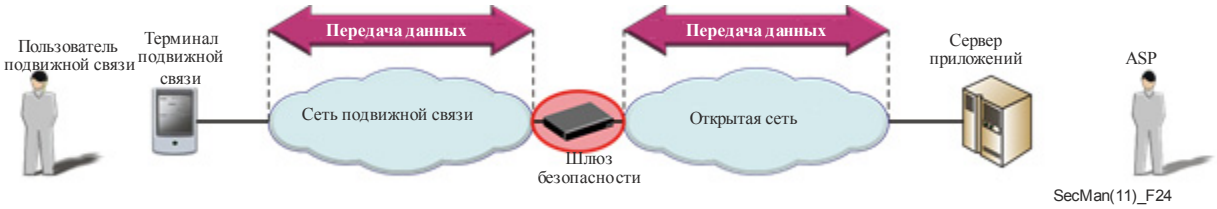


Рисунок 24 – Модель с использованием шлюза для подвижной передачи данных между оконечными пунктами – пользователем и ASP

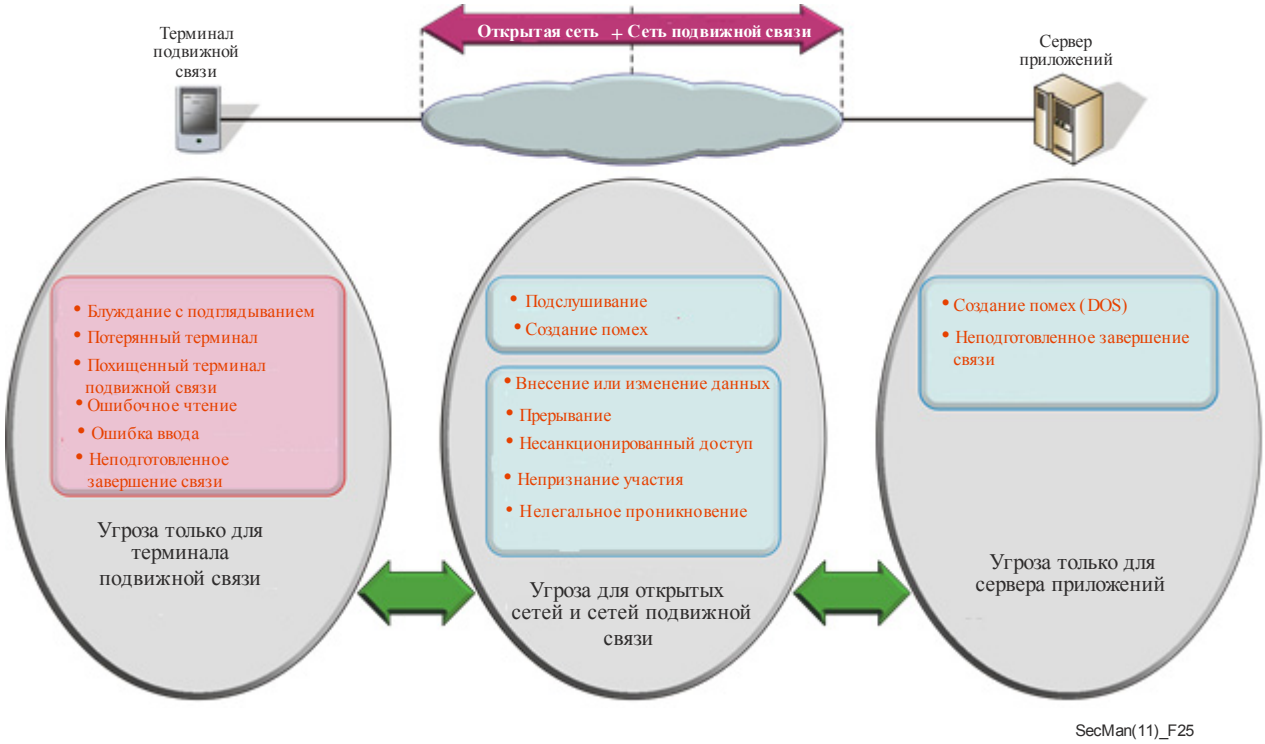


Рисунок 25 – Угрозы в подвижной связи между оконечными пунктами

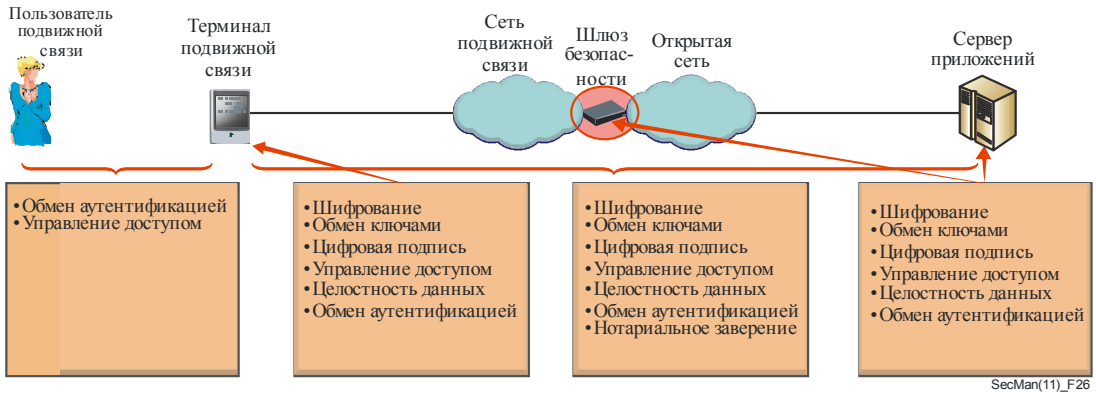


Рисунок 26 – Функции безопасности, запрашиваемые для каждого объекта и для отношений между объектами

8.2.1.2 Инфраструктура открытого ключа (PKI) для безопасной подвижной передачи данных между оконечными пунктами

Технология PKI чрезвычайно полезна для обеспечения выполнения ряда функций безопасности (например, конфиденциальности, цифровой подписи, целостности данных), необходимых для подвижной передачи данных между оконечными пунктами, но в силу особенностей подвижной передачи данных может потребоваться некоторая адаптация этой технологии. Руководящие указания по созданию PKI в подвижной среде представлены в Рекомендации МСЭ-Т X.1122, в которой рассматриваются и общая модель PKI, и модель PKI со шлюзом.

В общей модели (показана на рисунке 27) сертифицирующий орган (CA) на стороне пользователя подвижной связи выдает сертификат пользователя и управляет хранилищем и списком аннулирования сертификатов (CRL). Проверяющий орган предоставляет пользователю подвижной связи услугу проверки сертификата в режиме онлайн. CA на стороне ASP выдает сертификат ASP и управляет хранилищем ASP и CRL. Проверяющий орган на стороне ASP предоставляет услугу проверки сертификата для сертификатов ASP в режиме онлайн.

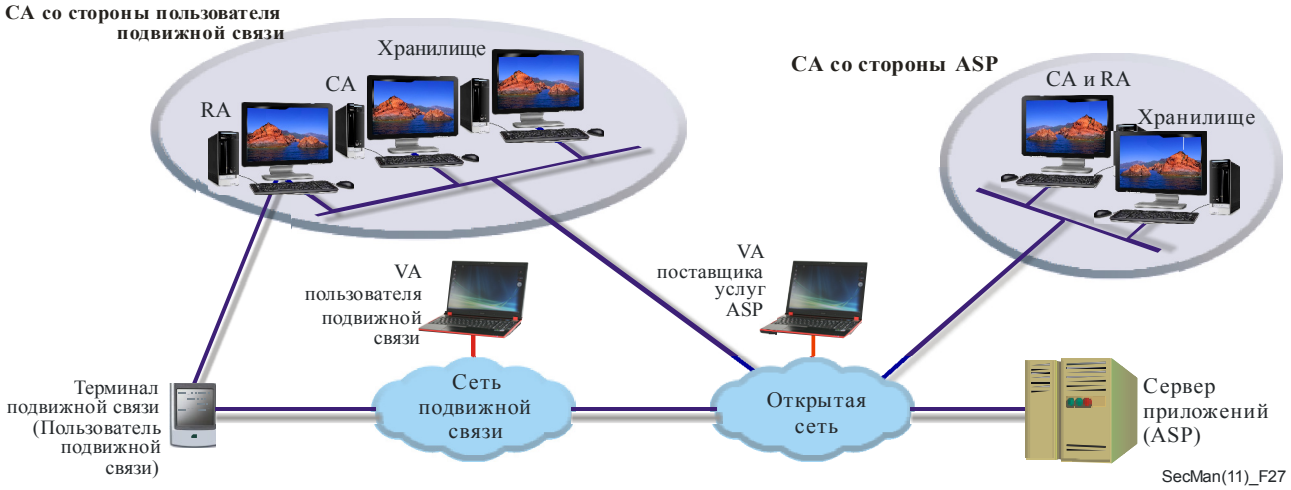


Рисунок 27 – Общая модель PKI для подвижной передачи данных между оконечными пунктами

Существет два метода выдачи сертификатов в зависимости от места генерирования открытых/секретных ключей: один метод предусматривает генерирование и изготовление пары криптографических ключей во время работы терминала подвижной связи, а при другом методе пара криптографических ключей генерируется в терминале подвижной связи или к терминалу подвижной связи прикрепляется защищенный маркер. На рисунке 28 показана процедура получения терминалом подвижной связи сертификата, когда пара криптографических ключей генерируется в терминале подвижной связи.

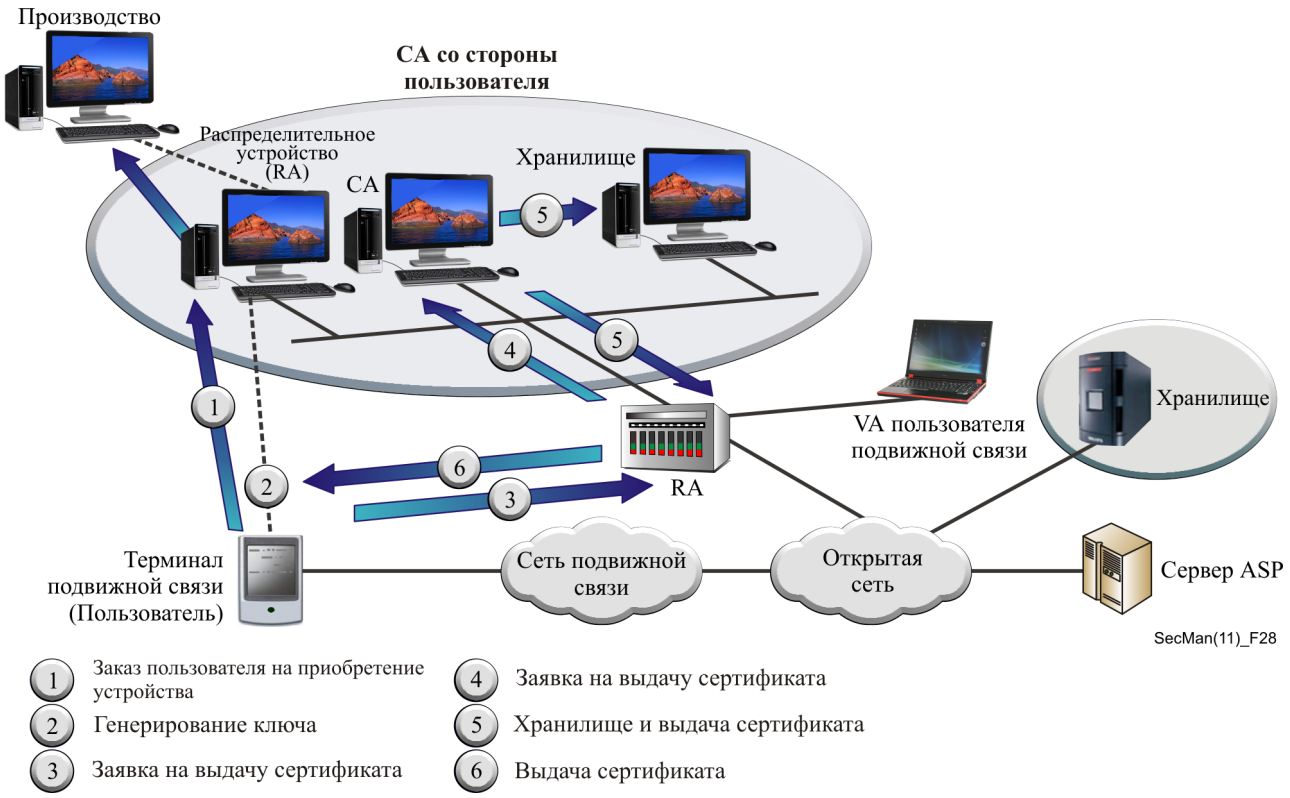


Рисунок 28 – Процедура выдачи сертификата для терминала подвижной связи

Терминал подвижной связи зачастую обладает ограниченными вычислительными возможностями и объемом памяти. Поэтому схема проверки сертификата в режиме онлайн имеет преимущество по сравнению с основанной на CRL схемой проверки сертификата в автономном режиме. На рисунке 29 показана процедура проверки сертификата в режиме онлайн для терминала подвижной связи.

Система PKI для подвижной связи между оконечными пунктами может использоваться либо для уровня сеанса связи, где предусмотрена поддержка таких услуг безопасности, как аутентификация клиента, аутентификация сервера, обеспечение конфиденциальности и целостности, либо для прикладного уровня, где предусмотрены услуги по обеспечению неотказуемости и конфиденциальности.

8.2.1.3 Система коррелированного реагирования для подвижной передачи данных

Система коррелированного реагирования была разработана для того, чтобы позволить терминалам или устройствам подвижной связи и сети работать вместе против угроз безопасности. В Рекомендации МСЭ-Т X.1125 описана основная архитектура системы коррелированного реагирования, в которой подвижная сеть и ее пользовательские терминалы могли интерактивно работать вместе для борьбы с различными угрозами безопасности для безопасной передачи данных между оконечными пунктами. К таким угрозам относятся,

например, вирусы, "черви", "троянские кони" или другие угрозы сети в отношении как подвижной сети, так и ее пользователей.

Такая архитектура предоставляет оператору сети расширенную возможность обеспечения безопасности с помощью обновлений программ безопасности подвижной станции, управления доступом к сети и ограничений прикладных услуг. В результате создается механизм, который препятствует тому, чтобы вирусы или "черви" быстро распространились через сеть оператора.

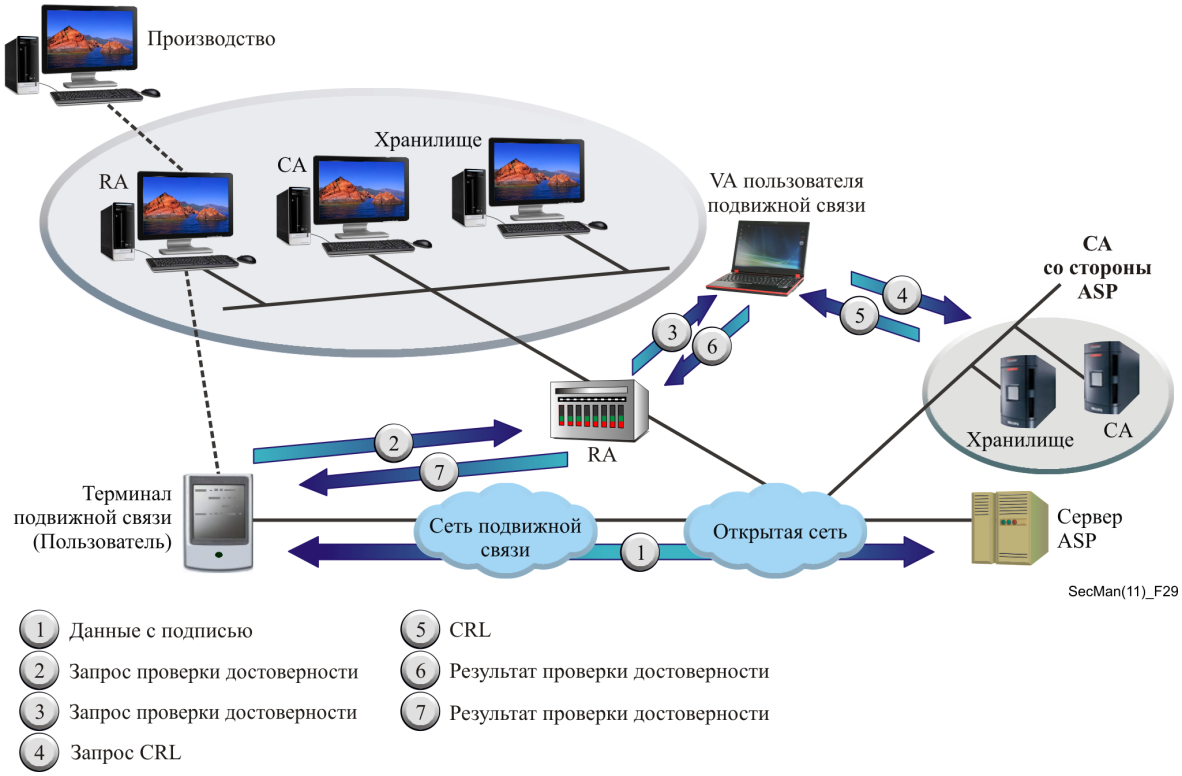


Рисунок 29 – Проверка сертификата для подвижной передачи данных между оконечными пунктами

8.2.1.4 Безопасные мобильные финансовые транзакции

В Рекомендации МСЭ-Т Y.2741 определяется общая архитектура при принятии решения в области безопасности для мобильной коммерции и мобильного банкинга в условиях СПП. В ней описываются основные участники, их роли и сценарии эксплуатации систем мобильной коммерции и мобильного банкинга. В этой Рекомендации также представлены примеры моделей реализации систем мобильной коммерции и мобильного банкинга.

8.3 Безопасность для домашних сетей

Поскольку домашняя сеть использует различные проводные или беспроводные технологии передачи, она подвергается угрозам, аналогичным тем, которым подвергается любая другая проводная или беспроводная сеть.

Для защиты услуг домашней сети Сектор МСЭ-Т разработал комплексный ряд решений и некоторые из них обсуждаются ниже.

8.3.1 Принципы безопасности для домашней сети

Для того чтобы создать структуру безопасности для домашней сети, Рекомендация МСЭ-Т X.1111 опирается на модель угроз, описанную в Рекомендации МСЭ-Т X.1121. Характеристики домашней сети можно обобщить следующим образом:

- в сети могут использоваться различные среды передачи;
- сеть может включать проводные и/или беспроводные технологии;
- существует множество возможных условий, которые необходимо учитывать с точки зрения безопасности;
- терминалы, которые могут носить с собой удаленные пользователи; и
- различные типы устройств домашней сети требуют различных уровней безопасности.

Основная модель домашней сети для обеспечения безопасности, которая показана на рисунке 30, может включать множество устройств, таких как КПК, ПК и телевизоры/видеомагнитофоны. В данной модели домашние устройства классифицируются по одному из трех типов:

- устройства типа A, такие как удаленные контроллеры, ПК или КПК, которые имеют возможность управлять устройствами типа B или типа C;
- устройства типа B – это мосты, которые соединяют устройства типа C (которые не имеют интерфейса связи) с сетью, т. е. устройства типа B соединяются с другими устройствами в сети с помощью использования собственного языка или механизма управления; и
- устройства типа C, такие как камеры безопасности и устройства A/V, которые предоставляют услуги для остальных устройств.

Некоторые устройства сочетают функции типа A и типа C.

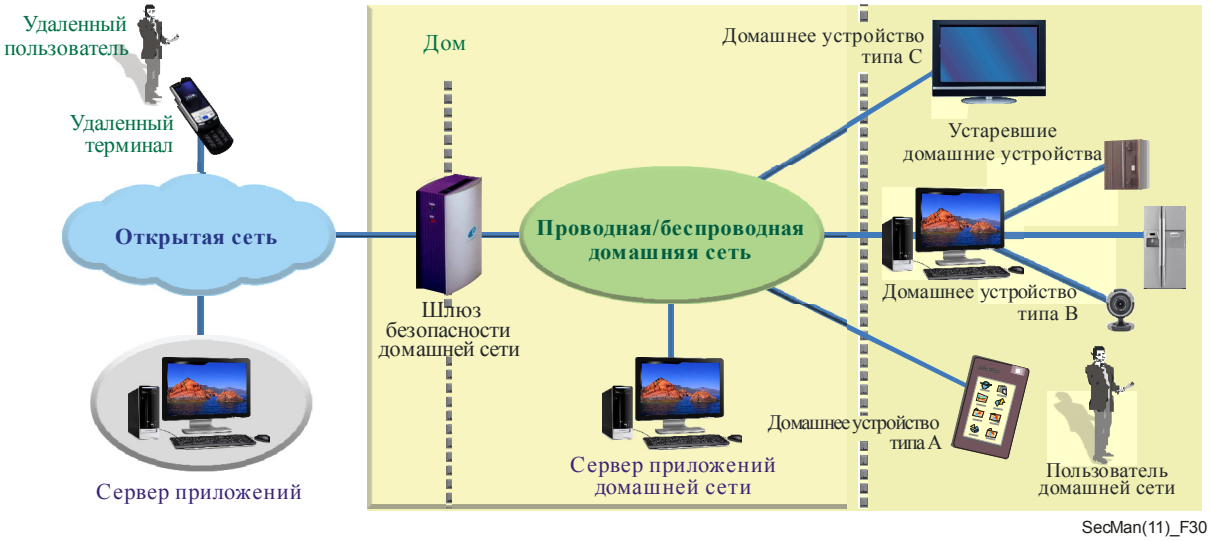


Рисунок 30 – Основная модель домашней сети для обеспечения безопасности

В Рекомендация МСЭ-Т X.1111 описаны угрозы безопасности и требования к безопасности с точки зрения пользователей домашней сети и удаленных пользователей. Кроме того, в ней классифицируются технологии безопасности с точки зрения функций, которые удовлетворяют требованиям к безопасности и местоположению, в котором технологии безопасности должны применяться.

8.3.2 Сертификация и аутентификация устройств в домашних сетях

Существует два варианта сертификации устройств в домашней сети: модель внешней выдачи, где все сертификаты домашних устройств выдаются внешним органом CA, и модель внутренней выдачи, в которой сертификаты устройств (включая подписанные им самим сертификаты и сертификаты конечного объекта) выдаются внутренним органом CA домашней сети. Обычно внутренний CA – это шлюз безопасности домашней сети с возможностью генерирования пары ключей и выдачи сертификата, т. е. шлюз домашней сети может выдать и сертификат CA, и сертификат домашнего устройства. Шлюз безопасности домашней сети может сам иметь сертификат устройства, который был выдан внешним сертификационным органом в целях использования для внешних услуг домашней сети. Такой сертификат устройства шлюза домашний сети с внешней выдачей может использоваться для аутентификации между шлюзом домашней сети и поставщиком услуг сети.

В Рекомендации МСЭ-Т X.1112 описаны структура для внутренней модели выдачи сертификата устройств, управления и использования для домашних сетей. Эта модель показана на рисунке 31.

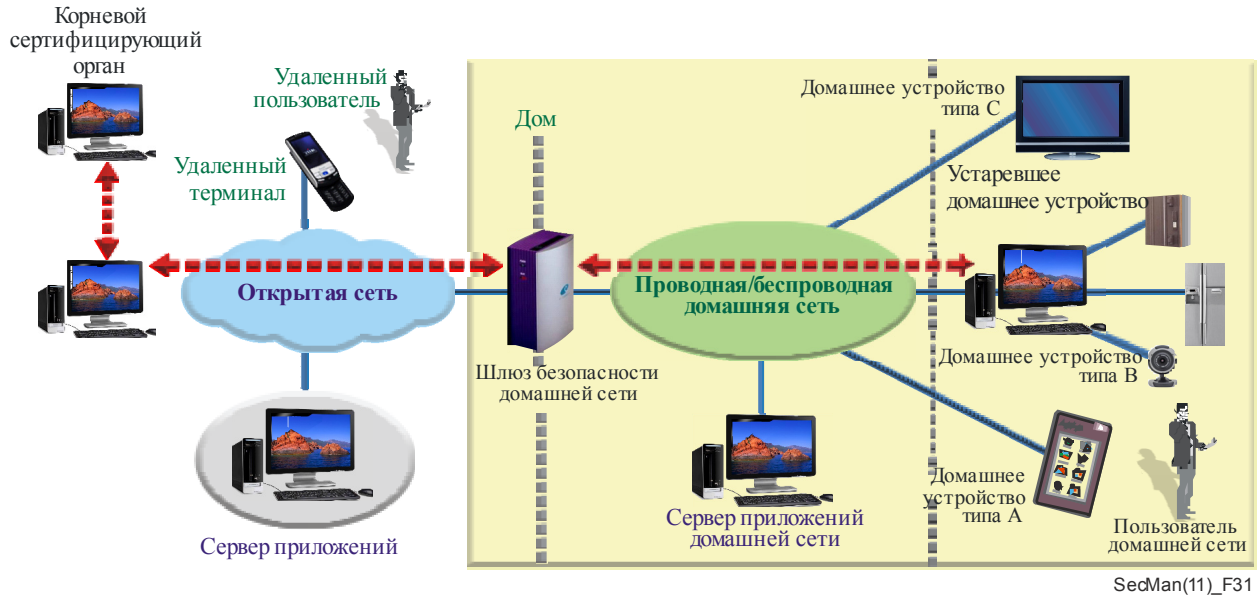


Рисунок 31 – Модель аутентификации устройства для безопасности домашней сети

Для аутентификации устройства каждому устройству в домашней сети необходим уникальный идентификатор. В частности, в качестве уникального элемента доверия при использовании в домашней сети будет необходим сертификат домашнего устройства.

На рисунке 32 показаны четыре типовых случая использования сертификата устройства: 1) между удаленным терминалом и шлюзом безопасности домашней сети; 2) между сервером приложений и шлюзом безопасности домашней сети; 3) между устройствами домашней сети и шлюзом безопасности домашней сети; и 4) между устройствами домашней сети.

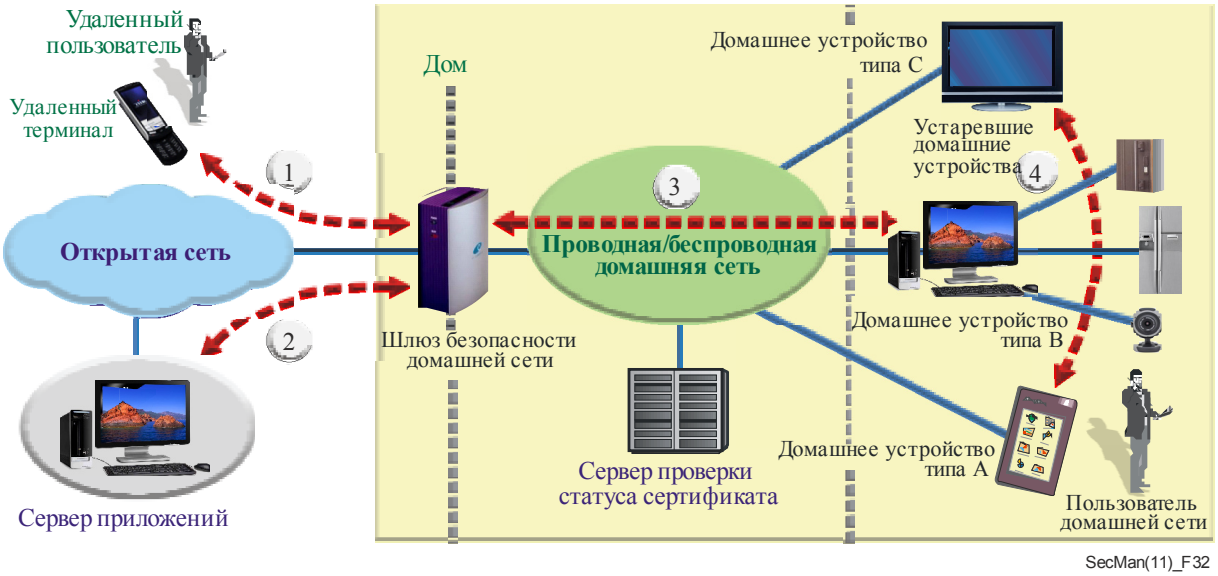


Рисунок 32 – Случай применения аутентификации устройств, основанный на общей модели безопасности домашней сети

Для того чтобы запрос внешних интернет-услуг был передан от устройства домашней сети к внешнему серверу приложений, устройство домашней сети, во-первых, должно пройти аутентификацию со шлюзом безопасности

домашней сети, используя собственный сертификат устройства. Затем шлюз безопасности домашней сети должен пройти аутентификацию с внешним сервером приложений с использованием сертификата шлюза домашней сети, выданным внешним CA. При использовании данного случая могут применяться различные протоколы приложений для поддержки безопасности услуг домашней сети.

8.3.3 Аутентификация пользователя для услуг домашних сетей

В некоторых средах требуется аутентификация пользователя-человека, а не процесса или устройства. В Рекомендации МСЭ-Т X.1113 представлены руководящие указания по аутентификации пользователя для домашней сети, с тем чтобы использовать различные технологии аутентификации, такие как пароли, сертификаты и биометрические данные. В ней также определены уровень гарантии безопасности и модель аутентификации в соответствии со сценарием услуги аутентификации. На рисунке 33 показаны потоки услуг аутентификации на основе общей модели безопасности домашней сети, определенной в Рекомендации МСЭ-Т X.1111. В данном примере удаленный пользователь пытается получить доступ к объектам в доме, в то время как пользователь домашней сети пытается получить доступ к объектам внутри и вне дома.

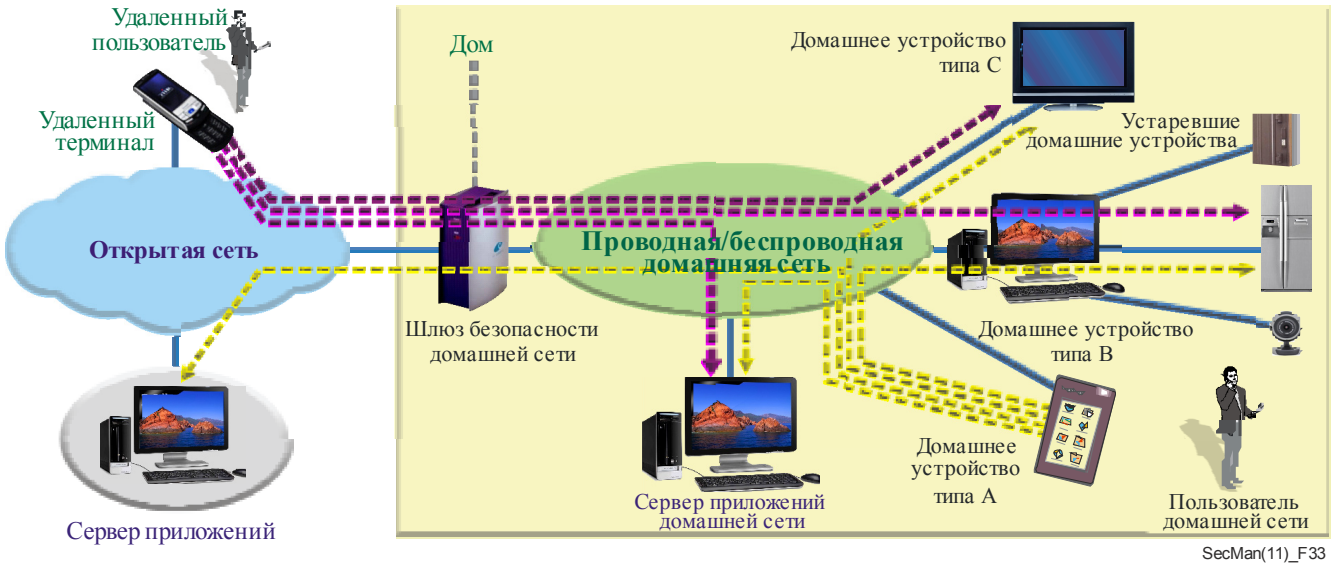


Рисунок 33 – Потоки для аутентификации услуг в домашней сети

8.4 IPCablecom

Система IPCablecom позволяет операторам систем кабельного телевидения предоставлять услуги, базирующиеся на протоколе IP в режиме реального времени (например, услуги голосовой связи) по сетям, модернизированным в части поддержки кабельных модемов.

8.4.1 Архитектура IPCablecom

Архитектура системы IPCablecom определена в Рекомендации МСЭ-Т J.160. Компоненты IPCablecom показаны на рисунке 34. Архитектура IPCablecom содержит и доверенные, и недоверенные элементы сети. Доверенные элементы сети обычно расположены в пределах управляемой магистральной сети оператора кабельной связи. Недоверенные элементы сети, такие как кабельный модем и адаптер медиатерминала (MTA) обычно располагаются вне объекта оператора кабельной сети в пределах дома абонента.

Рисунок 34 – Эталонная модель компонентов IPCablecom

8.4.2 Требования к безопасности для IPCablecom

Любой интерфейс протокола IPCablecom представляет собой объект для угроз, которые могут влиять и на абонента, и на поставщика услуг. Например, медиапоток может проходить через огромное число потенциально неизвестных поставщиков услуг интернета и магистральных услуг. В результате медиапоток может подвергаться преднамеренному подслушиванию, приводящему к потере секретности связи. Требуемые цели по обеспечению безопасности определены в архитектуре IPCablecom:

- обеспечить функциональные возможности передачи голоса в зоне жилой застройки на том же или более высоком уровне конфиденциальности, как и в сети КТСОП;
- предоставить защиту от атак на MTA; и
- защитить оператора кабельной сети от перерыва связи в сети, отказа в обслуживании и атак, заключающихся в краже услуги.

Конструктивные соображения должны включать конфиденциальность, аутентификацию, целостность и управление доступом.

Требования к безопасности определены в Рекомендации МСЭ-Т J.170. Угрозы, которым могут подвергаться пользователи, обобщены как:

- кража услуг, которая включает мошенничество с подпиской, неоплату услуг, клоны MTA (например, если MTA зарегистрирован под аккаунтом мошенника и является клоном), имитацию сервера сети и манипуляцию протоколом;
- раскрытие информации несущих каналов, которое включает: простое слежение, клоны MTA (например, MTA с общим доступом), манипуляцию протоколом, криптоанализ в автономном режиме и прерывание обслуживания;
- раскрытие сигнальной информации;
- кража услуг, основанных на MTA; и

- незаконная регистрация арендованного MTA другим поставщиком услуг.

8.4.3 Услуги и механизмы безопасности в IPCablecom

Безопасность в IPCablecom реализована в элементах нижних стеков, поэтому в основном используются механизмы, определенные IETF. Архитектура IPCablecom осуществляет защиту от этих угроз путем определения для каждого конкретного интерфейса протокола основного механизма безопасности (такого как IPSec), который обеспечивает интерфейс протокола необходимыми для него услугами безопасности.

Услуги безопасности, предоставляемые через основной слой услуг IPCablecom, включают аутентификацию, управление доступом, целостность, конфиденциальность и неотказуемость. Механизмы безопасности включают как протокол безопасности (например, IPSec, протокол безопасности RTP-уровня в режиме реального времени и протокол безопасности SNMPv3), так и поддерживающий протокол управления ключами (например, IKE, PKINIT/Kerberos). Наряду с этим базовые услуги безопасности IPCablecom включают механизм обеспечения сквозного шифрования медиапотоков RTP, что значительно снижает угрозу секретности.

8.5 IPCablecom2

IPCablecom2 представляет собой инициативу отрасли кабельной связи, направленной на поддержку конвергенции голоса, видео, данных и технологий подвижной связи.

8.5.1 Архитектура IPCablecom2

IPCablecom2 основывается на версии 6 подсистемы передачи мультимедийных данных по IP-сетям (IMS), как определено проектом партнерства третьего поколения (3GPP). Сфера 3GPP включает развитие архитектуры IP-связи на основе SIP для подвижных сетей. В результате эта архитектура формирует основу архитектуры IPCablecom2, определенной в Рекомендации МСЭ-Т J.360.

8.5.2 Требования к безопасности для IPCablecom2

Цели создания архитектуры безопасности для IPCablecom2 включают:

- поддержку механизмов конфиденциальности, аутентификации, целостности и управления доступом;
- защиту сети от отказа в обслуживании, прерывание связи в сети, атаки с целью кражи услуги;
- защиту оборудования пользователя (UE) (т. е. клиентов) от отказа в обслуживании из-за атак, уязвимостей для безопасности, несанкционированного доступа из сети;
- поддержку конфиденциальности конечного пользователя через механизмы шифрования и механизмы, которые управляют доступом к данным абонента, таким как существующая информация;
- механизмы устройства, UE и аутентификацию пользователя; обеспечение безопасности, безопасную сигнализацию и безопасную загрузку программного обеспечения; и
- возможность улучшения и расширения архитектуры в целях содействия ранее поставленным целям.

Общие угрозы, которые относятся к IPCablecom2, рассматриваются ниже.

Угрозы домену, пользующемуся доверием

Домен, пользующийся доверием, является логическим объединением элементов сети, которым доверяют при установлении связи. Угрозы для доменов, пользующихся доверием, относятся к интерфейсам, подключающим

элементы сети в пределах домена, интерфейсам между доменами, а также интерфейсам между UE и поставщиком услуг.

Кража услуги

Кража услуги может осуществляться многими способами, включая, но не ограничиваясь: манипуляцию с UE; эксплуатацию незащищенности протокола; спуфинг идентичности; клонирование UE (т. е. действие, имитирующее законное UE); и мошенничество с подпиской и неоплату услуг.

Прерывание и отказ в обслуживании

Включает общие атаки, приводящие к отказу в обслуживании; атаки заполнения (т. е. делающие конкретный элемент сети недоступным, как правило, путем направления излишнего количества сетевого трафика на его интерфейсы); и атаки с применением "зомби" (т. е. взломанных систем с множеством оконечных точек).

Угрозы каналу сигнализации

Атаки, заключающиеся в угрозах сигнализации, включают: взлом конфиденциальности сигнальной информации; атаки "человек–посредник" в результате перехвата и возможного изменения трафика, проходящего между двумя сторонами процесса связи; и атаки, приводящие к отказу в обслуживании в диапазоне канала сигнализации.

Угрозы несущим каналам

Угрозы несущим каналам относятся к трафику медийных данных, передаваемому между сторонами процесса связи.

Угрозы безопасности конкретному протоколу

Различные угрозы существуют в отношении отдельных протоколов мультимедийных данных.

8.5.3 Услуги и механизмы безопасности в IPCablecom2

Система IPCablecom2 широко использует безопасность транспортного уровня и другие механизмы, упомянутые в подсистеме передачи мультимедийных данных по IP-сетям 3GPP (3GPP 23.002 v6.10.0, *Network Architecture*, December 2005). В следующих разделах обобщаются усовершенствования IPCablecom2 для архитектуры безопасности IMS.

8.5.3.1 Аутентификация пользователя и абонентского устройства (UE)

Архитектура IPCablecom2 поддерживает следующие механизмы аутентификации:

- аутентификацию подсистемы передачи мультимедийных данных по IP-сетям и соглашение о ключах;
- аутентификацию профиля протокола инициирования сеанса связи (SIP); и
- сертификацию начальной загрузки.

Эта архитектура вмещает UE с полномочиями для нескольких аутентификаций. Например, UE может иметь сертификат для доступа к услугам при работе в кабельной сети и универсальную смарт-карту (UICC) для доступа к услугам при работе в сети сотовой связи.

Абонент может иметь несколько полномочий. Абонент может иметь несколько UE с разными возможностями, связанными с этими полномочиями. Например, абонент может иметь MTA с сертификатом для домашнего использования, а также UE для путешествий на основе UICC.

8.5.3.2 Безопасность сигнализации

В качестве опции для обеспечения безопасности сигнализации между UE и функцией управления сеансом вызова прокси-элемента, в IPCablecom2 добавляется безопасность транспортного уровня (TLS). Использование TLS (как определено подсистемой передачи мультимедийных данных по IP-сетям (IMS)) не является обязательным для безопасности сигнализации.

8.6 Безопасность в повсеместных сетях датчиков

Датчик – это простое устройство, которое генерирует электрический сигнал, представляющий собой измеряемое физическое свойство. Повсеместная сеть датчиков (USN) является сетью, которая использует датчики с низкой стоимостью, малой мощностью для получения сведений о содержании, для того чтобы доставить информацию от датчика и информационные услуги для всех в любом месте и в любое время. USN может охватывать широкую географическую зону и может поддерживать множество приложений. На рисунке 35 показаны потенциальные применения USN.

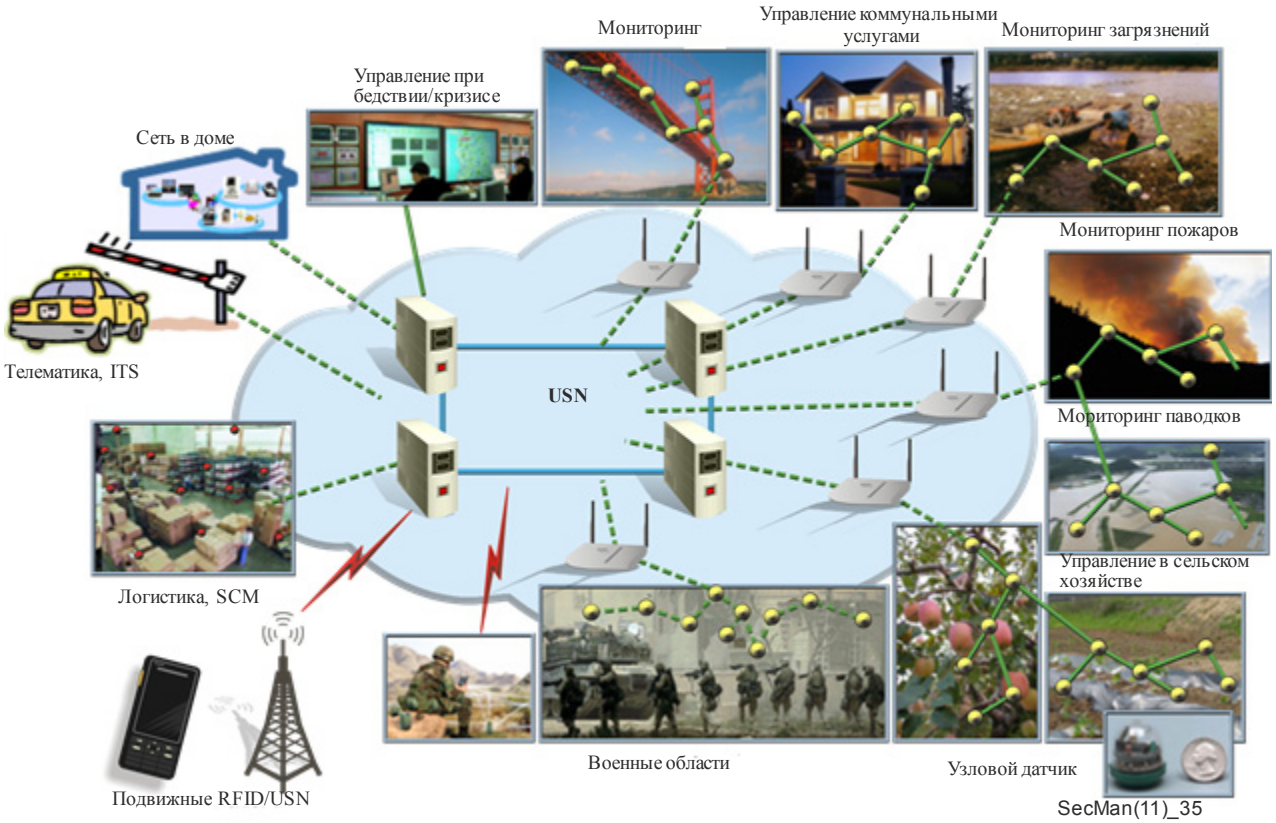


Рисунок 35 – Потенциальные применения USN

Сети датчиков обычно подключаются к сетям конечных пользователей, и в то время как основные сети передачи, вероятно, будут использовать технологии интернета и СПП, в них будут использоваться различные базовые технологии (такие как DSL, спутниковая сеть, GPRS, CDMA, GSM и т. д).

Так как передача информации со стороны USN подвергается многим потенциальным угрозам, для того чтобы противостоять этим угрозам, необходимы эффективные технологии безопасности.

8.6.1 Структура обеспечения безопасности для повсеместной сети датчиков

Последние достижения в технологии и электронных устройствах беспроводной связи облегчили процесс реализации повсеместной сети датчиков (USN). В принципе, USN состоит из трех частей: сети датчиков, содержащей большое количество узловых датчиков; базовой станции (называемой также шлюзом), обеспечивающей взаимодействие между сетями датчиков и сервером приложений; и сервера приложений, который управляет работой узловых датчиков или собирает сигналы от узловых датчиков.

В Рекомендации МСЭ-Т X.1311 описываются угрозы для безопасности и требования по обеспечению безопасности сети USN. Кроме того, этот проект Рекомендации распределяет по категориям методы обеспечения безопасности, которые удовлетворяют требованиям безопасности**,** и точки приложения методов обеспечения безопасности к модели безопасности USN.

Общая структура USN показана на рисунке 36. Домен сети датчиков может включать как беспроводные, так и проводные сети датчиков, и в соответствии с характеристиками и требованиями обслуживания может использоваться множество видов проводных и беспроводных технологий построения сетей.

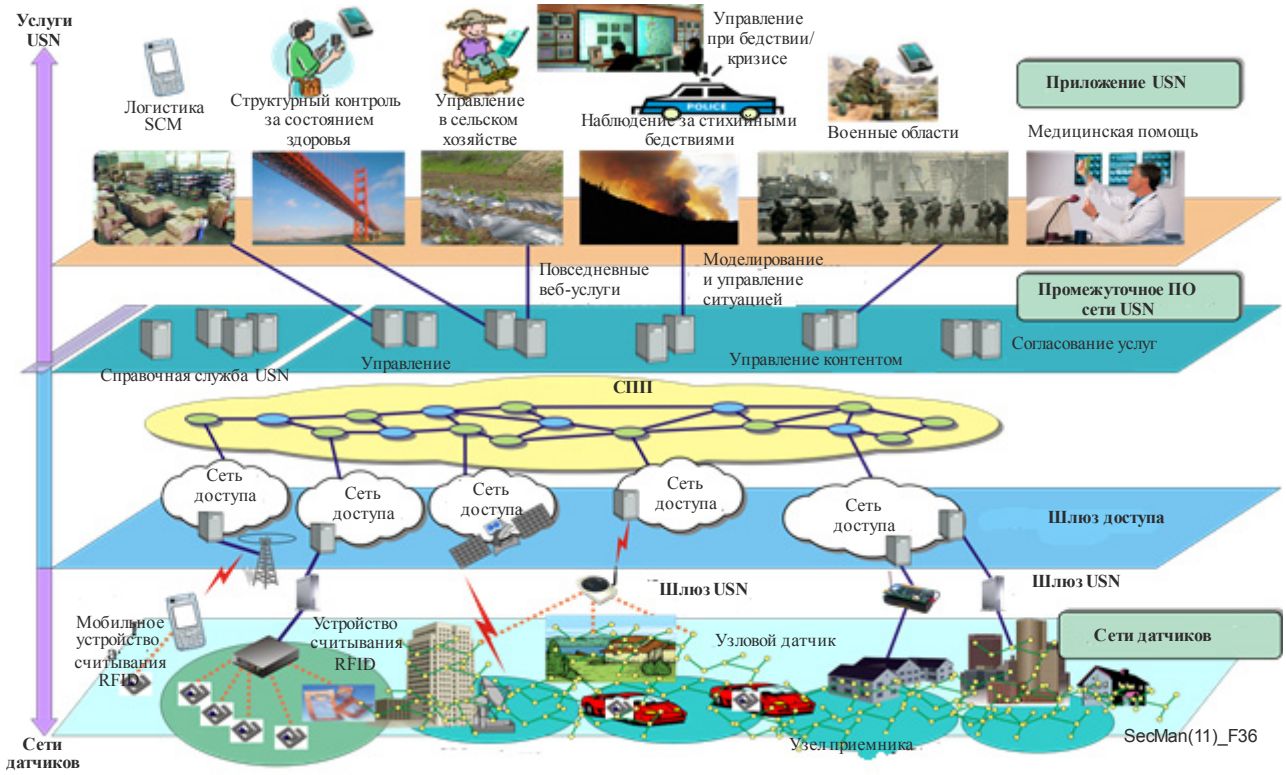


Рисунок 36 – Общая структура USN

Угрозы для USN включают угрозы как в сети IP, так и в сети SN. Существуют два типа угроз для SN: общие угрозы и угрозы, связанные с маршрутизацией. Угрозы для сети IP и связанные с маршрутизацией угрозы для обмена сообщениями в SN определяются в Рекомендациях МСЭ-Т X.800 и МСЭ-Т X.805 (см. главу 4 и рисунок 1). Кроме того, существуют конкретные угрозы для узлового датчика, такие как взлом узлового датчика, подслушивание, взлом или вскрытие считанных данных, атаки с целью отказа в обслуживании, и вредоносное или неправильное использование товарной сети. И наконец, семь дополнительных угроз были определены следующим образом:

- обманная, измененная или повторно использованная информация о маршрутизации;
- избирательная переадресация;

- атака для перехвата трафика;
- атаки "Сибилла";
- атаки "червоточина" (по перехвату пунктов);
- атаки заполнения HELLO; и
- спуфинг подтверждения.

Представленная на рисунке 37 модель обеспечения безопасности показывает общие принципы безопасности USN, основанные на сфере приложений USN, общей структуре USN и конфигурации сети USN. Эта модель основана на документе ISO/IEC 15408-1, *Evaluation criteria for IT*, и предназначена для содействия в разработке концепций обеспечения безопасности и установления взаимосвязей с безопасностью USN.

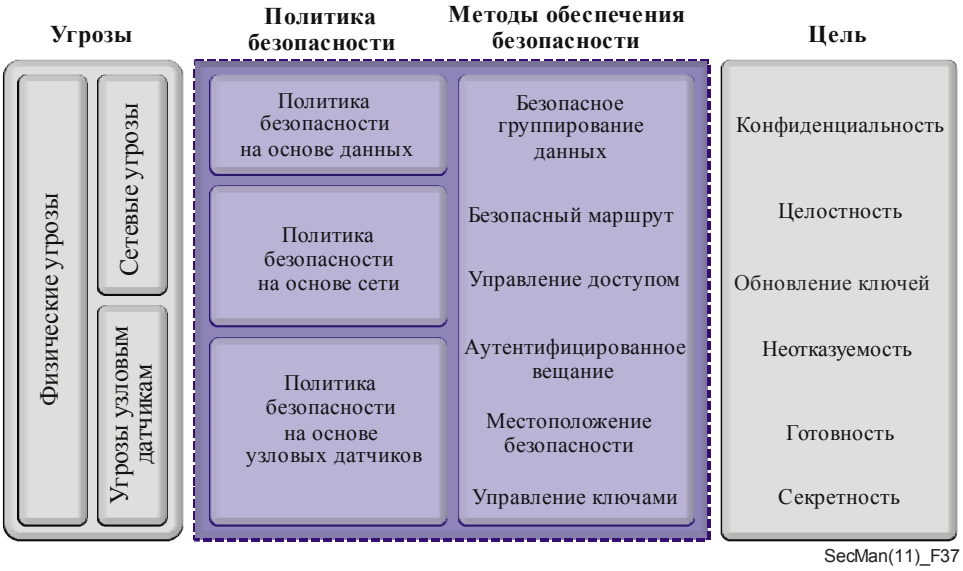


Рисунок 37 – Модель обеспечения безопасности для USN

8.6.2 Промежуточное программное обеспечение повсеместной сети датчиков (USN)

Промежуточное программное обеспечение USN – это промежуточный элемент, выполняющий функции, которые обычно требуются для различных видов приложений и услуг USN. Промежуточное программное обеспечение USN получает запросы от приложений USN и передает эти запросы в соответствующие сети датчиков. Аналогичным образом промежуточное программное обеспечение USN получает считанные или обработанные данные от сетей датчиков и передает их на соответствующие приложения USN. Промежуточное программное обеспечение USN может поддерживать такие функции обработки информации, как обработка запросов, обработка с учетом данных о содержании, обработка событий, мониторинг сети датчиков и т. п. Описание услуг и требования к ним для промежуточного программного обеспечения USN содержатся в Рекомендации МСЭ-Т F.744. Руководящие указания по обеспечению безопасности промежуточного программного обеспечения приведены в Рекомендации МСЭ-Т X.1312.

Промежуточное программное обеспечение USN располагается в модели обслуживания USN между приложением USN и сетью датчиков. Угрозы для безопасности промежуточного программного обеспечения USN можно разделить на три группы в соответствии с целевыми задачами: устройство, данные и сеть.

Угрозы для безопасности системы определяются как: несанкционированный доступ к промежуточному программному обеспечению USN; атаки DoS и DDoS на промежуточное программное обеспечение USN; вредоносная или нештатная передача трафика в направлении промежуточного программного обеспечения USN;

неправильное и злоумышленное использование системы промежуточного программного обеспечения USN; ошибки по невнимательности и общее для всех приложений нарушение установленных ограничений.

Угрозами безопасности для данных являются утечка информации и фальсификация данных.

Угрозами безопасности для связи с промежуточным программным управлением являются подслушивание, прерывание, захват соединения и создание помех.

Требования к безопасности для промежуточного программного обеспечения USN должны учитывать каждую их этих угроз.

На рисунке 38 показаны функции обеспечения безопасности промежуточного программного обеспечения USN.

Рисунок 38 – Функции обеспечения безопасности для промежуточного программного обеспечения USN

9. Кибербезопасность и реагирование на инциденты

9. Кибербезопасность и реагирование на инциденты

9.1 Совместное использование и обмен информацией о кибербезопасности

Кибератаки являются широко распространенным явлением, создающим целый ряд проблем для пользователей, поставщиков услуг и операторов. Эффективное реагирование на такие атаки зависит от осведомленности об источнике и характере конкретной атаки и от обмена информацией с организациями по контролю. Для противодействия кибератакам с помощью технических средств необходимо разработать структуру и требования для обнаружения и защиты от кибератак, смягчения последствий их воздействия и восстановления после кибератак, а также рассмотреть важные технические вопросы, с которыми сталкиваются операторы сетей, предприятия и правительства. Сектор МСЭ-Т уже разработал ряд Рекомендаций по эффективному совместному использованию информации о безопасности и уязвимостях по доменам и разрабатывает решения, касающиеся поддержки практики отчетности по вопросам электросвязи/ИКТ, реагирования на инциденты, мониторинга угроз и оценки рисков.

9.1.1 Обмен информацией о кибербезопасности (CYBEX)

Методы CYBEX, рассматриваемые в Рекомендациях МСЭ-Т серии X.1500, направлены на совершенствование обмена информацией о кибербезопасности способом, учитывающим тот факт, что и сами методы, и условия, в которых они используются, постоянно развиваются.

Методы, включенные в Рекомендации по проблемам CYBEX, позволят организациям электросвязи/ИКТ, в том числе группам реагирования на компьютерные инциденты (CIRT), которые находятся в их непосредственном или совместном ведении, получить информацию, необходимую для облегчения безопасных процессов сотрудничества и безопасного управления, в целях повышения уровня гарантий при обмене информацией между организациями и содействия в принятии решений, существенно повышая тем самым уровень конфиденциальности глобальных средств и услуг электросвязи/ИКТ. Кроме того, эти Рекомендации обеспечат согласованный подход к управлению и обмену информацией о кибербезопасности на глобальной основе и повысят осведомленность о кибербезопасности и улучшат сотрудничество в целях снижения влияния киберугроз, кибератак и вредоносного программного обеспечения.

9.1.2 Методы обмена информацией о кибербезопасности

В Рекомендации МСЭ-Т X.1500 представлена модель CYBEX и обсуждаются методы, которые могут использоваться для облегчения обмена информацией о кибербезопасности. Эти методы могут использоваться по отдельности или вместе в зависимости от требования или случая, для того чтобы повысить уровень кибербезопасности путем согласованного, комплексного, глобального, своевременного и гарантированного обмена информацией. В них не накладываются обязательства по обмену информаций, а также не рассматриваются средства получения или конечное использование обработанной информации. Эти методы включают структурированное глобальное обнаружение и функциональную совместимость информации о кибербезопасности, так чтобы обеспечить возможность развития, учитывающего постоянный прогресс в рамках многочисленных форумов по кибербезопасности.

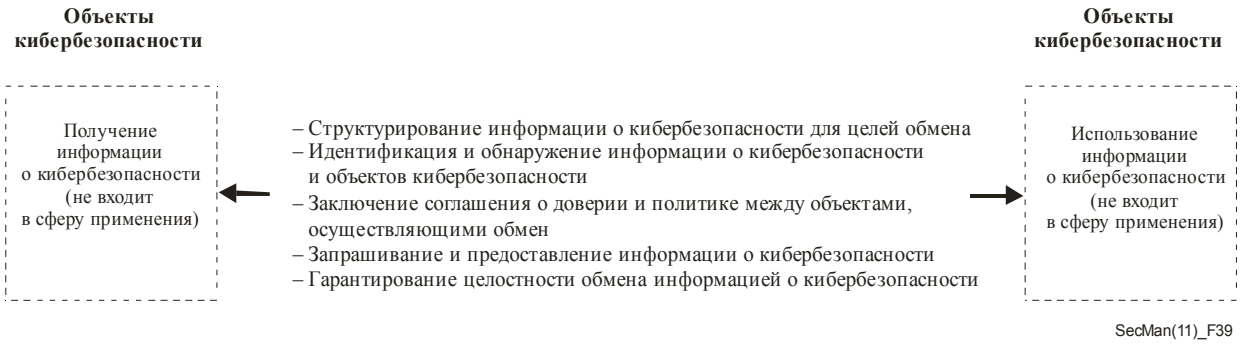


Рисунок 39 – Модель CYBEX

Показанная на рисунке 39 общая модель обмена информацией о кибербезопасности содержит основные функции, которые, в зависимости от случая, могут использоваться по отдельности или вместе, а также при необходимости могут быть расширены с целью облегчить гарантированный обмен информацией о кибербезопасности. Эти функции таковы:

- структурирование информации о кибербезопасности для целей обмена;
- идентификация и обнаружение информации о кибербезопасности и объектов кибербезопасности;
- заключение соглашения о доверии и политике между объектами, осуществляющими обмен;
- запрашивание и предоставление информации о кибербезопасности;
- гарантирование целостности обмена информацией о кибербезопасности

В Рекомендациях МСЭ-Т серии X.1500 эти методы далее сгруппированы в следующие блоки:

- слабые места, уязвимость и состояние;
- событие, инцидент и эвристика;
- политика обмена информацией;
- идентификация, обнаружение и запрос;
- гарантия идентичности;
- протоколы обмена.

9.1.3 Обмен информацией об уязвимостях

В Рекомендации МСЭ-Т X.1520 предлагается структурированное средство обмена информацией об уязвимостях и незащищенности в области безопасности и предусматривается введение общего идентификатора для широко известных проблем. В указанной Рекомендации определяется использование общеизвестных уязвимостей и незащищенности (CVE), с тем чтобы упростить обмен данными между отдельными средствами управления уязвимостями (инструментальные средства, репозитарии и услуги) с помощью предлагаемого общего идентификатора. Цель этой Рекомендации – сделать возможным совместное использование базы данных, касающихся уязвимости и других средств, и упростить сравнение инструментальных средств и услуг обеспечения безопасности. В CVE содержится только стандартный номер идентификатора с индикатором состояния, краткое описание и ссылки на соответствующие сообщения об уязвимостях и инструкции. (В данном документе не содержится информация, касающаяся, например, рисков, влияния, постоянная или подробная техническая информация.)

В CVE основное внимание отводится определению известных уязвимостей и незащищенности, обнаруженных средствами обеспечения безопасности, вместе с любыми выявленными новыми проблемами.

9.1.4 Оценка уязвимостей

В настоящее время менеджерам по ИКТ требуется выявлять и оценивать уязвимости, имеющиеся во множестве различных аппаратных и программных платформ. Затем необходимо установить приоритеты этих уязвимостей и устранить те из них, которые представляют наибольший риск. При наличии множества уязвимостей, каждая из которых оценивается по разным шкалам, именно менеджеры по ИКТ должны определить, каким образом сравнивать такие уязвимости и устанавливать их приоритеты.

Рекомендация МСЭ-Т X.1521 представляет открытую структуру, которая позволяет стандартизировать оценки уязвимостей, объяснить свойства и индивидуальные характеристики уязвимостей, использованные для получения оценки, и установить приоритеты рисков, сделав оценки уязвимостей соответствующими фактическому риску по отношению к другим уязвимостям.

Показатели системы CVSS разделяются на три группы: базовые показатели, временные показатели и показатели среды, как изображено на рисунке 40.

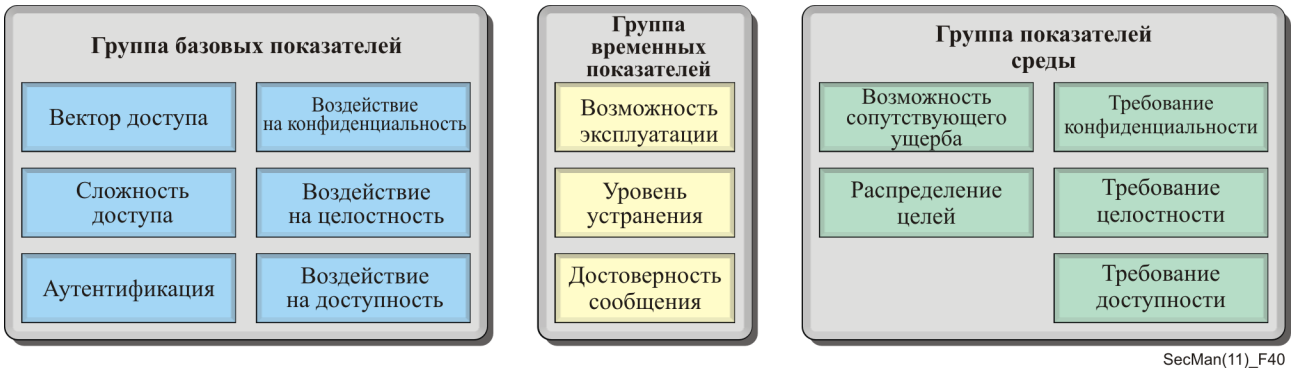


Рисунок 40 – Группы показателей системы CVSS

Базовые показатели отражают основные внутренние характеристики уязвимости, которые не изменяются во времени и не зависят от среды пользователей. Временны**е** показатели отражают характеристики уязвимости, которые изменяются во времени, но не зависят от среды пользователей. Показатели среды отражают характеристики уязвимости, которые относятся к конкретной среде пользователя и характерны только для нее.

Группа базовых показателей CVSS предназначена для определения основных характеристик уязвимости. Эта группа показателей дает пользователям четкое и интуитивно понятное представление об уязвимости. Кроме того, пользователи могут задействовать временны**е** показатели и показатели среды для обеспечения связанной с контекстом информации, которая более точно отражает риск для их уникальной среды. Благодаря этому пользователи, старающиеся снизить риски, которые связаны с уязвимостями, могут принимать более обоснованные решения.

Система CVSS используется различными способами.

- Поставщики бюллетеней с описанием уязвимости публикуют базовые и временны**е** оценки и векторы CVSS в своих бюллетенях. В этих бюллетенях содержится много информации, в том числе дата обнаружения, затронутые системы и координаты разработчиков для получения рекомендаций относительно корректировки.
- Разработчики программных приложений предоставляют своим клиентам базовые оценки и векторы CVSS, чтобы помочь им понять всю серьезность уязвимостей их продуктов, содействуя таким образом более эффективному управлению клиентами своими рисками в сфере ИКТ.

- Организации-пользователи задействуют систему CVSS для внутреннего применения при принятии более обоснованных решений, связанных с управлением уязвимостями. Эти организации используют сканеры или технологии мониторинга, чтобы первыми локализовать уязвимости хост-компьютеров и приложений. Они объединяют эти данные с базовыми и временны***ы***ми оценками, а также с оценками среды CVSS, чтобы получить информацию о риске, более тесно связанную с контекстом, и устранить те уязвимости, которые представляют самый большой риск для их систем.
- Организации, осуществляющие управление уязвимостями, сканируют сети с целью обнаружения уязвимостей ИКТ и предоставляют базовые оценки CVSS для каждой уязвимости на каждом хост-компьютере. Организации-пользователи используют затем этот поток данных для управления своими операциями по обеспечению безопасности и защиты от угроз ИКТ, обусловленных злым умыслом или случайностью.
- Фирмы, занимающиеся управлением рисками безопасности, используют оценки CVSS в качестве основы для расчета уровня риска или угрозы для организации. При объединении с такой информацией, как топология сети и ресурсы, данный подход может обеспечить клиентам более обоснованный взгляд на уровень их риска.
- Открытая структура CVSS позволяет исследователям осуществлять статистический анализ уязвимостей и их свойств.

9.1.5 Обнаружение информации о кибербезопасности

В поиске информации о кибербезопасности участвуют три объекта: устройство поиска, источник и каталог. Устройство поиска осуществляет поиск информации путем направления запросов к источнику, который предоставляет запрошенную информацию. Каталог регистрирует метаданные информации источника и помогает устройству поиска в поиске соответствующего источника.

В Рекомендации МСЭ-Т X.1570 представлены система обнаружения информации о кибербезопасности, а также механизм, обеспечивающий возможность такого обнаружения. В рамках этой системы рассматриваются вопросы опубликования информации о кибербезопасности, приобретения возможного списка и получения необходимой информации.

Схемы обнаружения основываются на информационных регистрах, которые могут быть централизованными или децентрализованными. В случае централизованного регистра для выявления и определения источников информации о кибербезопасности обычно используется механизм обнаружения на основе идентификатора объекта. В случае распределенных ресурсов сторона, осуществляющая поиск информации, использует механизм обнаружения на основе структуры описания ресурса. В данной Рекомендации описываются оба эти механизма.

Механизмы обнаружения предназначены для поиска семи следующих типов информации: базы данных о ресурсах пользователей, базы данных о ресурсах операторов, базы данных об инцидентах, базы данных о предупреждениях, базы знаний о продуктах и услугах, базы знаний о киберрисках и базы знаний о мерах противодействия. В модели онтологии, показанной на рисунке 41, описывается получение, накопление и использование информации о кибербезопасности, состоящей из набора доменов операций, ролей и типов информации; на рисунке также показаны взаимосвязи между типами информации, используемыми в данной модели.

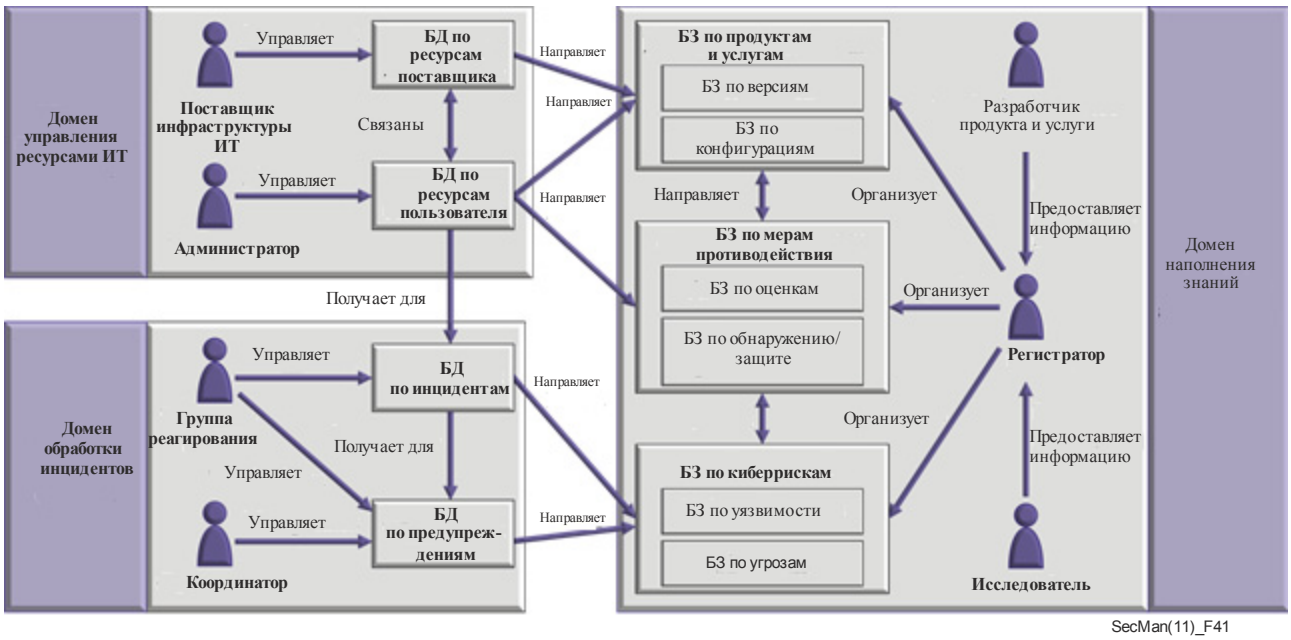


Рисунок 41 – Онтология оперативной информации о кибербезопасности

Роли, обозначаемые на рисунке пиктограммами с изображением человека, являются типовыми, а объекты, такие как CIRT, могут выполнять одну или несколько из этих функций. Данная модель используется для определения доменов операций кибербезопасности и далее применяется для идентификации требуемых объектов кибербезопасности, поддерживающих операции в каждом домене.

9.2 Обработка инцидентов

Последовательность в ходе обнаружения, реагирования на инциденты, связанные с безопасностью, и распространения информации о таких инцидентах является нормальным режимом работы по управлению системой безопасности. Пока все такие инциденты не будут надлежащим образом оценены и соответствующим образом обработаны, организации будут уязвимы для последующих, возможно более серьезных атак.

При обнаружении инцидента, связанного с безопасностью, не может появиться никакого сообщения об этом инциденте или проводиться его анализ до тех пор, пока не будет принята процедура обработки инцидента. Также не могут проводиться какие-либо процедуры по ускорению отправки сообщения или получению технической помощи или руководящих директив, даже если проблемы, затрагиваемые такими инцидентами, зачастую имеют последствия, выходящие далеко за пределы сферы ИТ или построения сетей. Например, инциденты могут повлечь за собой правовые, финансовые или репутационные риски или же они могут служить основанием для обеспечения соблюдения законов. Отсутствие эффективных процедур обработки инцидентов может привести к использованию скороспелых решений или обходных действий, вместо того чтобы надлежащим образом рассмотреть, задокументировать проблему и сообщить о ней, причем впоследствии имеется риск столкнуться с более серьезными проблемами.

Когда организации ориентированы на необходимость последовательного и эффективного управления системой безопасности сетей и операций, обработка инцидентов становится обычной практикой. Хорошо обученный и наделенный полномочиями персонал может оперативно и надлежащим образом обрабатывать инциденты безопасности.

Чтобы иметь возможность достичь успеха в обработке инцидента и в сообщении о нем, необходимо понимать, как обнаруживать, обрабатывать и разрешать инциденты. Путем установления общей структуры инцидентов (т. е. физических, административных или организационных и логических инцидентов) можно будет получить картину структуры и течения какого-либо инцидента. В *Рекомендации МСЭ-Т Е.409* представлено руководство для планирования организации по обнаружению и обработке инцидентов безопасности. Эта Рекомендация носит общий характер и не определяет и не рассматривает требований для конкретных сетей.

Последовательное использование терминологии является крайне важным элементом при подготовке сообщения или при обработке инцидента. Использование разной терминологии может привести к неправильному пониманию. Результатом этого может стать то, что инцидент безопасности ICN не получит ни должного внимания, ни быстрой обработки, которая нужна для ограничения и предотвращения повторения инцидента. Помимо всего прочего, определение того, что же рассматривается под термином "инцидент ", может меняться для разных профессий, организаций и лиц. В Рекомендации МСЭ-Т Е.409 определяется терминология для обнаружения инцидента и для сообщения о нем, а также показывается, каким образом классифицировать инциденты в соответствии со степенью их серьезности, как изображено на рисунке 42.

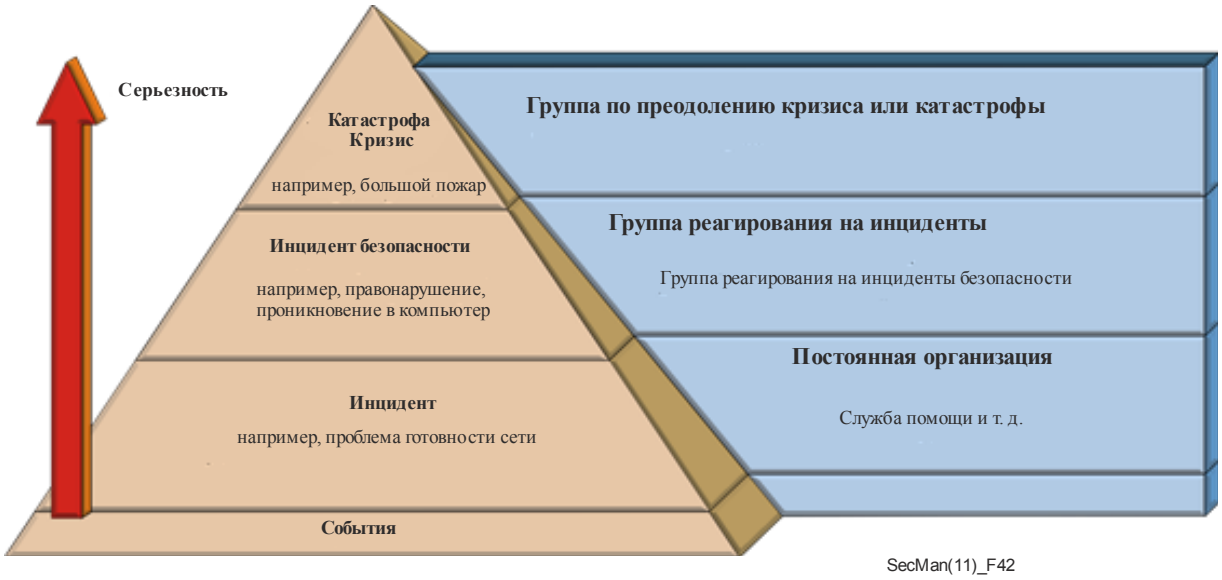


Рисунок 42 – Пирамида событий и инцидентов согласно МСЭ-Т Е.409

В Рекомендации МСЭ-Т Е.409 также определяется структура обработки инцидента (как показано на рисунке 43) и описываются процедуры для обнаружения, классификации, оценки, обработки инцидентов и проверки выполнения этих действий.

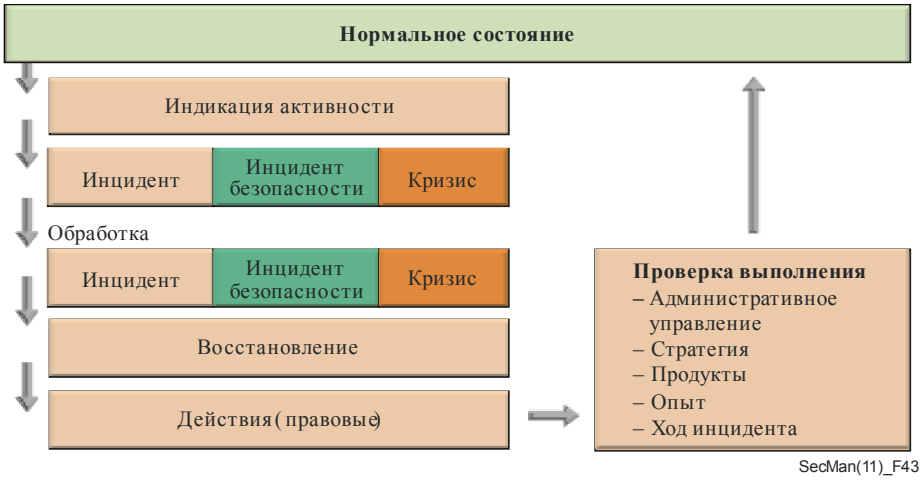


Рисунок 43 – Структура обработки инцидента согласно МСЭ-Т E.409

Недавно утвержденная Рекомендация МСЭ-Т X.1056 базируется на руководстве, представленном в Рекомендации МСЭ-Т E.409. Организациям электросвязи необходимо иметь процедуры как для обработки инцидентов, так и для предотвращения их повторения. В Рекомендации МСЭ-Т X.1056 описываются пять процедур высокого уровня по управлению инцидентами – подготовка, защита, обнаружение, приоритетность и реагирование, а также взаимосвязи с управлением системами безопасности. Эти процедуры показаны на рисунке 44.

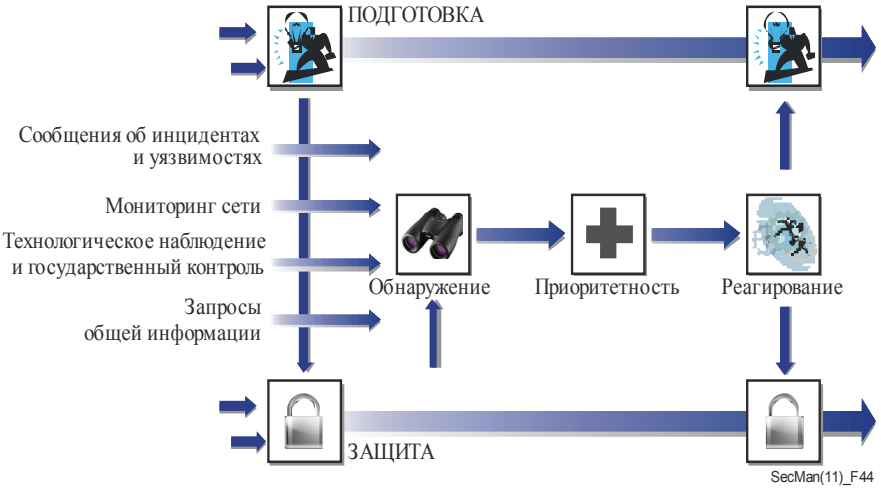


Рисунок 44 – Пять процедур высокого уровня по управлению инцидентами

Кроме того, в Рекомендации МСЭ-Т X.1056 определяется диапазон упреждающих услуг, услуг по реагированию на инциденты и услуг по управлению качеством обеспечения безопасности, которые может предоставить группа по управлению инцидентами в сфере безопасности.

10. Безопасность приложений

10 Безопасность приложений

С увеличением осведомленности о важности обеспечения безопасности сегодня разработчики приложений уделяют больше внимания необходимости создания систем безопасности в их продуктах, вместо попыток модернизации систем безопасности после отправки приложений в производство. Несмотря на это в большинстве приложений в определенные моменты их рабочего цикла обнаруживаются внутренние уязвимые места. Кроме того, развитие угроз часто раскрывает и использует ранее неизвестные уязвимые места.

В данном разделе изучаются средства безопасности некоторых приложений ИКТ с особым вниманием на средства безопасности, рассматриваемые в Рекомендациях МСЭ-Т.

10.1 Передача голоса (VoIP) и мультимедиа по IP-протоколу

VoIP, известная также как IP-телефония, – это предоставление по сети с использованием межсетевого протокола (IP) услуг, традиционно оказываемых по коммутируемой телефонной сети общего пользования (КТСОП) с коммутацией каналов. К таким услугам относятся прежде всего услуги по передаче речи, другие формы мультимедиа, включая передачу видеоряда и данных. VoIP включает также связанные дополнительные услуги и услуги интеллектуальной сети, такие как конференции (запараллеливание), переадресация вызова, постановка на ожидание вызова, многоканальность, перевод вызова на фиксированный номер телефона, прием вызова и следящая переадресация. Передача голоса по интернету представляет собой частный случай VoIP, когда трафик речевых сообщений переносится по магистралям общедоступного интернета.

Рекомендация МСЭ-Т H.323 является "зонтичной" Рекомендацией, формирующей основу для передачи звуковых сигналов, видеоряда и данных по сетям с коммутацией пакетов данных, включая интернет, локальные вычислительные сети (ЛВС) и территориально распределенные сети (ТРС), которые не обеспечивают гарантированного качества обслуживания (QoS). Эти сети доминируют в современных корпоративных настольных системах и включают сетевые технологии с коммутацией пакетов TCP/IP и с межсетевым обменом пакетами (IPX) по Ethernet, Fast Ethernet и маркерному кольцу (Token Ring). Согласно МСЭ-Т H.323 мультимедийные продукты и приложения различных производителей могут быть функционально совместимыми и таким образом обеспечивать пользователям возможность связи без проблем совместимости. Рекомендация МСЭ-Т H.323 была первым получившим определение протоколом VoIP и считается основой для функционирующих в среде VoIP продуктов для пользователей, коммерческой деятельности, поставщиков услуг индустрии развлечений. Технические описания безопасности для Рекомендаций МСЭ-Т серии H.323 содержатся в документе *Implementors Guide for ITU-T H.235 V3*, Рекомендациях МСЭ-Т сери H.235.x, которая включает девять структур и стандартов безопасности, и МСЭ-Т H.530. Подвижность для мультимедийных систем и услуг МСЭ-Т H.323 затрагивается в Рекомендации МСЭ-Т H.510.

МСЭ-Т H.323 содержит широкий обзор и включает как автономные устройства и встроенные технологии домашних компьютеров, так и связь между оконечными пунктами и между многими пунктами.

Рекомендация МСЭ-Т H.323 определяет четыре основных компонента для систем связи на базе сетей: терминалы, шлюзы, пропускные пункты и многоточечные блоки управления. Также возможно использование таких элементов, как пограничные или равноправные элементы. Указанные элементы представлены на рисунке 45.

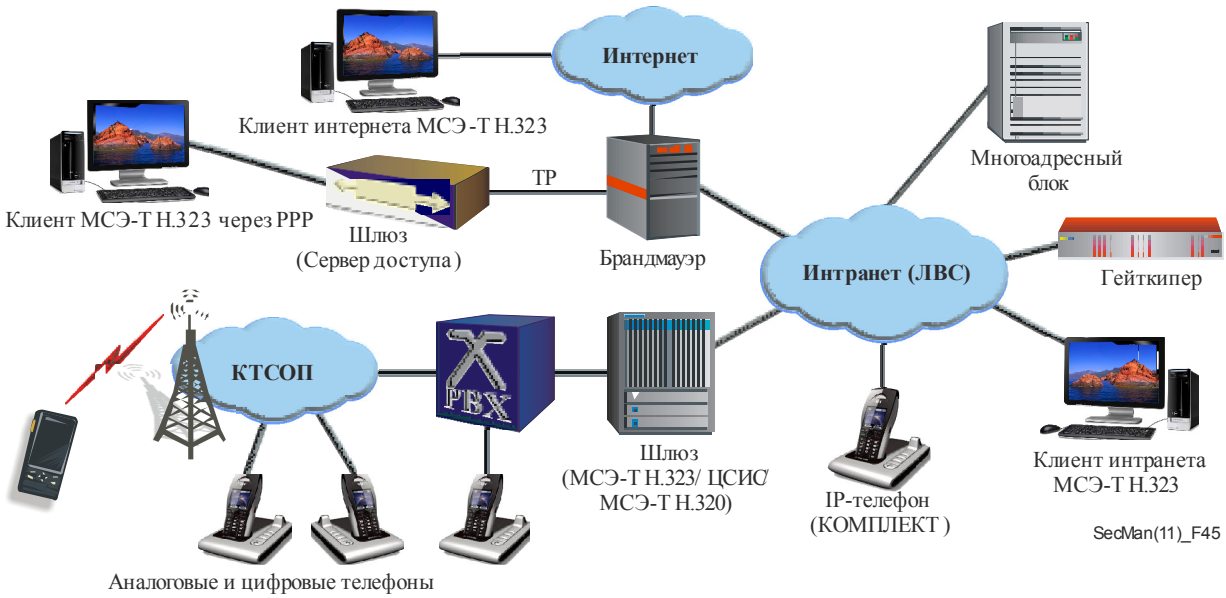


Рисунок 45 – Система H.323: компоненты и сценарии развертывания

Примерами применения МСЭ-Т H.323 являются оптовый транзит, выполняемый операторами, особенно для магистралей VoIP и услуги по телефонным карточкам. При организации корпоративной связи стандарт Рекомендации МСЭ-Т H.323 используется для IP-PBX, IP-centrex, голосового VPN, интегрированных систем передачи речевых сигналов и данных, телефонов Wi-Fi, реализации центров обслуживания вызовов, а также для обеспечения услуг подвижной связи. Эта Рекомендация широко применяется для аудио- и видеоконференций, для совмещения речи/данных/видео, а также для дистанционного обучения. Для домашних приложений используются широкополосный аудиовизуальный доступ, соединения ПК–телефон, телефон–ПК и ПК–ПК.

10.1.1 Проблемы безопасности для мультимедиа и VoIP

Вследствие того что все элементы системы согласно Рекомендации МСЭ-Т H.323 могут быть географически разнесены и в силу открытости сетей IP, возникает ряд угроз безопасности, как показано на рисунке 46.

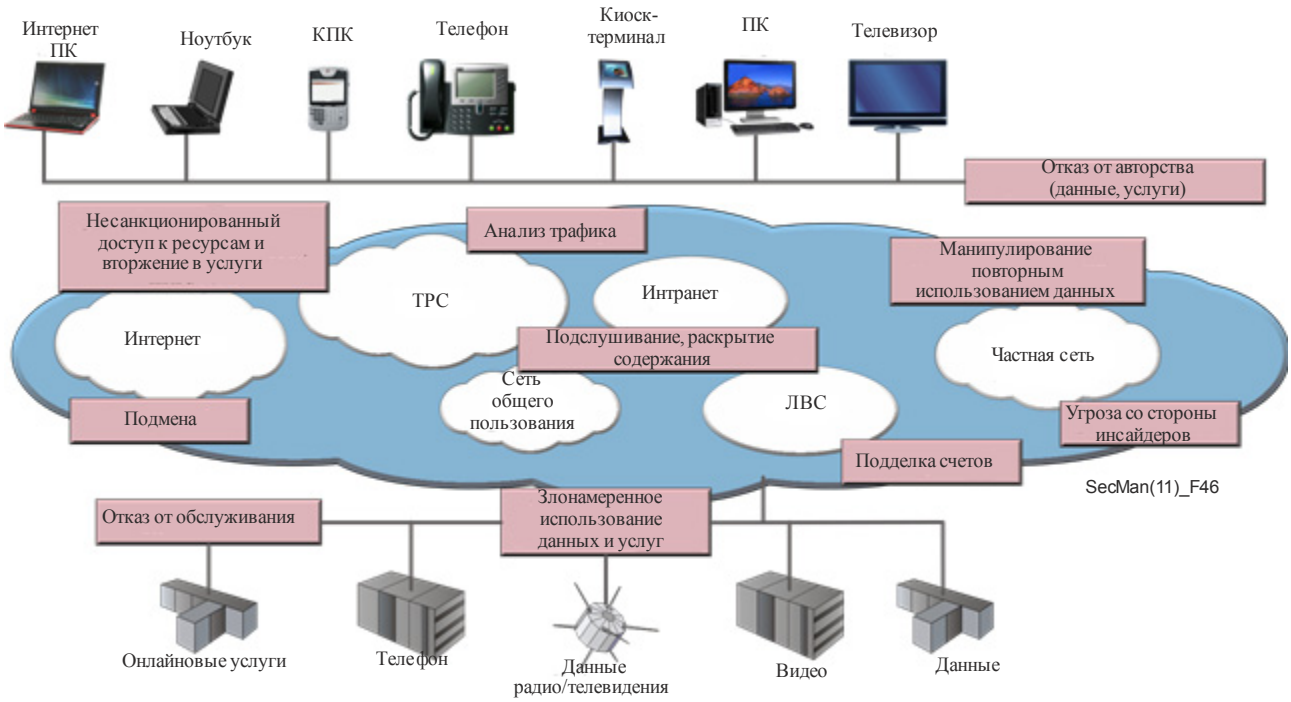


Рисунок 46 – Угрозы безопасности в среде мультимедийной связи

Основные требования к безопасности в среде мультимедийной связи и IP-телефонии описаны ниже.

- Аутентификация пользователя и терминала. Поставщикам услуг VoIP необходимо знать, кто пользуется их услугами, с тем чтобы правильно произвести расчеты и, возможно, выставить счет за обслуживание. В качестве необходимого условия для аутентификации пользователь и/или терминал должны быть идентифицированы. Затем пользователь/терминал должен доказать, что предъявленная идентификационная информация действительно является верной. Обычно это выполняется с помощью процедур надежной криптографической аутентификации (например, защищенный пароль или цифровые подписи согласно МСЭ-Т X.509).
- Аутентификация сервера. В силу того что для общения пользователей VoIP между собой обычно задействуется определенная инфраструктура VoIP, включая серверы, шлюзы и, возможно, методы многоадресной передачи, пользователи как фиксированной, так и подвижной связи заинтересованы в том, чтобы знать, с требуемым ли сервером и/или поставщиком услуг установлена связь.
- Аутентификация пользователя/терминала и сервера. Это необходимо для противодействия угрозам безопасности, например нелегального проникновения, атаки типа "человек–посредник", подмены IP-адреса и захвата соединения.
- Авторизация вызова. Представляет собой процесс принятия решения о том, действительно ли пользователь/терминал имеет разрешение на использование той или иной функции услуги (например, соединение с КТСОП) или ресурсов сети. Как правило, функции аутентификации и авторизации выполняются вместе, чтобы выполнить решение о предоставлении доступа. Аутентификация и авторизация помогают срывать такие атаки, как нелегальное проникновение, злонамеренное использование и подлог, манипулирование и отказ в обслуживании.
- Защита безопасности сигнализации. Предназначена для защиты протоколов сигнализации от манипулирования, злонамеренного использования, нарушения конфиденциальности и секретности. Протоколы сигнализации обычно защищены криптографическими средствами с применением шифрования, а также путем сохранения целостности и предотвращения повторной передачи перехваченных сообщений. Особое внимание должно быть уделено выполнению важнейших

эксплуатационных требований обеспечения связи в реальном масштабе времени, с тем чтобы избежать любого ухудшения обслуживания, вызванного процедурами обеспечения безопасности.

- Конфиденциальность речевой и мультимедийной связи. Достигается за счет шифрования пакетов речевых сообщений (для защиты от подслушивания) и медиапакетов (например, видео) мультимедийных приложений. Более совершенная защита медиапакетов включает также аутентификацию/защиту целостности полезной нагрузки.
- Управление ключами. Эта функция может составлять задачу, отдельную от VoIP-приложений (предоставление паролей), может быть объединена с сигнализацией, когда динамически согласуются профили безопасности с возможностями по обеспечению безопасности и должно осуществляться распределение ключей конкретно для данного сеанса.
- Междоменная безопасность. Эта функция предназначена для решения проблемы, возникающей вследствие того, что реализованные в неоднородных средах системы имеют различные характеристики безопасности в силу различий в потребностях, стратегиях безопасности и имеющихся возможностях обеспечения безопасности. По этой причине необходимо добиваться динамического согласования профилей безопасности и возможностей обеспечения безопасности, таких как криптографические алгоритмы и их параметры. Это приобретает особую важность при пересечении доменных границ и при наличии разных поставщиков услуг и различных сетей. Важным требованием к безопасности междоменной связи является возможность "бесшовного" перехода через брандмауэры и преодоления ограничений, налагаемых устройствами трансляции сетевых адресов (NAT).

Этот перечень не является всеобъемлющим, но включает основные аспекты безопасности согласно Рекомендации МСЭ-Т H.323. Вопросы безопасности, выходящие за рамки сферы применения Рекомендации МСЭ-Т H.323, включают стратегию безопасности, безопасность управления сетью, обеспечение безопасности, безопасность реализации, эксплуатационную безопасность и обработку инцидентов в сфере безопасности. Требования безопасности для многоадресной связи изложены в Рекомендации МСЭ-Т X.1101.

10.1.2 Обзор Рекомендаций подсерии H.235.x

Рекомендации МСЭ-Т серии H.235.x объединяют одиннадцать стандартов и одно руководство для реализующего объекта, которые вместе образуют спецификацию механизмов и протоколов безопасности плюс подробное руководство по реализации принципов безопасности в Рекомендациях МСЭ-Т серии H.323. Они предлагают масштабируемые решения безопасности для небольших групп, предприятий и крупных операторов и предлагают криптографическую защиту протоколов управления, а также мультимедийного потока данных аудио/видео.

МСЭ-Т H.235 предлагает средства согласования необходимых криптографических услуг, криптоалгоритмов и возможностей обеспечения безопасности. Функции управления ключами для установки динамических сеансовых ключей полностью интегрированы в квитирование сигнализации и, следовательно, сокращено время установления соединения. Поддерживаемые конфигурации включают "классическую" связь между оконечными пунктами, а также многоточечные конфигурации при использовании многоадресных блоков, когда в рамках одной группы осуществляется связь между несколькими мультимедийными терминалами.

МСЭ-Т H.235 использует специальные оптимизированные методы обеспечения безопасности, такие как шифрование методом эллиптических кривых и стандарт шифрования AES, чтобы соответствовать строгим ограничениям рабочих характеристик. Шифрование речи, если таковое реализовано, осуществляется на прикладном уровне путем шифрования полезной нагрузки RTP. Это позволяет осуществить реализацию, благодаря незначительному воздействию на оконечные точки за счет плотного взаимодействия с процессором цифровых сигналов и использования кодеков со сжатием речевого сигнала, а также за счет отсутствия зависимости от конкретной платформы операционной системы.

На рисунке 47 показана область действия МСЭ-Т H.235, которая охватывает условия для установления соединений (блоки МСЭ-Т H.225.0 и МСЭ-Т H.245) и двусторонней связи (шифрование полезной нагрузки RTP, содержащей сжатые аудио- и/или видеосигналы). Функциональные возможности включают механизмы аутентификации, целостности, секретности и неотказуемости. Гейткиперы осуществляют аутентификацию путем управления разрешениями в оконечных точках и обеспечивают механизмы неотказуемости. Безопасность транспортного и более низких уровней, базирующихся на IP, выходит за пределы области применения МСЭ-Т H.323 и МСЭ-Т H.235, но обычно реализуется с использованием протоколов обеспечения безопасности IP (IPSec) и обеспечения безопасности транспортного уровня (TLS). Когда этого требуют принципы создания оконечной системы, IPSec или TLS могут применяться для аутентификации и, при желании, для конфиденциальности на уровне IP, прозрачном для любого протокола (приложения), функционирующего на более высоких уровнях.

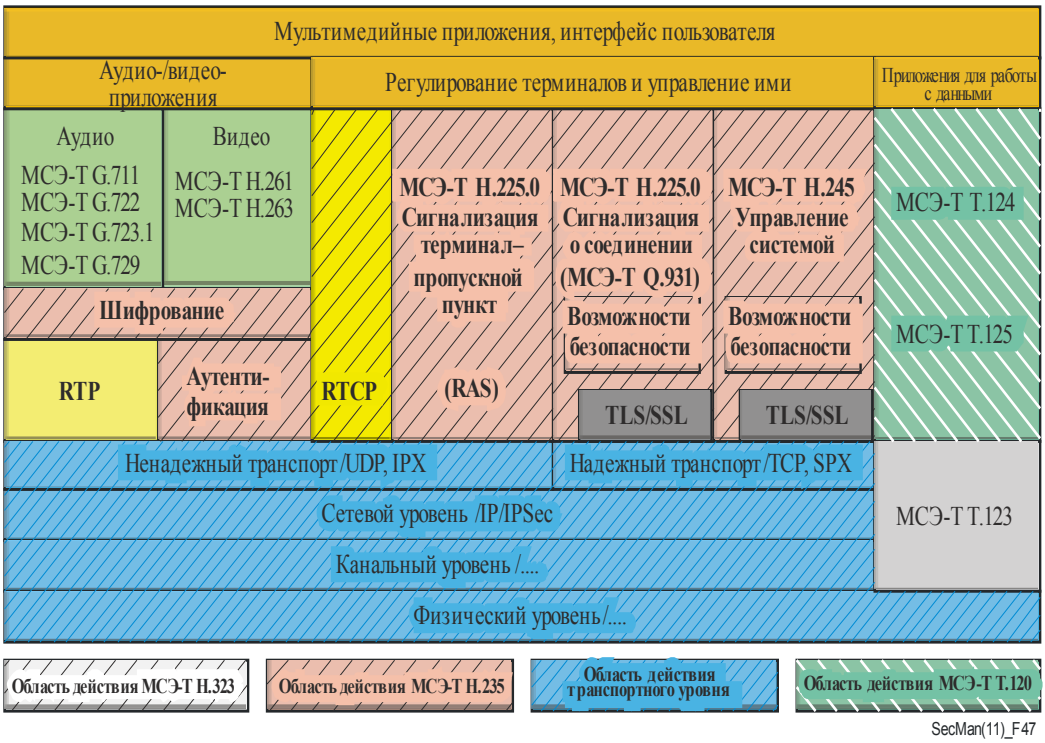


Рисунок 47 – Безопасность в МСЭ-Т H.323, как она обеспечивается МСЭ-Т H.235

Рекомендации МСЭ-Т серии H.235.x охватывают широкий спектр мер безопасности, предназначенных для использования в различных целевых средах (например, внутри/между предприятиями и операторами) и обладающих возможностью приспосабливаться к требованиям клиента и иметь особый сценарий в зависимости от местных факторов, например, доступной инфраструктуры безопасности и возможностей терминала (например, простые оконечные точки в сравнении с интеллектуальными оконечными точками).

Имеющиеся профили безопасности определяют методы безопасности, диапазон которых простирается от простых профилей с общим секретным ключом и защищенным паролем до более сложных профилей с цифровыми подписями и сертификатами PKI в соответствии с Рекомендацией МСЭ-Т X.509 (МСЭ-Т H.235.2). Это позволяет реализовывать как межсегментную защиту с использованием более простых, но менее масштабируемых методов, так и защиту между оконечными пунктами с использованием масштабируемых методов на базе PKI. Рекомендацию МСЭ-Т H.235.3 называют гибридным профилем защиты, поскольку в этой Рекомендации сочетаются симметричные процедуры безопасности согласно Рекомендации МСЭ-Т H.235.1, с использованием сертификатов на базе PKI и подписи согласно Рекомендации МСЭ-Т H.235.2, и тем самым достигаются оптимальные результаты и более короткое время установления соединения. Рекомендация МСЭ-Т

H.235.4 предоставляет меры защиты, направленные на обеспечение безопасности модели одноранговой сети. Также в ней определяются процедуры управления ключами в корпоративной и междоменной связи.

В целях обеспечения более сильной защиты систем, использующих персональные идентификационные номера (PIN) или пароли для аутентификации пользователей, Рекомендация МСЭ-Т H.235.5 предусматривает другую *структуру для надежной аутентификации в RAS с использованием слабо зашифрованных совместных секретных ключей* с помощью применения методов открытых ключей для надежного использования PIN/паролей. В Рекомендации МСЭ-Т H.235.6 собраны все процедуры, необходимые для шифрования потока данных RTP, включая сопровождающее управление ключами.

Безопасная мобильность пользователя и терминала в среде распределенных систем МСЭ-Т H.323 описана в Рекомендации МСЭ-Т H.530, в которой рассматриваются следующие аспекты безопасности:

- аутентификация мобильного терминала/пользователя и авторизация во внешних посещаемых доменах;
- аутентификация посещаемого домена;
- надежное управление ключами; и
- защита данных сигнализации между мобильным терминалом и посещаемым доменом.

В Рекомендации МСЭ-Т H.235.0 представлена общая структура безопасности для мультимедийных систем серии H. Рекомендация МСЭ-Т H.235.0 и Рекомендация МСЭ-Т серии H.350 обеспечивают масштабируемое управление ключами с применением облегченного протокола доступа к каталогу (LDAP) и уровня защищенных разъемов (SSL/TLS). В частности, серия МСЭ-Т H.350 обеспечивает функции, которые позволяют предприятиям и операторам осуществлять безопасное управление работой большого числа пользователей услуг передачи видеоданных и речевых сообщений по IP наряду со способом подключения услуг Рекомендации МСЭ-Т H.323, SIP, Рекомендации МСЭ-Т H.320 и базовых услуг обмена сообщениями к службе справочников, с тем чтобы к мультимедийной связи можно было бы применять современные практические методы управления идентичностью.

10.1.3 Устройства трансляции сетевого адреса и устройства брандмауэра

Интернет разрабатывался на основе принципа "сквозной" связи между оконечными пунктами. Это означает, что любое устройство в сети может напрямую связываться с любым другим устройством в сети. Однако из-за проблем, связанных с безопасностью и нехваткой сетевых адресов IPv4, брандмауэры (FW) и устройства трансляции сетевого адреса (NAT) часто используются на границах сети. Эти границы включают резидентный домен, домен поставщика услуг, домен предприятия и иногда домен страны. В рамках одного домена иногда используются несколько брандмауэров или устройств NAT. Межсетевые устройства брандмауэра предназначены для контроля за тем, как перемещается информация через границы сети, и обычно они настроены для блокирования большинства сообщений IP. Если только устройство брандмауэра явно не сконфигурировано таким образом, чтобы позволить пройти трафику Рекомендации МСЭ-Т H.323 из внешних устройств во внутренние устройства Рекомендации МСЭ-Т H.323, связь становится просто невозможной. Это вызывает проблему для любого пользователя оборудования Рекомендации МСЭ-Т H.323.

Устройства NAT транслируют адреса, используемые во внутреннем домене, в адреса, используемые во внешнем домене, и наоборот. Адреса, используемые в резидентном домене или домене предприятия, обычно, но не всегда, выделяются из адресных пространств частной сети, которые определены в IETF RFC 1918. Ими являются:

Класс	Диапазон адресов	Количество IP-адресов
A	10.0.0.0 – 10.255.255.255	16,777,215
B	172.16.0.0 – 172.31.255.255	1,048,575
C	192.168.0.0 – 192.168.255.255	65,535

Для большинства IP-протоколов эти устройства NAT создают еще более серьезную проблему рассогласования, особенно для тех протоколов, где IP-адреса передаются в самом протоколе. Рекомендация МСЭ-Т H.323, SIP и другие протоколы связи в реальном масштабе времени, которые функционируют в сетях с коммутацией пакетов, должны предоставлять IP-адрес и переносить информацию таким образом, чтобы другие стороны в связи знали, куда направить медиапотоки (например, аудио- и видеопотоки).

Проблемы, связанные с прохождением через NAT/FW, рассматриваются в трех Рекомендациях МСЭ-Т серии H.460, которые дают возможность сигналам связи, соответствующим Рекомендации МСЭ-Т H.323, бесшовно проходить через одно или несколько устройств NAT/FW. Это следующие Рекомендации: МСЭ-Т H.460.17, МСЭ-Т H.460.18 и МСЭ-Т H.460.19.

На рисунке 48 показано, как специальное устройство "посредник" может быть использовано, с тем чтобы помочь устройствам, "не знающим" NAT/FW, надлежащим образом пройти границы этих устройств.

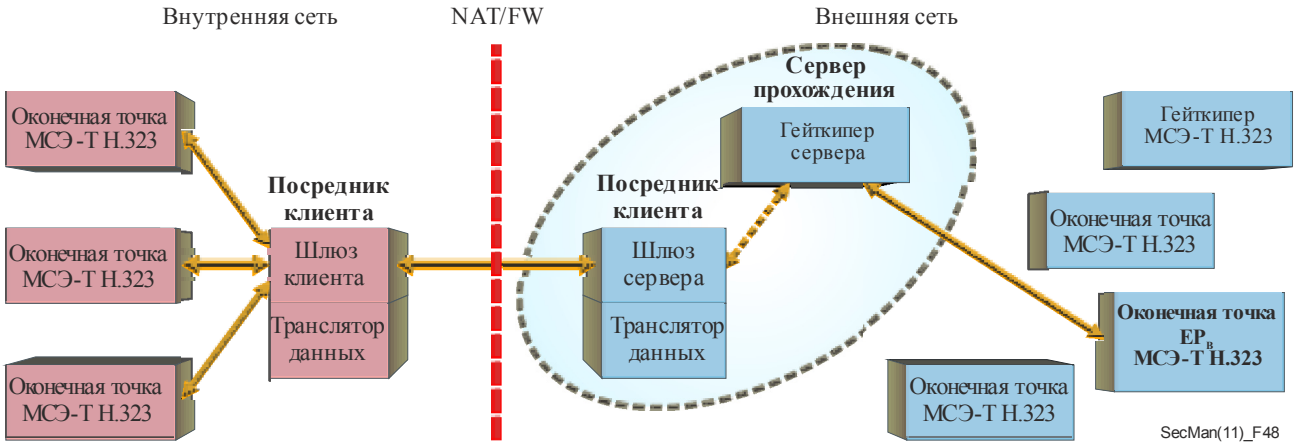


Рисунок 48 – Переход NAT/FW в архитектуре МСЭ-Т H.460.18

Вышеприведенная топология может использоваться, например, в том случае, когда предприятие желает контролировать маршрут, по которому сигнализация вызова Рекомендации МСЭ-Т H.323 и медиаданные передаются по сети. Однако Рекомендация МСЭ-Т H.460.17 и Рекомендация МСЭ-Т H.460.18 также позволяют оконечным точкам проходить границы NAT/FW без помощи каких-либо специальных внутренних устройств-"посредников". Одна такая топология показана на рисунке 49.

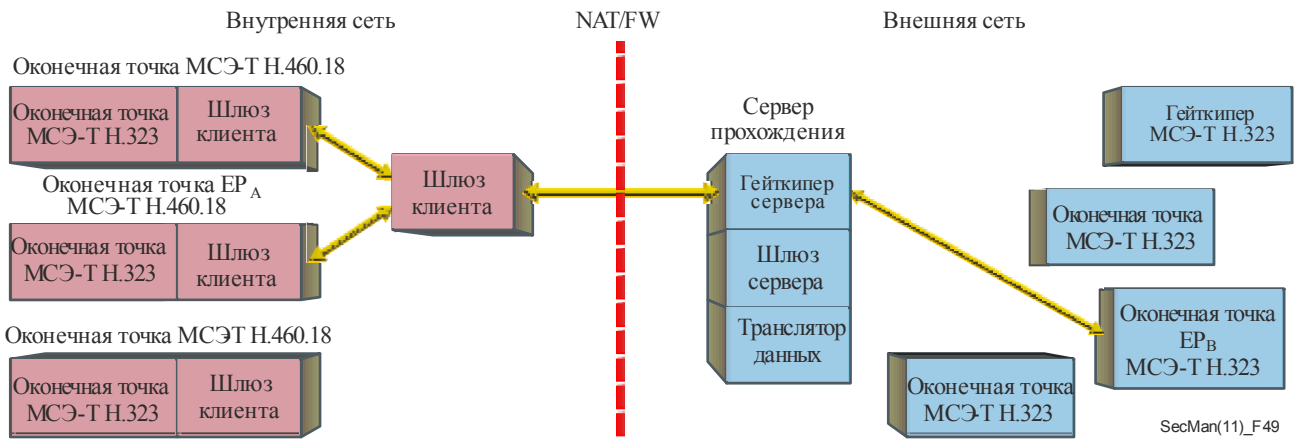


Рисунок 49 – Архитектура связи через гейткиперы

На рисунке 49 оконечные точки во внутренней сети связываются с гейткипером, который тоже приписан к внутренней сети для разрешения адреса внешних объектов (например, номера телефона или URL МСЭ-Т H.323 к адресу IP). Для обмена этой информацией об адресах гейткипер во внутренней сети связывается с гейткипером во внешней сети и передает эту информацию обратно вызывающей оконечной точке. Когда устройство во внутренней сети передает вызов на устройство во внешней сети, для открытия необходимых "микроканалов" через устройства NAT/FW для получения сигнала от внутренней сети к внешней сети оно использует процедуры, предусмотренные в Рекомендации МСЭ-Т H.460.18. Кроме того, для открытия необходимых "микроканалов" оно использует процедуры, предусмотренные в Рекомендации МСЭ-Т H.460.19, с тем чтобы позволить медиапотокам надлежащим образом проходить через внутреннюю сеть на внешнюю сеть, и наоборот.

Когда вызывающее и вызываемое устройства приписаны к разным частным сетям, разделенным устройствами NAT/FW и интернетом общего пользования, требуется иметь по крайней мере один "шлюз сервера" и один "ретранслятор медиаданных", предусмотренные в Рекомендации МСЭ-Т H.460.18, с тем чтобы надлежащим образом маршрутизировать сигнализацию и медиаданные между двумя частными сетями. Это сочетание устройств часто называется "пограничным контроллером сеансов связи". Причина состоит в том, что не существует способа, при помощи которого IP-пакет, находящийся внутри одной частной сети, мог бы войти в другую частную сеть без помощи какого-либо объекта в сети общего пользования, который выполнял бы функцию "посредника" для этого пакета.

10.2 IPTV

Положения безопасности для телевидения по межсетевому протоколу (IPTV) должны охватывать защиту контента, доставленного посредством служб IPTV, используемых оконечных устройств и предоставление таких услуг.

Для IPTV защита контента означает гарантии того, что конечный пользователь может использовать контент только в соответствии с правами, предоставленными правообладателем. Это касается защиты контента от незаконного копирования и распространения, перехвата, фальсификации и несанкционированного использования.

Защита оконечных устройств IPTV включает в себя гарантии того, что устройства, используемые конечным пользователем для получения услуг, могут надежно и безопасно использовать контент, осуществлять свои

права по использованию контента, а также защищать целостность и конфиденциальность контента и критических параметров обеспечения безопасности, например криптографических ключей.

Защита услуг IPTV включает гарантии того, что конечные пользователи могут запрашивать только те услуги и только тот контент, которые они имеют право получать. Также она включает защиту услуг от несанкционированного доступа.

Было утверждено несколько специальных Рекомендаций по безопасности IPTV. Рекомендация МСЭ-Т X.1191 определяет общую архитектуру безопасности для IPTV, как показано на рисунке 50. Следует отметить, что в сферу действия этой Рекомендации включены только те функции, которые применимы к конечному пользователю, поставщику сети и поставщику услуг. Функции, относящиеся к поставщику контента, являются предметом частных соглашений между заинтересованными сторонами и считаются вне области применения данной Рекомендации.

Рисунок 50 – Общая архитектура безопасности для IPTV

10.2.1 Механизмы для защиты контента IPTV

Механизмы безопасности, которые могут использоваться для защиты контента, включают:

- шифрование контента;
- нанесение водяных знаков (например, использование стеганографии для изменения определенных функций контента, легко обнаруживаемых без такого изменения);
- идентификацию отслеживания контента и информацию для облегчения расследований несанкционированного доступа и использования контента;
- маркировку контента (например, информацию о рейтинге, позволяющую обеспечить определенную степень управления доступом конечных пользователей к неподходящему контенту); и
- безопасное транскодирование (которое позволяет промежуточным сетевым узлам преобразовывать мультимедийный контент в иной формат или качество без дешифрования, тем самым сохраняя сквозную безопасность).

10.2.2 Механизмы для защиты услуги IPTV

Механизмы для защиты этой услуги включают:

- аутентификацию конечного пользователя (абонента) и/или оконечного устройства;
- авторизацию (для того чтобы гарантировать такое положение дел, при котором конечный пользователь или терминал имеют право доступа к услугам и/или контенту); и
- управление доступом (в частности для обеспечения того, чтобы к контенту, загруженному клиентом на сервер, мог иметь доступ только авторизованный поставщик услуг).

Рекомендация МСЭ-Т X.1192 определяет функциональные требования и механизмы для применения схемы безопасного транскодирования IPTV, Рекомендация МСЭ-Т X.1193 определяет структуру управления ключами для предоставления защищенных услуг телевидения по межсетевому протоколу (IPTV), а Рекомендация МСЭ-Т X.1195 определяет схему взаимодействия для защиты услуг и контента (SCP).

10.2.3 Защита информации абонента

Особого внимания при внедрении IPTV требует необходимость защиты информации абонента, которая может включать информацию с отслеживаемыми данными, например номер канала до и после изменения канала, время изменения, информацию пользователя касательно услуги электронной ТВ-программы, идентификацию пакета, время воспроизведения и пр. Эти данные могут считаться конфиденциальными, и должны быть предприняты меры для предотвращения их несанкционированного раскрытия посредством терминала, поставщика сети или услуг. Предложения по защите информации абонента содержатся в приложении к Рекомендации МСЭ-Т X.1191.

10.3 Защищенная факсимильная передача

Факсимильная передача остается популярным приложением, но уверенность в факсимильных услугах в высокой степени зависит от эффективности встроенных мер безопасности. Первоначально стандарты факсимильной передачи разрабатывались для передачи по КТСОП (Рекомендация МСЭ-Т T.4), а затем по ЦСИС (Рекомендация МСЭ-Т T.563). Недавно были определены расширения для факсимильных передач в режиме реального времени по IP-сетям, включая интернет (Рекомендация МСЭ-Т T.38) и при помощи систем накопления с последующей передачей (Рекомендация МСЭ-Т T.37).

Вне зависимости от режима передачи проблемы безопасности, стоящие перед факсимильными службами, включают конфиденциальность передаваемых данных, аутентификацию и неотказуемость. Эти проблемы стали

еще более важными, когда трафик перешел в интернет благодаря открытым и распределенным характеристикам этой среды передачи.

Вопросам безопасности факсимильной передачи посвящена Рекомендация МСЭ-Т Т.36, где определены два независимых технических решения, которые могут использоваться для шифрования документов при обмене. Одним из определяемых решений является использование алгоритма криптографии *Райвеста–Шамира–Адлемана* (RSA); другой метод использует комбинацию *управление ключами Готторна* (HKM) и *шифр факсимильных передач Готторна* (HFX). К указанным услугам безопасности относятся:

- взаимная аутентификация (обязательно);
- услуги безопасности (дополнительно), которые включают взаимную аутентификацию, целостность сообщений и подтверждение приема сообщения;
- услуги безопасности (дополнительно), которые включают взаимную аутентификацию, конфиденциальность сообщений (шифрование) и создание ключа сеанса связи; и
- услуги безопасности (дополнительно), которые включают взаимную аутентификацию, целостность сообщений, подтверждение приема сообщений, конфиденциальность сообщений (шифрование) и создание ключа сеанса связи.

Комбинация систем *управление ключами Готторна* (HKM) и *шифр факсимильных передач Готторна* (HFX) предоставляет следующие возможности для безопасной передачи данных между объектами:

- взаимную аутентификацию объектов;
- создание секретного ключа сеанса связи;
- конфиденциальность документа;
- подтверждение приема; и
- подтверждение или отрицание целостности документа.

10.4 Веб-услуги

Веб-технологии, включая архитектуры, ориентированные на услуги (SOA), широко применяются, так как они дают возможность эффективно и рентабельно разрабатывать и развертывать новые услуги и включать контент из разных источников для быстрого и легкого создания сложных услуг. Существует множество аспектов безопасности веб-услуг. Требуются механизмы аутентификации и единой регистрации (SSO), а также механизмы безопасности для поддержки подвижных веб-услуг.

Экономия за счет массового производства побудила поставщиков компьютерного оборудования разработать продукты с функциональными возможностями с высокой степенью обобщенности, поэтому они могут использоваться в наиболее широком спектре ситуаций. Эти продукты имеют максимально возможное преимущество доступа к данным и рабочему программному обеспечению, так что они могут использоваться во множестве возможных условий применения, включая те, где имеются либеральные правила безопасности. Когда необходимо применение более строгих правил безопасности, локальная конфигурация должна ограничить собственные преимущества платформы.

Политика безопасности крупных предприятий включает множество элементов и множество пунктов по контролю за ее проведением в жизнь. Элементы политики могут управляться различными отделами организации (например, персоналом ИТ, сотрудниками службы безопасности, людскими ресурсами, юридической службой и т. д.) и из различных пунктов по контролю за их проведением в жизнь (например, при помощи экстранета, сети ТРС и систем дистанционного доступа). Обычной практикой для каждого пункта обеспечения исполнения политики является независимое управление.

Использование общего языка для описания политики безопасности позволит предприятию управлять обеспечением исполнения всех элементов его политики безопасности во всех компонентах информационных систем. Управление политикой безопасности может включать некоторые или все приведенные ниже этапы: запись, обзор, испытания, утверждения, выпуск, объединение, анализ, изменение, снятие, поиск и обеспечение исполнения политики.

Кроме того, необходима структура обмена информацией безопасности. Для облегчения этого обмена были разработаны языки разметки, включая язык разметки, предусматривающий защиту данных, и расширяемый язык разметки контроля доступа (XACML). Изначально они были разработаны OASIS, но в настоящее время приняты и опубликованы МСЭ-Т при помощи OASIS.

10.4.1 Язык разметки, предусматривающий защиту данных

В Рекомендации МСЭ-Т X.1141 определяется язык разметки, предусматривающий защиту данных (SAML 2.0). Язык SAML является структурой на основе XML для обмена информацией о безопасности. Эта информация безопасности выражается в виде *подтверждений* относительно субъектов, где субъект – это элемент, идентифицированный в каком-либо домене безопасности. Одно утверждение может содержать несколько различных внутренних утверждений об аутентификации, авторизации и атрибутах.

Обычно существует несколько *поставщиков услуг*, которые могут использовать подтверждения о субъекте с целью управления доступом и предоставления специализированных услуг, и соответственно они становятся доверяющими сторонами подтверждающей стороны, которая называется *поставщиком идентификации*.

В МСЭ-Т X.1141 определены три разных типа заявлений об утверждениях, которые могут быть разработаны ответственным органом SAML. Все заявления, определенные в языке SAML, связываются с объектом. Тремя типами утверждения, определенными в МСЭ-Т X.1141, являются:

- аутентификация – объект утверждения был аутентифицирован определенными средствами в определенное время;
- атрибут – объект утверждения ассоциируется с представленными атрибутами; и
- решение об авторизации – просьба разрешить объекту утверждения доступ к определенному ресурсу.

В МСЭ-Т X.1141 также определен протокол, при помощи которого клиенты могут запросить подтверждения у органов SAML и получить от них ответ. Этот протокол, состоящий из форматов сообщений запроса и ответа на основе XML, может быть привязан к множеству различных основных сеансов связи и транспортных протоколов. Создавая свои отклики, органы SAML могут пользоваться разными источниками информации, например внешними резервами политики, которые были получены в качестве входящих данных при запросе.

Набор профилей определен для поддержки единой регистрации (SSO) браузеров и других клиентских устройств. На рисунке 51 показан основной шаблон для получения SSO.

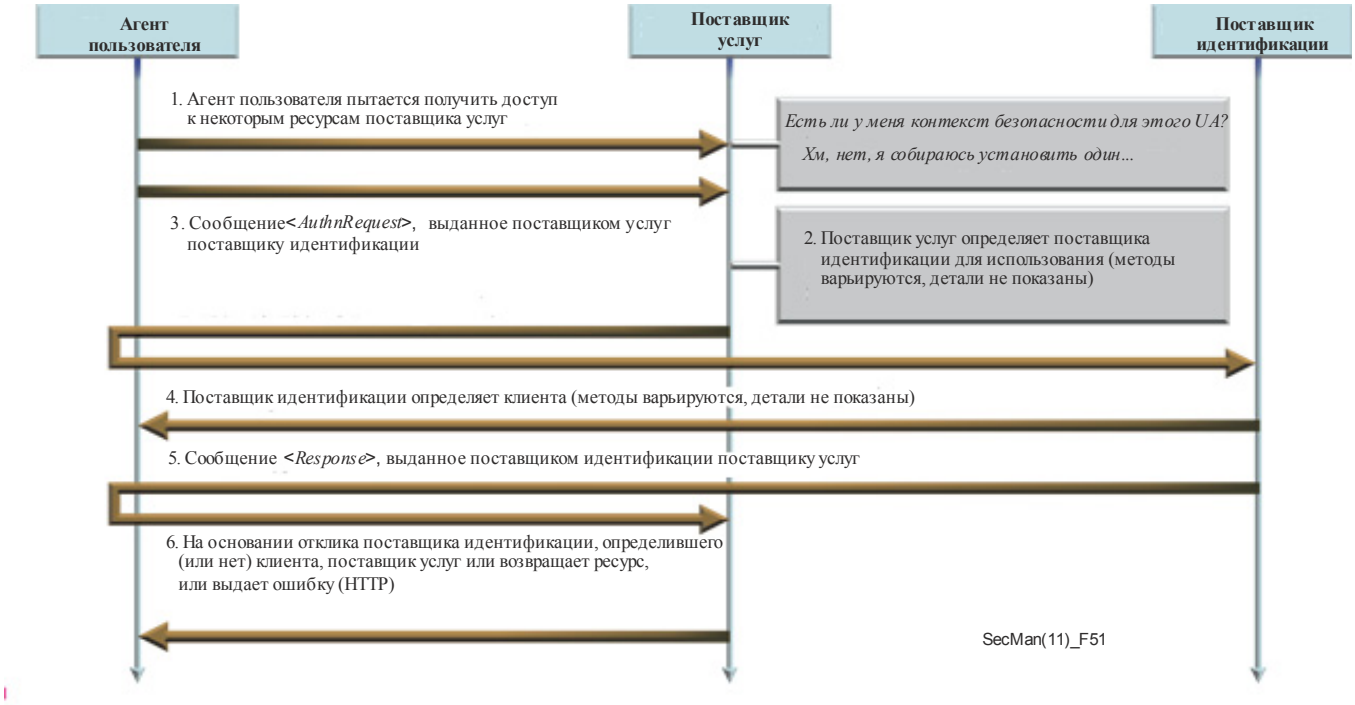


Рисунок 51 – Основной шаблон для получения SSO

10.4.2 Расширяемый язык разметки контроля доступа

Расширяемый язык разметки контроля доступа (XACML) является словарем XML для выражения стратегии управления доступом. Управление доступом заключается в принятии решения относительно удовлетворения запрашиваемого доступа к ресурсу и осуществления этого решения. В Рекомендации МСЭ-Т X.1142 определяется основа XACML, включая синтаксис языка, модели, контекст с моделью языка стратегии, правила синтаксиса и обработки информации. Для повышения безопасности при обмене стратегией на основе XACML в МСЭ-Т X.1142 также устанавливается профиль цифровой подписи XML языка XACML для организации защиты данных. Профиль секретности устанавливается с целью предоставления руководящих указаний для средств реализации. XACML подходит для разных условий применения.

10.5 Услуги на основе маркеров

В настоящее время широко распространены идентификационные маркеры (включая маркеры RFID), но беспокойство касательно риска нарушения конфиденциальности неуклонно растет. Отчасти это происходит из-за того, что технология RFID может автоматически собирать и обрабатывать данные, и существует риск преднамеренного или случайного раскрытия уязвимой и/или личной информации.

Для приложений, которые используют или опираются на идентификацию на основе маркеров в приложениях, которые включают личную информацию, например здравоохранение, паспорта и водительские удостоверения, вопрос конфиденциальности все больше становится серьезной проблемой.

В академических институтах и промышленности большинство попыток создания механизма защиты для информации, позволяющей установить личность (PII), было сосредоточено на протоколах аутентификации между маркером идентификации и терминалом получения ID. Однако эти попытки не охватывают вопрос полностью, так как значимая информация об идентификаторе все еще существует на сервере в сетевом домене. Одним из решений этой проблемы является использование механизма защиты PII на основе профиля.

В Рекомендации МСЭ-Т X.1171 исследуются угрозы для PII в среде, основанной на принципе "бизнес для потребителя" (B2C), в которой приложения используют идентификацию на основе маркеров. Она определяет требования к защите PII в таких условиях и создает защиту PII на основе определенного пользователем профиля правил PII.

Приложения отношений бизнеса и потребителя (B2C), использующие идентификацию на основе маркеров, могут быть разделены на три типа.

a) *Пользователь устройства как потребитель*. В этом типе службы потребитель получает информацию при помощи мобильного устройства для чтения. На рисунке 52 показана базовая модель приложения данного типа. Она состоит из двух основных сетевых операций: распознавание идентификатора и получение контента. Распознавание идентификатора является процедурой перевода или превращения идентификатора в адрес. Подвижной терминал со считывающим устройством сначала преобразует идентификатор после его получения от маркера ID при помощи услуги каталогизации, а затем осуществляет получение контента из сети.

Рисунок 52 – Основная модель применения B2C при помощи идентификации на основе меток

b) *Пользователь маркера ID как потребитель*. Типичный пример данного применения B2C при помощи идентификации на основе маркера имеет дело с управлением доступом и/или аутентификацией, например проверкой входа, паспортом, лицензией или службой постпродажного управления. В этом типе применения устройства для чтения могут быть встроены в фиксированные или подвижные терминалы. Для получения услуги потребитель представляет маркер ID (например, в паспорте или в билете).

c) *Потребитель как пользователь и маркера ID, и устройства*. В услуге получения информации о продукте потребитель также становится пользователем маркера после приобретения продукта с маркером и после изучения содержания информации о продукте на его/ее подвижном терминале. В другом примере можно рассмотреть услугу, относящуюся к здравоохранению, которая запускается картой пациента, позволяющей наносить маркеры ID. В данном приложении существует много типов потребителей, которые могут быть пользователями маркеров ID (например, пациент, врач, медицинская сестра). Пользователь маркера ID может просматривать записи пациента в его/ее медицинской карте, позволяющей наносить маркеры ID при помощи устройства для чтения на подвижном терминале.

Для приложений B2C, которые используют идентификацию на основе маркеров, существует два основных риска нарушения PII.

- Утечка информации, связанной с идентификатором. В данном примере атакующий может прочесть информацию от маркера ID, а пользователь помеченного продукта не будет знать об этом. Сначала атакующий считывает идентификатор с маркера ID, которую несет пользователь. Затем он/она преобразует идентификатор и запрашивает от услуги каталогизации данные о местоположении информации. Наконец, атакующий запрашивает информацию, соответствующую маркеру ID.

- Утечка данных исторического контекста. Атакующий может извлечь данные пользователя (например, предпочтения, привычки, области интереса и пр.) из данных исторического контекста, связанных с маркером ID. Атакующий может использовать эти данные для незаконных или коммерческих целей без согласия пользователя.

В МСЭ-Т X.1171 описаны следующие технические требования для защиты от нарушений PII в приложениях B2C.

- *Управление PII пользователем маркера ID*. Пользователь маркера ID должен уметь управлять или обновлять PII, связанный с его/ее маркером ID в сети. Таким образом, пользователь маркера ID может определить, какой PII следует удалить или оставить в приложении.
- *Аутентификация для пользователя маркера ID и/или пользователя устройства*. Для проведения процедур аутентификации в отношении пользователя маркера ID необходим сервер приложений, и сервер приложений при необходимости может обеспечить процедуру аутентификации в отношении пользователя устройства (некоторым приложениям, использующим идентификацию на основе маркера, не обязательно аутентифицировать пользователя).
- *Управление доступом к PII пользователя маркера ID в сервере приложений*. Для управления доступом к важной информации, связанной с PII пользователя маркера ID, необходим сервер приложений.
- *Конфиденциальность данных информации, связанной с маркером ID.* Для обеспечения конфиденциальности данных необходим сервер приложений, чтобы гарантировать, что информация, относящаяся к маркеру ID, не могла быть прочитана неавторизованными пользователями.
- *Согласие на сбор данных в журнале, событий, относящихся к пользователю устройства*. Сервер приложений может обеспечить процедуру согласия для сбора данных в журнале событий, относящихся к пользователю устройства, если этот тип сбора данных журнала событий необходим для приложения.

Следующий пример иллюстрирует услугу защиты PII (PPS) на основе пользовательского профиля политики PII. Сценарий услуги для PPS обычно происходит из процедуры персонализации маркера, например приобретения продукта с маркером. На рисунке 45 показан общий поток услуг PPS-приложения, использующего идентификацию на основе маркера.

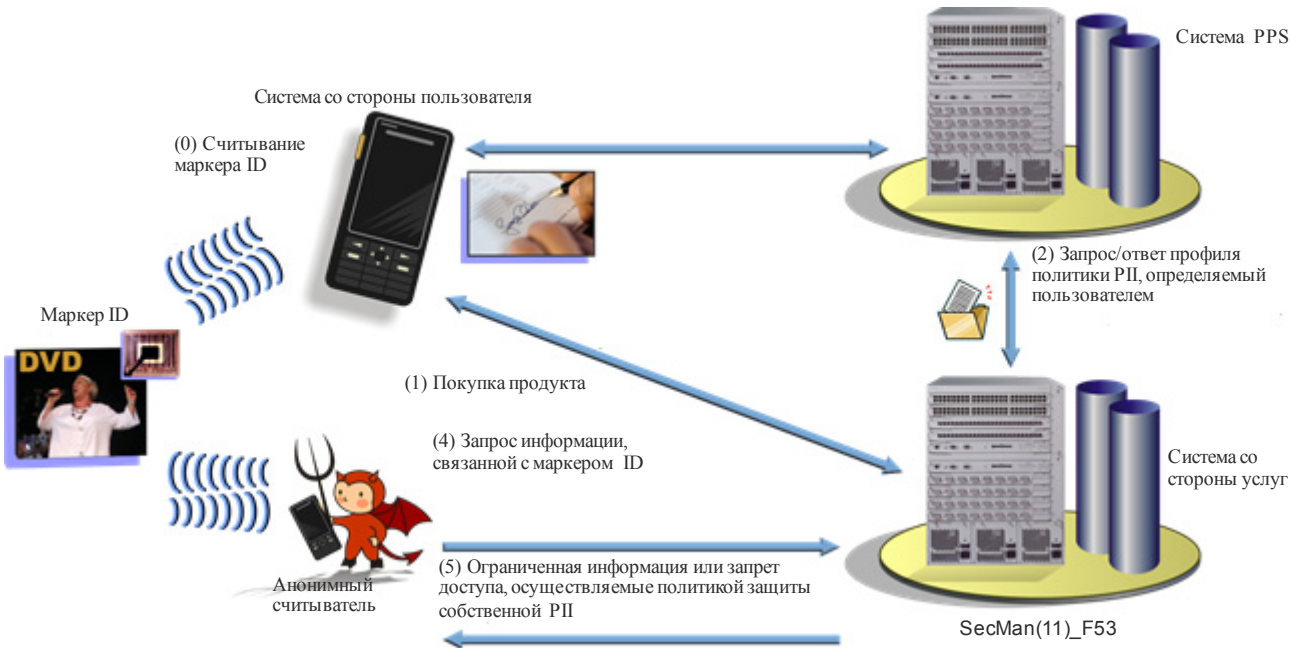


Рисунок 53 – Общий поток услуги для услуги защиты PII (PPS)

1) Потребитель считывает идентификатор продукта с маркером при помощи его/ее подвижного терминала со считывающим устройством.
2) Потребитель изучает относящуюся к продукту информацию в сети обслуживания приложений и затем приобретает продукт при помощи одного из нескольких методов оплаты. В этот момент потребитель становится пользователем маркера ID.
3) Приложение, использующее идентификацию на основе маркеров, затем запрашивает у системы PPS определяемый пользователем профиль политики PII, который соответствует определенному пользователем профилю PII для приложения.
4) Система PPS получает пользовательский профиль политики защиты PII для данного приложения.
5) Любой может запросить информацию, связанную с этим маркером ID, у обслуживающей системы.
6) Запрашивающий может изучить всю представленную обслуживающей системой информацию, если запрашивающий является пользователем маркера ID. В противном случае запрашивающий или не может получить доступ к любой информации, или может получить только ограниченную информацию.

11. Противодействие общим сетевым угрозам

11 Противодействие общим сетевым угрозам

Угрозы компьютерным системам и сетям, которые их связывают, многочисленны и разнообразны. Хотя множество атак могут быть начаты локально, подавляющее большинство атак на сегодняшний день осуществляются при помощи сетей связи. Тот факт, что большое и постоянно растущее количество компьютеров и сетевых устройств подключено к интернету и управляются в домах и на рабочих местах людьми с небольшими опытом, осведомленностью или знаниями о безопасности IT, в значительной степени увеличивает простоту и вероятность дистанционных, зачастую беспорядочных атак. Постоянно растет количество спама, шпионского программного обеспечения, вирусов и других средств осуществления атак. Атакующие часто надеются на слабо и недостаточно защищенные системы в качестве проводников их вредоносного программного обеспечения.

В данном разделе представлен обзор работы МСЭ-Т для ответа на некоторые из этих угроз.

11.1 Спам

Спам – это незатребованное, нежелательное или потенциально вредное сообщение. Хотя наиболее известной формой спама является спам в электронной почте, этот термин применяется также к другим формам, таким как спам при обмене мгновенными сообщениями, спам при обмене сообщениями в подвижной связи и спам VoIP. На самом деле смысловое значение данного термина развивается и расширяется с развитием технологий, которые предоставляют новые возможности для создания спама. Спам признается широкораспространенной проблемой, которая мешает законным действиям операторов электросвязи, поставщиков услуг и пользователей. Спам занимает ширину полосы и циклы обработки, в крайних случаях он приводит к отклонению атак услуг сетей массовой рассылки. Ни одна мера противодействия спаму не эффективна сама по себе и, учитывая быстроту и изобретательность спамеров, даже комбинация мер часто эффективна только в отношении снижения уровня спама. Примеры использованных мер включают регулирование, технические меры, международное сотрудничество и обучение пользователей и поставщиков интернет-услуг.

11.1.1 Технические стратегии в деле противостояния спаму

Работа МСЭ-Т в области борьбы со спамом концентрируется в основном на технических мерах противодействия. Разрабатываются Рекомендации с использованием структуры, которая предусматривает возможность расширения, как показано на рисунке 54.

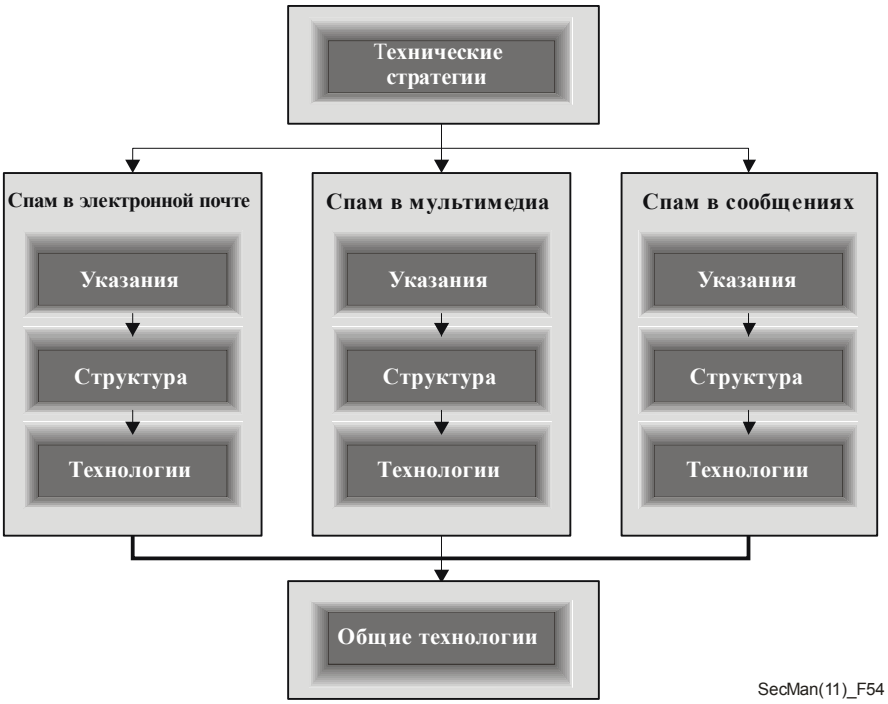


Рисунок 54 – Структура стандартизации для противодействия спаму

В Рекомендации МСЭ-Т X.1231 установлены требования для борьбы со спамом, и она служит точкой начала работы. В данной Рекомендации описаны разные типы спама и его общие характеристики и содержится обзор технических подходов к противодействию спаму. Также в ней предлагается общая модель, которая может использоваться для создания эффективной стратегии борьбы со спамом.

Эта модель является иерархической и имеет пять стратегий, распределенных по трем уровням. Взаимосвязи между стратегиями показаны на рисунке 55. Эта модель указывает, что существует высокая степень взаимосвязи между стратегиями, но что соображения затрат могут помешать использованию всех стратегий в отдельных случаях. Также необходима ориентация на потребителя в соответствии с конкретным сценарием применения.

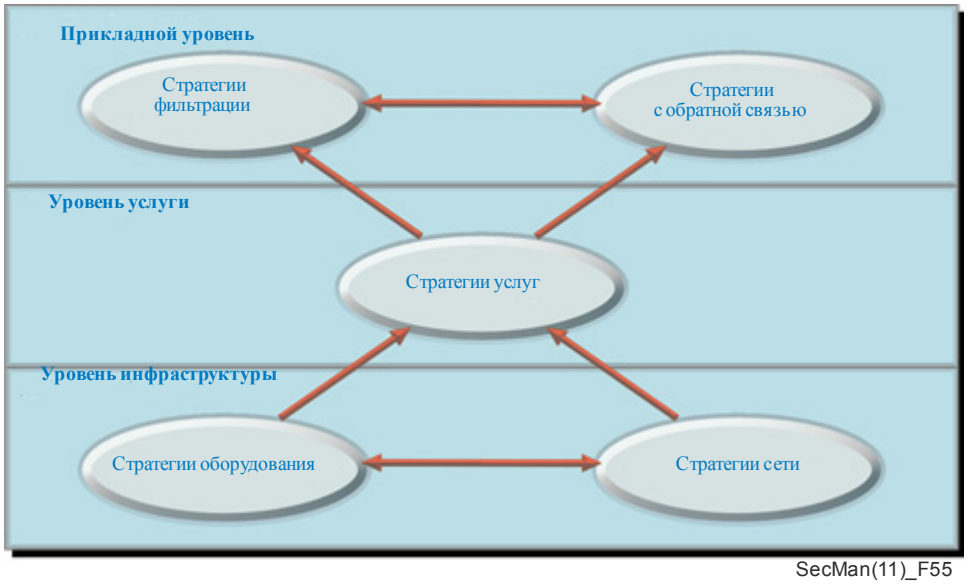


Рисунок 55 – Общая модель противодействия спаму

11.1.2 Спам в электронной почте

Самой известной формой спама является спам в электронной почте. Он представляет собой комплексную техническую проблему, и решения для его устранения должны поддерживаться соответствующими техническими мерами. Хотя действия правительства и законодательство полезны, их недостаточно, чтобы устранить проблемы, возникающие из-за спама в электронной почте. Вопрос осложняется из-за трудности в определении спамера, когда используется протокол SMTP.

Две Рекомендации предназначены помочь в противодействии спаму в электронной почте. Рекомендация МСЭ-Т X.1240 адресована пользователям, которые желают принять технические решения для противодействия спаму в электронной почте. В ней определены основные концепции, характеристики, эффекты и технические вопросы, связанные с противодействием спаму в электронной почте. Также в ней указаны существующие технические решения и соответствующие действия организаций по разработке стандартов и других групп, работающих над противодействием спаму в электронной почте.

В Рекомендации МСЭ-Т X.1241 описана рекомендованная структура домена обработки для борьбы со спамом и определены функциональные возможности основных модулей в домене. Эта структура устанавливает механизм, при помощи которого различные серверы электронной почты могут делиться информацией о спаме в электронной почте. Она направлена на содействие расширению сотрудничества между поставщиками услуг в борьбе со спамом. В частности она содержит структуру для создания методики связи для оповещения об обнаруженном спаме. Другой документ, *Дополнение 6* к *Рекомендациям МСЭ-Т серии X*, рассматривает международные форумы, где обсуждалась проблема спама и включает ситуационное исследование.

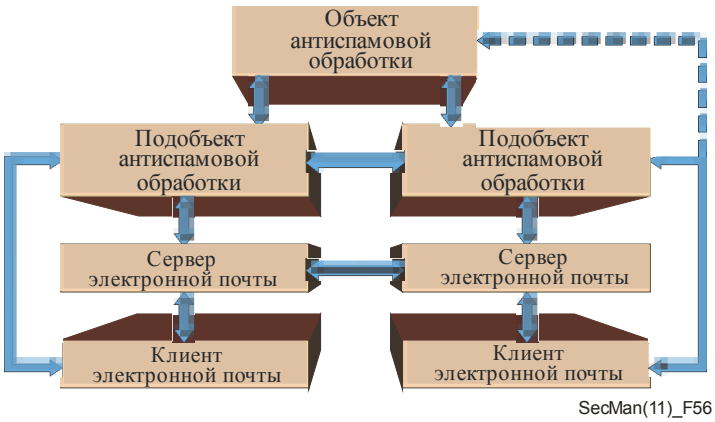


Рисунок 56 – Общая структура домена обработки для борьбы со спамом

На рисунке 56 показаны процессы структуры Рекомендации МСЭ-Т X.1241. Объект обработки для борьбы со спамом расположен в независимой системе, а подобъекты обработки для борьбы со спамом расположены у одного или нескольких поставщиков услуг электронной почты. Объект обработки доставляет новые правила подобъектам, которые должны проверить и уточнить правила. Также существует функция разрешения любых противоречий в правилах.

11.1.3 IP-мультимедийный спам

В Рекомендации МСЭ-Т X.1244 определены основные концепции, характеристики и технические вопросы, связанные с противодействием спаму в IP-мультимедийных приложениях, например IP-телефонии и службе мгновенных сообщений. Различные типы спама в IP-мультимедийных приложениях классифицированы и описаны в соответствии с их характеристиками. Этот стандарт описывает разные угрозы безопасности со стороны спама, которые могут стать причиной IP-мультимедийного спама, и определяет аспекты, которые должны учитываться для противодействия такому спаму. Некоторые технологии, разработанные для управления спамом в электронной почте, также могут использоваться для противодействия спаму в IP-мультимедийных приложениях. В Рекомендации МСЭ-Т X.1244 анализируются традиционные механизмы противодействия спаму и обсуждается их применимость для борьбы со спамом в IP-мультимедийных приложениях.

Технологии борьбы со спамом для IP-мультимедийного спама могут применяться в соответствии с конкретными характеристиками спама. В таблице 8 приведена классификация, используемая в Рекомендации МСЭ-Т X.1244.

Таблица 8 – Классификация спама в IP-мультимедийных приложениях

	Текст	**Голос**	**Видео**
В реальном времени	• Спам в службе мгновенных сообщений • Спам в чатах	• Спам в VoIP • Спам в службе мгновенных сообщений	• Спам в службе мгновенных сообщений
Не в реальном времени	• Спам в текстовых/ мультимедийных сообщениях • Текстовый спам в P2P-службе совместного пользования файлом • Текстовый спам на веб-сайте	• Спам в голосовых/ мультимедийных сообщениях • Голосовой спам в P2P-службе совместного пользования файлом • Голосовой спам на веб-сайте	• Спам в видео/ мультимедийных сообщениях • Видеоспам в P2P-службе совместного пользования файлом • Видеоспам на веб сайте

В Рекомендации МСЭ X.1245 представлена общая структура противодействия спаму в мультимедийных IP-приложениях, таких как IP-телефония, передача мгновенных сообщений и мультимедийная конференция.

На рисунке 57 показана структура противодействия спаму в мультимедийных приложениях на основе IP. Данная структура состоит из четырех функций противодействия спаму, т. е. базовые функции противодействия спаму (CASF), функции противодействия спаму на стороне получателя (RASF), функции противодействия спаму на стороне отправителя (SASF) и функции получателя спама (SRF). В настоящей Рекомендации описываются функциональные возможности и интерфейсы каждой функции, служащие для противодействия мультимедийному IP-спаму.

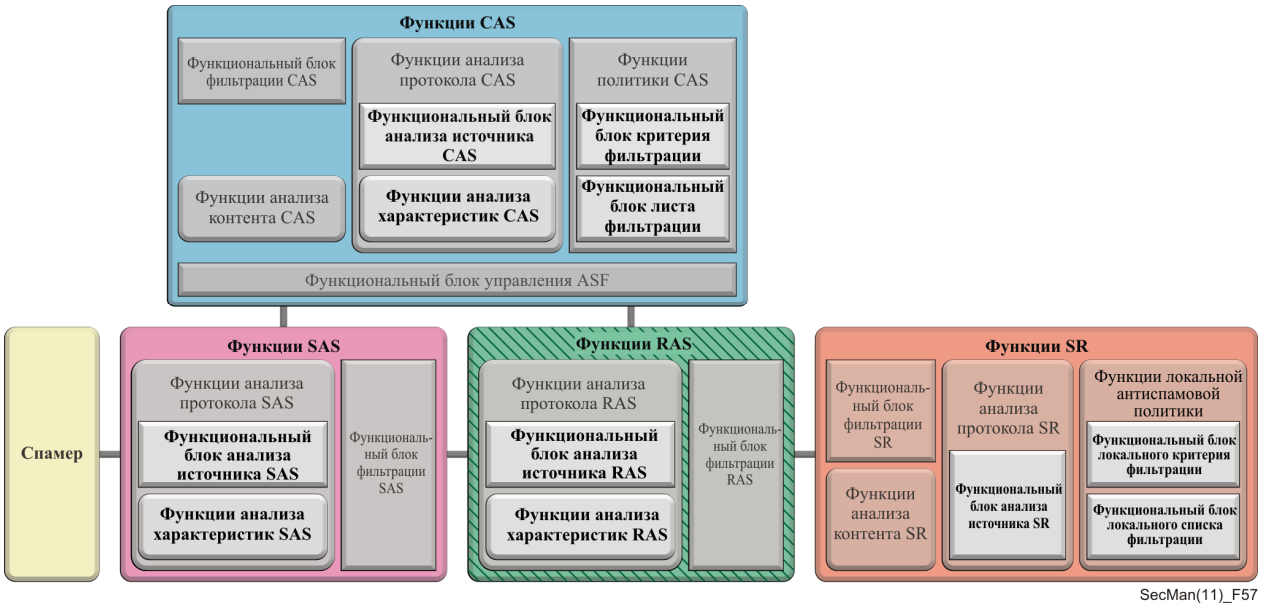


Рисунок 57 – Структура противодействия мультимедийному IP-спаму

В Дополнении 11 к Рекомендациям МСЭ-Т серии X описывается техническая структура, основанная на RBL, для противодействия спаму в VoIP. На рисунке 58 показаны четыре функциональных объекта для противодействия спаму в VoIP: система предупреждения спама в VoIP (VSPS), сервер политики предупреждения спама в VoIP (VSPPS), центральная система RBL для предупреждения спама в VoIP (VSP-RBL) и система репутации пользователя (URS). В этом Дополнении также приводятся функциональные возможности, процедуры и интерфейсы каждого функционального объекта для противодействия спаму в VoIP.

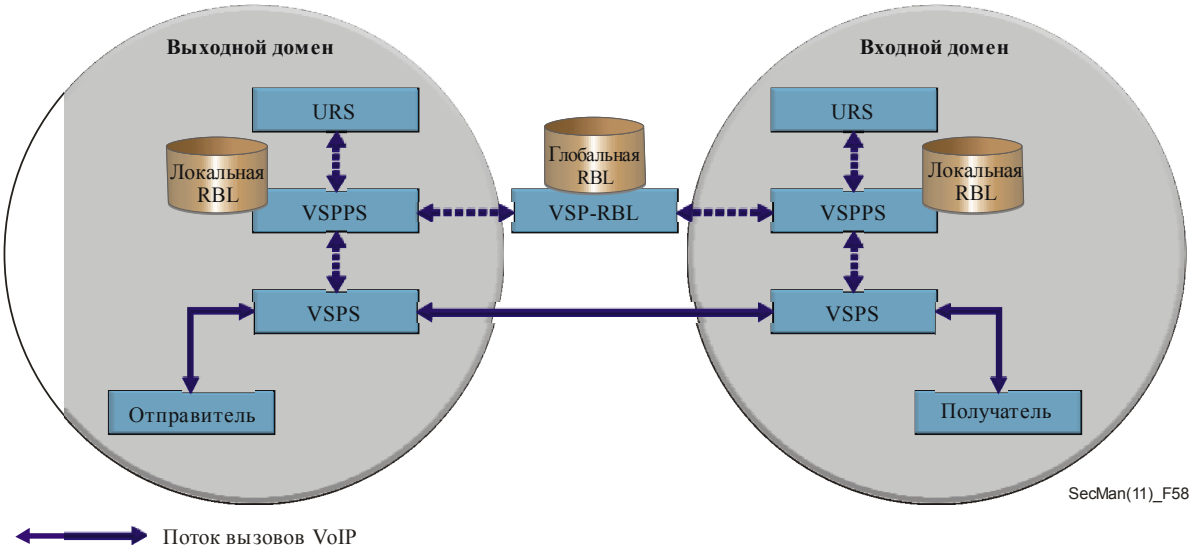


Рисунок 58 – Функциональная архитектура для противодействия спаму в VoIP

11.1.4 Спам при передаче мобильных сообщений

Спам при передаче мобильных сообщений включает как спам в *службе коротких сообщений* (SMS), так и спам в *службе мультимедийных сообщений* (MMS). В Рекомендации МСЭ-Т X.1242 определяются структура и функции системы фильтрации спама в SMS наряду с управлением услугой пользователям, протоколами связи и базовыми функциональными требованиями к оконечным устройствам с функциями SMS. Определяются методы, с помощью которых пользователи могут управлять (запрашивать, удалять и восстанавливать) отфильтрованные короткие сообщения. Правила фильтрации могут быть основаны на таких характеристиках, как адрес, номер телефона, время или содержание. Требования к программному обеспечению оконечных устройств, поддерживающих фильтрацию спама в SMS, содержатся в Дополнении к Рекомендации МСЭ-Т X.1242.

11.1.5 Система интерактивных шлюзов для противодействия спаму

Сотрудничество в сфере технологий признано в качестве ключевой составляющей в системе противодействия спаму. В Рекомендации МСЭ-Т X.1243 показывается такая система и определяются технические средства для противодействия междоменному спаму. Система шлюзов позволяет осуществлять оповещение о спаме в разных доменах и препятствует прохождению трафика спама из одного домена в другие. Дополнительно в настоящей Рекомендации определяется архитектура системы шлюзов, описываются основные элементы, протоколы и функции системы шлюзов и предлагаются механизмы для определения спама, совместного использования информации и особых действий для противодействия спаму.

11.2 Вредоносный код, шпионское и заведомо ложное программное обеспечение

Самому большому риску системы и сети подвергаются, вероятно, со стороны вредоносных кодов (вирусов, "червей", троянов и пр.), но шпионское и другое заведомо ложное программное обеспечение (например, программное обеспечение, которое осуществляет несанкционированные действия) также создает значительный риск. Если организации и частные лица внедряют ряд упреждающих мер (включая брандмауэры, антивирусные меры и меры борьбы со шпионским программным обеспечением) против этих угроз, то компромисс

практически гарантирован. Однако доступные меры противодействия разнятся по эффективности и не всегда дополняют друг друга.

Регуляторные органы во многих странах все чаще требуют от поставщиков услуг гарантий, касающихся мер по безопасности и защите, которые они предпринимают, и требуют, чтобы поставщики услуг делали еще больше, чтобы помочь пользователям добиться безопасного и защищенного пользования интернетом.

В Дополнении 9 к Рекомендациям МСЭ-Т серии X приведены руководящие указания по сокращению количества вредоносных программных средств в сетях ИКТ.

Рекомендация МСЭ-Т X.1207 является стандартом для:

a) предоставления примеров передового опыта, касающегося четких указаний, согласия пользователей и управления пользователем услугами веб-хостинга; и

b) предоставления примеров передового опыта по безопасности (посредством поставщиков услуг электросвязи) домашним пользователям для безопасного и защищенного использования персонального компьютера и интернета.

Рекомендация МСЭ-Т X.1207 дает четкие руководящие указания поставщикам услуг по безопасному управлению рисками, применению защищенных и безопасных продуктов, наблюдениям за сетью и откликам, поддержке, своевременному обновлению и безопасному веб-хостингу. Даются советы по руководящим указаниям пользователям, обучению и техническим защитным мерам для конечных пользователей. В самостоятельном дополнении приведены ссылки на дополнительные материалы по ресурсам.

11.3 Уведомление и распространение обновлений программного обеспечения

Вредоносный код может распространяться с пугающей скоростью, и даже имея защитные меры по последнему слову техники, новые угрозы могут распространяться так быстро, что системы и сети, не имеющие новейших обновлений, весьма уязвимы. Также системы особенно уязвимы для взлома "нулевого дня" (т. е. новых, неизвестных до сего момента угроз, для которых пока еще не разработано антивирусных ключей или патчей). В таких условиях важны своевременные распространение и установка обновлений. Однако существует множество проблем, связанных с распространением и внедрением этих обновлений.

Большая часть серийно выпускаемого программного обеспечения, включая операционные системы и системы обеспечения безопасности (антивирусы, противошпионское программное обеспечение, брандмауэры и т. п.), имеет функцию, позволяющую выполнять автоматическое обновление. Однако это должен разрешить пользователь. Когда пользователю просто указывается, что доступны обновления (или, вероятно, что обновления загружены), этот пользователь должен предпринять действия, чтобы разрешить загрузку и/или установку обновлений. Многие обновления требуют перезагрузки системы после установки, что отдельные пользователи могут делать или не делать сразу же. Организации с хорошо управляемой программой безопасности обычно централизованно управляют обновлением, принудительно обновляя системы конечных пользователей. И наоборот, обновление личных систем (например, домашних компьютеров) и обновления в небольших организациях обычно происходит достаточно бессистемно.

Другой проблемой регулярного обновления является то, что поставщики программного обеспечения не применяют последовательных действий для оповещения пользователей о том, что обновления доступны, или для сообщения пользователям о возможных последствиях отказа от установки обновлений. Кроме того, у них нет единообразного способа оповещения пользователей о новейших примерах передового опыта в поддержании безопасности программного обеспечения. Кроме того, не существует надежного метода оповещения о проблемах, замеченных пользователями, и последующего внедрения обновлений.

В Рекомендации МСЭ-Т X.1206 обсуждаются трудности, связанные с поддержанием программного обеспечения в соответствии с современными требованиями и предоставления независимого от производителя способа решения этих проблем. Как только зарегистрирован ресурс, автоматически для пользователя или напрямую для приложения могут быть доступны обновления информации об уязвимости и вставки или обновления в программу. В Рекомендации МСЭ-Т X.1206 предложена структура, которую каждый поставщик может использовать для оповещения, а также для предоставления информации об уязвимости и распространения необходимых вставок/обновлений в программу. Также в ней определяется формат информации, который должен применяться в компонентах и между ними.

МСЭ-Т X.1206 позволяет системным администраторам узнавать о состоянии любого ресурса, за который они отвечают. В ней описываются проблемы технического обслуживания ресурса с точки зрения идентификации ресурса, а также с точки зрения распространения информации и управления системой/сетью. Также представлено описание безопасности, которая должна учитываться в независимой от поставщика структуре.

Определения структур данных в отношении компонентов, которые необходимы для этой работы, включая соответствующие схемы XML, представлены в Рекомендации МСЭ-Т X.1206 вместе с форматом информации, который должен применяться в компонентах и между ними при реализации этой структуры.

12. Будущее стандартизации безопасности ИКТ

12 Будущее стандартизации безопасности ИКТ

В 1865 году МСЭ учредил Международный телеграфный союз. Хотя его первой областью изучения был телеграф, в настоящее время работа МСЭ охватывает весь сектор ИКТ – от цифрового вещания до интернета и от технологий подвижной связи до телевидения 3D. В последние годы разработка стандартов ИКТ значительно ускорилась на фоне быстрого роста использования интернета и других сетей и понимания необходимости защиты пользователей и систем от растущего числа и разнообразия угроз безопасности.

В этом Руководстве представлен широкий обзор некоторых ключевых инициатив и достижений Исследовательских комиссий МСЭ-Т, связанных с безопасностью, и делается попытка содействовать большему пониманию работы и возникающих технических проблем, стоящих перед пользователями и создателями сетей. Читателей поощряют использовать преимущества обширных онлайновых ресурсов МСЭ-Т для получения подробной информации по вопросам, представленным здесь, и использовать документы Рекомендаций и руководящих указаний для помощи в создании более безопасного онлайн-окружения и повышения уверенности пользователя в действиях в онлайн-среде.

Если заглянуть в будущее, то сети электросвязи и компьютерные сети будут продолжать сближаться. Сети и приложения по предоставлению услуг на веб-основе продолжат быстрый рост и станут все более значимыми, но угрозы продолжат развиваться и останутся постоянной проблемой, требующей создания и развития эффективных мер противодействия этим угрозам. Также будет необходимо создать лучшее, более безопасное устройство и реализацию систем и сетей так, чтобы снизить им присущие уязвимости. При этом возможности глобального сообщества по электросвязи/ИКТ в плане реагирования на угрозы и ослабления их влияния повысятся в случае совместного использования информации об угрозах, о чем свидетельствует наша работа по обмену информацией о кибербезопасности.

193 Государства-Члена и примерно 700 членов Секторов МСЭ будут продолжать реагировать на эти проблемы, не переставая разрабатывать технические Рекомендации и руководящие указания по безопасности в насыщенной программе работ, которая основывается на потребностях членов и управляется организационной структурой, созданной на Всемирной ассамблее по стандартизации электросвязи. Когда это возможно, во избежание дублирования попыток МСЭ-Т будет сотрудничать с другими организациями по разработке стандартов для получения гармонизированных и максимально эффективных и оперативных решений.

13. Источники дополнительной информации

13 Источники дополнительной информации

В этом Руководстве представлен широкий обзор совместной работы МСЭ-Т в области безопасности. Более подробная информация, включая многие стандарты, находится в свободном доступе на веб-сайте МСЭ-Т.

13.1 Обзор работы ИК17

В качестве первого шага на домашней странице ИК17 МСЭ-Т представлены ссылки на информацию о работе ИК17, включая руководства и презентации, обзоры разрабатываемых Рекомендаций, и основном персонале. Ссылки на ведущую Исследовательскую комиссию по безопасности электросвязи и ведущую Исследовательскую комиссию по управлению определением идентичности (IdM) дают информацию о деятельности и результатах работы этих двух ведущих Исследовательских комиссий.

13.2 Сборник по безопасности

Этот Сборник содержит сведения о Рекомендациях МСЭ, связанной с ними информации и деятельности МСЭ по безопасности. Он состоит из пяти частей, каждую из которых можно загрузить:

- каталог утвержденных Рекомендаций, относящихся к безопасности электросвязи, который включает Рекомендации, предназначенные для целей безопасности, и Рекомендации, описывающие или использующие функции, относящиеся к интересам и потребностям в области безопасности;
- список утвержденных МСЭ-Т определений в области безопасности, взятых из утвержденных Рекомендаций МСЭ-Т;
- обзор Исследовательских комиссий МСЭ-Т, осуществляющих виды деятельности, относящиеся к безопасности;
- обзор рассматриваемых Рекомендаций в рамках Исследовательских комиссий МСЭ-Т по вопросу безопасности;
- обзор других видов деятельности МСЭ по безопасности.

13.3 Дорожная карта по стандартам безопасности

Дорожная карта по стандартам безопасности является онлайновым ресурсом, предоставляющим информацию о существующих стандартах безопасности ИКТ и ведущейся работе в ключевых организациях по разработке стандартов. В дополнение к информации о работе МСЭ-Т в области безопасности, дорожная карта содержит информацию по работе над стандартами безопасности ИСО/МЭК, ATIS, ENISA, ETSI, IEEE, IETF, OASIS, 3GPP и 3GPP2.

Дорожная карта состоит из шести частей, а информация напрямую доступна в режиме онлайн.

Часть 1. *Организации по разработке стандартов ИКТ и их работа*, которая содержит информацию о структуре дорожной карты и о каждой из перечисленных организаций по разработке стандартов. В части 1 также представлены ссылки на существующие глоссарии и словари по безопасности.

Часть 2. *Утвержденные стандарты безопасности ИКТ*, которая содержит базу данных (с возможностями поиска) утвержденных стандартов безопасности с прямыми ссылками на большинство стандартов.

Часть 3. *Разрабатываемые стандарты безопасности*.

Часть 4. *Потребности в будущем и предложенные новые стандарты безопасности*.

Часть 5. *Примеры передового опыта по безопасности*.

Часть 6. *Ситуация по управлению определением идентичности (IdM): стандарты, организации и сравнительный анализ данных по IdM*.

13.4 Руководящие указания по внедрению систем безопасности

В Дополнении 3 к Рекомендациям МСЭ-Т серии X представлены более подробные основные положения по некоторым вопросам, обсуждаемым в данном Руководстве, и предложены руководящие указания для реализации системы и сети безопасности, которые могут использоваться для реализации программы безопасности сети. Эти руководящие указания направлены на четыре области: технические правила безопасности; идентификация ресурсов; угрозы, уязвимости и смягчение последствий; а также оценка безопасности. Руководящие указания отражают ключевые компоненты, необходимые для создания и управления технической политикой, необходимой для управления сетями, возможно, объединяющих множество операторов и содержащих продукцию и системы множества поставщиков. Также представлены руководящие указания по регуляторным вопросам.

13.5 Дополнительная информация по каталогу

Что касается более подробной информация о Рекомендациях МСЭ-Т серии X, то санкционированным источником информации являются сами Рекомендации МСЭ-Т серии X. Дополнительная методическая информация и Руководящие указания для реализующего объекта содержатся по адресу: www.x500standard.com. По следующим ссылкам можно найти дополнительную информацию:

Информацию об аутентификации пользователей можно найти по адресу:
http://www.x500standard.com/index.php?n=X509.X509ProtectingDirectory.

Информация об управлении доступом содержится по адресу:
http://www.x500standard.com/index.php?n=X500.AccessControl.

Более подробное описание характеристик персональных данных согласно МСЭ-Т X.500 доступно по адресу:
http://www.x500standard.com/index.php?n=X500.DataPrivacyProtection.

Онлайновый учебный материал по МСЭ-Т X.500 доступен по адресу:
http://www.x500standard.com/index.php?n=Participate.Tutorial.

Белые книги МСЭ-Т X.500 доступны по адресу:
http://www.x500standard.com/index.php?n=Participate.Whitepapers.

Приложение А
Определения в области безопасности

Приложение А

Определения в области безопасности

Следующая таблица содержит определения терминов, использованных в данном Руководстве. Все определения взяты из существующих Рекомендаций МСЭ-Т. Более полный список определений содержится в перечне утвержденных МСЭ-Т определений в области безопасности, который ведется 17-й Исследовательской комиссией.

Термин (англ.)	Термин	Определение	Ссылка
Access control	Управление доступом	1. Предотвращение несанкционированного использования ресурса, в том числе предотвращение использования ресурса неразрешенным образом 2. Ограничение потока информации от ресурсов системы только информацией от уполномоченных лиц, программ, процессов и других системных ресурсов сети	МСЭ-Т X.800 МСЭ-Т J.170
Access control list	Список для управления доступом	Список объектов, имеющих полномочия на получение доступа к ресурсу, и их прав доступа	МСЭ-Т X.800
Access control policy	Правила управления доступом	Набор правил, которые определяют условия, при которых доступ может иметь место	МСЭ-Т X.812
Accidental threats	Случайные угрозы	Угрозы, не связанные с умышленным намерением. Примеры известных случайных угроз включают нарушения работы системы, грубые эксплуатационные ошибки и ошибки в программном обеспечении	МСЭ-Т X.800
Accountability	Отчетность	Свойство, гарантирующее, что действия объекта могут отслеживаться с однозначной привязкой к конкретному объекту	МСЭ-Т X.800
Algorithm	Алгоритм	Математический процесс, который может использоваться для скремблирования и дескремблирования потока данных	МСЭ-Т J.93
Attack	Атака	Действия, предпринимаемые в целях обхода механизмов обеспечения безопасности системы или в целях использования их недостатков. При непосредственном злонамеренном воздействии на систему используются недостатки базовых алгоритмов, принципов или свойств механизма обеспечения безопасности. Косвенные злонамеренные воздействия предпринимаются путем обхода механизма безопасности или принуждения системы к неправильному использованию этого механизма	МСЭ-Т H.235
Attribute	Атрибут	В контексте обработки сообщений – единица информации, компонент списка атрибутов, который описывает пользователя или список рассылки и который может также обнаружить его в зависимости от физической или организационной структуры системы обработки сообщений (или лежащей в ее основе сети)	МСЭ-Т X.400
Attribute Authority (AA)	Орган по присвоению атрибутов	1. Орган, который назначает привилегии путем выдачи сертификатов атрибутов 2. Объект, которому один или несколько объектов доверяют создание и подпись сертификатов атрибутов. ПРИМЕЧАНИЕ. – Сертифицирующий орган может быть также органом по присвоению атрибутов	МСЭ-Т X.509 МСЭ-Т X.842
Attribute certificate	Сертификат атрибута	Структура данных, имеющая цифровую подпись органа по присвоению атрибутов, которая связывает некоторые	МСЭ-Т X.509

Термин (англ.)	Термин	Определение	Ссылка
		значения атрибутов с идентификационной информацией о держателе этого атрибута	
Authentication	Аутентификация	1. Процесс подтверждения идентификации. ПРИМЕЧАНИЕ. – См. Администратор доступа и Верификатор и две отличительные формы аутентификации (аутентификация источника данных + аутентификация объекта). Аутентификация может быть односторонней или взаимной. Односторонняя аутентификация обеспечивает уверенность в идентификации только одного администратора доступа. Взаимная аутентификация обеспечивает уверенность в идентификации обоих администраторов доступа 2. Обеспечение уверенности в заявленной идентификации объекта 3. См. Аутентификация источника данных и Аутентификация одноранговых объектов. Термин "аутентификация" не используется применительно к целостности данных; вместо него используется термин "целостность данных" 4. Подтверждение идентификации объектов, относящихся к установлению ассоциаций. Например, они могут быть прикладными объектами, прикладными процессами и человеком – пользователем приложений. ПРИМЕЧАНИЕ. – Данный термин был определен для разъяснения того, что рассматривается более широкая сфера аутентификации, по сравнению с аутентификацией одноранговых объектов из Рекомендации (МККТТ) МСЭ-Т X.800 5. Процесс проверки идентификационной информации, предъявленной одним объектом другому объекту 6. Процесс, предназначенный для предоставления возможности системе проводить достоверную проверку идентификации стороны	МСЭ-Т X.811 МСЭ-Т X.811 МСЭ-Т X.800 МСЭ-Т X.217 МСЭ-Т J.170 МСЭ-Т J.93
Authentication exchange	Обмен данными аутентификации	1. Механизм, предназначенный для идентификации объекта посредством обмена информацией 2. Последовательность одной или нескольких передач информации по обмену данными аутентификации в целях осуществления аутентификации	МСЭ-Т X.800 МСЭ-Т X.811
Authentication service	Услуга аутентификации	Услуга аутентификации предоставляет доказательство того, что идентификация объекта или субъекта на самом деле является идентификацией, которая заявлена им. В зависимости от действующего субъекта и целей идентификации могут потребоваться следующие виды аутентификации: аутентификация пользователя, аутентификация одноранговых объектов, аутентификация происхождения данных. Примерами механизмов, используемых для реализации услуги аутентификации, являются пароли и персональные идентификационные номера (PIN) (простая аутентификация), а также методы, основанные на шифровании (надежная аутентификация)	МСЭ-Т M.3016.2
Authority	Орган	Объект, ответственный за выдачу сертификатов. Определены два типа органов: сертифицирующий орган, который выдает сертификаты открытых ключей, и орган по присвоению атрибутов, который выдает сертификаты атрибутов	МСЭ-Т X.509
Authorization	Авторизация	1. Предоставление прав, которое включает предоставление доступа на основании прав доступа. ПРИМЕЧАНИЕ. – Данное определение подразумевает права на осуществление некоторой деятельности (такой как доступ к данным) и что они были предоставлены	МСЭ-Т X.800

Термин (англ.)	Термин	Определение	Ссылка
		некоторому процессу, объекту или агенту-человеку 2. Предоставление разрешения на основании идентификации, прошедшей аутентификацию 3. Действие по предоставлению доступа к услуге или устройству при наличии разрешения на такой доступ	МСЭ-Т H.235 МСЭ-Т J.170
Availability	Готовность	Свойство быть доступным и годным к эксплуатации по запросу имеющего полномочия объекта	МСЭ-Т X.800
Capability	Возможность	Маркер, который используется в качестве идентификатора для ресурса, обозначающего, что владение маркером дает права доступа к данному ресурсу	МСЭ-Т X.800
Certificate	Сертификат	Набор относящихся к безопасности данных, который выдан органом обеспечения безопасности или пользующейся доверием третьей стороной, в совокупности с информацией о безопасности, которая используется для предоставления услуг обеспечения целостности и аутентификации источника данных в отношении данных (сертификат безопасности – X.810). Термин имеет отношение к сертификатам "открытого ключа", которые являются значениями, представляющими открытый ключ владельца (или иную факультативную информацию) как проверенный и подписанный пользующимся доверием органом в формате, не допускающем фальсификацию	МСЭ-Т H.235
Certificate policy	Правила применения сертификата	Поименованный набор правил, которые определяют применимость сертификата к конкретному семейству и/или классу приложений с общими требованиями к обеспечению безопасности. Например, стратегия применения данного сертификата может указывать применимость типа сертификата к аутентификации транзакций электронного обмена данными для торговли товарами в пределах данного ценового диапазона	МСЭ-Т X.509
Certificate Revocation List (CRL)	Список аннулирования сертификатов	1. Подписанный список, определяющий набор сертификатов, которые распределитель сертификатов более не считает действительными. В дополнение к общему термину CRL определены несколько конкретных типов CRL для списков CRL, охватывающих конкретные сферы применения 2. Список CRL включает порядковые номера аннулированных сертификатов, например, ввиду того, что ключ был раскрыт или, поскольку субъект больше не работает в компании, срок действия которых еще не истек	МСЭ-Т X.509 МСЭ-Т Q.817
Certification Authority (CA)	Сертифицирующий орган	1. Орган, которому одним или более пользователями доверено создавать и распределять сертификаты открытых ключей. Сертифицирующий орган может выполнять факультативную функцию по созданию ключей пользователей 2. Объект, которому доверено (в контексте стратегии обеспечения безопасности) создавать сертификаты безопасности, содержащие один или более классов данных, относящихся к обеспечению безопасности	МСЭ-Т X.509 МСЭ-Т X.810
Ciphertext	Шифротекст	Данные, созданные с применением шифрования. Семантическое содержание результирующих данных не доступно ПРИМЕЧАНИЕ. – Шифротекст может тоже пройти процедуру шифрования, в результате чего будут созданы супершифрованные данные	МСЭ-Т X.800
Cleartext	Незашифрованный текст	Открытые данные, семантическое содержание которых доступно	МСЭ-Т X.800
Confidentiality	Конфиденциальность	Свойство, которое служит для предотвращения раскрытия информации объектами или процессами, не имеющими разрешения на это	МСЭ-Т X.800
Confidentiality service	Услуга обеспечения	Услуга обеспечения конфиденциальности предоставляет	МСЭ-Т

Термин (англ.)	Термин	Определение	Ссылка
	конфиденциальности	защиту от неразрешенного раскрытия данных обмена. Различают следующие виды услуг обеспечения конфиденциальности: конфиденциальность отдельных полей; конфиденциальность соединений; конфиденциальность потока данных	M.3016.2
Credentials	Полномочия	Данные, которые передаются для установления заявленной идентификации объекта	МСЭ-Т X.800
Cryptanalysis	Криптоанализ	1. Анализ криптографической системы и/или входных и выходных данных для извлечения секретных переменных и/или уязвимых данных, включая открытый текст 2. Процесс восстановления незашифрованного текста сообщения или ключа шифрования без доступа к ключу 3. Наука восстановления незашифрованного текста сообщения или ключа шифрования без доступа к ключу (к электронному ключу в электронных криптографических системах)	МСЭ-Т X.800 МСЭ-Т J.170 МСЭ-Т J.93
Cryptographic algorithm	Криптографический алгоритм	Математическая функция, которая вычисляет результат по одному или нескольким входным значениям	МСЭ-Т H.235
Cryptographic system, cryptosystem	Криптографическая система, криптосистема	1. Набор преобразований из незашифрованного текста в шифротекст и наоборот. Конкретное(ые) преобразование(я), которое(ые) должно(ы) использоваться, выбирается(ются) ключами. Преобразования обычно описывается математическим алгоритмом 2. Криптосистема – это просто алгоритм, который может преобразовывать входные данные в нечто нераспознаваемое (шифрование) и обратно преобразовывать нераспознаваемые данные в их исходную форму (дешифрование). Методы шифрования RSA описаны в МСЭ-Т X.509	МСЭ-Т X.509 МСЭ-Т Q.815
Cryptography	Криптография	Дисциплина, включающая принципы, средства и методы для преобразования данных, для того чтобы скрыть содержащуюся в них информацию, предотвратить их скрытое изменение и/или предотвратить несанкционированное использование. ПРИМЕЧАНИЕ. – Криптография определяет методы, используемые при шифровании и дешифровании. Воздействие на криптографический принцип, средство или метод называется криптоанализом	МСЭ-Т X.800
Data confidentiality	Конфиденциальность данных	Данная услуга может использоваться для обеспечения защиты данных от несанкционированного раскрытия их содержания. Услугу обеспечения конфиденциальности данных поддерживает структура аутентификации. Может применяться для защиты данных от несанкционированного перехвата	МСЭ-Т X.509
Data integrity	Целостность данных	Показатель того, что данные не были изменены или разрушены несанкционированным образом	МСЭ-Т X.800
Data origin authentication	Аутентификация источника данных	1. Подтверждение того, что источник полученных данных соответствует заявленному 2. Подтверждение идентификации администратора доступа, ответственного за конкретный блок данных	МСЭ-Т X.800 МСЭ-Т X.811
Decipherment	Дешифрование	Инверсия соответствующего обратимого шифрования	МСЭ-Т X.800
Decryption	Дешифрация	См. Дешифрование	МСЭ-Т X.800
Delegation	Делегирование	Передача полномочия от одного объекта, который владеет данным полномочием, другому объекту	МСЭ-Т X.509
Denial of service	Отказ в обслуживании	Недопущение санкционированного доступа к ресурсам или задержка выполнения операций, критических по времени	МСЭ-Т X.800

Термин (англ.)	Термин	Определение	Ссылка
Digital signature	Цифровая подпись	1. Данные, добавленные к блоку данных, или криптографическое преобразование (см. Криптография) блока данных, которое позволяет получателю данных удостовериться в происхождении и целостности блока данных и обеспечить защиту от мошенничества, например получателем 2. Криптографическое преобразование блока данных, которое позволяет получателю блока данных удостовериться в происхождении и целостности блока данных и обеспечить защиту отправителя и получателя блока данных от мошенничества со стороны третьих сторон, а также отправителя от мошенничества со стороны получателя	МСЭ-Т X.800 МСЭ-Т X.843
Directory service	Услуга каталога	Услуга поиска и извлечения из каталога информации о хорошо определенных объектах, которая может содержать данные о сертификатах, номерах телефонов, условиях доступа, адресах и т. д. Примером является услуга каталога, соответствующая Рекомендации МСЭ-Т X.500	МСЭ-Т X.843
Eavesdropping	Перехват информации	Нарушение конфиденциальности путем слежения за связью.	МСЭ-Т M.3016.0
Encipherment	Шифрование	1. Криптографическое преобразование данных (см. Криптография) для создания шифротекста ПРИМЕЧАНИЕ. – Шифрование может быть необратимым, и в этом случае выполнение соответствующего процесса дешифрования невозможно 2. Шифрование (зашифровывание) – это процесс превращения данных в нечитаемые для несанкционированных объектов данные путем применения криптографического алгоритма (алгоритма шифрования). Дешифрование (дешифрация) является обратной операцией, в результате которой криптотекст преобразуется в открытый текст	МСЭ-Т X.800 МСЭ-Т H.235
Encryption	Зашифровывание	1. Метод, используемый для преобразования информации в форме открытого текста в шифротекст 2. Процесс скремблирования сигналов для недопущения несанкционированного доступа (см. также Шифрование)	МСЭ-Т J.170 МСЭ-Т J.93
End-to-end encipherment	Сквозное шифрование	Шифрование данных в пределах системы или на стороне источника с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне назначения. (См. также Межканальное шифрование)	МСЭ-Т X.800
Entity	Объект	1. Человек, организация, компонент аппаратного обеспечения или элемент программного обеспечения 2. Любой конкретный или абстрактный предмет интереса. В то время как обычно слово "объект" может использоваться для именования чего-либо, в контексте моделирования оно относится к объектам моделирования в предметной области	МСЭ-Т X.842 МСЭ-Т X.902
Entity authentication	Аутентификация объекта	Подтверждение идентификации администратора доступа в контексте взаимоотношений в области связи. ПРИМЕЧАНИЕ. – Аутентифицированная идентификация администратора доступа удостоверяется только тогда, когда данная услуга аннулирована. Обеспечение непрерывности аутентификации может быть достигнуто с помощью методов, описанных в п. 5.2.7 Рек. МСЭ-Т X.811	МСЭ-Т X.811
Evidence	Доказательство	Информация, которая сама по себе или при использовании вместе с другой информацией, может применяться для разрешения спора ПРИМЕЧАНИЕ. – Конкретными формами доказательств являются цифровые подписи, защитные оболочки и маркеры безопасности. Цифровые подписи используются вместе с методами открытых ключей, тогда как	МСЭ-Т X.813

Термин (англ.)	Термин	Определение	Ссылка
		защитные оболочки и маркеры безопасности применяются вместе с методами секретных ключей	
Forgery	Фальсификация	Объект фабрикует информацию и заявляет, что такая информация была получена от другого объекта или направлена другому объекту	МСЭ-Т M.3016.0
Hash function	Хэш-функция	Функция (математическая), которая отображает значения из крупного (возможно очень крупного) набора значений в меньший диапазон значений	МСЭ-Т X.810
Indirect attack	Непрямая попытка нарушения защиты системы	Попытка нарушения защиты системы, не основанная на недостатках конкретного механизма обеспечения безопасности (например, попытки нарушения защиты в обход механизма или попытки нарушения защиты, рассчитанные на систему, неправильно использующую механизм)	МСЭ-Т X.814
Integrity	Целостность	Показатель того, что данные не были изменены несанкционированным образом. (См. также Целостность данных)	МСЭ-Т H.235
Integrity service	Услуга обеспечения целостности	Услуга обеспечения целостности предоставляет способы гарантирования правильности данных обмена, защиту от изменения, удаления, создания (вставки) и повторного использования данных обмена. Различают следующие виды услуг обеспечения безопасности: целостность отдельных полей; целостность соединения без восстановления; целостность соединения с восстановлением	МСЭ-Т M.3016.2
Intentional threats	Намеренные угрозы	К таким угрозам относятся угрозы от случайного просмотра с использованием легко доступных инструментов слежения до изощренных попыток нарушения защиты с использованием специальных знаний о системе. Намеренная угроза, если она реализована, может считаться "попыткой нарушения защиты"	МСЭ-Т X.800
IPCablecom	Система IPCablecom	Проект МСЭ-Т, включающий архитектуру и серию Рекомендаций, который обеспечивает возможность доставки услуг в реальном времени по сетям кабельного телевидения с использованием кабельных модемов	МСЭ-Т J.160
Kerberos	Протокол Kerberos	Протокол сетевой аутентификации с секретным ключом, который использует на выбор криптографические алгоритмы шифрования и централизованную базу данных ключей для аутентификации	МСЭ-Т J.170
Key	Ключ	1. Последовательность символов, которые управляют операциями шифрования и дешифрования 2. Математическая величина, введенная в выбранный криптографический алгоритм	МСЭ-Т X.800 МСЭ-Т J.170
Key exchange	Обмен ключами	Обмен между объектами открытыми ключами, которые должны использоваться для кодирования связи между этими объектами	МСЭ-Т J.170
Key management	Управление ключами	Создание, хранение, рассылка, удаление, архивирование и применение ключей в соответствии со стратегией обеспечения безопасности	МСЭ-Т X.800
Man-in-the-middle attack	Атака "человек посередине"	Атака, при которой злоумышленник может читать, вставлять и изменять по своему желанию сообщения между двумя сторонами без того, чтобы какая-либо из сторон знала, что канал между ними взломан	МСЭ-Т X.1151
Masquerade	Подмена	Предпринимаемая объектом попытка представить себя другим объектом	МСЭ-Т X.800
Mutual authentication	Взаимная аутентификация	Обеспечение идентификации обоих администраторов доступа	МСЭ-Т X.811
Non-repudiation	Неотказуемость	1. Способность предотвратить последующее непризнание отправителем факта отправки сообщения или выполнения действия 2. Защита от отказа признания одним из участвующих в	МСЭ-Т J.170 МСЭ-Т

Термин (англ.)	Термин	Определение	Ссылка
		сеансе связи объектов участия во всем или в части сеанса связи 3. Процесс, обеспечивающий невозможность непризнания отправителем сообщения (например, запроса на услугу "разовая плата за просмотр программы") факта его направления	H.235 МСЭ-Т J.93
Notarization	Нотариальное заверение	Регистрация данных с участием пользующейся доверием третьей стороны, которая позволяет впоследствии удостоверить соответствие характеристик таких данных, как информационное наполнение, источник, время и доставка	МСЭ-Т X.800
Passive threat	Пассивная угроза	Угроза несанкционированного раскрытия содержания информации без изменения состояния системы	МСЭ-Т X.800
Password	Пароль	1. Конфиденциальная информация аутентификации, состоящая, как правило, из строки символов 2. Относится к строке пароля, вводимого пользователем: понимается, что он является присвоенным ключом безопасности, который совместно используется подвижным пользователем и его домашним доменом. Данный пароль пользователя и полученное совместно используемое секретное значение пользователя применяются в целях аутентификации пользователя	МСЭ-Т X.800 МСЭ-Т H.530
Physical security	Физическая безопасность	Меры, предпринимаемые для обеспечения физической защиты ресурсов от умышленных и случайных угроз	МСЭ-Т X.800
Principal	Администратор доступа	Объект, идентификация которого может быть аутентифицирована	МСЭ-Т X.811
Privacy	Секретность	1. Право частного лица контролировать или воздействовать на то, какая касающаяся его информация может быть собрана и сохранена, а также кем и кому содержание этой информация может быть открыто. ПРИМЕЧАНИЕ. – Учитывая, что данный термин относится к правам частных лиц, он не может быть предельно точным и следует воздерживаться от его использования, за исключением случаев обоснования уровня необходимой безопасности 2. Режим связи, при котором расшифровывать сообщения могут только имеющие на это разрешение стороны. Как правило это достигается с помощью шифрования и использования коллективного(ых) ключа(ей) к шифру	МСЭ-Т X.800 МСЭ-Т H.235
Private key	Секретный ключ	1. Это ключ (в криптосистеме с открытым ключом) из пары ключей пользователя, который известен только пользователю 2. Ключ, который используется с асимметричным криптографическим алгоритмом и количество владельцев которого ограничено (обычно единственным объектом). 3. Ключ, который используется в криптографии с открытым ключом, принадлежит конкретному объекту и должен оставаться секретным	МСЭ-Т X.509 МСЭ-Т X.810 МСЭ-Т J.170
Privilege	Полномочие	Атрибут или свойство, назначенное объекту соответствующим органом	МСЭ-Т X.509
Privilege Management Infrastructure (PMI)	Инфраструктура управления привилегиями (PMI)	Инфраструктура, способная поддерживать управление привилегиями при поддержке комплексной услуги авторизации и при взаимодействии с инфраструктурой открытых ключей	МСЭ-Т X.509
Public key	Открытый ключ	1. Это ключ (в криптосистеме с открытым ключом) из пары ключей пользователя, который известен всем 2. Ключ, который используется с асимметричным криптографическим алгоритмом и доступ к которому может быть открытым 3. Ключ, используемый в криптографии с открытым ключом, который принадлежит конкретному объекту и распространяется открытым способом. Другие объекты используют этот ключ для кодирования данных,	МСЭ-Т X.509 МСЭ-Т X.810 МСЭ-Т J.170

Термин (англ.)	Термин	Определение	Ссылка
		подлежащих отправке владельцу ключа	
Public key certificate	Сертификат открытого ключа	1. Открытый ключ пользователя и некоторая другая информация, не поддающиеся подделке благодаря шифрованию, вместе с личным ключом выдавшего его сертифицирующего органа 2. Значения, представляющие собой открытый ключ владельцев (и другую факультативную информацию), которые проверены и подписаны доверенным органом в формате, не поддающемся подделке 3. Увязывание открытого ключа объекта с одним или более атрибутами, связанными с его идентификационной информацией, также называемое цифровым сертификатом	МСЭ-Т X.509 МСЭ-Т H.235 МСЭ-Т J.170
Public key cryptography	Криптография с открытым ключом	Криптографический метод, основанный на алгоритме личного и открытого ключей, при котором сообщение кодируется с помощью открытого ключа, но может быть декодировано только при помощи личного ключа. Известен также как система личного открытого ключа (РРК). ПРИМЕЧАНИЕ. – Знание открытого ключа не раскрывает личного ключа. Пример: Сторона А хотела бы разделить личный и открытый ключи и публично направить открытый ключ всем, кто пожелал бы связаться со Стороной А, но сохранить в секрете личный ключ. Далее, в то время как любой, кто имеет открытый ключ, сможет закодировать сообщения для Стороны А, раскодировать их можно будет только при наличии личного ключа, имеющегося у Стороны А	МСЭ-Т J.93
Public Key Infrastructure (PKI)	Инфраструктура открытых ключей (PKI)	Инфраструктура, способная поддерживать управление открытыми ключами, обеспечивающее поддержку услуг аутентификации, кодирования, целостности и фиксации авторства	МСЭ-Т X.509
Relying party	Доверяющая сторона	Пользователь или агент, который при принятии решения полагается на данные сертификата	МСЭ-Т X.509
Replay	Повторное использование	Сообщение или его часть повторяется для создания неразрешенного результата. Например, действительное сообщение, содержащее информацию аутентификации, может быть повторно использовано другим объектом в целях своей аутентификации (как тем, чем он не является)	МСЭ-Т X.800
Repudiation	Непризнание участия	1. Отказ признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи 2. Объект, задействованный в обмене информацией, последовательно отрицает этот факт 3. Если пользователь системы MHS (в случае системы MHS) или система MTS в дальнейшем могут отрицать факт представления, приема или создания сообщения, включая отрицание происхождения, отрицание представления, отрицание доставки	МСЭ-Т X.800 МСЭ-Т M.3016.0 МСЭ-Т X.402
Revocation list certificate	Сертификат из списка аннулированных	Сертификат безопасности, который указан в списке сертификатов безопасности как аннулированный	МСЭ-Т X.810
Secret key	Секретный ключ	Ключ, используемый с асимметричным криптографическим алгоритмом. Обладание секретным ключом ограничено (обычно двумя объектами)	МСЭ-Т X.810
Security	Безопасность	Термин "безопасность" используется в смысле минимизации незащищенности активов и ресурсов. Активом является что-либо представляющее ценность. Незащищенность – это любое слабое место, которое может использоваться для нарушения работы системы или содержащейся в ней информации. Какая-либо угроза является потенциальным нарушением безопасности	МСЭ-Т X.800

Термин (англ.)	Термин	Определение	Ссылка
Security alarm	Сигнал о нарушении безопасности	Сообщение, создаваемое в случае обнаружения события, имеющего отношение к безопасности, которое в соответствии со стратегией обеспечения безопасности определяется как условие нарушения безопасности. Сигнал о нарушении безопасности имеет целью своевременно обратить внимание соответствующих объектов	МСЭ-Т X.816
Security audit	Проверка безопасности	Независимый анализ или рассмотрение системных записей и действий для проверки на соответствие управляющих функций системы, с целью обеспечения соответствия установленным стратегическим и эксплуатационным процедурам, для выявления нарушения безопасности и для предложения каких-либо изменений в управлении, стратегии или процедурах	МСЭ-Т X.800
Security audit trail	Данные проверки безопасности	Данные, которые собраны и могут быть использованы для содействия проведению проверки безопасности	МСЭ-Т X.800
Security certificate	Сертификат безопасности	Набор связанных с безопасностью данных, выданных органом безопасности или пользующейся доверием третьей стороной, вместе с информацией безопасности, которая используется для обеспечения услуг целостности и аутентификации источника данных. ПРИМЕЧАНИЕ. – Все сертификаты считаются сертификатами безопасности. Термин "сертификат безопасности" в Рекомендациях МСЭ-Т серии X.800 принят во избежание терминологического несоответствия с Рекомендацией МСЭ-Т X.509	МСЭ-Т X.810
Security domain	Домен безопасности	1. Совокупность пользователей и систем, подчиняющихся общей стратегии обеспечения безопасности 2. Набор ресурсов, подчиняющихся одной стратегии обеспечения безопасности	МСЭ-Т X.841 МСЭ-Т X.411
Security Information (SI)	Информация о безопасности (ИБ)	Информация, необходимая для реализации услуг обеспечения безопасности	МСЭ-Т X.810
Security management	Управление обеспечением безопасностью	Управление обеспечением безопасности включает любую деятельность по установлению, поддержанию и удалению аспектов системы, связанных с обеспечением безопасности. Тематика охватывает: управление услугами обеспечения безопасности; установку механизмов обеспечения безопасности; управление ключами защиты (часть управления); установление идентификации, ключи, данные управления доступом и т. д.; управление данными проверки безопасности и сигналами нарушения безопасности	МСЭ-Т M.3016.0
Security model	Модель безопасности	Основа для описания услуг обеспечения безопасности, которые противодействуют потенциальным угрозам системе MTS, и элементов обеспечения безопасности, которые поддерживают эти услуги	МСЭ-Т X.402
Security policy	Политика безопасности	1. Набор правил, установленных органом безопасности, который управляет использованием и предоставлением услуг и средств обеспечения безопасности 2. Набор критериев для предоставления услуг обеспечения безопасности. ПРИМЕЧАНИЕ. – См. Стратегия обеспечения безопасности на основе идентификации и на основе правил. Полная стратегия обеспечения безопасности неизбежно затрагивает многие вопросы, выходящие за рамки ВОС (взаимодействие открытых систем)	МСЭ-Т X.509 МСЭ-Т X.800
Security service	Услуга безопасности	Услуга, предоставляемая каким-либо уровнем открытых систем связи, которая гарантирует достаточную защиту систем или процессов передачи данных	МСЭ-Т X.800
Security threat (threat)	Угроза безопасности (угроза)	Потенциальное нарушение безопасности	МСЭ-Т X.800
Security token	Маркер	Набор данных, передаваемых между объектами связи,	МСЭ-Т

Термин (англ.)	Термин	Определение	Ссылка
	безопасности	который защищен одной или несколькими услугами обеспечения безопасности вместе с информацией о безопасности, которая используется при их предоставлении	X.810
Sensitivity	Критичность	Характеристика ресурса, которая косвенно выражает его значение или важность	МСЭ-Т X.509
Shared secret	Коллективное секретное значение	Относится к ключу системы защиты для криптографических алгоритмов; может быть получено исходя из пароля	МСЭ-Т H.530
Signature	Подпись	См. Цифровая подпись	МСЭ-Т X.800
Simple Authentication	Простая аутентификация	Аутентификация посредством соглашений о простых паролях	МСЭ-Т X.509
Source of authority (SOA)	Источник полномочий (ИП)	Орган по присвоению атрибутов, которому верификатор полномочий для конкретного ресурса доверяет как высшему органу по назначению набора полномочий	МСЭ-Т X.509
Spam	Спам	Незатребованная и нежелательная электронная почта	МСЭ-Т H.235
Spoofing	Спуфинг	Имитация законного ресурса или пользователя	МСЭ-Т X.509
Strong authentication	Надежная аутентификация	Аутентификация с помощью криптографически полученных полномочий	МСЭ-Т X.811
Sybil attack	Атака "Сибилла"	Атака, в ходе которой разрушается система репутации одноранговой сети в результате создания объектов с псевдонимами и использования их для получения непропорционально большого влияния	
Threat	Угроза	Потенциальное нарушение безопасности	МСЭ-Т X.800
Token	Маркер	См. Маркер безопасности	
Trojan horse	"Троянский конь"	При проникновении в систему "троянский конь" помимо разрешенной функции обладает несанкционированной функцией. "Троянский конь" – это ретрансляция, при которой происходит также копирование сообщений по неразрешенному каналу	МСЭ-Т X.800
Trust	Доверие	Говорят, что объект X доверяет объекту Y в отношении ряда действий, если и только если объект X полагается на объект Y, который ведет себя определенным образом по отношению к этим действиям	МСЭ-Т X.810
Trusted functionality	Функциональная возможность, пользующаяся доверием	Функциональная возможность, воспринимаемая как подходящая по определенным критериям, например как установленная в соответствии со стратегией обеспечения безопасности	МСЭ-Т X.800
Trusted Third Party (TTP)	Пользующаяся доверием третья сторона	Орган безопасности или его агент, пользующийся доверием (других объектов) в отношении некоторых связанных с безопасностью действий (в контексте стратегии обеспечения безопасности)	МСЭ-Т X.810
Ubiquitous Sensor Network (USN)	Повсеместная сеть датчиков (USN)	Низкозатратная сеть, в которой используются маломощные датчики для разработки осведомленности о содержании, с тем чтобы предоставить услуги обнаружения информации и сведений для всех, в любом месте и в любое время. USN может охватывать широкий географический район и может поддерживать множество приложений	
Unauthorized access	Несанкционирован-ный доступ	Объект пытается осуществить доступ к данным в нарушение действующей стратегии обеспечения безопасности	МСЭ-Т M.3016.0
User authentication	Аутентификация пользователя	Установление доказательства идентификации пользователя-человека или прикладного процесса	МСЭ-Т M.3016.0
Verifier	Верификатор	Является объектом, требующим аутентификации, или представляет его. Верификатор включает функции, необходимые для осуществления обменов в целях	МСЭ-Т X.811

Термин (англ.)	Термин	Определение	Ссылка
		аутентификации	
Vulnerability	Уязвимость	Любое слабое место, которое может быть использовано для нарушения системы или информации, которая в ней содержится	МСЭ-Т X.800
ITU-T X.509 certificate	Сертификат МСЭ-Т X.509	Спецификация сертификата открытого ключа, разработанная как часть каталога стандартов МСЭ-Т X.500	МСЭ-Т J.170

Приложение В
Акронимы и сокращения

Приложение В

Акронимы и сокращения

Сокращение	Расшифровка	Определение
ACI	Access Control Information	Информация об управлении доступом
AES	Advanced Encryption Standard Algorithm	Усовершенствованный стандартный алгоритм шифрования
ASN.1	Abstract Syntax Notation One	Абстрактная синтаксическая нотация версии один
ASP	Application Service Provider	Поставщик прикладных услуг
ATIS	Alliance for Telecommunications Industry Solutions	Альянс для принятия решений в области электросвязи
A/V	Audiovisual	Аудиовизуальный
BioAPI	Biometric Application Program/programming Interface	Программа/программный интерфейс биометрических приложений
BPON	Broadband Passive Optical Network	Широкополосная пассивная оптическая сеть
B2C	Business-to-Customer	Бизнес для потребителя
CA	Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates	Сертифицирующий орган. Доверенная организация, которая принимает приложения сертификатов от объектов, аутентифицирует приложения, выдает сертификат и осуществляет ведение информации о статусе сертификатов
CASF	Core anti-spam functions	Базовые функции противодействия спаму
CIRT	Computer Incident Response Team	Группа реагирования на компьютерные инциденты
CDMA	Code Division Multiple Access	Многостанционный доступ с кодовым разделением (МДКР)
CMIP	Common Management Information Protocol	Протокол передачи общей управляющей информации
CORBA	Common Object Request Broker Architecture	Общая архитектура посредника запросов объектов
CP	Certificate Policy	Стратегия в отношении сертификатов
CPS	Certification Practice Statement	Свидетельство о практике проведения сертификации
CRL	Certificate Revocation List	Список аннулирования сертификатов
CVE	Common vulnerabilities and exposures	Общеизвестные уязвимости и незащищенности
CVSS	Common vulnerabilitiy storing system	Система оценки общеизвестных уязвимостей
CYBEX	Cybersecurity information exchange	Обмен информацией о кибербезопасности
DNS	Domain Name Server/System/Service	Сервер/система/услуга имен доменов
DSL	Digital Subscriber Loop	Цифровой абонентский шлейф
EAP	Extensible Authentication Protocol	Расширяемый протокол аутентификации
ENISA	European Network and Information Security Agency	Европейское агентство по вопросам сетевой и информационной безопасности
ETSI	European Telecommunications Standards Institute	Европейский институт стандартизации по электросвязи
FMC	Fixed Mobile Convergence	Конвергенция фиксированной и подвижной связи
FW	Firewall	Брандмауэр
GK	Gatekeeper	Гейткипер
GPRS	General Packet Radio System	Служба пакетной передачи данных общего пользования

GSM	Global System for Mobile communications	Глобальная система подвижной связи
GW	Gateway	Шлюз
HFX	Hawthorne Facsimile Cipher	Шифр факсимильных передач Готторна
HKM	Hawthorne Key Management algorithm	Алгоритм управления ключами Готторна
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
ICT	Information and Communication Technology	Информационно-коммуникационные технологии (ИКТ)
ID	Identifier	Идентификатор
IdM	Identity Management	Управление определением идентичности
IEC	International Electrotechnical Commission	Международная электротехническая комиссия (МЭК)
IEEE	Institute of Electrical and Electronics Engineers	Институт инженеров по электротехнике и радиоэлектронике
IETF	Internet Engineering Task Force	Комитет по инженерным проблемам интернета
IKE	Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPSec.	Межсетевой обмен ключами – это механизм управления ключами, используемый для согласования и выведения ключей для SA в IPSec
IM	Instant Messaging	Обмен мгновенными сообщениями
IMS	IP Multimedia Subsystem	Подсистема передачи мультимедийных данных по IP-сетям
IMT-2000	International Mobile Telecommunications 2000	Международная подвижная электросвязь 2000 (МПЭ-2000)
IP	Internet Protocol	Межсетевой протокол
IPSec	Internet Protocol Security	Безопасность межсетевого протокола
IPTV	Internet Protocol TeleVision	Телевидение по межсетевому протоколу
IPX	Internet Packet Exchange	Обмен межсетевыми протоколами
ISMF	Information Security Management Framework	Концепция управления информационной безопасностью
ISMS	Information Security Management System	Система управления информационной безопасностью
ISO	International Organization for Standardization	Международная организация по стандартизации (ИСО)
ITU-T	Telecommunication Standardization Sector of the International Telecommunication Union	Сектор стандартизации электросвязи Международного союза электросвязи (МСЭ-Т)
LAN	Local Area Network	Локальная вычислительная сеть (ЛВС)
LDAP	Lightweight Directory Access Protocol	Облегченный протокол доступа к каталогу
MD5	Message Digest No. 5 (a secure hash algorithm)	Протокол Message Digest No. 5 (алгоритм защитного хэширования)
MIS	Management Information System	Система передачи управляющей информации
MMS	Multimedia Messaging Service	Служба мультимедийных сообщений
MTA	Message Transfer Agent (In messaging) Media Terminal adapter (In cable technology)	Агент передачи сообщения (при передаче сообщений) Адаптер медиатерминала (в кабельных сетях)
MWSSG	Mobile Web Services Security Gateway	Шлюз безопасности подвижных веб-услуг
NAT	Network Address Translation	Трансляция сетевого адреса
NGN	Next Generation Network	Сеть последующих поколений (СПП)
OASIS	Organization for the Advancement of Structured Information Standards	Организация по развитию стандартов структурированной информации
OMG	Object Management Group	Группа управления объектами
OSI	Open Systems Interconnection	Взаимосвязь открытых систем (ВОС)

P2P	Peer-to-peer	Одноранговый
PC	Personal Computer	Персональный компьютер (ПК)
PDA	Personal Data Assistant	Карманный персональный компьютер (КПК)
PIN	Personal Identification Number	Персональный идентификационный номер
PII	Personally Identifiable Information	Персональная идентификационная информация
PKI	Public-key Infrastructure	Инфраструктура открытого ключа
PKINIT	Public-key Cryptography Initial Authentication	Первоначальная аутентификация по криптографии с открытым ключом
PMI	Privilege Management Infrastructure	Инфраструктура управления полномочиями
PSS	PII Protection Service	Услуга защиты PII
PSTN	Public Switched Telephone Network	Телефонная сеть общего пользования с коммутацией каналов (КТСОП)
QoS	Quality of Service	Качество обслуживания
RASF	Recipient-side anti-spam functions	Функции противодействия спаму на стороне получателя
RBAC	Role-Based Access Control	Управление доступом по ролевому признаку
RBL	Real-time blocking list	Список нарушителей, проверяемый в режиме реального времени
RFID	Radio Frequency Identification	Радиочастотная идентификация
RSA	Rivest, Shamir and Adleman (public-key algorithm)	Алгоритм Райвеста, Шамира и Адлемана (алгоритм шифрования с открытыми ключами)
RTP	Real time protocol	Протокол реального времени
SAML	Security Assertion Markup Language	Язык разметки, предусматривающий защиту данных
SASF	Sender-side anti-spam functions	Функции противодействия спаму на стороне отправителя
SG	Study Group	Исследовательская комиссия (ИК)
SHA1	Secure Hash Algorithm 1	Защищенный алгоритм хэширования № 1
SIP	Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants	Протокол инициирования сеанса связи. Протокол управления (сигнализация) прикладного уровня для создания, изменения и завершения сеансов с одним или более участниками
SMS	Short Message Service	Служба коротких сообщений
SMTP	Simple Mail Transfer Protocol	Простой протокол передачи сообщений электронной почты
SNMP	Simple Network Management Protocol	Простой протокол управления сетью
SoA	Source of Authority	Источник полномочий
SOA	Service Oriented Architecture	Архитектура, ориентированная на обслуживание
SPAK	Secure Password-based Authentication protocol with Key exchange	Протокол аутентификации на базе секретного пароля с обменом ключами
SSL	Secure Socket Layer	Уровень защищенных разъемов
SSO	Single Sign-On	Единая регистрация
TCP/IP	Transmission Control Protocol/Internet Protocol	Протокол управления передачей/Межсетевой протокол
TLS	Transport Layer Security	Безопасность транспортного уровня
TMN	Telecommunication Management Network	Сеть управления электросвязью (СУЭ)
TNSS	Telecommunication IP-based network security system	Система обеспечения безопасности в сетях электросвязи на основе IP

UE	User Equipment	Оборудование пользователя
UICC	Universal Integrated Circuit Card	Международная смарт-карта
URS	User reputation system	Система репутации пользователя
USN	Ubiquitous Sensor Network	Повсеместная сеть датчиков
VoIP	Voice over IP	Передача голоса по IP
VPN	Virtual Private Network	Виртуальная частная сеть
VSPPS	VoIP spam prevention policy server	Сервер политики предупреждения спама в VoIP
VSPS	VoIP spam prevention policy server	Система предупреждения спама в VoIP
WAN	Wide Area Network	Территориально распределенная сеть (ТРС)
Wi-Fi	Wireless Fidelity (trademark of the Wi-Fi Alliance for certified products based on the IEEE 802.11 standards)	Беспроводной интернет (торговая марка Wi-Fi альянса для сертифицированных продуктов, основанных на стандартах IEEE 802.11)
WTSA	World Telecommunication Standardization Assembly	Всемирная ассамблея по стандартизации электросвязи (ВАСЭ)
XACML	eXtensible Access Control Markup Language	Расширяемый язык разметки контроля доступа
XML	eXtensible Markup Language	Расширяемый язык разметки
3G	3rd Generation	Третье поколение
3GPP	3rd Generation Partnership Project	Проект партнерства третьего поколения
3GPP2	3rd Generation Partnership Project 2	2-й проект партнерства третьего поколения

Приложение С
Перечень Исследовательских комиссий МСЭ-Т, связанных с проблемой безопасности

Приложение C

Перечень Исследовательских комиссий МСЭ-Т, связанных с проблемой безопасности

Деятельность большинства Исследовательских комиссий затрагивает некоторые аспекты безопасности электросвязи и/или ИКТ. Каждая Исследовательская комиссия отвечает за решение проблем безопасности в пределах собственной сферы ответственности, но ИК17, основным направлением которой является безопасность, была назначена ведущей Исследовательской комиссией по безопасности. В таблице 9 представлены описания роли Исследовательских комиссий в вопросах, связанных с проблемой безопасности, и список соответствующих обязанностей ведущих Исследовательских комиссий.

Таблица 9 – Исследовательские комиссии, имеющие обязанности, связанные с проблемой безопасности

Исследовательская комиссия	Название	Обязанности/роль в вопросах безопасности
ИК2	Эксплуатационные аспекты предоставления услуг и управления электросвязью	Ведущая Исследовательская комиссия по вопросам определения услуг, нумерации и маршрутизации Ведущая Исследовательская комиссия по вопросам электросвязи для оказания помощи при бедствиях/раннего предупреждения Ведущая Исследовательская комиссия по вопросам управления электросвязью
ИК5	Окружающая среда и изменение климата	Ведущая Исследовательская комиссия по вопросам электромагнитной совместимости и воздействия электромагнитных полей Ведущая Исследовательская комиссия по вопросам ИКТ и изменения климата
ИК9	Передача телевизионных и звуковых программ и интегрированные широкополосные кабельные сети	Ведущая Исследовательская комиссия по вопросам интегрированных широкополосных кабельных и телевизионных сетей
ИК11	Требования к сигнализации, протоколы и спецификации тестирования	Ведущая Исследовательская комиссия по вопросам сигнализации и протоколов Ведущая Исследовательская комиссия по вопросам интеллектуальных сетей Ведущая Исследовательская комиссия по вопросам спецификации тестирования
ИК12	Показатели работы, QoS и QoE	Ведущая Исследовательская комиссия по вопросам качества обслуживания и оценки пользователем качества услуги
ИК13	Будущие сети, включая сети подвижной связи и СПП	Ведущая Исследовательская комиссия по вопросам будущих сетей и СПП Ведущая Исследовательская комиссия по вопросам управления мобильностью и конвергенции сетей подвижной и фиксированной связи
ИК15	Инфраструктура оптических транспортных сетей и сетей доступа	Ведущая Исследовательская комиссия по транспортным аспектам сетей доступа Ведущая Исследовательская комиссия по вопросам оптической технологии Ведущая Исследовательская комиссия по вопросам оптических транспортных сетей
ИК16	Кодирование, системы и приложения мультимедиа	Ведущая Исследовательская комиссия по вопросам кодирования, систем и приложений мультимедиа Ведущая Исследовательская комиссия по вопросам повсеместных приложений (электронное "все", например электронное здравоохранение) Ведущая Исследовательская комиссия по вопросам информационно-коммуникационной доступности для людей с ограниченными возможностями
ИК17	Безопасность	Ведущая Исследовательская комиссия по вопросам безопасности электросвязи Ведущая Исследовательская комиссия по вопросам управления определением идентичности Ведущая Исследовательская комиссия по вопросам языков и методов описания

Приложение D
Рекомендации по безопасности и другие публикации, указанные в этом Руководстве

Приложение D
Рекомендации по безопасности и другие публикации, указанные в этом Руководстве

В данном Приложении содержится полный список Рекомендаций МСЭ-Т, указанных в этом Руководстве с гиперссылками, поэтому читатели, использующие электронную версию документа, смогут перейти непосредственно по ссылке и скачать Рекомендации. Как отмечено в документе, МСЭ-Т разработал множество стандартов по вопросам безопасности совместно с другими организациями по разработке стандартов. Публикуемые в настоящее время общие/двойные тексты Рекомендаций по вопросам безопасности ИКТ также включены в эту таблицу. Полный список Рекомендаций МСЭ-Т доступен в режиме онлайн по адресу: http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx. Рекомендации МСЭ-Т по вопросам безопасности доступны через часть 2 (База данных) дорожной карты по стандартам безопасности (www.itu.int/МСЭ-T/studygroups/com17/ict/index.html).

Рекомендация	Название	Эквивалентный документ
МСЭ-Т E.408	Требования к безопасности сетей электросвязи	
МСЭ-Т E.409	Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи	
ITU-T F.744	Service description and requirements for ubiquitous sensor network middleware	
МСЭ-Т G.827	Параметры и цели функции готовности для сквозных международных цифровых трактов с постоянной скоростью передачи	
МСЭ-Т G.1000	Электросвязь. Качество обслуживания: структура и определения	
МСЭ-Т G.1030	Оценка сквозного качества в IP-сетях для приложений передачи данных	
МСЭ-Т G.1050	Модель сети для оценки качества передачи мультимедиа по межсетевому протоколу	
МСЭ-Т G.1081	Точки контроля качественных показателей для IPTV	
МСЭ-Т H.235.0	H.323 Безопасность: Инфраструктура защиты в мультимедийных системах серии H (H.323 и других, основанных на H.245)	
МСЭ-Т H.235.1	H.323 Безопасность: Базовый профиль безопасности	
МСЭ-Т H.235.2	H.323 Безопасность: Профиль безопасности с подписью	
МСЭ-Т H.235.3	H.323 Безопасность: Гибридный профиль безопасности	
МСЭ-Т H.235.4	H.323 Безопасность: Защита соединения с прямой и селективной маршрутизацией	
МСЭ-Т H.235.5	H.323 Безопасность: Структура для надежной аутентификации в RAS с использованием слабо зашифрованных совместных секретных ключей	
МСЭ-Т H.235.6	Профиль шифрования речи с управлением внутренним ключом H.235/H.245	
МСЭ-Т H.235 Implementers' Guide	Руководство по реализации для H.235 V3: "Безопасность и шифрование для серии H (H.323 и другие мультимедийные терминалы на базе H.245)"	
МСЭ-Т H.323	Мультимедийные системы связи на основе пакетов	
МСЭ-Т H.350	Архитектура служб каталогов для мультимедийной конференц-связи	
МСЭ-Т H.460.17	Применение сигнальных линий связи H.225.0 в качестве транспорта для сообщений H.323 RAS	

Рекомендация	Название	Эквивалентный документ
МСЭ-Т H.460.18	Передача сигнализации H.323 через трансляторы сетевых адресов и брандмауэры	
МСЭ-Т H.460.19	Передача медиасигналов H.323 через трансляторы сетевых адресов и брандмауэры	
МСЭ-Т H.510	Подвижность для мультимедийных систем и услуг H.323	
МСЭ-Т H.530	Симметричные процедуры обеспечения безопасности для подвижной связи H.323 в H.510	
МСЭ-Т J.160	Структура архитектуры для предоставления критичных по времени услуг по сетям кабельного телевидения с использованием кабельных модемов	
МСЭ-Т J.170	Спецификация обеспечения безопасности IPCablecom	
МСЭ-Т J.360	Структура архитектуры IPCablecom2	
МСЭ-Т M.3010	Принципы сети управления электросвязью	
МСЭ-Т M.3016.0	Безопасность для плоскости административного управления: обзор	
МСЭ-Т M.3016.1	Безопасность для плоскости административного управления: требования по безопасности	
МСЭ-Т M.3016.2	Безопасность для плоскости управления: услуги по обеспечению безопасности	
МСЭ-Т M.3016.3	Безопасность для плоскости управления: механизм обеспечения безопасности	
МСЭ-Т M.3016.4	Безопасность для уровня управления: проформа структуры	
МСЭ-Т M.3208.2	Услуги управления СУЭ для выделенных сетей и сетей с переконфигурируемыми цепями: Управление соединением заранее предоставленных каналов связи для предоставления услуги аренды выделенной сети	
МСЭ-Т M.3210.1	Услуги управления СУЭ для управления обеспечением безопасности сетей IMT-2000	
МСЭ-Т Q.816	Услуги СУЭ на основе CORBA	
МСЭ-Т Q.834.3	Описание UML для требований интерфейса управления широкополосных пассивных оптических сетей	
МСЭ-Т Q.834.4	Спецификация интерфейса CORBA для широкополосных пассивных оптических сетей, основанная на требованиях интерфейса UML	
МСЭ-Т Q.1701	Концепция для сетей IMT-2000	
МСЭ-Т Q.1702	Долговременный прогноз в отношении сетевых аспектов для систем после IMT-2000	
МСЭ-Т Q.1703	Концепция услуг и функций сети для сетевых аспектов систем после IMT-2000	
МСЭ-Т Q.1741.1	Ссылки на IMT-2000 для версии 1999 года, эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN	Идентифицирует документы 3GPP
МСЭ-Т Q.1742.1	Связь стандартов IMT-2000 со стандартом развитой основной сети ANSI-41 с сетью доступа cdma2000	Идентифицирует документы 3GPP2
МСЭ-Т T.4	Стандартизация факсимильных терминалов Группы 3 для документальной электросвязи	
МСЭ-Т T.36	Возможности обеспечения безопасности при использовании факсимильных терминалов Группы 3	
МСЭ-Т T.37	Процедуры передачи факсимильных данных путем хранения и передачи по интернету	
МСЭ-Т T.38	Процедуры для передачи факсимильных данных Группы 3 в реальном времени по IP-сетям	
МСЭ-Т T.563	Характеристики терминалов для факсимильной аппаратуры Группы 4	
МСЭ-Т X.500	Справочник: обзор понятий, моделей и услуг	ИСО/МЭК 9594-1

Рекомендация	Название	Эквивалентный документ
МСЭ-Т X.501	Справочник: модели	ИСО/МЭК 9594-2
МСЭ-Т X.509	Справочник: структуры сертификатов открытых ключей и атрибутов	ИСО/МЭК 9594-8
МСЭ-Т X.511	Справочник: Абстрактное определение услуги	ИСО/МЭК 9594-3
МСЭ-Т X.518	Справочник: Процедуры для распределенных операций	ИСО/МЭК 9594-4
МСЭ-Т X.519	Справочник: Спецификация протокола	ИСО/МЭК 9594-5
МСЭ-Т X.520	Справочник: Отдельные типы атрибутов	ИСО/МЭК 9594-6
МСЭ-Т X.521	Справочник: отдельные классы объектов	ИСО/МЭК 9594-7
МСЭ-Т X.525	Справочник: Репликация	ИСО/МЭК 9594-9
МСЭ-Т X.530	Справочник: Использование управления системами для администрирования справочников	ИСО/МЭК 9594-10
МСЭ-Т X.711	Общий протокол управления информацией: спецификация	ИСО/МЭК 9596-1
МСЭ-Т X.736	Управление системами: функция оповещения о нарушении безопасности	ИСО/МЭК 10164-7
МСЭ-Т X.740	Управление системами: Функция предоставления данных проверки безопасности	ИСО/МЭК 10164-8
МСЭ-Т X.741	Управление системами: объекты и атрибуты для контроля за доступом	ИСО/МЭК 10164-9
МСЭ-Т X.780	Руководству СУЭ для определения объектов, управляемых CORBA	
МСЭ-Т X.780.1	Руководящие указания по СУЭ для определения интерфейсов крупномодульных объектов, управляемых при помощи CORBA	
МСЭ-Т X.780.2	Руководящие указания по СУЭ для определения ориентированных на услугу объектов, управляемых при помощи CORBA и передовых объектов	
МСЭ-Т X.781	Требования и руководящие указания по проформам Деклараций соответствия внедрения, связанных с системами на основе CORBA	
МСЭ-Т X.790	Функция исправления неполадок для приложений МСЭ-Т	
МСЭ-Т X.800	Архитектура обеспечения безопасности в среде взаимодействия открытых систем для приложений МККТТ	ИСО/МЭК 7498-2
МСЭ-Т X.802	Модель обеспечения безопасности низших уровней	ИСО/МЭК TR 13594
МСЭ-Т X.803	Модель обеспечения безопасности высших уровней	ИСО/МЭК 10745
МСЭ-Т X.805	Архитектура безопасности для систем, обеспечивающих связь между оконечными пунктами	ИСО/МЭК 18028-2
МСЭ-Т X.810	Инфраструктура обеспечения безопасности открытых систем: Обзор	ИСО/МЭК 10181-1
МСЭ-Т X.811	Инфраструктура обеспечения безопасности открытых систем: основа аутентификации	ИСО/МЭК 10181-2
МСЭ-Т X.812	Инфраструктура обеспечения безопасности открытых систем: основа управления доступом	ИСО/МЭК 10181-3
МСЭ-Т X.813	Инфраструктура обеспечения безопасности открытых систем: основа обеспечения неотказуемости	ИСО/МЭК 10181-4
МСЭ-Т X.814	Инфраструктура обеспечения безопасности открытых систем: основа обеспечения конфиденциальности	ИСО/МЭК 10181-5
МСЭ-Т X.815	Инфраструктура обеспечения безопасности открытых систем: основа обеспечения целостности	ИСО/МЭК 10181-6
МСЭ-Т X.816	Инфраструктура обеспечения безопасности открытых систем: основа проверки безопасности и сигналов нарушения безопасности	ИСО/МЭК 10181-7
МСЭ-Т X.830	Типичные высшие уровни обеспечения безопасности: обзор, модели и нотация	ИСО/МЭК 11586-1
МСЭ-Т X.831	Типичные высшие уровни обеспечения безопасности: определение услуги, обеспечиваемой элементом услуги обмена данными о безопасности (SESE)	ИСО/МЭК 11586-2

Рекомендация	Название	Эквивалентный документ
МСЭ-Т X.832	Типичные высшие уровни обеспечения безопасности: определение протокола элемента услуги обмена данными о безопасности (SESE)	ИСО/МЭК 11586-3
МСЭ-Т X.833	Типичные высшие уровни обеспечения безопасности: спецификация синтаксиса защиты перехода	ИСО/МЭК 11586-4
МСЭ-Т X.834	Типичные высшие уровни обеспечения безопасности: проформа свидетельства о соответствии протокольной реализации (PICS) элемента услуги обмена данными о безопасности (SESE)	ИСО/МЭК 11586-5
МСЭ-Т X.835	Типичные высшие уровни обеспечения безопасности: проформа PICS защиты синтаксиса перехода	ИСО/МЭК 11586-6
МСЭ-Т X.841	Информационные технологии – Информационные объекты, относящиеся к обеспечению безопасности, для управления доступом	ИСО/МЭК 15816
МСЭ-Т X.842	Информационные технологии – Руководящие принципы для использования услуг пользующейся доверием третьей стороны и управления ими	ИСО/МЭК TR 14516
МСЭ-Т X.843	Информационные технологии – Спецификации услуг TTP для поддержки применения цифровых подписей	ИСО/МЭК 15945
МСЭ-Т X.1031	Роли конечных пользователей и сетей электросвязи в рамках архитектуры безопасности	
МСЭ-Т X.1032	Архитектура внешних взаимосвязей для системы безопасности сети электросвязи на базе IP	
МСЭ-Т X.1034	Руководящие указания по расширяемому протоколу аутентификации, основанному на аутентификации и управлении ключами в сети передачи данных	
МСЭ-Т X.1035	Протокол обмена ключами (PAK) с аутентификацией по паролю	
МСЭ-Т X.1036	Структура для создания, хранения, распространения и выполнения правил для обеспечения безопасности сети	
МСЭ-Т X.1051	Методы обеспечения безопасности – Руководство по управлению информационной безопасностью для организаций электросвязи, основанное на ИСО/МЭК 27002	ИСО/МЭК 27011
ITU-T X.1052	Information security management framework	
МСЭ-Т X.1055	Управление рисками и руководство по профилям рисков для организаций электросвязи	
МСЭ-Т X.1056	Руководящие указания для организаций электросвязи по управлению инцидентами в области безопасности	
ITU-T X.1057	Asset management guidelines in telecommunication organizations	
МСЭ-Т X.1081	Основа для спецификации аспектов защиты и безопасности телебиометрии	
ITU-T X.1080.1	e-Health and world-wide telemedicines – Generic telecommunication protocol	
МСЭ-Т X.1082	Телебиометрия, связанная с психологией человека	ИСО/МЭК 80000-14
МСЭ-Т X.1083	Биометрия – протокол сетевого взаимодействия BioAPI	ИСО/МЭК 24708
МСЭ-Т X.1084	Механизм телебиометрической системы – Часть 1: Общий протокол биометрической аутентификации и профили модели системы для систем электросвязи	
МСЭ-Т X.1086	Процедуры телебиометрической защиты – Руководство по техническим и организационным мерам противодействия для безопасности биометрических данных	
МСЭ-Т X.1088	Структура цифрового телебиометрического ключа (TDK) – Структура для генерирования и защиты цифрового телебиометрического ключа	
МСЭ-Т X.1089	Инфраструктура телебиометрической аутентификации (TAI)	
ITU-T X.1090	Authentication framework with one-time telebiometric templates	

Рекомендация	Название	Эквивалентный документ
ITU-T X.1101	Security requirements and framework for multicast communication	
МСЭ-Т X.1111	Концепция технологий безопасности для домашней сети	
МСЭ-Т X.1112	Профиль сертификата устройства для домашней сети	
МСЭ-Т X.1113	Руководство по механизмам аутентификации пользователя для услуг домашней сети	
ITU-T X.1114	Authorization framework for home network	
МСЭ-Т X.1121	Концепция технологий безопасности для подвижной связи между конечными пунктами	
МСЭ-Т X.1122	Руководящие указания по созданию защищенных систем подвижной связи на основе PKI	
МСЭ-Т X.1123	Различные услуги безопасности для защищенной подвижной передачи данных между конечными пунктами	
МСЭ-Т X.1124	Архитектура аутентификации архитектура для подвижной связи между конечными пунктами	
МСЭ-Т X.1125	Система коррелированного реагирования в подвижной передаче данных	
МСЭ-Т X.1141	Язык разметки, предусматривающий защиту данных (SAML 2.0)	OASIS SAML 2.0
МСЭ-Т X.1142	Расширяемый язык разметки контроля доступа (XACML 2.0)	OASIS XACML 2.0
МСЭ-Т X.1143	Архитектура безопасности для защиты сообщений в подвижных веб-услугах	
МСЭ-Т X.1151	Руководство по протоколу аутентификации на базе секретного пароля с обменом ключами	
МСЭ-Т X.1152	Методы безопасной передачи данных между конечными пунктами с использованием услуг доверенной третьей стороны	
ITU-T X.1153	Management framework of a one-time password-based authentication service	
ITU-T X.1161	Framework for secure peer-to-peer communications	
МСЭ-Т X.1162	Архитектура безопасности и работы для одноранговых сетей	
МСЭ-Т X.1171	Угрозы и требования к защите информации, позволяющей установить личность в приложениях, использующих идентификацию на основе маркеров	
МСЭ-Т X.1191	Функциональные требования и архитектура аспектов безопасности IPTV	
ITU-T X.1192	Functional requirements and mechanisms for the secure transcodable scheme of IPTV	
ITU-T X.1193	Key management framework for secure internet protocol television (IPTV) services	
ITU-T X.1195	Service and content protection interoperability scheme	
МСЭ-Т X.1205	Обзор кибербезопасности	
МСЭ-Т X.1206	Независимая от поставщика концепция автоматического уведомления об информации по безопасности и распространение обновлений	
МСЭ-Т X.1207	Руководство для поставщиков услуг электросвязи по оценке рисков шпионских программ и потенциально нежелательного программного обеспечения	
МСЭ-Т X.1209	Возможности и контекстные сценарии для совместного использования и обмена информацией о кибербезопасности	
МСЭ-Т X.1231	Технические стратегии в деле противодействия спаму	

Рекомендация	Название	Эквивалентный документ
МСЭ-Т X.1240	Технологии, используемые в борьбе со спамом в электронной почте	
МСЭ-Т X.1241	Технические основы противодействия спаму в электронной почте	
МСЭ-Т X.1242	Система фильтрации спама в службе коротких сообщений (СМС), основанная на правилах, определенных пользователем	
МСЭ-Т X.1243	Система интерактивных шлюзов для противодействия спаму	
МСЭ-Т X.1244	Общие аспекты противодействия спаму в мультимедийных IP-приложениях	
МСЭ-Т X.1245	Структура противодействия спаму в мультимедийных IP-приложениях	
МСЭ-Т X.1250	Основные возможности для расширенного глобального управления идентичностью и взаимодействием	
МСЭ-Т X.1251	Структура для управления цифровой идентичностью со стороны пользователя	
МСЭ-Т X.1252	Базовые термины и определения в области управления определением идентичности	
МСЭ-Т X.1253	Руководящие указания по обеспечению безопасности для систем управления определением идентичности	
МСЭ-Т X.1303	Общий протокол оповещения (CAP 1.1)	OASIS CAP v1.1
ITU-T X.1311	Security framework for ubiquitous sensor network	
ITU-T X.1312	Ubiquitous sensor network middleware security guidelines	
МСЭ-Т X.1500	Методы обмена информацией о кибербезопасности	
МСЭ-Т X.1520	Общеизвестные уязвимости и незащищенности	
МСЭ-Т X.1521	Система оценки общеизвестных уязвимостей	
МСЭ-Т X.1570	Механизмы обнаружения, используемые при обмене информацией о кибербезопасности	
МСЭ-Т Y.2001	Общий обзор СПП	
МСЭ-Т Y.2701	Требования к безопасности для СПП версии 1	
МСЭ-Т Y.2702	Требования к аутентификации и авторизации для СПП варианта 1	
МСЭ-Т Y.2703	Применение услуги AAA в СПП	
МСЭ-Т Y.2704	Механизмы и процедуры безопасности для сетей последующих поколений	
МСЭ-Т Y.2720	Основы управления определением идентичности в СПП	
МСЭ-Т Y.2721	Требования к управлению определением идентичности в СПП и случаи применения	
МСЭ-Т Y.2722	Механизмы управления определением идентичности в СПП	
МСЭ-Т Y.2740	Требования к безопасности мобильных дистанционных финансовых транзакций в сетях последующих поколений	
МСЭ-Т Y.2741	Архитектура безопасных мобильных финансовых транзакций в сетях последующих поколений	
МСЭ-Т Y.2760	Концепция безопасности мобильности в СПП	
Дополнения к Рекомендациям МСЭ-Т серии X		
Supplement 3	ITU-T X.800–849 series – Supplement on guidelines for implementing system and network security	
Supplement 6	ITU-T X.1240 series – Supplement on countering spam and associated	

Рекомендация	Название	Эквивалентный документ
	threats	
Supplement 7	ITU-T X.1250 series – Supplement on overview of identity management in the context of cybersecurity	
Supplement 8	ITU-T X.1205 – Supplement on best practices against botnet threats	
Supplement 9	ITU-T X.1205 – Guidelines for reducing malware in ICT networks	
Supplement 10	ITU-T X.1205 – Supplement on usability of network traceback	
Supplement 11	ITU-T X.1245 – Supplement on framework based on real-time blocking lists for countering VoIP spam	
Справочники МСЭ-Т		
ссылка	Технологии внешних установок для сетей общего пользования	
ссылка	Применение компьютеров и микропроцессоров для создания, установки и защиты кабелей электросвязи	

МСЭ-Т – Бюро стандартизации электросвязи (БСЭ)
Place des Nations – CH-1211 Geneva 20 – Switzerland
Эл. почта: tsbmail@itu.int Веб-сайт: www.itu.int/ITU-T

Отпечатано в Швейцарии
Женева, 2012 г.
ISBN 978-92-61-14004-5