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

2009 г.

МСЭ-Т

ITU Международный союз 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

Безопасность в электросвязи и информационных технологиях

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

Сентябрь 2009 г.

Предисловие

Малколм Джонсон
Директор
Бюро стандартизации электросвязи МСЭ

Еще сравнительно недавно проблема безопасности в электросвязи и информационных технологиях относилась 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 стала касаться практически каждого человека.

Возросшее внимание к проблеме безопасности информационно-коммуникационных технологий можно объяснить, в частности, часто сообщаемыми случаями распространения вирусов и "червей", проникновения хакеров и возникновения угрозы 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 компьютерных и телекоммуникационных систем органов государственной власти, промышленности, торговли, ключевых инфраструктур и индивидуальных потребителей. Кроме того, все большее число стран принимают законодательство о защите данных, которое требует соблюдения установленных стандартов в отношении конфиденциальности и целостности данных.

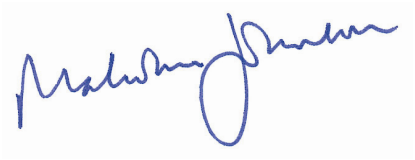
В настоящее время широко признано, что безопасность следует встраивать в системы, а не подстраивать под них, и что для того, чтобы безопасность была действительно эффективной, ее необходимо учитывать на всех этапах существования системы от планирования и проектирования до реализации, развертывания и, наконец, отключения. Ошибки адекватного учета безопасности на этапе разработки проекта и во время развертывания системы могут привести к появлению уязвимых элементов. Комитеты по стандартам играют очень значимую роль в защите систем связи и информационных технологий, обеспечивая осведомленность в вопросах безопасности, заботясь о том, чтобы аспекты безопасности стали одним из главных элементов технических спецификаций, и снабжая конструкторов и пользователей техническими стандартами руководящими указаниями в отношении того, как сделать системы и услуги связи достаточно надежными, чтобы они могли противостоять кибератакам.

В течение многих лет МСЭ-Т активно занимается проблемой безопасности в электросвязи и информационных технологиях, но с расширением использования сетей объем работы значительно возрастает 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 к множеству ресурсов, доступных в МСЭ-Т для оказания содействия пользователям в решении стоящих перед нами проблем безопасности сетей.

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 увлеченных людей из общественных организаций. 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.

Руководство задумано как справочник в помощь руководителям и менеджерам, ответственным или интересующимся проблемами безопасности информации и электросвязи, а также в помощь технологам, регламентарным органам и всем другим, желающим лучше понимать вопросы безопасности ИКТ и соответствующих Рекомендаций МСЭ-Т, в которых они рассматриваются. Надеюсь, что данное Руководство окажется полезным для тех, кто занимается вопросами безопасности ИКТ, и авторы будут благодарны читателям за предложения в отношении следующих изданий.



Малколм Джонсон
Директор
Бюро стандартизации электросвязи МСЭ

Содержание

Стр.

Стр.

Стр.

Стр.

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. Особой благодарности заслуживают Докладчики, редакторы и координаторы исследовательских комиссий МСЭ-Т по вопросам безопасности, советники МСЭ/БСЭ, участвующие в исследованиях по безопасности и, в частности Герберт Бертайн – бывший председатель ведущей исследовательской комиссии МСЭ-Т по безопасности электросвязи и Майкл Хэрроп – бывший Докладчик по проекту безопасности.

Резюме

Цель настоящего Руководства заключается в том, чтобы представить обширное введение в работу МСЭ-Т в области безопасности. Оно предназначено для тех, кто отвечает или интересуется проблемами безопасности информации и электросвязи и соответствующими стандартами и для тех, кому нужно просто лучше понимать вопросы безопасности ИКТ и соответствующие Рекомендации МСЭ-Т.

Документ начинается с обзора работ МСЭ-Т в области безопасности. В этот раздел включены ссылки на некоторые ключевые ресурсы МСЭ-Т в сфере безопасности и дополнительную информацию. Кроме того, эта вводная часть Руководства содержит сводную таблицу, в которой показано, каким образом это Руководство может использоваться различными читателями.

Далее основные требования по защите приложений ИКТ, услуг и информации приведены в разделе, где разъяснены угрозы и уязвимости, которые обусловливают требования, рассмотрена роль стандартов в удовлетворении требований, и описаны некоторые функции, необходимые для защиты различных участников, причем особое внимание уделено использованию и работе средств ИКТ. Кроме того, в этом разделе приводятся обоснования для стандартов безопасности ИКТ, и описываются перспективы деятельности МСЭ-Т в этой области.

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 определяет рамки, в которых определенным образом могут применяться различные методы обеспечения безопасности. Они также стандартизуют лежащие в их основе услуги 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. В этом разделе приводится также ссылка на руководящие указания по безопасности, относящиеся к важнейшим действиям, связанным с жизненным циклом безопасности сети.

Затем рассмотрены некоторые темы по управлению безопасностью в разделе, где исследуется управление информационной безопасностью, управление рисками, а также реагирование и обработка инцидентов.

Затем обсуждается каталог и его роль в поддержке услуг безопасности, и связанные темы аутентификации и управления определением идентичности. В этом разделе представлены такие темы, как инфраструктуры открытых ключей, телебиометрия, т. е. персональная идентификация и аутентификация с использованием биометрических устройств в сфере электросвязи, а также защита персональных данных, этот раздел также рассматривает важность защиты информационной базы Каталога.

Затем приводится обсуждение защиты сетевой инфраструктуры, в которой рассмотрены темы, относящиеся к управлению сетью и общим услугам управления безопасностью.

Далее описаны некоторые конкретные примеры и подходы к безопасности сети. Этот раздел начинается с рассмотрения требований к безопасности для сетей последующих поколений, затем следует обзор 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 Протокола интернет. Затем следует рассмотрение положений безопасности для домашних сетей и кабельного телевидения. В конце описываются проблемы безопасности в повсеместных сетях датчиков.

Несмотря на то, что разработчики приложений сегодня уделяют больше внимания необходимости встраивать безопасность в свои продукты, а не пытаться подстроить безопасность поле того, как приложение уже реализовано в продукции, приложения все еще подвергаются риску со стороны развивающейся среды угроз и со стороны внутренних уязвимостей. В этом разделе по безопасности приложений рассматривается множество

приложений ИКТ, включая передачу голоса по IP, IPTV и защищенную факсимильную передачу, и особый акцент сделан на функции безопасности, которые определены в Рекомендациях МСЭ-Т.

В следующем разделе исследуется, как противостоять некоторым общим угрозам в сети, таким как спам, вредоносный код и шпионское программное обеспечение. В нем также рассматривается важность своевременных уведомлений и распространения обновлений, 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. Затем следует обзор источников дополнительной информации.

Также добавлены приложения, содержащие определения и сокращения, используемые в этом Руководстве, сводный список Исследовательских комиссий, занимающихся проблемами безопасности, и полный список Рекомендаций, упомянутых в этом Руководстве.

Введение в 4-е издание

Структура и содержание данного четвертого издания Руководства были значительно пересмотрены. С того времени, когда в 2003 году было опубликовано первое издание Руководства, МСЭ-Т включило в свою деятельность множество новых сфер. Кроме того, было завершено и опубликовано огромное количество новых Рекомендаций, и сами Исследовательские комиссии были реструктурированы после Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) в 2008 году. Любая попытка охватить подробно всю эту работу приводит к получению большого, сложного и громоздкого документа. После консультаций с членами МСЭ-Т, для этого издания были установлены некоторые руководящие принципы. Они включают в себя следующие:

- 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.

1. Введение

1 Введение

1.1 Цели и область применения данного Руководства

Это 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.

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 материалы и дополнительные справочные материалы. В частности, оно содержит прямые ссылки на Рекомендации МСЭ-Т и на соответствующие справочные материалы и информационные документы. Оно объединяет выбранные материалы по безопасности из Рекомендаций МСЭ-Т в одну публикацию и разъясняет взаимосвязи различных аспектов работы. Включены также и результаты, достигнутые в стандартизации МСЭ-Т в сфере безопасности со времени второго 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 работу по кибербезопасности (www.itu.int/cybersecurity) и Отчет МСЭ-D о передовом опыте.

1.2 Как пользоваться Руководством

Это 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. Руководство может использоваться различными способами. В Таблице 1 показано, как оно может использоваться для удовлетворения потребностей различных групп читателей.

Таблица 1 – Как 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 в области стандартизации Высокоуровневая дорожная карта к соответствующим стандартам	В Руководстве непосредственно рассматриваются эти потребности
	Инженеры разработчики и инженеры по внедрению	Дорожная карта к соответствующим стандартам 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 в области стандартизации Высокоуровневая дорожная карта к соответствующим стандартам	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
	Не технические	Могут интересоваться техническими подробностями в определенных областях	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 в области стандартизации	В Руководстве предоставляется дорожная карта и ссылки на подробный разъяснительный текст для определенных областей
Правительство	Руководители и менеджеры	Широкий обзор сферы приложения усилий в области стандартизации Высокоуровневая дорожная карта к соответствующим стандартам	В Руководстве непосредственно рассматриваются эти потребности
	Регуляторы		
	Политики		
Неправительственные организации	Руководители/ менеджеры	Широкий обзор сферы приложения усилий в области стандартизации Высокоуровневая дорожная карта к соответствующим стандартам	В Руководстве непосредственно рассматриваются эти потребности
	Развитие и создание человеческого потенциала	Дорожная карта к соответствующим стандартам Технические подробности в определенных областях	Руководство предоставляет ссылки на подробный разъяснительный текст для определенных областей Рекомендации предоставляет технические подробности

2. Обзор видов деятельности МСЭ-Т в области безопасности

2 Обзор видов деятельности МСЭ-Т в области безопасности

2.1 Введение

Работа МСЭ-Т в области безопасности ИКТ выполняется уже более двух десятилетий, в течение этого времени несколько Исследовательских комиссий разрабатывали Рекомендации и руководящие указания во множестве ключевых областей. 17-я Исследовательская комиссия (ИК17) сегодня несет основную ответственность за работу МСЭ-Т в области безопасности 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, связанные 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 содержит обзор справочных и информационных публикаций МСЭ-Т и предоставляет графическое отображение выполняемых в настоящее время работ в области безопасности.

2.2 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 – ведущей Исследовательской комиссии по безопасности 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, 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 Главе 12.

2.3 Обзор основных тем и Рекомендаций по безопасности

Таблица 2 является быстрой ссылкой 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

Тема	Подтема	Примеры соответствующих Рекомендаций и публикаций
3. Требования к безопасности	3.2 Угрозы, риски и уязвимости 3.3 Цели безопасности 3.4 Обоснование стандартов безопасности 3.6 Требования к персональной и физической безопасности	X.1205: Обзор кибербезопасности E.408: Сети электросвязи Требования к безопасности X.1051: Руководство по управлению информационной безопасностью для организаций электросвязи Технологии внешних установок для сетей общего пользования Применение компьютеров и микропроцессоров для создания, установки и защиты кабелей электросвязи
4. Архитектуры безопасности	4.1 Архитектура безопасности открытых систем 4.2 Услуги безопасности 4.3 Архитектура безопасности для систем, обеспечивающих связь между конечными пунктами 4.3.2 Доступность сети и ее компонентов 4.4 Руководящие указания по реализации 4.5 Архитектуры, зависящие от приложений	X.800: Архитектура безопасности открытых систем X.805: Архитектура безопасности для систем связи между конечными пунктами X.810: Обзор концепции безопасности X.Sup3: МСЭ-Т Серий X.800–X.849 – Дополнения к Руководящим указаниям по внедрению системы и безопасности сети X.1162: Архитектура безопасности и работы для одноранговых сетей X.1161: Концепция защиты одноранговой связи X.1143: Архитектура безопасности для защиты сообщений в подвижных веб-услугах.
5. Управление безопасностью	5.1 Управление информационной безопасностью 5.2 Управление рисками 5.3 Обработка инцидентов	X.1051: Руководство по управлению информационной безопасностью для организаций электросвязи X.1055: Управление рисками и руководство по профилям рисков для организаций электросвязи E.409: Организация и безопасная обработка инцидентов
6. Управление каталогом, аутентификацией и идентичностью	6.1 Защита информации каталога 6.1.4 Защита персональных данных 6.2 Механизм безопасности с открытым ключом 6.2.3 Инфраструктуры открытых ключей 6.4 Управление определением идентичности 6.5 Телебиометрия	X.500: Обзор концепций, моделей и услуг X.509: Каталог: Концепции открытого ключа и сертификата атрибута X.1171: Угрозы и требования для защиты персональной идентификационной информации в приложениях, использующих идентификацию на базе меток Y.2720: Концепция управления идентичностью в СПП X.1081: Концепция для спецификации аспектов защиты и безопасности телебиометрии, X.1089: Инфраструктура телебиометрической аутентификации
7. Защита сетевой инфраструктуры	7.1 Сеть управления электросвязью 7.2 Архитектура управления сетью 7.4 Защита действий по контролю и управлению 7.5 Защита сетевых приложений 7.6 Общие услуги управления безопасностью 7.6.4 Услуги безопасности CORBA	M.3010: Принципы для сети управления электросвязью X.790: Функция исправления неполадок для приложений МСЭ-Т X.711: Общий протокол управления информацией X.736: Функции аварийной сигнализации системы безопасности X.740: Функции отслеживания проверки безопасности X.780: Руководству СУЭ для определения объектов, управляемых CORBA
8. Некоторые конкретные подходы к безопасности сети	8.1 Безопасность сетей последующих поколений (СПП) 8.2 Безопасность подвижной связи 8.3 Безопасность ля домашних сетей 8.4 Требования к безопасности для IPCablecom 8.6 Безопасность в повсеместных сетях датчиков	Y.2001: Общий обзор СПП Y.2701: Требования к безопасности для СПП, релиз 1 X.1121: Концепция технологий безопасности для подвижной связи между конечными пунктами X.1111: Концепция технологий безопасности для домашней сети J.170: Спецификация безопасности IPCablecom
9. Безопасность приложения	9.1 Передача голоса (VoIP) и мультимедиа по IP протоколу 9.2 IPTV 9.3 Защищенная факсимильная передача 9.4 Веб-услуги 9.5 Услуг на основе меток	H.235: Концепция безопасности мультимедийных систем серии H X.1191: Функциональные требования и архитектура для аспектов безопасности IPTV T.36: Возможности безопасности для использования с факсимильными терминалами Группы 3 X.1141: Язык разметки, предусматривающий защиту данных (SAML 2.0)
10. Противостояние общим сетевым угрозам	10.1 Противостояние спаму 10.2 Вредоносный код, шпионское и заведомо ложное программное обеспечение 10.3 Уведомление и распространение обновлений программного обеспечения	X.1231: Технические стратегии в деле противостояния спаму X.1240: Технологии, используемые в борьбе со спамом в электронной почте X.1244: Общие аспекты противостояния спаму в мультимедийных IP-приложениях X.1207: Руководство для поставщиков услуг электросвязи по оценке рисков шпионских программ и потенциально нежелательного программного обеспечения X.1206: Независимая от поставщика концепция автоматического уведомления об информации по безопасности и распространение обновлений
Полный набор Рекомендаций МСЭ-Т по безопасности представлен по адресу: http://www.itu.int/ITU-T/Рекомендация		

3. Требования к безопасности

3 Требования к безопасности

3.1 Введение

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; каковы уязвимые элементы, связанные с этими ресурсами; и общие риски, которым эти угрозы и уязвимые элементы подвергают ресурсы.

В этом разделе представлены основные требования по защите приложений ИКТ, услуг и информации, точки зрения на угрозы и уязвимые элементы, которые обусловливают требования, рассматривается роль стандартов в удовлетворении требований, и определяются некоторые особенности, которые необходимы для защиты различных сторон, участвующих в применении и работе с приложениями 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, сведения в этом разделе носят общий характер. Требования для конкретных приложений и сред рассматриваются в следующих разделах.

3.2 Угрозы, риски и уязвимости

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

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

Ресурсы, которые должны быть защищены, включают в себя:

- услуги в области связи и компьютерных операций;
- информация 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* 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.

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.

Рекомендации МСЭ-Т различают четыре вида уязвимости:

- 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, не применение 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. 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, уязвимость защиты будет существовать на протяжении всего срока эксплуатации системы или протокола, если не принять конкретных мер по устранению уязвимости. Риски нарушения безопасности, обусловленные свойствами протокола, в случае стандартизованных протоколов могут быть весьма существенными и глобальными по масштабу. Поэтому важно понять и выявить уязвимость протоколов и принять меры по устранению уязвимых элементов при их обнаружении.

Организации по стандартизации как несут ответственность, так 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 уязвимости, связанные с обработкой информации и сетями связи, невозможно обеспечить адекватную защиту без систематического применения защиты в соответствии с установленной политикой. Политика 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 Е.408 *Требования к безопасности сетей электросвязи*, 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 Е.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 Х.1205 *Обзор кибербезопасности* представлена классификация угроз безопасности с организационной точки зрения и обсуждение угроз на различных уровнях сети.

3.3 Общие задачи безопасности для сетей ИКТ

Задачи безопасности для сетей электросвязи состоят в следующем:

a) Доступ к сетям 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 пользователи должны нести ответственность за свои, и только свои действия в сетях электросвязи.

e) В целях обеспечения готовности сети электросвязи должны быть защищены от нежелательного доступа или воздействия.

f) Следует обеспечить возможность получения от сетей электросвязи информации, связанной с безопасностью, но только санкционированные пользователи должны иметь возможность получения такой информации.

g) В случае обнаружения нарушений безопасности они должны обрабатываться управляемым способом, согласно заранее установленному плану, с тем чтобы минимизировать потенциальный ущерб.

h) При обнаружении взлома защиты необходимо иметь возможность восстановить нормальные уровни защиты.

i) Архитектура безопасности сетей электросвязи должна обеспечивать определенную гибкость, чтобы поддерживать разные стратегии безопасности, например различную эффективность механизмов защиты.

Задачи(а) могут (может) быть выполнены(а) путем внедрения следующих услуг безопасности:

- конфиденциальность;
- целостность данных, систем и программ;

- отчетность, включая аутентификацию, сохранность информации и контроль за доступом; и
- готовность.

Одним из типов сетей ИКТ, приобретающих все большую значимость, является сеть последующих поколений (СПП). Требования к безопасности и задачи СПП рассмотрены в Разделе 8.

3.4 Обоснование стандартов безопасности

Требования к общей структуре сетевой безопасности для международной электросвязи обусловлены совокупностью различных факторов, включающих потребителей/абонентов, общественность/органы власти и операторов сетей/поставщиков услуг. Желательно, чтобы требования к безопасности сети электросвязи исходили из стандартов международного уровня, что будет способствовать общности подходов и взаимопомощи, а также будет более экономически эффективным, 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.

Существенными преимуществами применения стандартных решений и для продавцов, и для пользователей систем являются экономия за счет масштаба при разработке продуктов и взаимодействие компонентов в сетях электросвязи.

3.5 Эволюция стандартов безопасности МСЭ-Т

Работа МСЭ-Т в области безопасности за последние годы значительно расширилась, как можно видеть из дальнейших разделов, в которых многие отдельные Рекомендации рассматриваются более подробно. Здесь рассматриваются некоторые ключевые аспекты этого развития, особенно те из них, которые связаны с требованиями по обеспечению безопасности.

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 1991 году в Рекомендации МСЭ-Т X.800 *Архитектура обеспечения безопасности в среде взаимодействия открытых систем для приложений МККТТ*. Вышеупомянутая Рекомендация МСЭ-Т E.408 *Требования к безопасности сетей электросвязи*, которая была опубликована в 2004 году, основывается на принципах и терминологии Рек. МСЭ-Т X.800. Рекомендация МСЭ-Т E.408 носит общий характер и не выделяет и не определяет требования для конкретных сетей. Не были рассмотрены новые услуги безопасности. Вместо этого, 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 *Обзор кибербезопасности*. 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 защита в глубину и контроль за доступом. Рассматривает 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, профессиональная подготовка, 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 переданной и/или сохраненной 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. 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 строгого выполнения обязательств, а также для гарантий соблюдения личной тайны пользователя. Технологии кибербезопасности также могут использоваться для установления достоверности пользователя.

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, сетей, приложений и ресурсов. Также безопасность должна быть всесторонней во всех уровнях сетей. Принятие уровневого подхода к проблеме безопасности, который в союзе с сильным управлением на основе заданных правил и обеспечение их выполнения предоставит профессионалам по безопасности выбор решения по этому вопросу, который будет модульным, гибким и расширяемым.

Современные методы обеспечения кибербезопасности включают в себя:

- Криптографию: эта мощная технология поддерживает ряд услуг безопасности, включая шифрование данных при передаче и во время хранения.
- Контроль за доступом: цель состоит в ограничении возможности пользователей в доступе, использовании, просмотре или изменении информации в главных компьютерах или сетях.
- Целостность системы: цель состоит в обеспечении того, чтобы система и ее данные не были изменены или искажены неуполномоченными сторонами или несанкционированным образом.
- Аудит, регистрацию и мониторинг: помогает системным администраторам собирать и анализировать сетевые журналы во время и после злонамеренных воздействий. Данные могут использоваться для оценки эффективности стратегии безопасности, которая применена в сети.

– Управление: помогает системным администраторам при анализе и настройке параметров безопасности на их главных компьютерах и сетях. Административный контроль может использоваться для проверки точности функционирования сети и подключения настройки элементов.

3.6 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 Рек. МСЭ-Т X.1051, *Руководство по управлению информационной безопасностью для организаций электросвязи*. 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 Рек. 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 публикациях МСЭ-Т *Технологии внешних установок для сетей общего пользования* (1991 г.) и *Применение компьютеров и микропроцессоров для создания, установки и защиты кабелей электросвязи* (1999 г.). В этих документах также рассматривается мониторинг систем в целях предотвращения повреждений и предложены 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 электросвязи. Это привело к созданию *архитектуры безопасности для взаимосвязи открытых систем* (Рек. 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 а*рхитектуры безопасности для систем, обеспечивающих связь между оконечными точками* (Рекомендация МСЭ-Т X.805), а также множеству определяемых приложением архитектур для таких областей, как управление сетью, одноранговая связь и подвижные веб-сервера. Описанная далее в данном разделе Рекомендация МСЭ-Т X.805 дополняет другие Рекомендации 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 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, МСЭ-Т X.800 содержит общее описание услуг обеспечения безопасности и соответствующих механизмов, которые могут использоваться для оказания этих услуг. Кроме того, в ней определяется наиболее пригодное расположение услуг обеспечения безопасности для базовой эталонной модели взаимосвязи открытых систем (OSI) с семью уровнями, т. е. уровня, на котором следует реализовывать услуги обеспечения безопасности.

МСЭ-Т X.800 касается только тех видимых аспектов канала связи, которые позволяют оконечным системам добиться безопасной передачи информации между ними. Она не является спецификацией по реализации систем и не служит основой для оценки соответствия варианта реализации тому или иному стандарту безопасности. В ней также не указаны сколько-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 понятия, содержащиеся в МСЭ-Т X.800, 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*, *контроль за доступом*, *конфиденциальность данных*, *целостность данных* и *сохранность информации*), наряду с более общими (всеобъемлющими) услугами, такими как *проверенные функциональные возможности*, *обнаружение событий*, а также *проверка безопасности* и *восстановление защиты*. До принятия МСЭ-Т X.800 существовал широкий круг представлений о том, какие базовые услуги безопасности необходимы и в чем именно должна заключаться каждая услуга. В МСЭ-Т X.800 отражена четко согласованная международная позиция в отношении этих услуг.

Ценность и общая применимость МСЭ-Т X.800 основана на том, что она отражает единодушие 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 МСЭ-Т. X.800 была выявлена необходимость в дополнительных стандартах, связанных с безопасностью связи. В результате началась работа по разработке 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 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 системных объектов внутри систем и на взаимодействие между системами. Они не предусматривают методику построения систем или механизмов.

Структуры относятся как к элементам данных, так и к последовательности операций, но не к элементам протокола, которые используются для предоставления конкретных услуг обеспечения безопасности. Эти услуги могут применяться к взаимодействующим объектам систем, а также к данным обмена между ними, и к данным, которые управляются системами.

В *Обзоре структуры безопасности* (Рекомендация МСЭ-Т X.810) представлены различные структуры и описаны общие понятия, включая домены безопасности, ответственный объект и политику защиты, которые используются во всех структурах. В нем также описан формат общих данных, который может быть использован для безопасной передачи информации, как в целях аутентификации, так и для контроля за 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 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. *Структура аутентификации* (Рекомендация МСЭ-Т X.811) определяет основные понятия аутентификации; устанавливает возможные классы механизма аутентификации; определяет услуги для этих классов механизма аутентификации; устанавливает функциональные требования для протоколов поддержки этих классов аутентификации; и устанавливает требования по общему управлению аутентификацией.

Контроль за 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, аутентификация и проверка, а также эксплуатационные требования в отношении контроля за доступом.

Неотказуемость – это способность не допустить, чтобы объекты впоследствии отказались от того, что они выполнили действия. Неотказуемость связана с установлением доказательств, которые впоследствии могут быть использованы для опровержения ложных утверждений. В МСЭ-Т-Т. X.800 предусмотрены 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. *Структура неотказуемости* расширяет понятия услуг по обеспечению неотказуемости, как они описаны в МСЭ-Т-Т. X.800, и предусматривает основу для развития этих услуг. Она также устанавливает возможные механизмы поддержки этих услуг и общие эксплуатационные требования в отношении неотказуемости.

Конфиденциальность – это характеристика, которая делает информацию недоступной или не раскрываемой для неуполномоченных лиц, объектов или процессов. Цель услуги обеспечения конфиденциальности состоит в том, чтобы защитить информацию от несанкционированного раскрытия. Структура обеспечения конфиденциальности (Рекомендация МСЭ-X.814) относится к конфиденциальности информации при поиске, передаче и управлении; она определяет основные понятия конфиденциальности, и возможные классы механизмов обеспечения конфиденциальности и средства, необходимые для каждого класса этих механизмов. Она также устанавливает процесс управления и необходимые вспомогательные услуги, а 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. *Концепция целостности* (Рекомендация МСЭ-Т X.815) относится к целостности 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 связанные услуги, необходимые для поддержки этого класса механизмов. Обратите внимание, что, хотя стандарты архитектуры безопасности концентрируются главным образом на целостности данных, другие аспекты целостности, например, целостность системы также имеют для безопасности больше значение.

4.3 Архитектура безопасности для систем, обеспечивающих связь между конечными пунктами

В 2003 году, после более пристального рассмотрения архитектуры безопасности для сетей была утверждена Рекомендация МСЭ-Т X.805 *Архитектура безопасности для систем, обеспечивающих связь между конечными пунктами*. Эта архитектура, которая строится на базе некоторых концепций 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 МСЭ-Т X.805

Архитектура X.805 определяется тремя основными понятиями: уровнями безопасности, плоскостями и аспектами (параметрами X.805) для сети между конечными пунктами. При распределении требований 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.

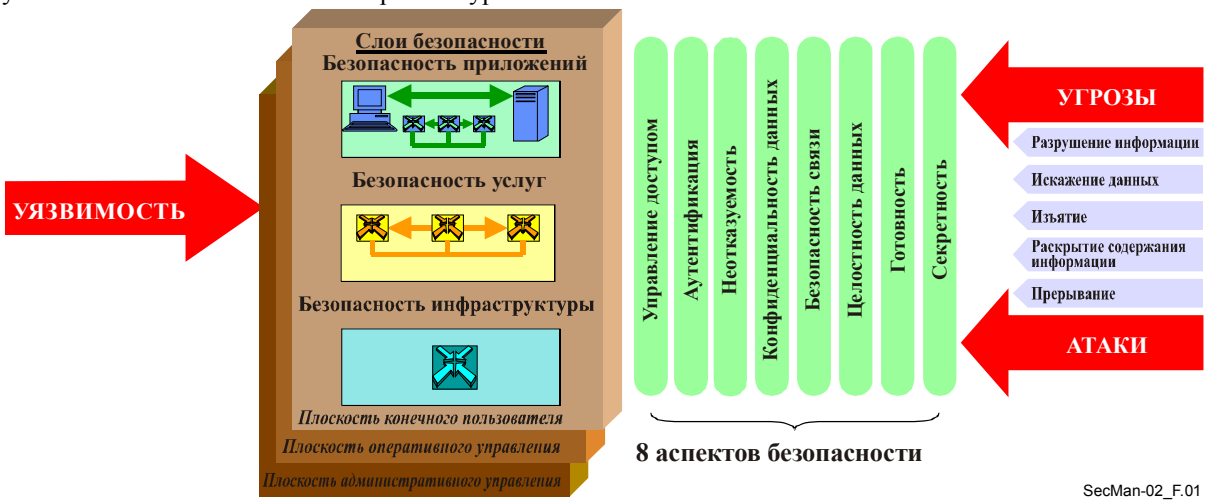


Рисунок 1 – Элементы архитектуры безопасности согласно Рекомендации МСЭ-Т X.805

В МСЭ-Т X.805 *аспектом безопасности* называется набор мер безопасности, разработанных для конкретного аспекта безопасности сети. Основные услуги безопасности МСЭ-Т X.800 – *Контроль за доступом, Аутентификация, Конфиденциальность данных, Целостность данных* и *Неотказуемость* соответствуют функциональным возможностям соответствующих *аспектов безопасности* МСЭ-Т X.805, показанных на Рисунке 1. Кроме того, МСЭ-Т X.805 вводит три аспекта: *Безопасность связи, Доступность* и *Секретность*, которых нет в МСЭ-Т X.800. Эти аспекты обеспечивают дополнительную защиту сети и защищают от всех основных угроз безопасности. Эти аспекты не ограничиваются сетью, но также распространяются на приложения и информацию конечного пользователя. Аспекты безопасности применяются к поставщикам услуги или предприятиям, предоставляющим своим потребителям услуги безопасности.

Восемь аспектов безопасности МСЭ-Т X.805 это:

- аспект *Контроль за доступом,* который обеспечивает защиту ресурсов сети от несанкционированного использования и гарантирует, что к сетевым элементам, хранимой информации, информационным потокам, услугам и приложениям будут допущены только уполномоченный персонал или уполномоченные устройства;
- аспект *Аутентификация,* которая подтверждает идентичности объектов связи, гарантирует достоверность заявленной идентичности объектов, участвующих в связи, например, физического лица, устройства, услуги или применения, а также гарантирует, что объект не пытается выдать себя за другой объект или воспроизвести несанкционированным образом предыдущее сообщение;
- аспект *Неотказуемость*, который обеспечивает средства для предотвращения отрицания физическим лицом или объектом факта совершения им конкретного действия в отношении данных посредством предъявления имеющегося доказательства различных действий, связанных с сетью, например, доказательство обязательства, намерения или совершения; доказательство происхождения данных, доказательство права собственности, доказательство использования ресурса. Она также обеспечивает наличие доказательств, которые могут быть предъявлены третьей стороне и использоваться в подтверждение того, что какое-либо событие или действие имело место;
- аспект *Конфиденциальность данных*, который обеспечивает защиту данных от несанкционированного раскрытия и гарантирует, что содержание данных не будет понято неуполномоченными объектами;
- аспект *Безопасность связи,* который гарантирует, что информация передается только между уполномоченными конечными точками, то есть информация не изменяет направления и не перехватывается при передаче между этими конечными точками;
- аспект *Целостность данных,* который гарантирует, что данные защищены от несанкционированного изменения, удаления, создания и дублирования, а также обеспечивает создание сигнала тревоги, в случае действий, которые могли бы нарушить целостность данных;
- 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 из-за событий, влияющих на сеть; 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.

Как показано на Рисунке 1, в дополнение к аспектам безопасности, МСЭ-Т X.805 определяет три уровня секретности и три плоскости. 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. Это три следующих слоя:

- *слой инфраструктуры*, который состоит из сетевых средств передачи данных, а также из отдельных сетевых элементов. Примерами элементов, относящихся к этому слою, являются 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 управлением сетью, контролем за сетью или сигнальными операциями, а также операциями конечного пользователя. Сети следует разрабатывать так, чтобы события в одной плоскости безопасности были бы изолированы от других плоскостей безопасности.

Плоскости безопасности это следующие плоскости:

- *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 сигнальными операциями для настройки (и модификации) сквозной связи по сети независимо от среды передачи и технологии, используемой в сети; и
- *плоскость конечного пользователя*, которая связана с сигнальными операциями для настройки (и модификации) сквозной связи по сети независимо от среды передачи и технологии, используемой в сети. Эта плоскость также служит для защиты потоков данных конечного пользователя.

Архитектура, предусмотренная в МСЭ-Т-Т X.805, может служить руководством для разработки всеобъемлющей политики в области безопасности, 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. Архитектура безопасности X.805 может помочь в поддержании программы безопасности, обеспечивая учет каждого аспекта безопасности на каждом слое и в каждой плоскости безопасности при внесении изменений в программу безопасности.

Несмотря на то, что 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 *Роли конечных пользователей и сетей электросвязи в рамках архитектуры безопасности.*

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 введены в этот аспект.

Инфраструктура как слой безопасности состоит из сетевых средств передачи, а также отдельных сетевых элементов, защищаемых аспектов безопасности. Слой инфраструктуры представляет собой блоки основания сетей, их услуг и приложений. Примерами компонентов, которые относятся к слою инфраструктуры, являются

отдельные маршрутизаторы, коммутаторы и серверы, а также линии связи между отдельными маршрутизаторами, коммутаторами и серверами.

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 *Параметры и значения показателей готовности для сквозных международных цифровых трактов с постоянной скоростью передачи* 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 к 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, это: МСЭ-Т G.1000 *Электросвязь. Качество обслуживания: Структура и определения*; МСЭ-Т G.1030 *Оценка сквозного качества в IP сетях для приложений передачи данных*; *Модель сети для оценки качества мультимедийной передачи по интернет-протоколу*; и МСЭ-Т G.1081 *Точки контроля качественных показателей для IPTV*.

4.4 Руководящие указания по реализации

Все стандарты архитектуры безопасности МСЭ-Т являются составными частями серии Рекомендаций безопасности МСЭ-Т X.800-849. Руководящие указания по реализации приведены в дополнении к этой серии Рекомендаций (X Дополнение 3 к серии МСЭ-Т X.800–X.849 – *Дополнения к руководству по реализации системы и безопасность сети*). В этом дополнении содержатся руководящие указания по важнейшим действиям по 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 архитектуры, определяемых приложениями

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

4.5.1 Одноранговая связь

Одноранговая связь (P2P) – это пример сетевых архитектур, в которой все пользователи имеют равные права и ответственность, в отличие от модели клиент-сервер. В случае связи P2P пользователь может быть как сервером, так и клиентом. Когда в сети P2P передаются данные или сообщения один пользователь связывается непосредственно с другим. Так как трафик обрабатывается и распределяется для каждого пользователя, для сети P2P не требуется сверхмощных компьютеров или широкополосных сетей.

Сеть P2P – это наложенная сеть 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.

С быстрым прогрессом сетей электросвязи и компьютерных технологий, все больше и больше информации и вычислительных ресурсов будут доступными на распределенных узлах, а не на ограниченном числе централизованных серверов.

Сети P2P обычно используются для связи между узлами через временные соединения. Такие сети полезны для многих целей. Совместное использование файлов, содержащих звук, изображение, текст или что-либо другое в

цифровом формате, используется очень широко. Для передачи данных в реальном времени, например, телефонного трафика, также используется технология P2P.

4.5.1.1 Архитектура безопасности и работы для одноранговых сетей

Общая архитектурная модель, связанная с безопасностью, которая может быть применена в различных P2P сетях, 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.

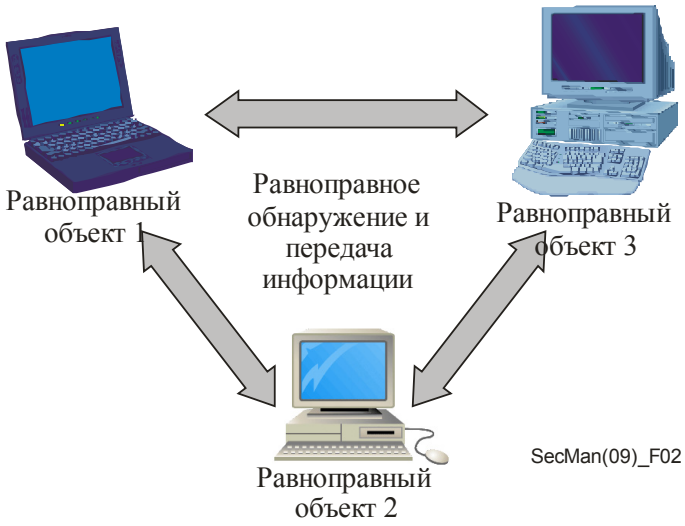


Рисунок 2 – Архитектура услуги P2P

На Рисунке 3 показана физическая и логическая архитектура сети P2P. В физической сети P2P пользователь может присоединиться к услугам P2P с помощью 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 участником поставщиком услуг, расположенным в домене другой сети.

На Рисунке 3 также 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.

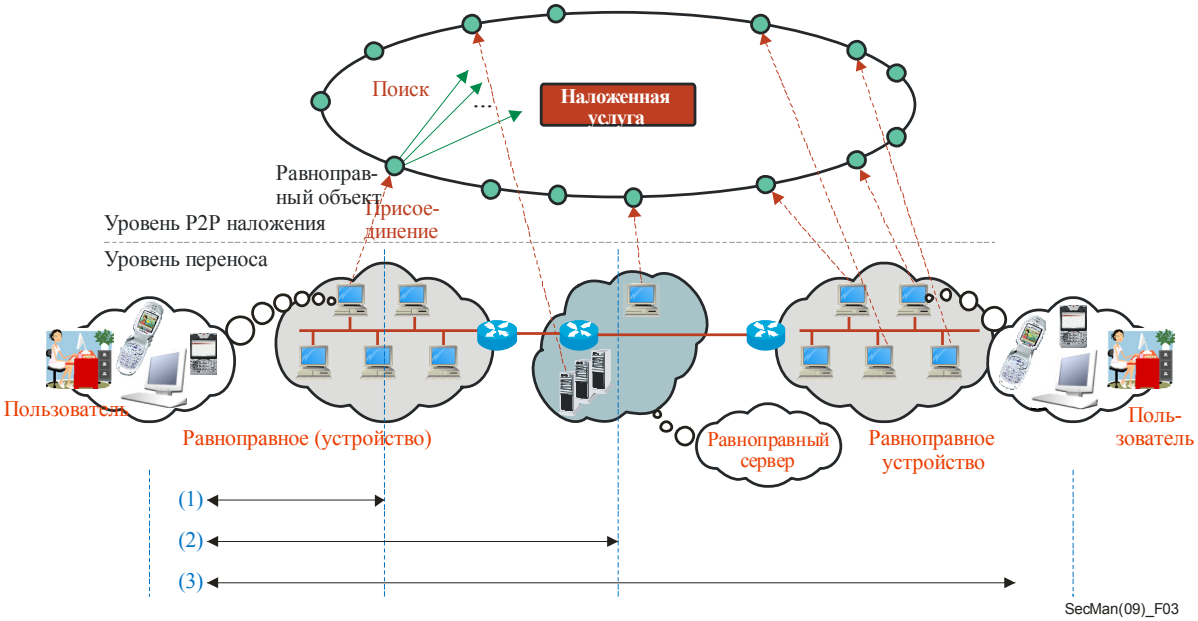


Рисунок 3 – Архитектурная эталонная модель для сети P2P

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 "*Концепция защиты одноранговой связи*".

Угрозы соединениям P2P включают в себя подслушивание, постановку помех, вторжение и внесение изменений, несанкционированный доступ, непризнание авторства, активное вмешательство в соединение и атак типа Sybil. Меры противодействия угрозам для P2P показаны в Таблице 3.

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

Функции / Требования	Шифрования	Обмен ключами	Цифровая подпись	Управление доверием	Контроль за доступом	Целостность данных	Обмен аутентификацией	Нотариальное заверение	Защищенная маршрутизация	Управление 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
Сохранность информации			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, *Архитектура безопасности для защиты сообщений в подвижных веб-услугах*. 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 полных веб-услуг и традиционные приложения, которые не поддерживают стеки протокола полных веб-услуг;
- механизмы аутентификации сообщений, 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 МСЭ-Т X.1143 для подвижных веб-услуг.

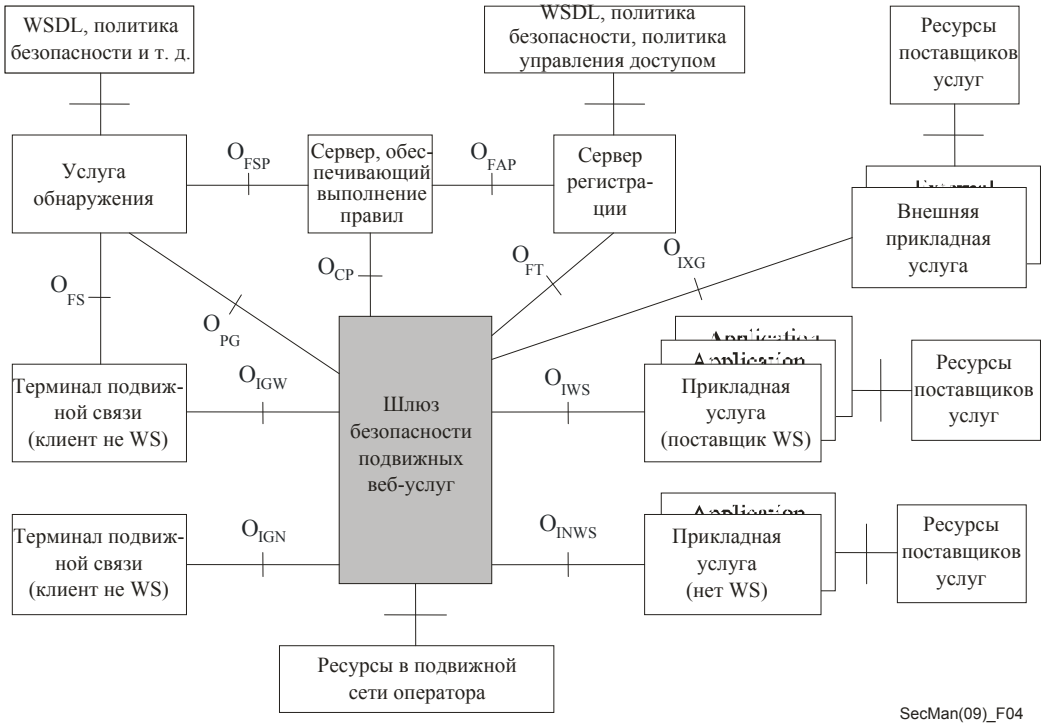


Рисунок 4 – Архитектура безопасности для подвижных веб-услуг

Архитектура безопасности состоит из следующих компонентов:

- Подвижные терминалы, которые являются клиентами подвижных веб-услуг;
- Шлюз безопасности подвижных веб-услуг (MWSSG). Все запросы от подвижных клиентов передаются на MWSSG, который также выполняет контроль за доступом;
- Служба принятия решений, которая управляет политикой безопасности, относящейся к безопасной обработке сообщений и политикой контроля за доступом для сообщений;
- Служба приложений, которая предоставляет клиентам различные коммерческие услуги;
- Служба обнаружения, которая хранит информацию интерфейса для служб приложений и соответствующие правила безопасности для доступа клиентов к службам приложений; и
- Сервер 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 контроля за доступом к целевыми услугам.

4.6 Архитектура безопасности и модели 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; 8.5.1 Архитектура IPCablecom2; и 9.2 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.

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 защиту своей информации путем внедрения структурированного процесса управления безопасностью.

Эффективное управление информационной безопасностью достигается путем реализации набора соответствующих мер управления. Эти меры управления, которые применяются к устройствам электросвязи, услугам и приложениям, должны быть сформированы, 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 безопасности, так и бизнеса.

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).

Наиболее широко используемой спецификацией ISMS является та, что опубликована в серии стандартов ИСО/МЭК серии 27000 по ISMS, в которую входят стандарты по основам ISMS, требования, кодекс применения, руководящие указания по реализации и связанным тематикам. МСЭ-Т и ИСО/МЭК совместно разработали Рекомендацию МСЭ-Т X.1051 | ИСО/МЭК 27011 *Руководство по управлению информационной безопасностью для организаций электросвязи*, основанную 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 содержит 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;

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

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

- информация, относящаяся к организациям электросвязи, 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 должен предоставляться только по необходимости. В качестве продолжения положений о готовности, организациям электросвязи следует отдавать приоритет важнейшим сеансам связи в неотложных случаях, и соответствовать регламентарным требованиям.

Управление информационной безопасностью в организациях электросвязи требуется вне зависимости от среды или режима передачи. Если управление информационной безопасностью не реализовано надлежащим образом, то риск, связанный с использованием системы, возрастает.

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 организации электросвязи 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 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 кратко введена в Разделе 3 при обсуждении Рекомендации МСЭ-Т X.1205 *Обзор кибербезопасности*. Более подробные руководящие указания по управлению рисками содержатся в Рекомендации МСЭ-Т X.1055 *Управление рисками и руководство по профилям рисков для организаций электросвязи*, которая определяет процессы и методы по снижению рисков информационной безопасности. Эти процессы и методы 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.

Разработано множество 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 5.

Рисунок 5 – 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 том, что касается их критичности, а также для оказания помощи в определении 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.

5.3 Обработка инцидентов

Последовательность в определении, реагировании и распространении информации об инцидентах, связанных с безопасностью, это ежедневная составляющая управления безопасностью. В том случае, если такие инциденты не оцениваются и не обрабатываются должным образом, организации оказываются уязвимыми для последующих, возможно более серьезных атак.

В том случае, если процедура обработки инцидентов не налажена, то при обнаружении инцидента, связанного с безопасностью, может не формироваться надлежащего сообщения или не выполняться надлежащего анализа этого инцидента. Кроме того, могут отсутствовать процедуры продвижения сообщений или получения технической помощи или руководящих указаний, даже в том случае, когда проблемы, возникающие при таких инцидентах, часто влекут за собой последствия, которые распространяются далеко за пределы IT или сетей. Например, инциденты могут приводить к возникновению юридических, финансовых или имиджевых рисков, или они могут быть причиной для вмешательства правоохранительных органов. Отсутствие эффективных процедур обработки инцидентов может привести к применению "скороспелых решений" или решению проблемы обходным способом, вместо того, чтобы надлежащим образом рассмотреть, задокументировать и сообщить о проблеме, в таком случае существует риск возникновения более серьезных проблем в будущем.

Так как организации осознают потребность в последовательном и эффективном управлении безопасностью сетей и операций, обработка инцидентов становится все более обычным делом. Надлежащим образом обученная группа или подразделение с соответствующими полномочиями может точно и правильно обрабатывать инциденты в области безопасности.

Для того, чтобы успешно обрабатывать и сообщать об инцидентах, необходимо понимать, как инциденты обнаруживаются, управляются и разрешаются. Создавая общую структуру для обработки инцидентов, т. е. физических, административных или организационных и логических инцидентов, можно получить общую картину структуры и потока инцидента. В Рекомендации МСЭ-Т E.409 *Организация и безопасная обработка инцидентов: Руководящие указания для организаций электросвязи*, содержится обзор и структура, которые обеспечивают руководство для планирования организации по обнаружению и обработке инцидентов, связанных с безопасностью. Она носит общий характер и не определяет и не рассматривает требования для конкретных сетей.

При сообщении и обработке инцидентов важно иметь единую терминологию. Использование различной терминологии может привести к непониманию, результатом которого может стать либо не придания инциденту безопасности должного внимания, либо не выполнение необходимых действий по его обработке для того, чтобы остановить инцидент и предотвратить его повторное возникновение. Кроме того, определение того, что считается инцидентом, может быть различным среди специалистов различных профессии, различных организаций и людей. Рекомендация МСЭ-Т E.409 пытается стандартизировать терминологию по обнаружению и описанию инцидента, а также классифицирует инциденты по их серьезности, как показано на Рисунке 6.

Рисунок 6 – МСЭ-Т E.409 – пирамида событий и инцидентов

В Рекомендации МСЭ-Т E.409 также определяется структура обработки инцидентов, как показано на Рисунке 7 и устанавливаются процедуры для обнаружения, классификации, оценки, обработки инцидентов и последующих действий.

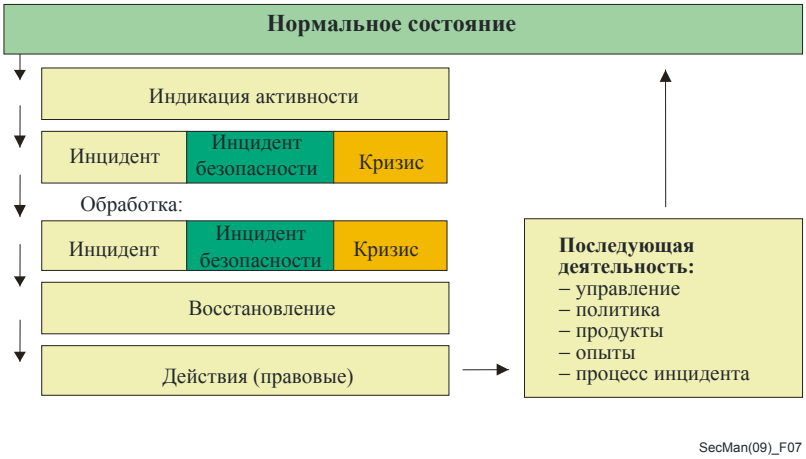


Рисунок 7 – МСЭ-Т E.409 – структура обработки инцидентов

Недавно одобренная Рекомендация МСЭ-Т X.1056 *Управление инцидентами безопасности – руководящие указания для организаций электросвязи*, создана на руководящих указаниях, приведенных в Рекомендации МСЭ-Т E.409. Организациям электросвязи необходимо внедрить процессы как по обработке инцидентов, так и по предотвращению их повторного возникновения. В Рекомендации МСЭ-Т X.1056 описано пять высокоуровневых процессов управления безопасностью и их взаимосвязи. Они показаны на Рисунке 8 и Рисунке 9.

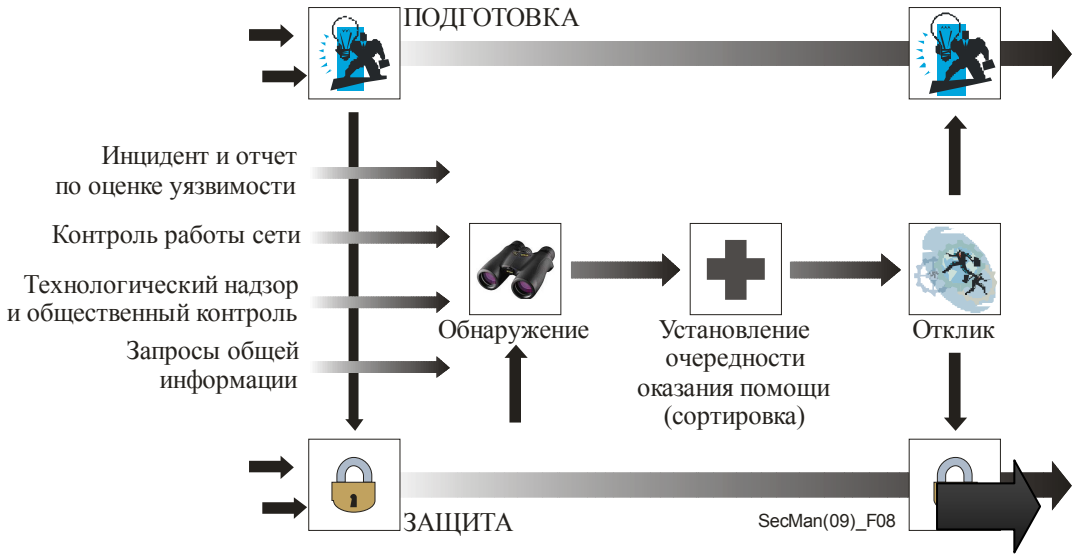


Рисунок 8 – Пять высокоуровневых процессов управления безопасностью

(Источник: Аналитический Обзор SEI MOSAIC: Технический Отчет CMU/SEI-2004-TR-015 – Определение процессов управления инцидентами для CSIRT: Незавершенные работы)

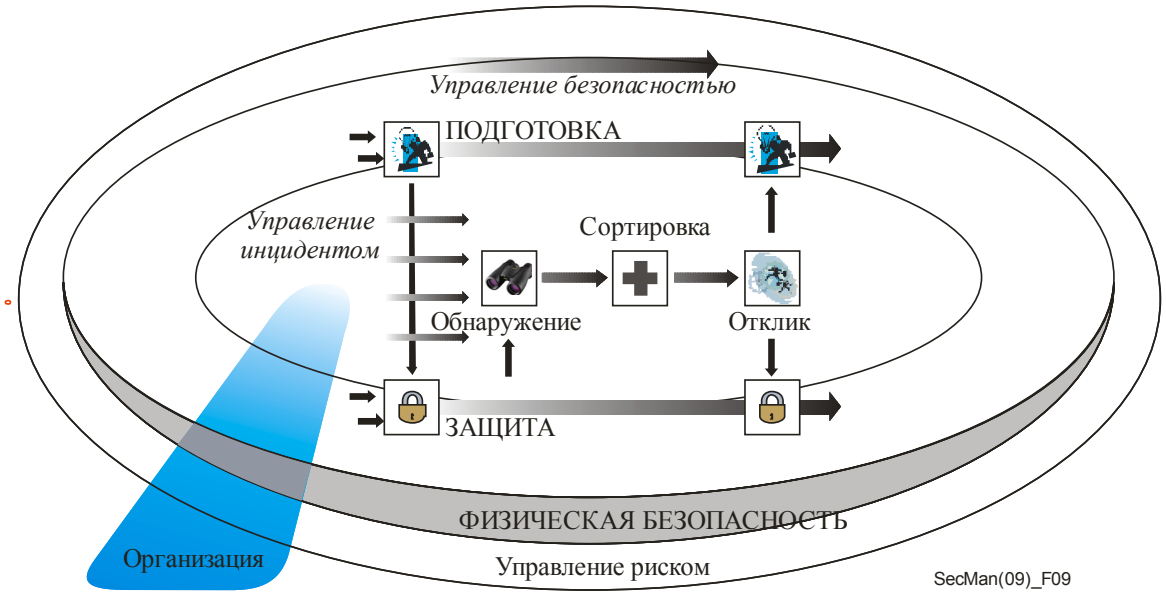


Рисунок 9 – Сравнение управления инцидентами и управления безопасностью

(Источник: Аналитический Обзор SEI MOSAIC: Технический Отчет CMU/SEI-2004-TR-015 – Определение процессов управления инцидентами для CSIRT: Незавершенные работы)

Кроме того, Рекомендация МСЭ-Т X.1056 определяет диапазон реактивных и проактивных услуг управления, а также услуг управления качеством безопасности, которое должна обеспечить команда по управлению инцидентами в области безопасности.

6. Управление каталогом, аутентификацией и определением идентичности

6 Управление каталогом, аутентификацией и определением идентичности

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 вводится в Рекомендации МСЭ-Т X.500 *Каталог: Обзор концепций, моделей и услуг*, и разработан в Рекомендациях МСЭ-Т X.501 *Каталог: Модели*, МСЭ-Т X.509 *Каталог: Концепции открытого ключа и сертификата атрибута* и МСЭ-Т X.519 *Каталог: Спецификации протокола*, 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 предоставлении услуг безопасности путем определения и поддержания регистрационных данных, аутентификации в форме сертификатов безопасности. В частности, Рекомендации МСЭ-Т серии X.500 рассмотрено два аспекта безопасности:

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

Этот раздел начинается с обсуждения важности безопасности самого каталога и необходимость защищать информацию 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

При работе по проблемам каталога в центре внимания постоянно находится защита информации, которая является главной целью управления определением идентичности. Защита информации каталога – это главным образом вопрос секретности, т. е. защиты от несанкционированного раскрытия важных персональных данных, но она также включает в себя 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 право и кому *необходимо* ее знать.

Существует три аспекта защиты информации:

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

Почти самого начала функции по защите информации являются важнейшей частью МСЭ-Т X.500. МСЭ-Т X.500 – единственная спецификация каталога, имеющая эти важные функции.

6.1.2 Аутентификация пользователей каталога

Каталог, соответствующий МСЭ-Т X.500, может допускать анонимный доступ к некоторой незначительной информации. Однако для получения доступа к более важным данным, требуется некоторый уровень аутентификации пользователей. МСЭ-Т X.500 предлагает несколько уровней аутентификации, включая следующие:

a) только имя;

b) имя плюс незащищенный пароль, т. е. имя и пароль, который передается в виде открытого текста;

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 входа.

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

6.1.3 Контроль за доступом к каталогу

Контроль за 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 контроля за доступом. Элемент информации, который должен быть защищен, называется защищаемым элементом. Защищаемые элементы можно сгруппировать по обычным свойствам контроля за 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 потребует более высокого уровня аутентификации, чем получение менее важной информации.

Контроль за 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.

Контроль за доступом касается "права знать". Однако "необходимость знать" – это нечто большее, чем просто контроль за доступом. Обладание *правом знать* не позволяет пользователю получить информацию, если не установлена *необходимость знать*, 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 право доступа к некоторой информации, это право 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 МСЭ-Т X.500 является уникальной и очень мощной. Защита персональных данных – эта проблема возникает, главным образом, 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 МСЭ-Т X.500 приведена созданная в виде таблиц концепция административного управления услугой, которая помимо управления общими услугами, обеспечивает 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 типу услуги и типу 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 должны гарантировать, что поиск направлен на получение информация об одном объекте или малом их числе. Это не даст возможности тому, кто ищет, запрашивать огромные массивы информации, и предотвратит ее прочесывание;
- список элементов информация, относящихся к данному типу услуги; и
- управляющую информацию по отдельным объектам, представленным в каталоге. Используемая таблица взаимодействует с управляющей информацией объекта я целью ограничения объема информации, предоставляемой об этом объекте. 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, предоставить фальшивый адрес. Другие объекты могут не желать сообщать свой электронный адрес 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 – недавно утвержденная Рекомендация МСЭ-Т X.1171 *Угрозы и требования для защиты персональной идентификационной информации в приложениях, использующих идентификацию на базе меток*, которые более подробно рассматриваются в Разделе 9.5, касающемся услуг на основе меток, а 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 Усиленная аутентификация: механизмы обеспечения безопасности с открытым ключом

Инфраструктура с открытым ключом (PKI) упрощает управление открытым ключом для предоставления услуг аутентификации, шифрования, целостности и сохранности информации. Фундаментальной технологией для PKI является шифрование с открытым ключом, которое описано ниже. Рекомендация МСЭ-Т X.509 *Каталог: Структуры открытого ключа и сертификата атрибута* – это стандарт PKI для надежной аутентификации, основанной на сертификатах открытого ключа органах по сертификации. В дополнение к определению структуры аутентификации для PKI, МСЭ-Т X.509 также описывает инфраструктуру управления полномочиями (PMI), которая используется для проверки прав и полномочий пользователей в контексте надежной авторизации, основанной на сертификатах атрибутов и органах по присвоению атрибутов. Компоненты PKI и PMI показаны на Рисунке 10.

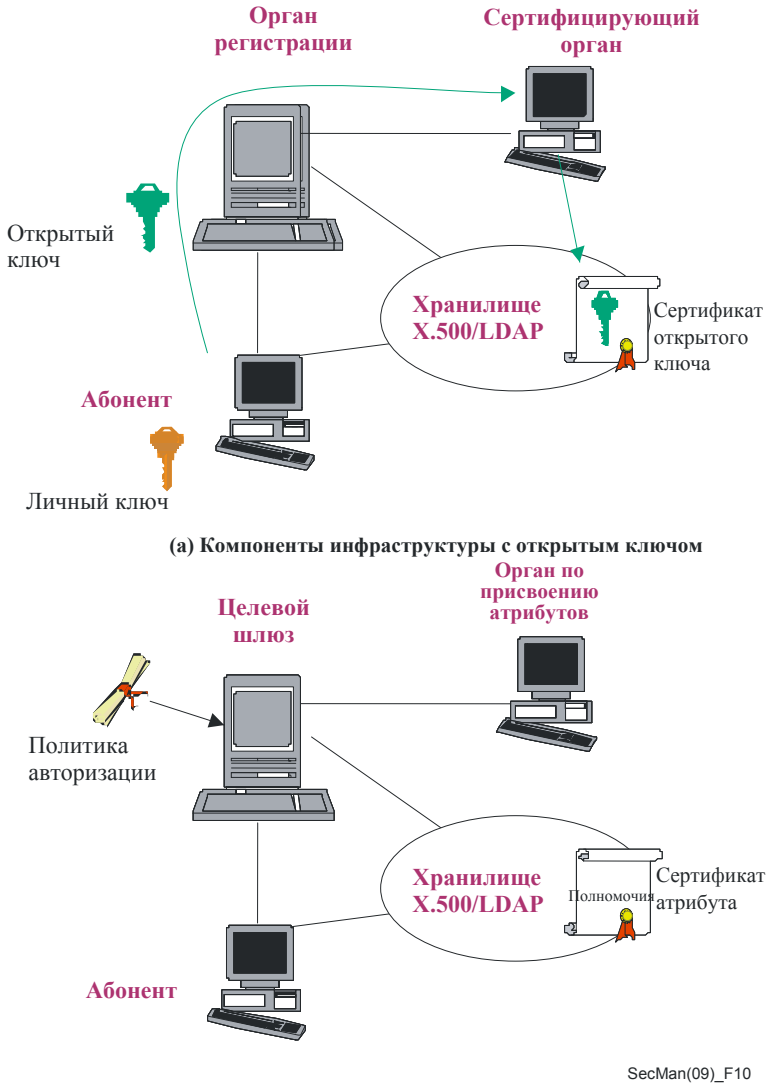


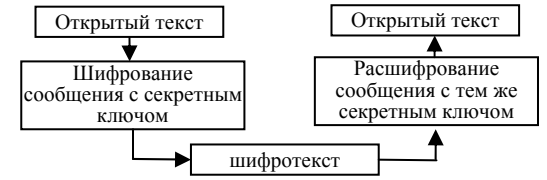
Рисунок 10 – Компоненты PKI и PMI

6.2.1 Шифрование с секретным и с открытым ключом

Симметричным (или с секретным ключом) шифрованием называется криптографическая система, в которой один и тот же ключ используется и для шифрования, и для дешифрования, как показано на Рисунке 11 (a). В симметричной криптосистеме стороны, между которыми устанавливается связь, используют уникальный секретный ключ. Это ключ должен быть передан участникам с обеспечением секретности, так как знание ключа шифрования означает знание ключа дешифрования и наоборот.

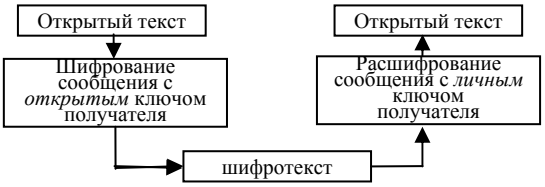
Асимметричное (или с открытым ключом) шифрование использует пару ключей – открытый ключ и секретный ключ, как показано на Рисунке 11 (b). Открытые ключи могут широко распространяться, но секретные ключи должны всегда храниться в секрете. Секретный ключ обычно содержится в смарт-карте или метке. Открытый 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 использую 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 большего числа пользователей
– Наилучший пример: DES (стандарт шифрования данных)

(b) 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 с секретным ключом
– Наилучший пример: RSA

(b) Шифрование с асимметричным (или открытым) ключом

SecMan(09)_F11

Рисунок 11 – Иллюстрация процессов шифрования с секретным и с отрытым 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, отрытые 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 целое сообщение. 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 хэш шифруется с применением секретного ключа отправителя и присоединяется к сообщению. Получатель может проверить достоверность цифровой подписи, дешифровав цифровую подпись с отрытым 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 отрытым ключом существенно зависит от достоверности отрытых ключей. Обычно отрытые ключи публикуются в виде цифровых сертификатов, которые хранятся в каталоге МСЭ-Т X.500. Сертификат содержит не только отрытый 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 отрытые 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 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, для 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 с может быть опубликован без ограничений, например на веб-сайте, в директории LDAP или в V-карте[1], присоединяемой к сообщениям электронной почты. Подпись CA гарантирует, что его содержание не может быть изменено без обнаружения.

Для того чтобы дать пользователю возможность подтверждения подлинности сертификата отрытого ключа, 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, являющегося "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 важнейших компонентов инфраструктуры открытого ключа является метод безопасного распространения открытых ключей для корневых CA, который гарантирует действительную принадлежность открытого ключа корневому CA, наименование которого указано в подписанном им самим сертификате. Без этого мы не можем быть уверены в том, что некто не маскируется под корневой CA.

6.2.3 Инфраструктуры открытых ключей

Основным назначением PKI является выдача сертификатов открытых ключей и управление ими, включая сертификаты корневого CA. 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 CA функционирует в соответствии с набором стратегических процедур. В МСЭ-Т X.509 предусмотрены механизмы для распространения некоторой части информации об этой стратегии в полях расширения сертификатов МСЭ-Т X.509, выданных данным CA. Стратегические правила и процедуры, которым следует CA, обычно определяются в стратегии применения сертификатов (CP) в заявлении о практике применения сертификатов (CPS), публикуемых этим CA. Указанные документы способствуют обеспечению общей основы для оценки того, насколько можно доверять сертификатам открытых ключей,

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

выданным этим CA, 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 МСЭ-Т X.509 (1988, 1993 и 1997 гг.) указаны основные элементы, необходимые для инфраструктуры открытых ключей, включая определение сертификатов открытого ключа. Пересмотренная 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 полномочиями (PMI).

6.2.4 Инфраструктура управления полномочиями

Инфраструктура управления полномочиями (PMI) управляет полномочиями в целях содействия всеобъемлющей службе авторизации с PKI. Описанные механизмы позволяют осуществлять установку полномочий 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 4 показано сходство двух инфраструктур.

Таблица 4 – Сравнение параметров инфраструктуры управления полномочиями и инфраструктуры открытого ключа

Инфраструктура управления полномочиями	Инфраструктура открытого ключа
Источник полномочий (SoA)	Корневой сертифицирующий орган (исходная точка доверия)
Орган по присвоению атрибутов (AA)	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 полномочий 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 5.

Таблица 5 – Структура сертификатов атрибутов согласно X.509

Версия
Держатель
Распределитель
Подпись (ID алгоритма)
Серийный номер сертификата
Срок действия
Атрибуты
Уникальный ID распределителя
Расширения

Сертификаты атрибутов также применяются в телебиометрии (см. Раздел 6.5) для создания биометрических сертификатов для увязания 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 МСЭ-Т X.509 описаны пять компонентов для управления PMI: контролер полномочий, верификатор полномочий, объектный метод, стратегия присвоения полномочий и переменные среды (см. Рисунок 12).

Верификатор полномочий может управлять доступом к объектному методу с помощью контролера полномочий в соответствии со стратегией предоставления полномочий.

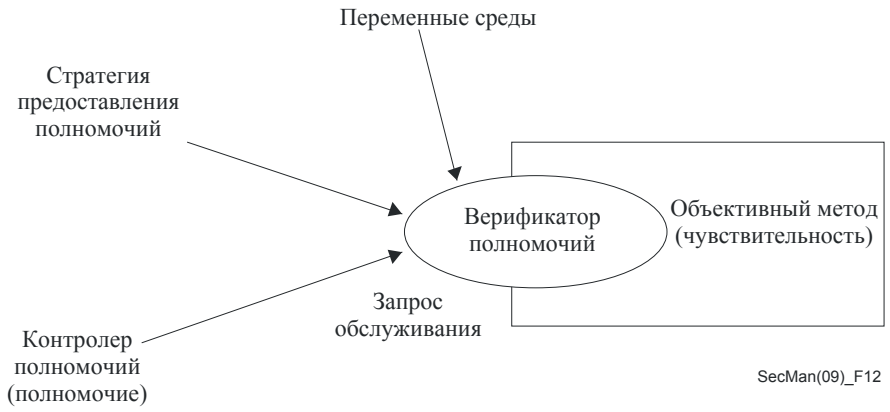


Рисунок 12 – Модель управления PMI согласно Рекомендации МСЭ-Т X.509

Если для какого-либо варианта реализации требуется делегирование полномочий, в МСЭ-Т X.509 рассмотрены четыре компонента модели делегирования для PMI: верификатор полномочий, источник полномочий, другие органы по присвоению атрибутов и контролер полномочий (см. Рисунок 13).

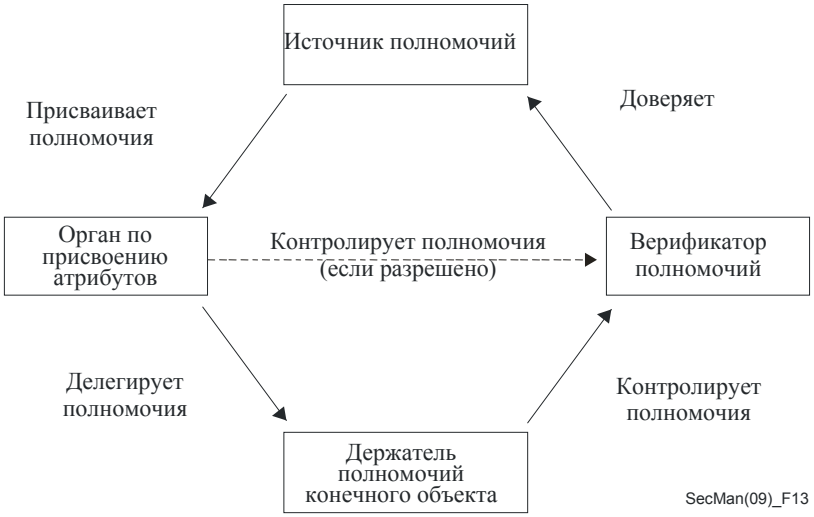


Рисунок 13 – Модель делегирования для PMI согласно X.509

В последних реализациях схем авторизации, которые соответствуют модели контроля за 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 *Руководящие указания для протокола аутентификации на базе секретного пароля с обменом ключами*, 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 не требуется никакой другой инфраструктуры (например. PKI). Ожидается, что в ближайшем будущем он будет все более важен для многих приложений. SPAK обеспечивает как аутентификацию пользователя, так и точный 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 14).

Рисунок 14 – 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 управления 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 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 15. 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 совместно 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 аутентификатором и запрашивающим объектом для гарантий конфиденциальности и возможности аутентификации сообщений.

Аутентификация и управление ключами в целом состоят из четырех рабочих этапов: обнаружение возможностей безопасности, аутентификация EAP, распространение ключей и управление ключами (см. Рисунок 15). На этапе возможностей безопасности запрашивающий объект согласует возможности 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 как результат работы протокола EAP. На этапе распространения ключей, сервер аутентификации передает главный секрет аутентификатору, с тем чтобы позволить во время аутентификации создание разных ключей шифрования для последующего сеанса связи между запрашивающим объектом и аутентификатором. С целью предотвращения многократного использования одного и того же секретного ключа, в каждом сеансе связи должны использоваться новые ключи шифрования. Наконец, на этапе управления ключами аутентификатор обменивается случайными числами с запрашивающим объектом для получения новых ключей шифрования, что обеспечивает безупречную секретность.

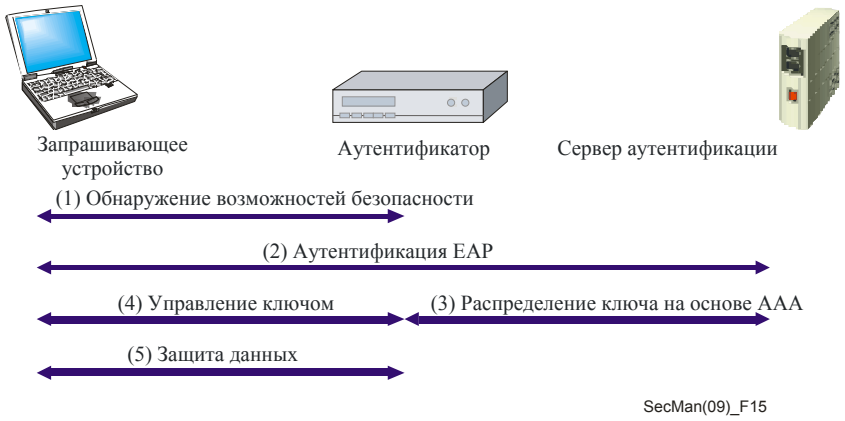


Рисунок 15 – Четыре рабочих этапа для аутентификации и управления ключами на нижнем уровне

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 отражения 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 в себя 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 полномочий (вместо полномочий "все или ничего") и упрощает процесс изменения полномочий 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 предоставить доступ к объектам как внутри, так и вне организации.

IdM обеспечивает достоверность информации об идентичности таким образом, что она поддерживает безопасное, заслуживающее доверие контроль за доступом. Эта возможность получена 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 противоположность 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 в себя:

- создание, изменение, приостановку, архивацию и уничтожение информации об идентичности;
- распознавание идентичности, которая отражает объекты в определенном контексте и роли;
- создание и оценка доверия между объектами; и
- определение местонахождения идентичности (например, посредством авторитетного поставщика идентичности, который отвечает перед законом за поддержку идентификаторов, полномочий и некоторых или всех атрибутов объекта).

В дополнении к подсерии МСЭ-Т X.1250 Обзор управления идентичностью в контексте кибербезопасности представлено краткое Введение в вопрос управления определением идентичности.

6.4.2 Работы МСЭ-Т по управлению определением идентичности

Хотя все еще продолжается обсуждение некоторых основополагающих концепций и базового словаря, ИК17 продолжает работу во многих областях (ведущая ИК по IdM), как и ИК2 (эксплуатационные аспекты предоставления услуг и управление электросвязью) и ИК13 (будущие сети, включая сети подвижной связи и СПП).

ИК2 отвечает за проведение исследований, относящихся к обеспечению совместимости формата и структуры IdM идентификаторов и к определению интерфейсов к системам управления для обеспечения передачи информации, касающейся идентичности внутри организационных доменов и между ними.

ИК13 отвечает за особую для СПП функциональную архитектуру управления определением идентичности, которая поддерживает услуги идентичности добавленной стоимости, безопасный обмен информацией об идентичности и применением запараллеливания/взаимодействия между различными наборами форматов информации идентичности. SG 13 также отвечает за идентификацию любых угроз управлению определением идентичности в пределах СПП и механизмы противостояния им. Уже утверждена Рекомендация МСЭ-Т Y.2720 *Структура управление определением идентичности СПП*. В этом стандарте описывается структурный подход к разработке, определению и реализации решений IdM и облегчению взаимодействия в гетерогенных условиях.

ИК17 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 в себя: 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; защита информации, подлежащей личной идентификации (PII); и создание механизмов, гарантирующих, что доступ к PII разрешен только, когда уместно. В сентябре 2009 года были утверждены две Рекомендации: Рекомендация МСЭ-Т X.1250 *Основные возможности для расширения всемирного управления определением идентичности и взаимодействия* и Рекомендация МСЭ-Т X.1251 *Структура для управления пользователем определением цифровой идентичност*и. Кроме того, создается основной набор связанных с IdM определений, с тем чтобы помочь гарантировать единообразную и согласующуюся терминологию в стандартах IdM МСЭ-Т.

Для координации работы IdM МСЭ-Т была создана Совместная группа по координации деятельности для управления определением идентичности (JCA-IdM). Также была создана IdM – Глобальная инициатива по стандартизации (IdM-GSI), с тем чтобы гармонизировать различные подходы по всему миру к IdM и чтобы сотрудничать с другими органами, работающими над этим вопросам. На странице Ведущей Исследовательской

комиссии IdM представлена расширенная информация по деятельности IdM, утвержденным и создающимся Рекомендациям IdM и другой информации, связанной с работой IdM.

6.5 Телебиометрия

Телебиометрия занимается персональной идентификацией и аутентификацией с использованием биометрических устройств в сфере 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 в себя: взаимодействие человека и окружающей среды; биометрические цифровые ключи; биометрические расширения сертификатов 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 (коэффициент ложного признания), определенная пороговым параметром. Поэтому поставщик услуг не может требовать поддержания единообразного уровня точности; и
- точность биометрического подтверждения может ухудшаться со старением конечных пользователей, так как биометрия использует характеристики человеческого тела.

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

На Рисунке 16 показана аутентификация конечного пользователя при помощи открытой сети неличного общения.

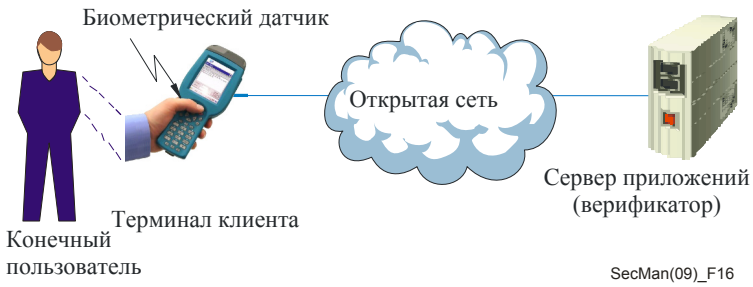


Рисунок 16 – Телебиометрическая аутентификация конечного пользователя

6.5.2 Генерация телебиометрического ключа и защита

Структура создания цифрового биометрического ключа определена в Рекомендации МСЭ-Т X.1088 *Структура создания и защиты биометрического цифрового ключа*. 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. Предлагается два метода:

- создание биометрического ключа, в котором ключ создается из биометрического шаблона (Рисунок 17); и
- привязка/восстановление биометрического ключа, в котором ключ хранится в базе данных и может быть извлечен при помощи биометрической аутентификации (Рисунок 18).

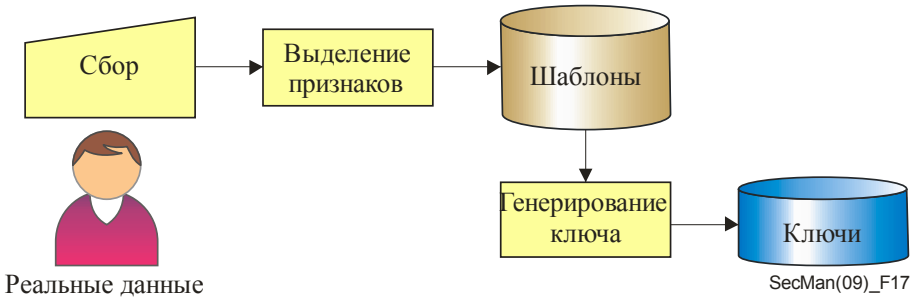


Рисунок 17 – Создание биометрического ключа

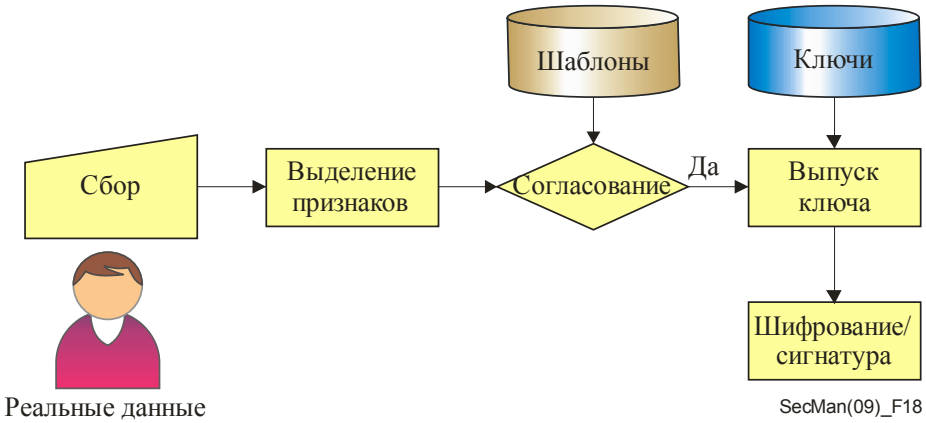


Рисунок 18 – Привязка/восстановление биометрического ключа

6.5.3 Аспекты защиты и безопасности телебиометрии

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

6.5.4 Телебиометрия, связанная с психологией человека

Аспекты защиты и безопасности телебиометрии также рассмотрены в Рекомендации МСЭ-Т X.1082 *Телебиометрия, связанная с психологией человека*, 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 дает имена, определения и символы для значений и оборудования для телебиометрии, связанной с психологией человека, т. е. человеческие характеристики и излучения можно определить при помощи датчика. Также она включает в себя значения и оборудование, имеющие отношение к воздействию на человека, вызванное использованием устройств телебиометрии.

6.5.5 Другие разработки в сфере стандартов телебиометрии

Для создания биометрических сертификатов были разработаны расширения сертификатов МСЭ-Т X.509, используемых в инфраструктурах открытых ключей или инфраструктуре управления полномочиями. Они указаны в Рекомендации МСЭ-Т X.1089 *Инфраструктура телебиометрической аутентификации.*

В Рекомендации МСЭ-Т X.1083 *Протокол сетевого взаимодействия BioAPI* определяется синтаксис, использующий ASN.1, семантика и кодирование сообщений, которые позволяют приложению, совместимому с BioAPI, запросить у провайдеров услуг, совместимых с BioAPI (BSP), выполнение биометрических операций с пересечением узла или границ обработки, а также позволяет им иметь возможность получить извещение о событиях, происходящих у этих удаленных BSP.

7. Защита сетевой инфраструктуры

7 Защита сетевой инфраструктуры

Данные, используемые для контроля и управления трафиком сети управления электросвязью, 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 *Принципы для сети управления электросвязью*. Этот трафик обязательно должен быть защищен. Обычно категории трафика управления определяются в переводе на информацию, необходимую для выполнения функций управления обработкой отказов, конфигурацией, функциями расчетов и управления безопасностью. Область управления безопасностью сети охватывает как настройку сети управления безопасностью, так и управление безопасностью информации, которая связана с тремя плоскостями архитектуры безопасности X.805.

Действия по управлению, связанные с элементами инфраструктуры сети, 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 контроль за доступом и 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.

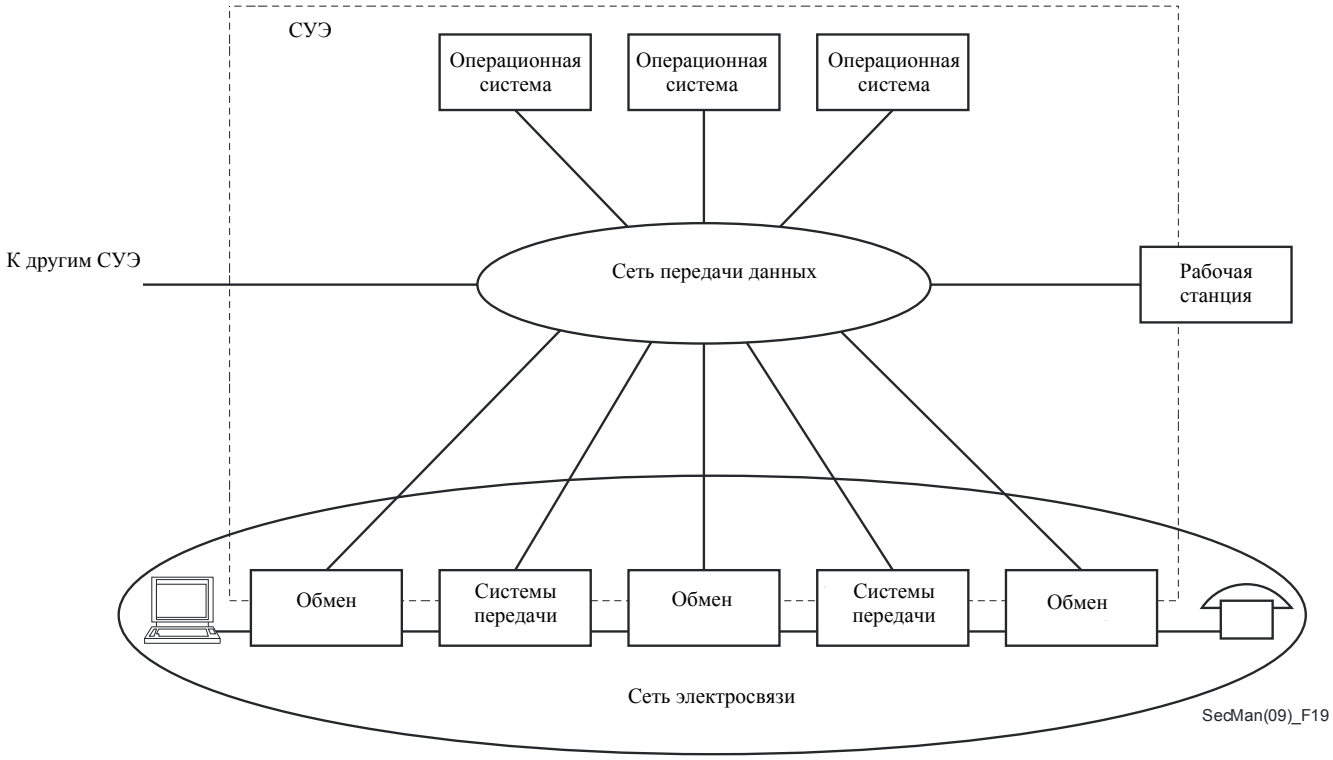
Другие приложения управления сетью включают в себя приложения, связанные со средой, в которой должны взаимодействовать различные поставщики услуг, с тем чтобы обеспечивалось сквозное предоставление услуги между оконечными пунктами. Среди примеров такой услуги – средства связи, предоставляемые регламентарным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

7.1 Сеть управления электросвязью

СУЭ является отдельной сетью, изолированной от инфраструктуры сети общего пользования, поэтому какие-либо перерывы связи, возникающие вследствие угрозы 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. Несмотря на то что 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.

7.2 Архитектура управления сетью

Архитектура для обеспечения сетевого управления сетью электросвязи описана в Рекомендации МСЭ-Т М.3010. На Рисунке 19 показана взаимосвязь между СУЭ и сетью электросвязи. Архитектура управления сетью устанавливает интерфейсы, которые определяют процессы обмена, необходимые для выполнения функций эксплуатации, управления, поддержки и предоставления услуг.



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

Рисунок 19 – Взаимосвязь между СУЭ и сетью электросвязи

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

При анализе управления безопасности сети, следует рассматривать два его аспекта. Первый относится к плоскости управления для сквозных действий пользователя между оконечными точками, например, услуги VoIP. 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*, который 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 X.805 архитектуры существует несколько рекомендаций, посвященных функциям управления для трех уровней плоскости управления (см. Рисунок 1). Кроме того, как сказано в последующих подразделах, существуют другие Рекомендации, которые определяют всеобщие или широкоиспользуемые услуги, такие, как отчеты об аварийных ситуациях при физическом 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 полномочиями 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 20 показаны различные объекты, используемые для создания, удаления, распределения и применения информации контроля за доступом для пользователей системы управления элементами. В списке полномочий пользователя каждого авторизованного пользователя содержится перечень разрешенных функций управления. Диспетчер контроля за доступом проверяет идентификатор и пароль пользователя управляющих функций и предоставляет доступ к функциональным возможностям, разрешенным в списке полномочий.

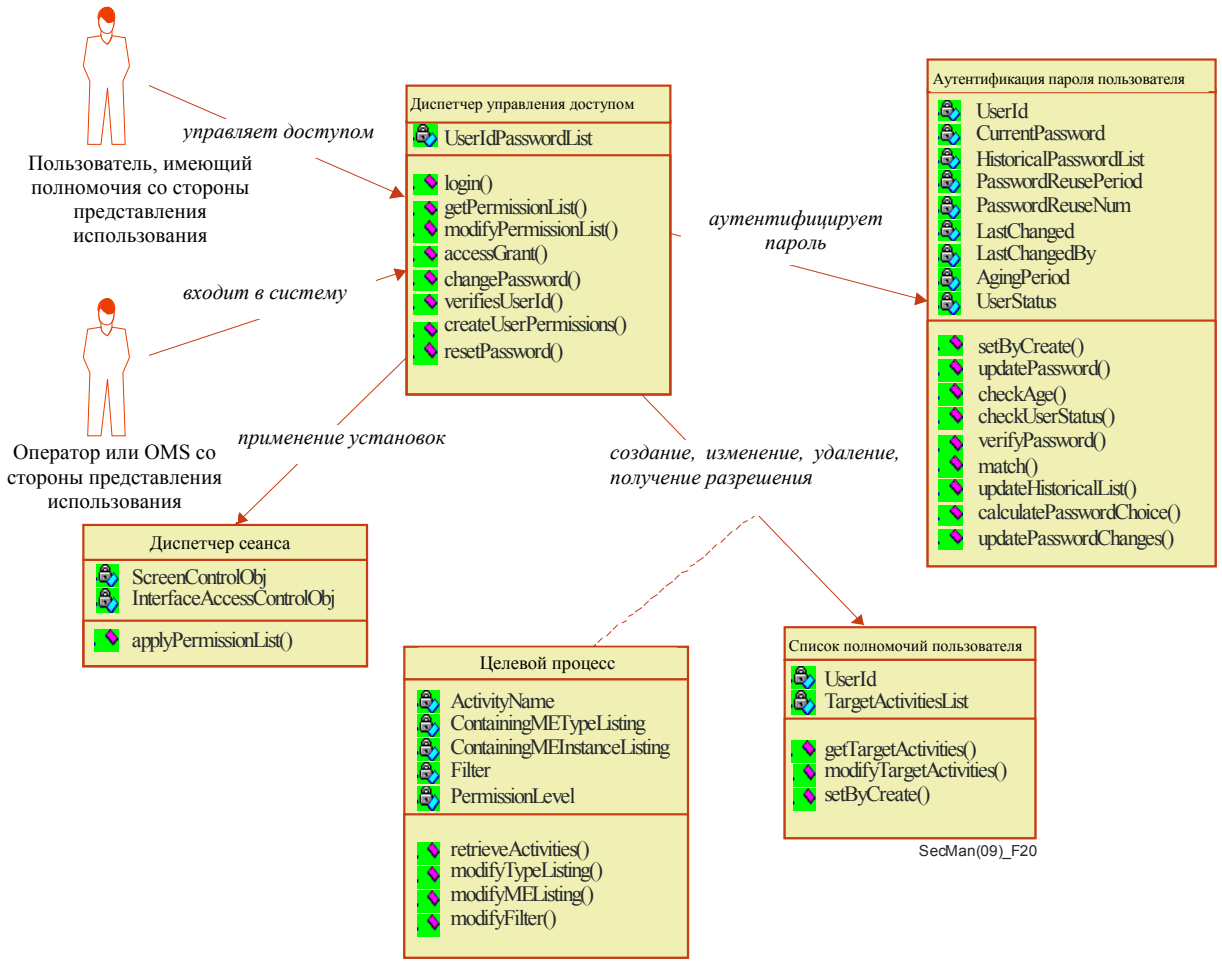


Рисунок 20 – Администрирование полномочий пользователя по МСЭ-Т Q.834.3

7.4 Защита действий по контролю и мониторингу

В пересечении плоскости управления и слоя услуг важны два аспекта. 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 *Управление соединениями в линиях связи заранее предоставленных услуг для создания услуг выделенного канала* 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 X.805, которые связаны с данной услугой, являются: аутентификация одноранговых объектов; контроль целостности данных для предотвращения неразрешенного изменения данных в процессе их транзита; и контроль за 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 *Услуги управления СУЭ для управление безопасностью систем IMT-2000*, 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 обнаружения мошенничества в домашней сети собирает информацию об абоненте, зарегистрировавшемся в посещаемой сети. В сценариях a) и b) на Рисунке 21 показано инициирование мониторинга процесса управления домашней сетью или посещаемой сетью. Для системы обнаружения мошенничества в домашней сети требуется информация 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 данных на уровне услуги или абонента. Система обнаружения мошенничества может проанализировать мошенническое поведение и инициировать соответствующие аварийные сигналы.

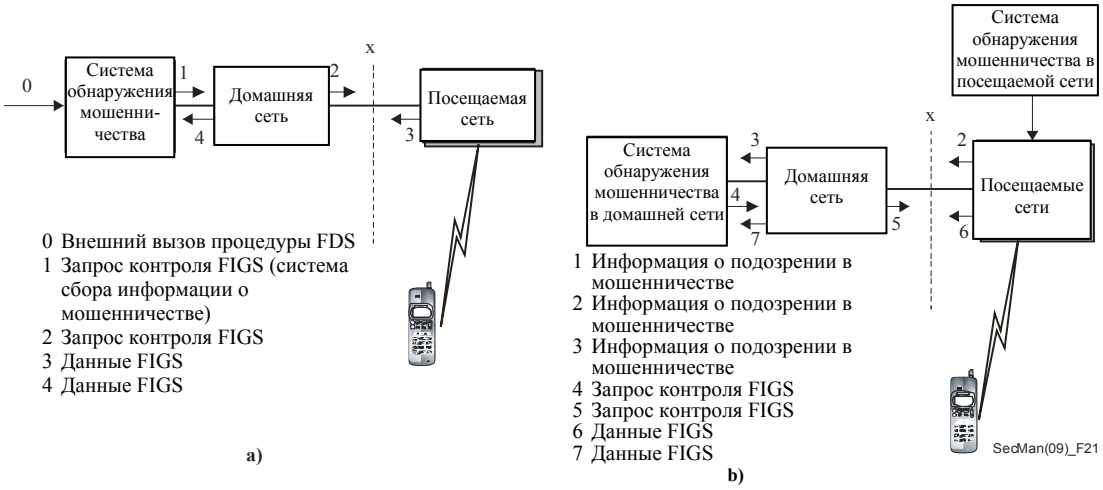


Рисунок 21 – Обнаружение мошенничества для беспроводных служб

7.5 Защита сетевых приложений

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 со справочниками. 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 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 соединения между оконечными пунктами 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 22 показаны виды взаимодействия, которые должны быть защищены. Осуществляется администрирование преимуществ 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.

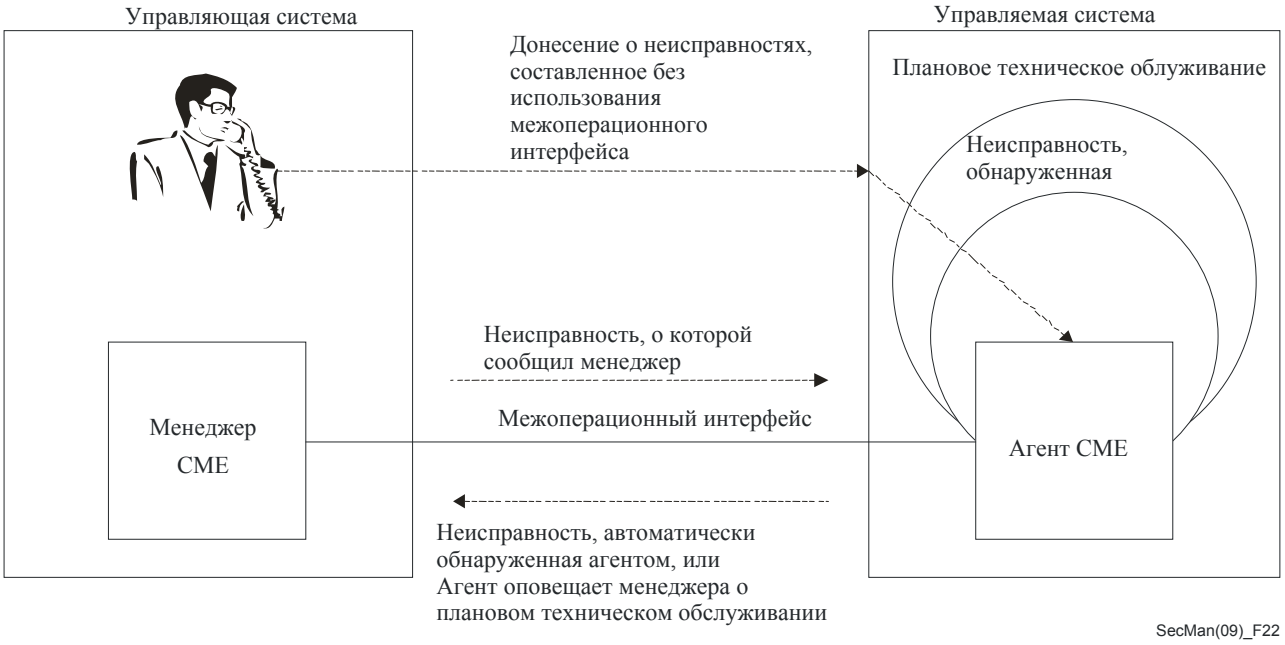


Рисунок 22 – Составление отчета о неисправности

В Рекомендации МСЭ-Т X.790 *Функция исправления неполадок для приложений МСЭ-Т* содержится описание такого приложения управления и приводятся механизмы, такие как список контроля за 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 X.805. Обычно они применяются, когда используется *Общий протокол управления информацией (CMIP)* (Рекомендация МСЭ-Т X.711). Ниже приведено краткое описание услуг, включенных в эти Рекомендации.

7.6.1 Функции 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 нарушения 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, детектор нарушения безопасности и пр. Причины аварийного сигнала связаны с типами событий, как показано в Таблице 6.

Таблица 6 – 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 отказ в обеспечении сохранности информации 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 *Функции аварийной сигнализации системы безопасности*.

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 в себя соединения, разрыв соединения, применение механизмов безопасности, действия по управлению и проверка использования. *Функции отслеживания проверки безопасности* определены в Рекомендации МСЭ-Т X.740.

7.6.3 Контроль доступа для управляемых объектов

Модель, связанная с назначением функции контроля за доступом различным управляемым объектам, очень подробно описана в Рекомендации МСЭ-Т X.741 *Объекты и атрибуты для контроля за доступом*. Требования, которые соответствуют приведенным в этой Рекомендации определениям контроля за доступом, включают: защиту информации контроля за доступом от несанкционированного введения, удаления и изменения; разрешенные операции соответствуют правам доступа для инициаторов операций; и предотвращают передачу информации управления не имеющим доступа получателям. С целью удовлетворения этих требований описаны различные уровни контроля за доступом. В отношении операций по управлению обеспечивается ограничение доступа на множественных уровнях. Политика контроля за доступом может применять одну или несколько определенных схем (например, список контроля за доступом, на основе функциональных возможностей, метки и контекста). В модели МСЭ-Т X.741 решение о том, разрешить или не разрешить запрашиваемую операцию, принимается на основе политики контроля доступа и информации контроля за 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 серии МСЭ-Т X.700 предполагают использование CMIP как протокола интерфейса управления, существуют и другие тенденции, которые теперь отражены в этих Рекомендациях. Они включают в себя использование протоколов, услуг и моделей объектов на основе Обобщённой архитектуры обработчика объектных запросов (CORBA) для интерфейсов управления. Особого внимания заслуживают: Рекомендация МСЭ-Т X.780, *Руководство СУЭ для определения объектов, управляемых CORBA*; Рекомендация МСЭ-Т X.780.1, *Руководство СУЭ для определения крупномодульных интерфейсов объектов, управляемых CORBA*; Рекомендация МСЭ-Т X.780.2 *Руководство СУЭ для определения ориентированных на услуги объектов, управляемых CORBA, и фасадных объектов*; и Рекомендация МСЭ-Т X.781 *Требования и руководящие указания для проформ внедрения заявлений о соответствии, связанных с системами на основе CORBA*. 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 эта Рекомендация 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 интернет-протокола. 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 многоканальную широкополосную передачу данных и транспортные технологии, 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 *Общий обзор СПП*.

8.1.1 Задачи безопасности СПП и требования

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 и появлением новых СПП появляется уязвимость безопасности, для которой нет заранее известных автоматических средств, такие уязвимости должны быть должным образом задокументированы, с тем чтобы администраторы сети и конечные пользователи могли ее смягчить.

Изучение безопасности СПП должно обращаться к архитектуре сети и развивать ее, для того чтобы:

- обеспечить максимальную защиту сети и ресурсов конечного пользователя;
- предусматривать сильно распределенную разведку между оконечными пунктами;
- предусматривать сосуществование многоканальных сетевых технологий;
- обеспечить механизмы безопасности для оконечных пунктов;
- обеспечить решения безопасности, которые применяются в некоторых административных доменах;
- обеспечить управление определением идентичности безопасности, которая включает, но не ограничивается:
  - надежную аутентификацию объектов СПП, например, пользователей, устройств пользователей, поставщиков сети, поставщиков услуг, поставщиков идентификации и т. д.;
  - предотвращение несанкционированного доступа к данным идентификации в СПП;
  - безопасный обмен идентификационной информацией между федеральными объектами в СПП;
  - поддержку хранения записей использования идентификационной информации в СПП;
  - поддержку личной информации пользователя и анонимности в СПП; и
  - возможность поддержки пользователей СПП, для того чтобы помочь им надежно управлять информацией о своей идентичности (например, изменением профиля пользователя, сменой паролей, предоставлением услуг на основе местоположения, просмотром записей о выставлении счетов и т. д.);

- предоставлять решения по безопасности IPTV, которые были бы экономически выгодны и оказывали существенное влияние на показатели работы, качество обслуживания, удобство и масштабируемость. Типы защиты, которые должны обеспечивать безопасность IPTV включают, но не ограничиваются:
  - защиту содержания;
  - защиту услуги;
  - защиту сети;
  - защиту терминала; и
  - защиту абонента.

Рекомендация МСЭ-Т Y.2701 *Требования к безопасности для СПП, версия 1*, которая основана на принципах МСЭ-Т X.805, определяет требования к безопасности для защиты СПС от угроз безопасности и охватывает некоторые технические аспекты управления идентичностью.

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

- ее инфраструктура и средства поставщика услуг и сети, 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, а также 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.

Требования должны обеспечить безопасность на основе сети для соединения конечных пользователей, находящихся в пределах административных доменов нескольких сетей, как показано на Рисунке 23.

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

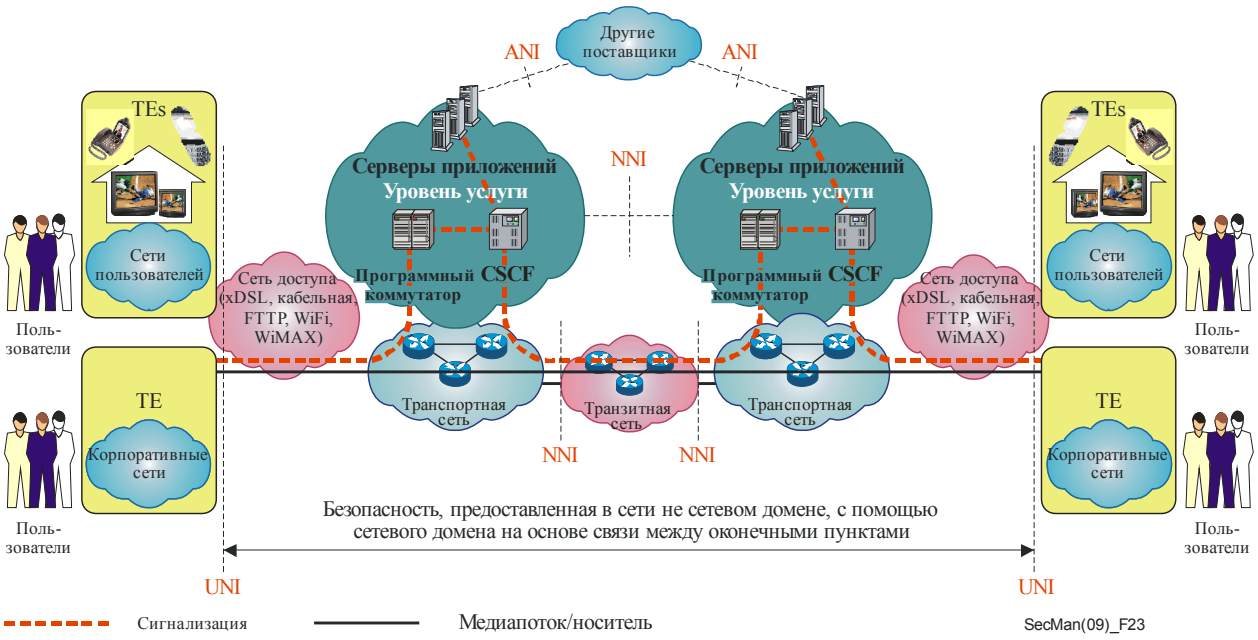


Рисунок 23 – Безопасность связи в пределах многоканальных сетей

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 для защиты пользователей, сетей и приложений должны соблюдаться, чтобы защитить пользователей, сети и приложения, предоставляющие доступ.

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 уязвимость будут угрожать беспроводным подвижным сетям, которые используют IP в качестве своего транспортного протокола. Кроме того, новые угрозы будут связаны с подлинной природой самих беспроводных сетей, т. е. их подвижностью. Механизмы безопасности, 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 полного спектра услуг между оконечными пунктами, а также она должна быть достаточно гибкой, для того чтобы предоставить различные уровни безопасности в соответствии с предоставляемой услугой/приложением. С развертыванием подвижных услуг и приложений IP, меры безопасности стали более важны для пользователя, оператора и поставщика услуг.

Участие многообразных сетей увеличивает возможность для угроз, таких как незаконный перехват профилей пользователей, содержания (например, голоса или передачи данных), а также информации аутентификации.

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 технологий цифровой подвижной электросвязи и системами для фиксированных и подвижных систем беспроводного доступа.

Деятельность МСЭ по IMT-2000 включает международную стандартизацию, в том числе 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 Рекомендации МСЭ-Т Q.1701 *Структура для сетей IMT-2000*, МСЭ-Т Q.1702 *Долгосрочный прогноз сетевых вопросов для систем, следующих за IMT-2000* и МСЭ-Т Q.1703 *Возможности услуг и сетей в рамках сетевых вопросов для систем, следующих за IMT-2000*.

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

8.2.1 Безопасность подвижной передачи данных между конечными пунктами

В настоящее время широко доступны терминалы подвижной связи с возможностью передачи данных, например, мобильные телефоны IMT-2000, переносные компьютеры и КПК с радио-картой, и различные прикладные услуги, такие как электронная коммерция, использующие терминалы, подключенные к сети подвижной связи. Для бизнес-приложений, а также для защиты конечного пользователя эффективная безопасность имеет большое значение.

Сети подвижной связи являются особенно уязвимыми в связи с природой беспроводной сети и уязвимости, присущей технологиям беспроводной связи. 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 решения подвижной связи между оконечными пунктами МСЭ-Т разработала полный набор решений по безопасности, некоторые из которых обсуждаются ниже.

8.2.1.1 Структура для безопасности подвижной передачи данных между оконечными пунктами

В Рекомендации МСЭ-Т X.1121 *Структура технологий безопасности подвижной передачи данных между оконечными пунктами* описаны две модели подвижной передачи данных между пользователем подвижной связи и поставщиком прикладных услуг (ASP): общая модель и модель со шлюзом, как показано на Рисунке 24 и Рисунке 25. ASP предоставляет услугу пользователям подвижной связи через сервер приложений. В модели со шлюзом, шлюз безопасности ретранслирует пакеты с 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 26 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.

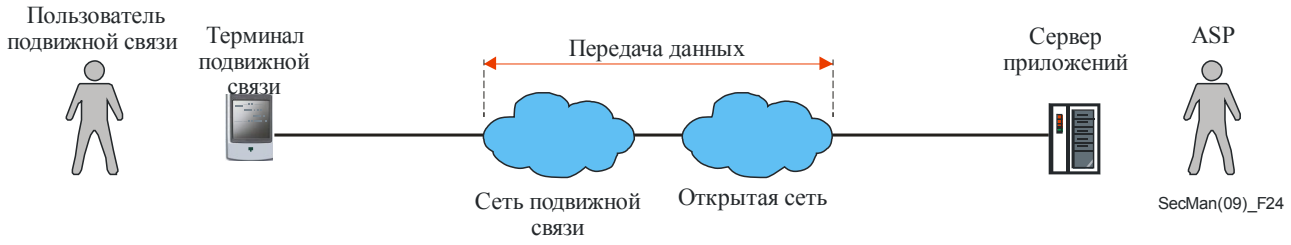


Рисунок 24 – Общая модель передачи данных между оконечными пунктами между пользователем и ASP

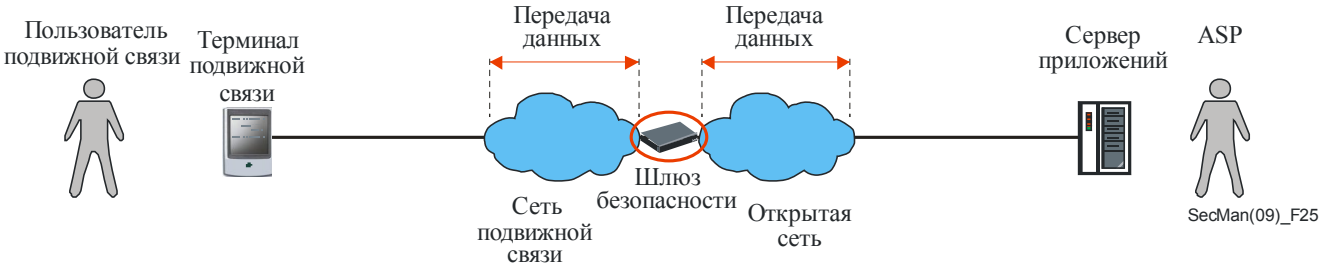


Рисунок 25 – Модель подвижной передачи данных между оконечными пунктами между пользователем и ASP с использованием шлюза

Рисунок 26 – Угрозы в подвижной связи между оконечными пунктами

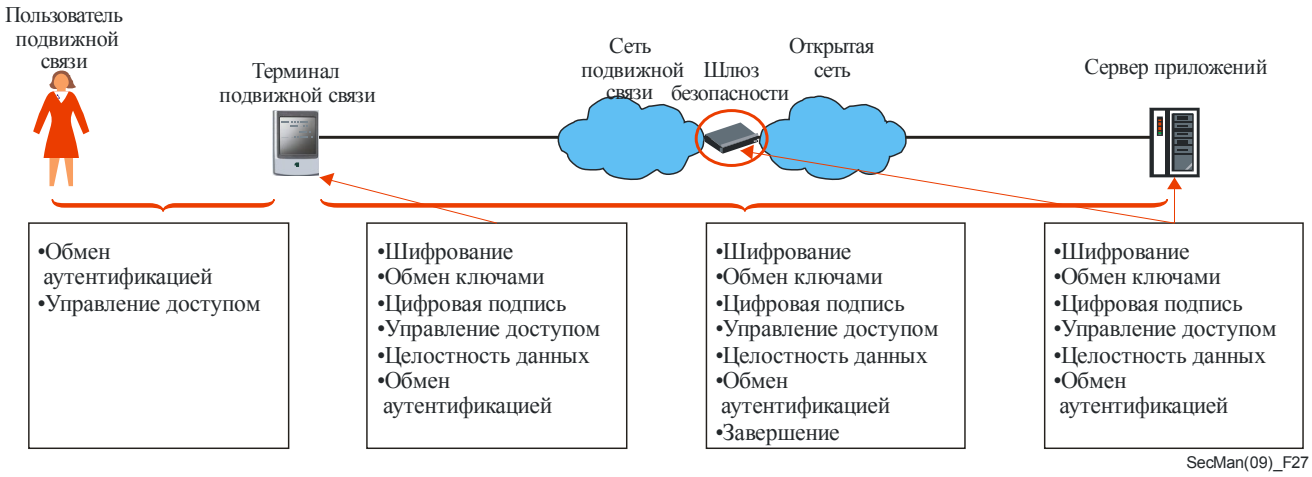


Рисунок 27 – Функции безопасности, запрашиваемые для каждого объекта и для отношений между объектами

8.2.1.2 PKI безопасности подвижной передачи данных между конечными 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 технологии PKI. Руководящие указания по созданию PKI в подвижной среде представлены в Рекомендации МСЭ-Т X.1122 *Руководящие указания по созданию безопасных подвижных систем на основе инфраструктуры открытого ключа (PKI)*, в которой рассматриваются и общая модель PKI, и модель со шлюзом PKI.

В общей модели (показана на Рисунке 28) 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 он-

лайн. 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 он-лайн.

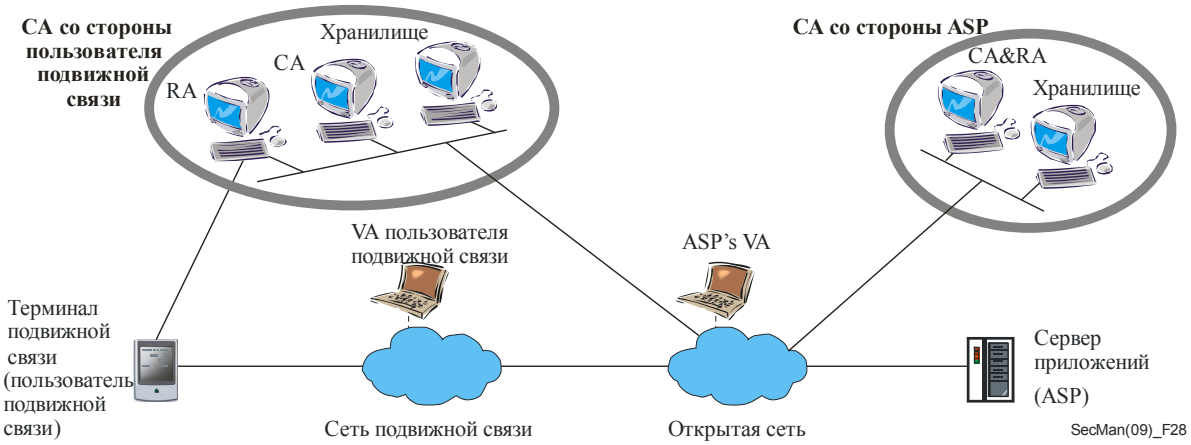


Рисунок 28 – Общая модель PKI для подвижной передачи данных между оконечными пунктами

Существует два метода выдачи сертификатов, в зависимости от места генерирования открытых/секретных ключей: один метод предусматривает генерирование и изготовление пары криптографических ключей на месте производства 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 29 показана процедура получения терминалом подвижной связи сертификата, когда пара криптографических ключей генерируется в терминале подвижной связи.

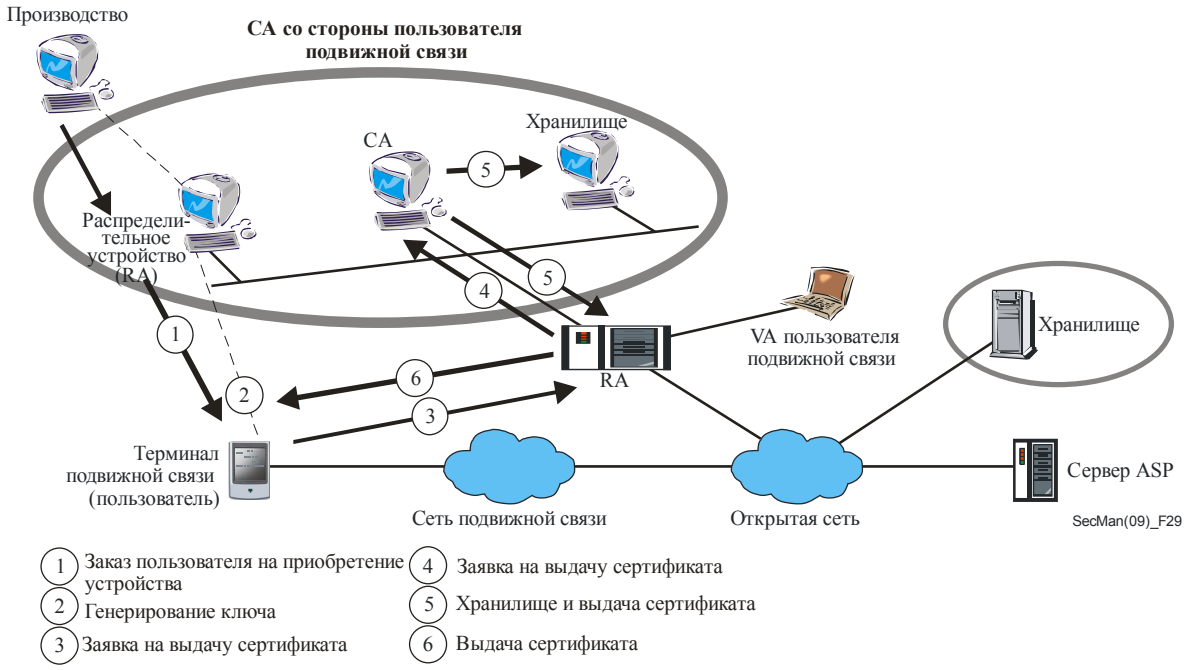


Рисунок 29 – Процедура выдачи сертификата для терминала подвижной связи

Терминал подвижной связи обладает ограниченными вычислительными возможностями и объемом памяти. Поэтому схема проверки сертификата в режиме он-лайн имеет преимущество по сравнению с основанной на CRL схемой проверки сертификата в автономном режиме. На Рисунке 30 показана процедура проверки сертификата в режиме он-лайн для терминала подвижной связи.

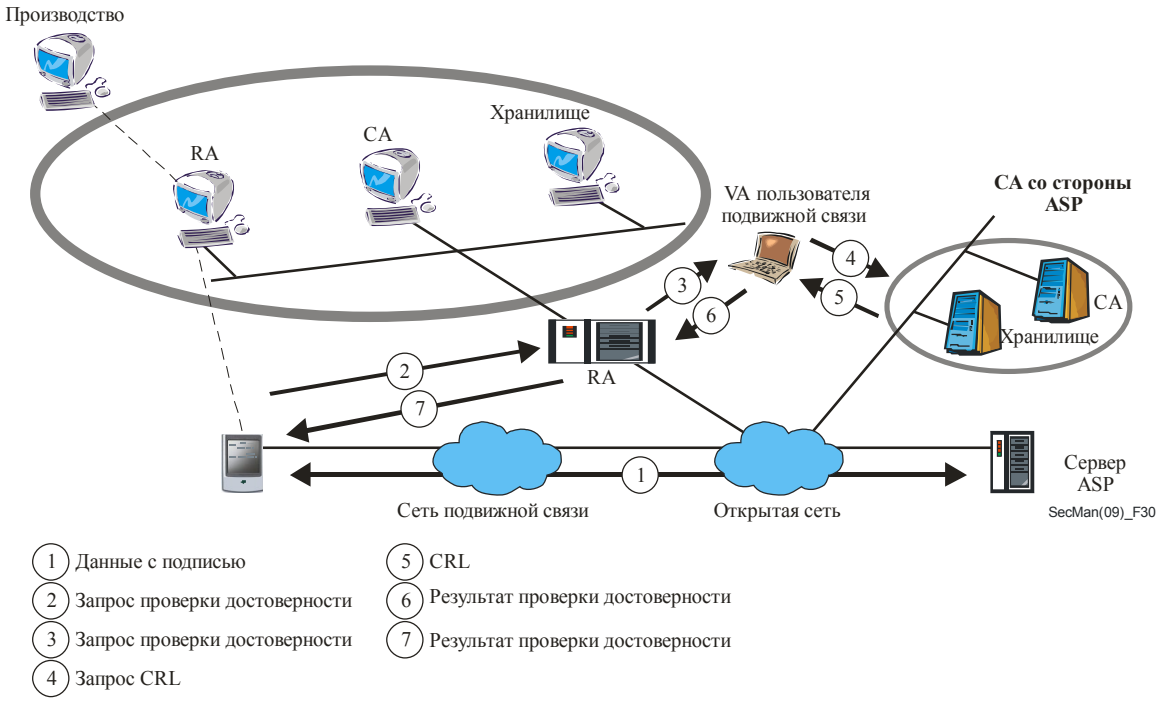


Рисунок 30 – Проверка сертификата для подвижной передачи данных между оконечными пунктами

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 услуг, либо для прикладного уровня, где предусмотрены услуги по обеспечению сохранности информации 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 безопасности с помощью обновления безопасности подвижной станции, контроля за доступом к сети и ограничением прикладных услуг. В результате создается механизм, который препятствует тому, чтобы вирусы или черви быстро распространились через сеть оператора.

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 домашней сети от этих угроз, МСЭ-Т разработала комплексный ряд решений для услуг домашней сети, некоторые из которых обсуждаются ниже.

8.3.1 Принципы безопасности для домашней сети

Для того чтобы создать структуру безопасности для домашней сети Рекомендация МСЭ-Т X.1111 *Структура технологий безопасности для домашних сетей* 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 учесть с точки зрения безопасности;
- удаленные терминалы, которые могут носить с собой удаленные пользователи; и
- различные типы устройств домашней сети требуют различные уровни безопасности.

Основная модель домашней сети для обеспечения безопасности, которая показана на Рисунке 31 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 типов A и типов C.

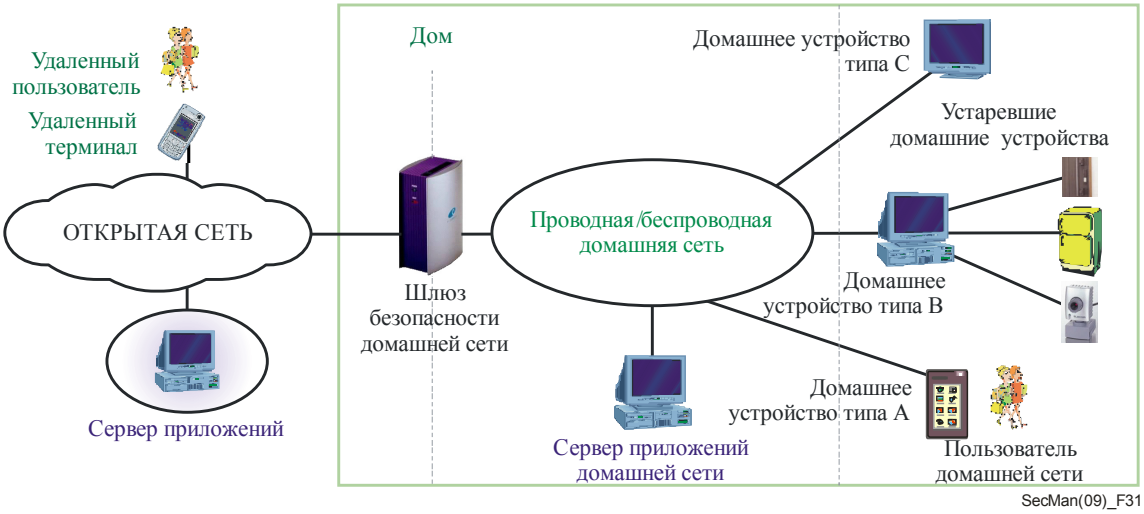


Рисунок 31 – Основная модель домашней сети для обеспечения безопасности

В Рекомендации 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 устройств и аутентификация в домашних сетях

Существует два варианта сертификации устройства 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 домашний 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 домашний сети может сам иметь сертификат устройства, который был выдан внешним сертификационным органом для 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, управление и использование для домашних сетей. Модель показана на Рисунке 32.

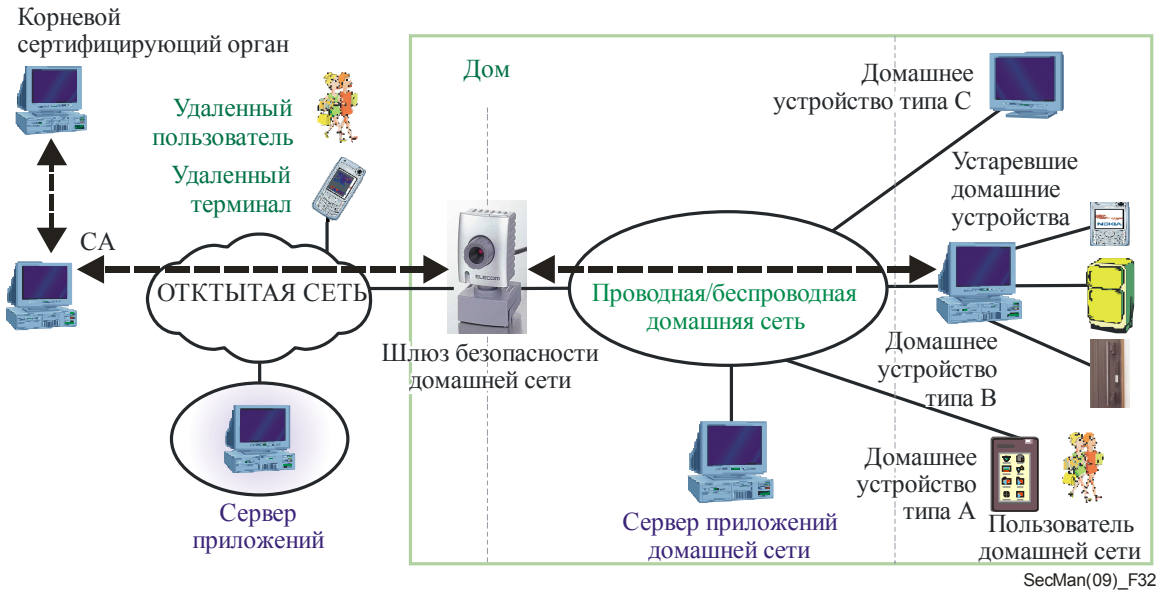


Рисунок 32 – Модель аутентификации устройства для безопасности домашней сети

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 33 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.

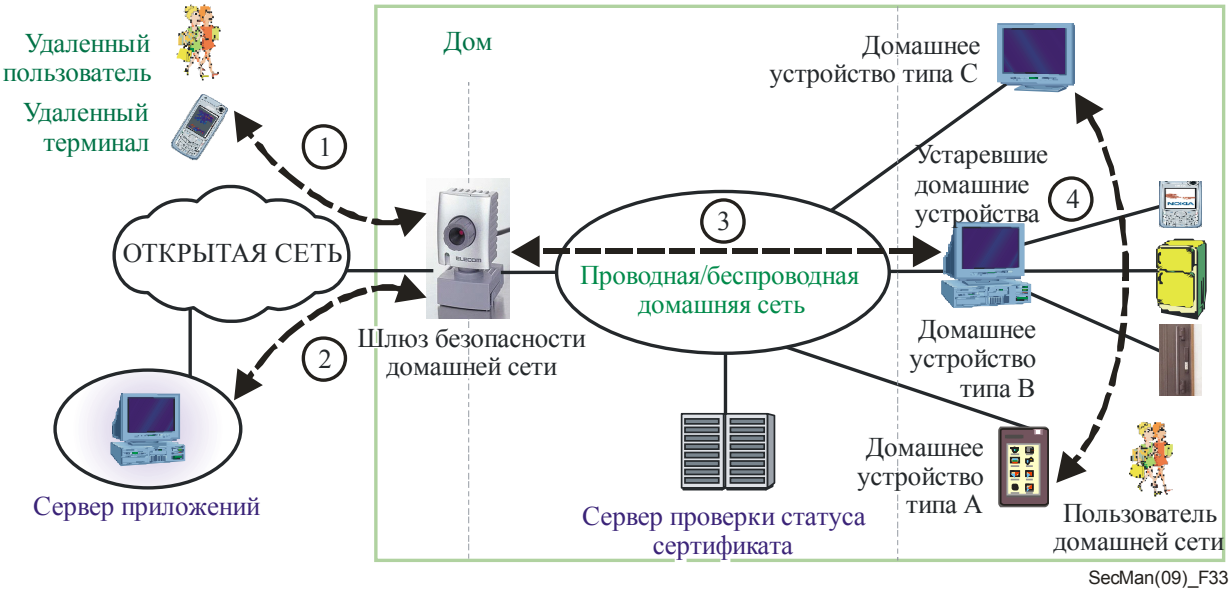


Рисунок 33 – Случай аутентификации устройств, основанной на общей модели безопасности домашней сети

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 аутентификации пользователя-человека, а не процесса или устройства. В этих случаях система аутентификации требует, чтобы пользователь-человек доказал свою уникальность. Такая уникальность, как правило, основана на таких характеристиках, как использование каких-то известных данных, какой-то имеющейся информации или некоторых неизменных характеристик пользователя.

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 34 показаны потоки услуг аутентификации на основе общей модели безопасности домашней сети, определенной в 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.

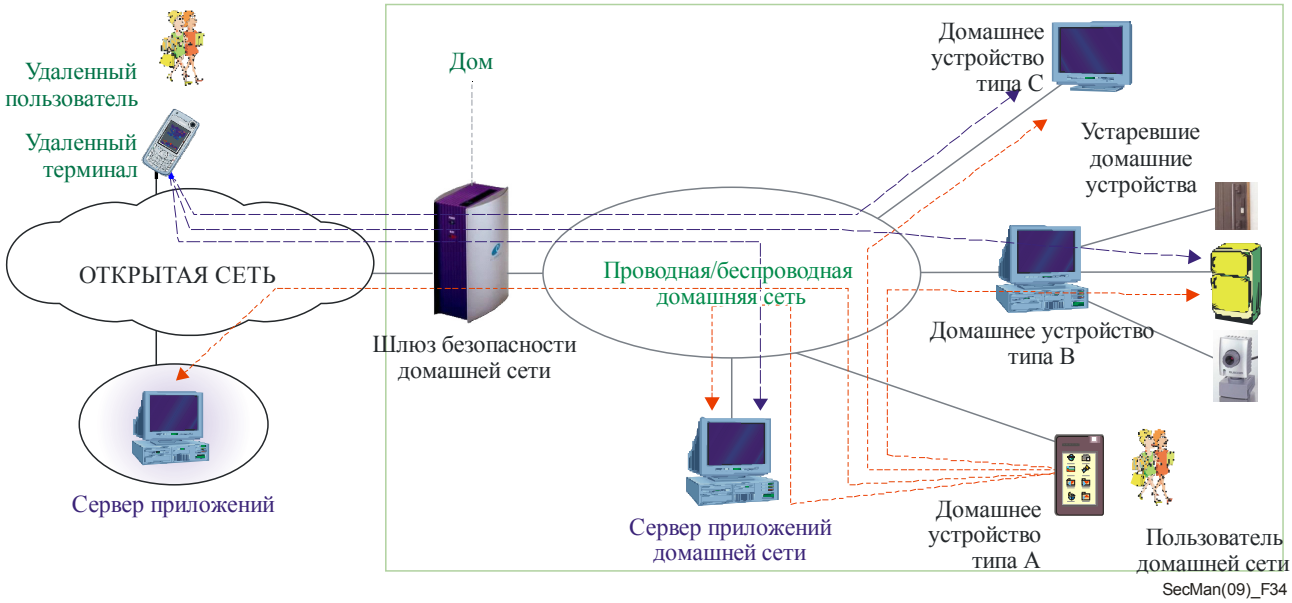


Рисунок 34 – Потоки для аутентификации услуг в домашней сети

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 кабельных модемов.

8.4.1 Архитектура IPCablecom

Архитектура системы IPCablecom определена в Рекомендации МСЭ-Т J.160. Компоненты IPCablecom показаны на Рисунке 35. Архитектура IPCablecom содержит и доверенные, и недоверенные элементы сети. Доверенные элементы сети обычно расположены в пределах управляемой магистральной сети оператора кабельной сети. Недоверенные элементы сети, такие как кабельный модем и адаптер медиатерминала (MTA) обычно располагаются за пределами объекта оператора кабельной сети в пределах дома абонента.

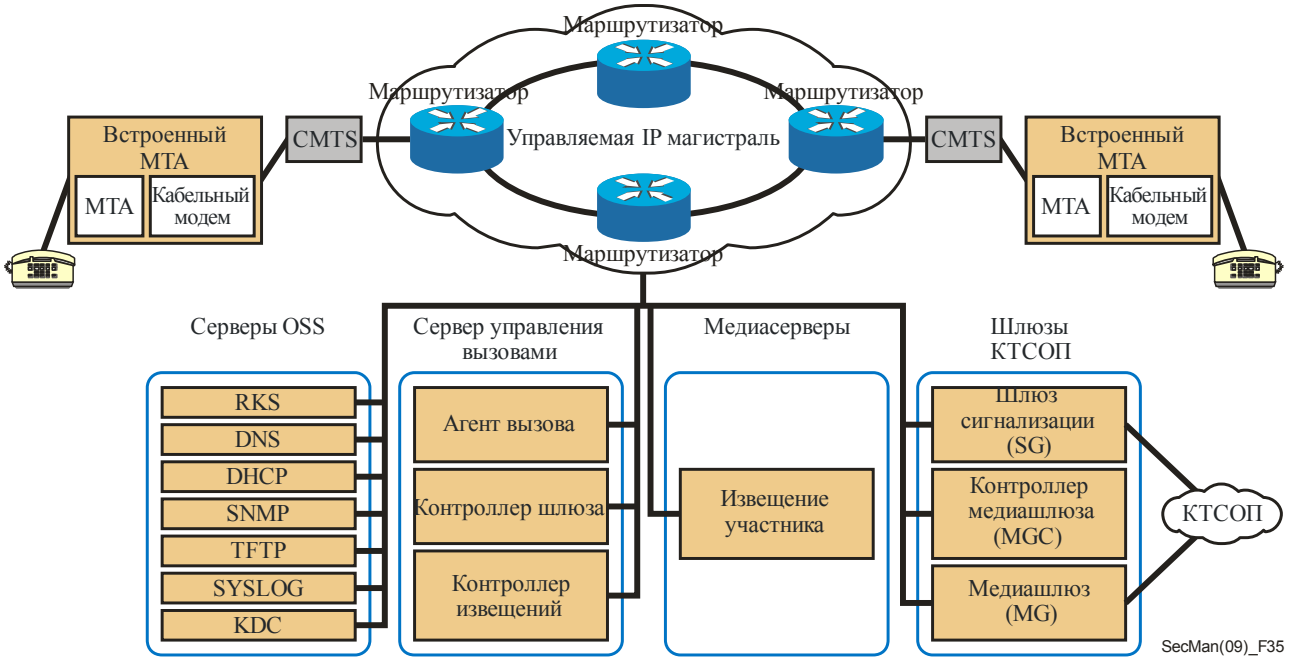


Рисунок 35 – Эталонная модель компонентного IPCablecom

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. Задачи создания безопасности определены в архитектуре IP Cablecom:

- обеспечить функциональную возможность передачи голоса в зоне жилой застройки на том же или более высоком уровне конфиденциальности, как и 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 контроль за доступом.

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

- кража услуг, которая включает мошенничество по подписке; 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, манипуляция протоколом, криптоанализ в автономном режиме и прерывание связи при обслуживании;
- раскрытие служебной информации;
- кража услуг, основанных на MTA; и
- незаконная регистрация с разными поставщиками услуг арендованного MTA.

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 с помощью определенного для каждого конкретного интерфейса протокола основного механизма безопасности (такого как IPSec), который обеспечивает интерфейс протокола необходимыми для него услугами безопасности. В контексте архитектуры X.805 обзор услуги безопасности для IPCablecom охватывает все девять ячеек, образуемых тремя плоскостями и тремя слоями, показанными на Рисунке 1.

Услуги безопасности, предоставляемые через основной слой услуг IPCablecom, включают аутентификацию, контроль за доступом, целостность, конфиденциальность и сохранность информации. 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 издание технических спецификаций для сетей подвижных систем GSM и системы третьего поколения (3G), а также развитие архитектуры для подвижных сетей на основе SIP по IP-сетям. В результате, архитектура *подсистемы передачи мультимедийных данных по IP-сетям* 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 контроля за доступом;
- защиту сети от отказа в обслуживании, прерывание связи в сети, атак, заключающихся в краже услуги;
- защиту оборудования пользователя (UE), т. е. клиента, от отказа в обслуживания из-за атак, уязвимости 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 аутентификации пользователя; обеспечение безопасности, безопасная сигнализация и безопасная загрузка программного обеспечения; и
- улучшение и расширение архитектуры IMS в целях содействия ранее поставленным целям.

Общие угрозы, которые относятся к IPCablecom2:

Угрозы домену, пользующемуся доверием

Домен, пользующийся доверием, является логическим объединением элементов сети, которым доверяют при установлении связи. Домен, пользующийся доверием, может быть разграничен физическими или логическими границами. Связь через домены, пользующиеся доверием, всегда должна быть защищена с помощью аутентификации и авторизации. Кроме того, интерфейсы, подключающие элементы сети в пределах домена, интерфейсы между доменами, а также интерфейсы между UE и поставщиком услуг должны быть защищены от различных угроз.

Кража услуги

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

Прерывание связи 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 мультимедийных данных на свои интерфейсы); и атаки с применением "зомби", т. е. взломанных систем с множеством конечных точек).

Угрозы каналу сигнализации

В среде с мультимедийными данными сообщения сигнализации включают данные, относящиеся к идентичности, услугам, маршрутизации и другим подверженным риску и важным данным. Мультимедийные компоненты, такие как прокси-сервера, существуют в домене доступа, подвергая их большому количеству угроз. Атаки, заключающиеся в угрозах сигнализации, включают: взлом конфиденциальности информации сигнализации; атаки "человек-посредник" в результате перехвата и возможного изменения трафика, проходящего между двумя связанными сторонами; и атаки, приводящие к отказу в обслуживании в диапазоне канала сигнализации.

Угрозы несущим каналам

Угрозы несущим каналам относятся к трафику мультимедийных данных, передаваемому между связанными сторонами.

Угрозы безопасности конкретному протоколу

Различные угрозы существуют в отношении отдельных протоколов мультимедийных данных.

8.5.3 Услуги и механизмы безопасности в IPCablecom2

IPCablecom2 широко использует безопасность транспортного уровня и другие механизмы, упомянутые в 3GPP Подсистемы передачи мультимедийных данных по IP-сетям (3GPP 23.002 v6.10.0, *Архитектура сети*, декабрь 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:

- аутентификация подсистемы передачи мультимедийных данных по IP-сетям и соглашение о ключе;
- аутентификация профиля протокола инициирования сеанса связи (SIP); и
- сертификация начальной загрузки.

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 вызовом сеанса с прокси-элементом, в IPCablecom2 добавляется безопасность на транспортном уровне (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, который представляет собой измеряемое физическое свойство. Повсеместная сеть датчиков (USN) представляет собой сеть, которая использует датчики с низкой стоимостью, малой мощностью для разработки информированности 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 область и может поддерживать множество приложений. На Рисунке 36 показаны потенциальные применения USN.

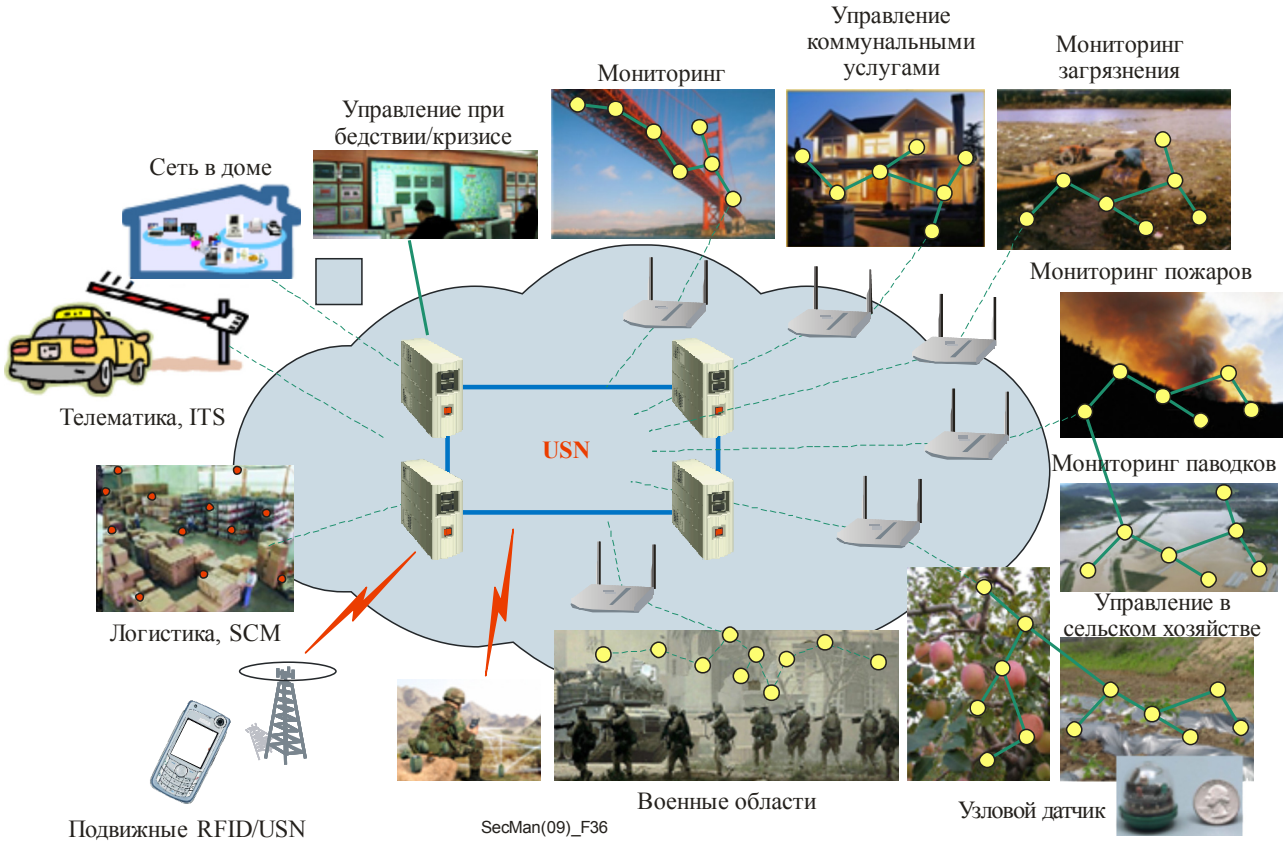


Рисунок 36 – Потенциальные применения USN

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 основные технологии , например 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.

В дополнение к стандартным сетевым угрозам (тем, которые обсуждались в Разделе 3) существуют конкретные угрозы для USN. Они включают:

- **взлом узлового датчика**, через одиночные датчики, подверженные атакам, или взломанные, или через злоумышленника, устанавливающего незаконные датчики;

- **подслушивание**, с помощью мониторинга передач между узлами;
- **взлом или вскрытие считанных данных**;
- **атаки, приводящие к отказу в обслуживании**, направленные против датчиков или соединений; и
- **вредоносное или неправильное использование датчиков сети**, например, использование датчиков для незаконных целей.

Кроме того, USN является объектом для ряда угроз, связанных с маршрутизацией между узловыми датчиками.

Характеристики сети датчиков очень усложняют процесс создания безопасной сети. Например, из-за ограниченной вычислительной мощности и памяти узловых датчиков и ограниченной мощности и полосы пропускания, невозможно использование криптографии с открытым ключом или хранение уникальных ключей с узлами. Кроме того, датчики могут быть расположены в агрессивных средах, и перед развертыванием их точное местоположение не может быть известно. Наконец, сеть датчиков сильно зависит от ее базовой станции, которая является не только единственной потенциальной точкой отказа, но и заманчивой целью для потенциальных атак.

Промежуточное программное обеспечение USN предоставляет платформу для общих приложений, для того чтобы поддержать различные функций со стороны приложений и услуг USN, а также, для того чтобы управлять сетями датчиков. Большое количество данных, собранных с помощью сети датчика хранится, управляется и анализируется промежуточным программным обеспечением USN, которое также должно передавать данные безопасно для соответствующих приложений. Меры безопасности, а также возможности промежуточного программного обеспечения должны быть направлены на обеспечение безопасности данных при хранении и в процессе передачи.

Несмотря на то, что рекомендация в отношении USN до сих пор не завершена, полным ходом идут работы по решению потребности в безопасности самих USN, а также промежуточного программного обеспечения для USN.

9. Безопасность приложения

9 Безопасность приложения

С увеличением осведомленности о важности безопасности, сегодня разработчики приложений уделяют больше внимания необходимости создания 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.

9.1 Передача голоса (VoIP) и мультимедиа по IP протоколу

VoIP, известная также как IP-телефония – это предоставление по сети с использованием протокола IP (на котором базируется интернет) услуг, традиционно предоставляемых по коммутируемой телефонной сети общего пользования (КТСОП) с коммутацией каналов. К таким услугам относятся прежде всего услуги по передаче речи, другие формы передачи, включая передачу видеоряда и данных. VoIP включает также связанные дополнительные услуги, такие как конференции (запараллеливание), переадресация вызова, постановка на ожидание вызова, многоканальность, изменение маршрута прохождения вызова, ожидание и прием сигнала, обратный опрос, следящая переадресация и многие другие услуги интеллектуальной сети и в некоторых случаях также передача данных в диапазоне тональных частот. Передача голоса по интернету представляет собой частный случай VoIP, когда трафик речевых сообщений переносится по магистралям общедоступного интернета.

Рекомендация МСЭ-Т H.323, *Мультимедийные системы связи на основе пакетов*, является "зонтичной" Рекомендацией МСЭ-Т, формирующей основу для передачи звуковых сигналов, видеоряда и данных по сетям с коммутацией пакетов данных, включая интернет, локальные вычислительные сети (ЛВС) и региональные распределенные сети (WAN), 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 IPX по Ethernet, Fast Ethernet и 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. МСЭ-Т H.323 был первым получившим определение протоколом VoIP и считается основой для функционирующих в среде VoIP продуктов, применяемых в сферах торговли, коммерческой деятельности, обслуживания, индустрии развлечений и профессиональных приложений. Техническое описание безопасности для серии Рекомендаций МСЭ-Т H.323 содержится в Рекомендации МСЭ-Т H.Imp235 *Руководство для внедряющих сторон для МСЭ-Т H.235 V3: "Безопасность и шифрование для мультимедийных терминалов серии H (МСЭ-Т H.323 и другие на основе МСЭ-Т H.245)*", МСЭ-Т H.235.x, серии из девяти структур и стандартов безопасности и МСЭ-Т H.530, *Симметричные процедуры безопасности для мобильности H.323 в МСЭ-Т H.510*. 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 37.

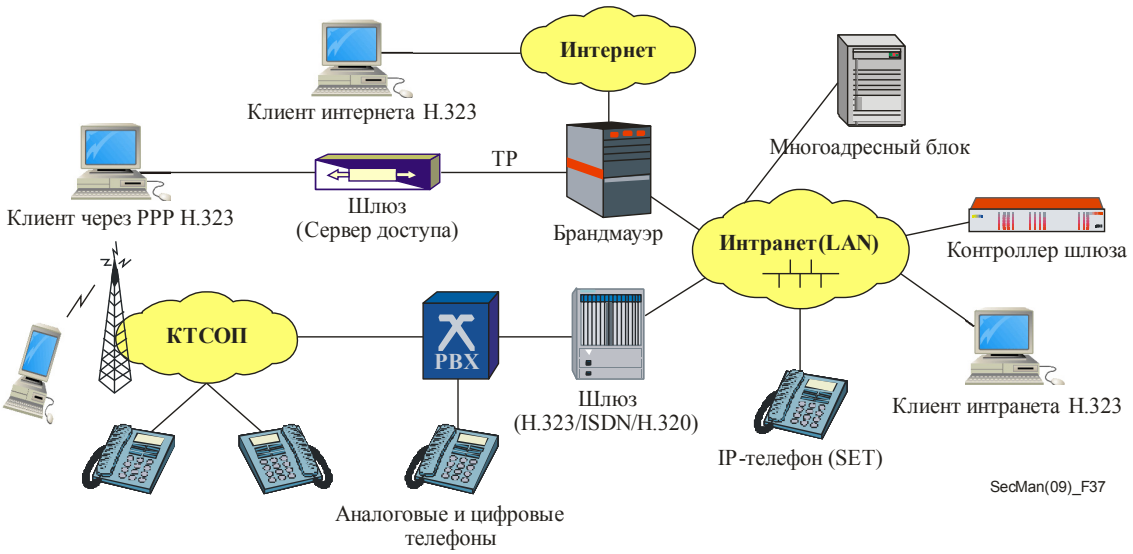


Рисунок 37 – Система H.323: компоненты и сценарии развертывания

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 МСЭ-Т H.323 используется для IP-PBX, IP-centrex, голосового VPN, интегрированных систем передачи речевых сигналов и данных, телефонов WiFi, реализации центров обслуживания вызовов, а также для обеспечения услуг мобильности. В области профессиональной связи этот стандарт широко применяется для речевых (или аудио-) и видеоконференций, для совмещения речи/данных/видео, а также для дистанционного обучения. Для домашних приложений используются широкополосный аудиовизуальный доступ, соединение ПК–телефон, телефон–ПК и ПК–ПК; оно может также использоваться для доставки клиентам новостей и иной информации.

9.1.1 Проблемы безопасности для мультимедиа и VoIP

Вследствие того что все элементы системы H.323 могут быть географически разнесены и в силу открытости сетей IP, возникает ряд угроз безопасности, как показано на Рисунке 38.

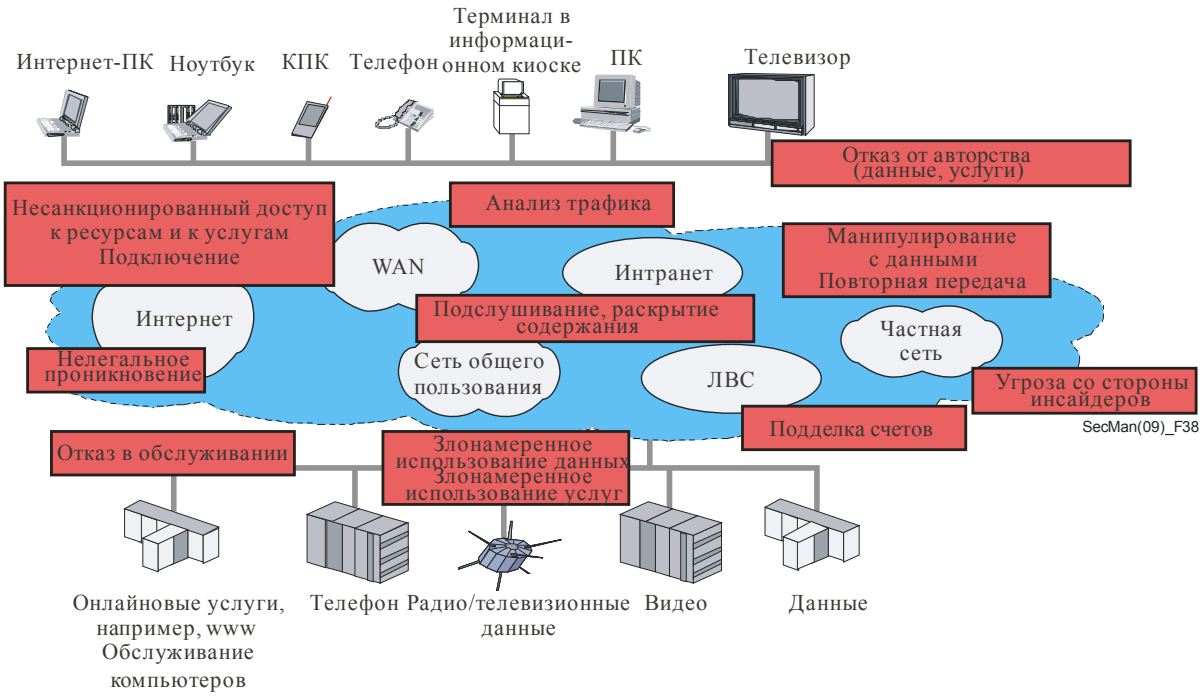


Рисунок 38 – Угрозы безопасности в среде мультимедийной связи

Основные вопросы обеспечения безопасности в среде мультимедийной связи и IP-телефонии дополнительно описаны ниже:

- Аутентификация пользователя и терминала: поставщикам услуг VoIP необходимо знать, кто пользуется их услугами, с тем чтобы правильно произвести расчет и, возможно, выставить счет за обслуживание. В качестве необходимого условия для аутентификации пользователь и/или терминал должны идентифицироваться по какому-либо идентификационному признаку. Затем пользователь/терминал должны доказать, что предъявленная идентификационная информация действительно является верной. Обычно это выполняется с помощью процедур криптографической аутентификации (например, защищенный пароль или цифровые подписи X.509).
- Аутентификация сервера: в силу того, что для общения пользователей VoIP между собой обычно задействуется определенная инфраструктура VoIP, включая серверы (пропускные пункты, многоточечные блоки, шлюзы), пользователи заинтересованы в том, чтобы знать, с требуемым ли сервером и/или поставщиком услуг установлена связь. Этот аспект включает пользователей фиксированной и подвижной связи.
- 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 ресурсов услуги, таких как функции услуги, например, соединение с КТСОП, или ресурсов сети (QoS, полоса пропускания, кодеки и т. д.). Как правило, функции аутентификации и авторизации выполняются вместе, с тем 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 связи: Достигается за счет шифрования пакетов речевых сообщений и противодействует подслушиванию. Как правило, медиапакеты, например, видео, мультимедийных приложений также шифруются. Более современная защита медиапакетов включает также аутентификацию/защиту целостности полезной нагрузки.
- Управление ключами: Охватывает не только выполнение всех задач, необходимых для обеспечения безопасного распространения данных ключей между сторонами – к пользователям и серверам, но и такие задачи, как обновление ключей, у которых истек срок службы или которые были утеряны Управление ключами может составлять задачу, отдельную от VoIP приложений (предоставление паролей), или может быть объединено с сигнализацией, когда динамически согласуются профили безопасности с возможностями по обеспечению безопасности и должно осуществляться распространение ключей конкретно для данного сеанса.
- Междоменная безопасность: Предназначена для решения проблемы, возникающей вследствие того, что реализованные в неоднородной среде системы имеют различные характеристики безопасности в силу различий в потребностях, в стратегии безопасности и в имеющихся возможностях обеспечения безопасности. По этой причине необходимо добиваться динамического согласования профилей безопасности и возможностей 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 МСЭ-Т H.323. Вопросы безопасности, выходящие за рамки обзора МСЭ-Т H.323, включают в себя стратегию безопасности, безопасность управления сетью, обеспечение безопасности, безопасность реализации, эксплуатационная безопасность или разрешение случаев нарушения безопасности.

9.1.2 Обзор серии Рекомендаций H.235.x

Серия Рекомендаций H.235.x объединяет одиннадцать стандартов, плюс одно руководство для реализующего объекта, определяет структуру безопасности, включая спецификацию механизмов безопасности и протоколов безопасности для подсерии Рекомендаций МСЭ-Т H.323. Они предлагают масштабируемые решения безопасности для небольших групп, предприятий и крупномасштабных несущих и предлагают криптографическую защиту протоколов управления, а также мультимедийного потока данных аудио/видео.

МСЭ-Т H.235 предлагает средства согласования желаемых и 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 в себя "классическую" связь между оконечными пунктами, а также многоточечную конфигурацию при использовании многоточечных 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 современный 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 получить выгоду, благодаря незначительному воздействию на оконечные точки за счет плотного взаимодействия с процессором цифровой обработки сигналов и использования кодеков со сжатием речевого сигнала, а также за счет отсутствия зависимости от типа платформы операционной системы.

На Рисунке 39 показана область действия МСЭ-Т H.235, который осуществляет 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 сохранности информации. Пропускные пункты осуществляют аутентификацию путем управления разрешениями в конечных точках и обеспечивают механизмы поддержания сохранности информации. 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.

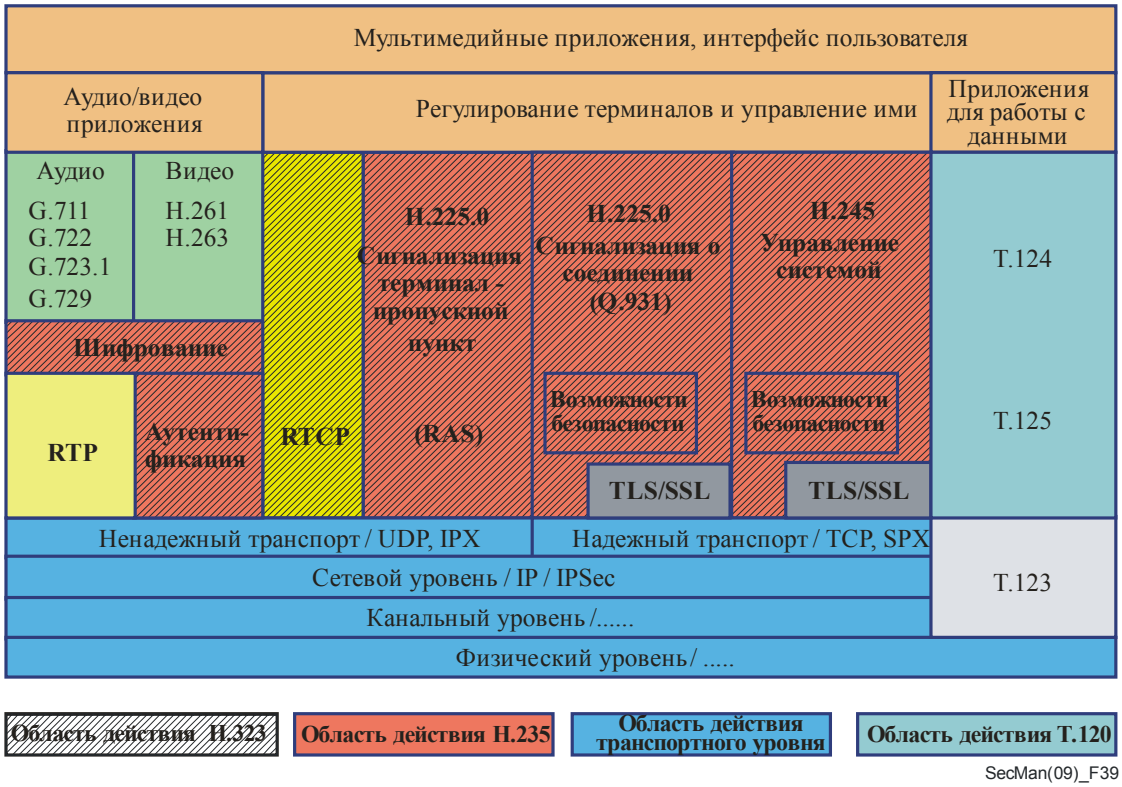


Рисунок 39 – Безопасность в МСЭ-Т H.323, как она обеспечивается МСЭ-Т H.235

Рекомендации МСЭ-Т серии H.235.x охватывают широкий спектр мер безопасности, предназначенных для использования в различных средах, например, для связи между предприятиями и внутри предприятий 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 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 возможностей на базе PKI. МСЭ-Т H.235.3 называют гибридным профилем защиты, поскольку в этой Рекомендации сочетаются симметричные процедуры безопасности, предусмотренные в МСЭ-Т H.235.1, с использованием сертификатов на базе PKI и подписи согласно МСЭ-Т H.235.2, и тем самым достигаются оптимальные результаты и более короткое время соединения. МСЭ-Т H.235.4 ослабляет жесткую зависимость от архитектуры, центром которой является сервер, с пропускными пунктами маршрутизаторами и 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, 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 *Профиль шифрования речи с управлением внутренним ключом H.235/H.245* собраны все процедуры, необходимые для шифрования потока данных RTP, включая сопровождающее управление ключами, которое полностью выражено в полях сигнализации МСЭ-Т H.245.

Безопасная мобильность пользователя и терминала в среде распределенных систем МСЭ-Т H.323 описана в Рекомендации МСЭ-Т H.530 *Симметричные процедуры безопасности для мобильности МСЭ-Т H.323 в МСЭ-Т H.510*, 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. Рекомендации серии МСЭ-Т H.235.0 и МСЭ-Т 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 МСЭ-Т H.323, SIP, МСЭ-Т H.320 и базовых услуг обмена сообщениями к службе справочников, с тем чтобы к мультимедийной связи можно было бы применять современные методы управления идентичностью.

9.1.3 Трансляция сетевого адреса и устройства брандмауэра

Интернет разрабатывался на основе принципа "прямой" связи между конечными 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 NAT часто используются на границе сети. Эти границы включают резидентный домен, домен поставщика услуг, домен предприятия и иногда домен страны. В рамках одного домена иногда используется несколько брандмауэров или устройств NAT. Межсетевые устройства защиты предназначены для жесткого контроля за тем, как перемещается информация по границам сети, и обычно они настроены для блокирования большинства сообщений IP. Если межсетевое устройство защиты явно не сконфигурировано таким образом, чтобы позволить пройти трафику МСЭ-Т H.323 из внешних устройств во внутренние устройства МСЭ-Т H.323, связь становится просто невозможной. Это вызывает проблему для любого пользователя оборудования МСЭ-Т H.323.

Устройства NAT транслируют адрес, используемый 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	Число 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. 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 серии МСЭ-Т H.460, которые дают возможность сигналам связи, соответствующим МСЭ-Т H.323, бесшовно проходить через одно или несколько устройств NAT/FW. Это следующие Рекомендации: МСЭ-Т H.460.17 *Использование каналов сигнализации вызова по стандарту H.225.0 в качестве транспорта для сообщений RAS H.323*; МСЭ-Т H.460.18 *Передача сигнализации H.323 через трансляторы сетевых адресов и межсетевые устройства защиты*; и МСЭ-Т H.460.19, *Передача медиаданных H.323 через трансляторы сетевых адресов и межсетевые устройства защиты*.

На Рисунке 40 показано, как специальное устройство "посредник" может быть использовано, с тем чтобы помочь устройствам, "не знающим" NAT/FW, надлежащим образом пройти границы этих устройств.

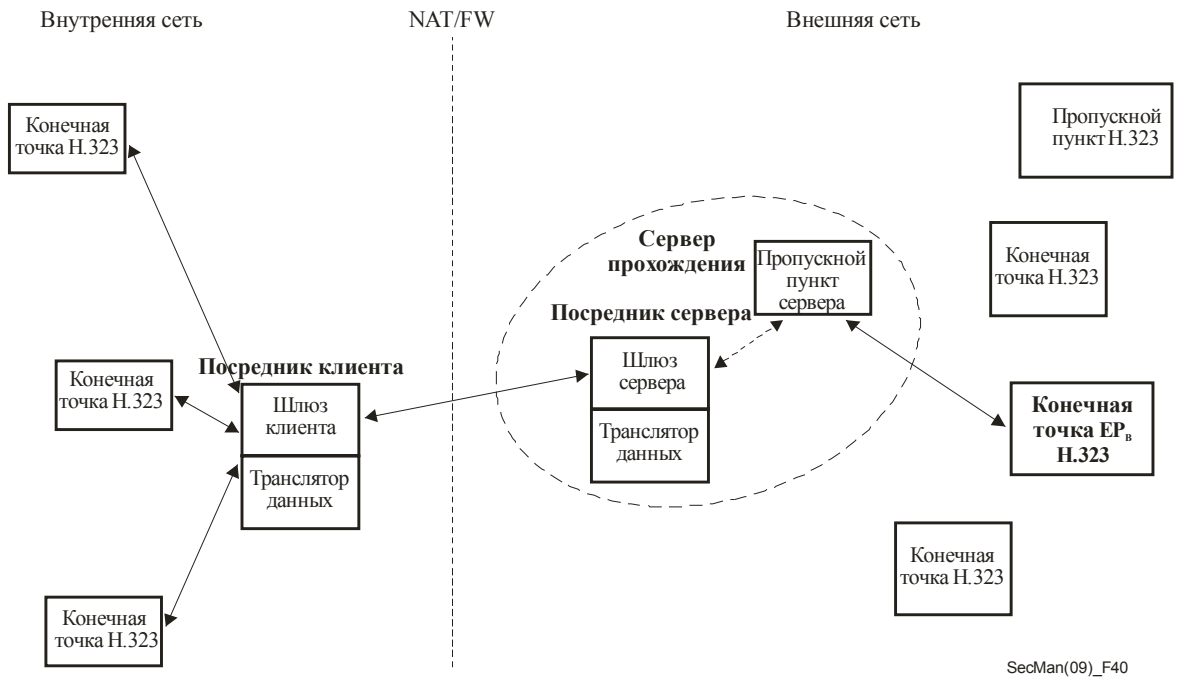


Рисунок 40 – Переход NAT/FW в архитектуре H.460.18

Вышеприведенная топология может использоваться в например, в том случае, когда предприятие желает контролировать маршрут, по которому сигнализация вызова МСЭ-Т H.323 и медиаданные передаются по сети. Однако МСЭ-Т H.460.17 и МСЭ-Т H.460.18 также позволяют конечным точкам проходить границы NAT/FW без помощи каких-либо специальных внутренних устройств-"посредников". Одна такая топология показана на Рисунке 41:

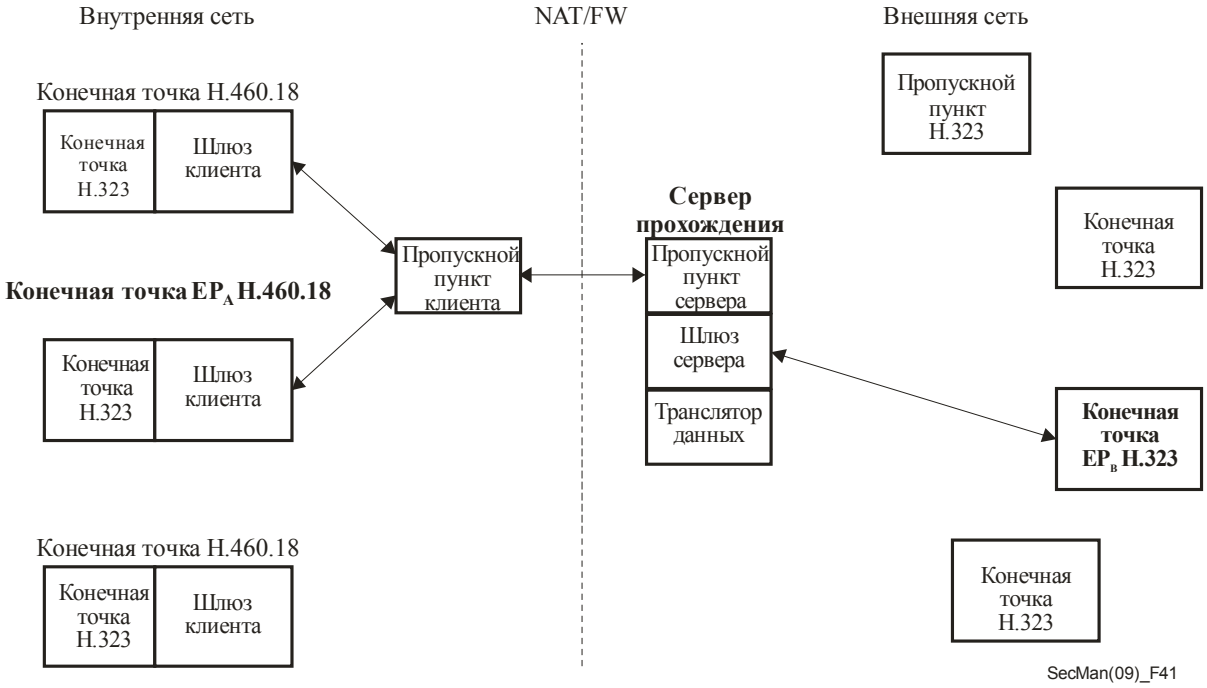


Рисунок 41 – Архитектура связи через шлюзовые соединения

На Рисунке 41 конечные точки во внутренней сети связываются со шлюзом, 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 шлюз во внутренней сети связывается со шлюзом во внешней сети и передает эту информацию обратно вызывающей конечной точке. Когда устройство из внутренней сети передает вызов на устройство из внешней сети, для открытия необходимых "микроканалов" через устройства NAT/FW для получения сигнала от внутренней сети к внешней сети оно использует процедуры, предусмотренные в МСЭ-Т H.460.18. Кроме того, для открытия необходимых "микроканалов" оно использует процедуры, предусмотренные в МСЭ-Т H.460.19, с тем чтобы позволить потокам 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 данных", предусмотренные в МСЭ-Т H.460.18, с тем чтобы надлежащим образом маршрутизировать сигнализацию и данные между двумя отдельными 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 сети, мог бы войти в другую сеть без помощи какого-либо объекта из сети общего пользования, который выполнил бы функцию "посредника" для этого пакета.

9.2 IPTV

Положения безопасности для IP-телевидения (IPTV) должны охватывать защиту содержания, доставленного посредством служб IPTV, используемых оконечных устройств и предоставления 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, контролировать соблюдение правил использования контента, а также защищать целостность и конфиденциальность контента и критических параметров безопасности, например, криптографических ключей.

Защита услуг IPTV включает в себя 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.

В настоящее время готовится нескольких специальных Рекомендаций по безопасности IPTV, а Рекомендация МСЭ-Т X.1191 *Функциональные требования и архитектура для аспектов безопасности IPTV* уже принята. На Рисунке 42 показана общая архитектура безопасности для IPTV, определенная в этой Рекомендации. Обратите внимание, что в обзор этой Рекомендации включены только те функции, которые применимы к конечному пользователю, поставщику сети и поставщику услуг. Функции, относящиеся к поставщику услуг, являются предметом частных соглашений между заинтересованными сторонами и считаются вне зоны рассмотрения данной Рекомендации.

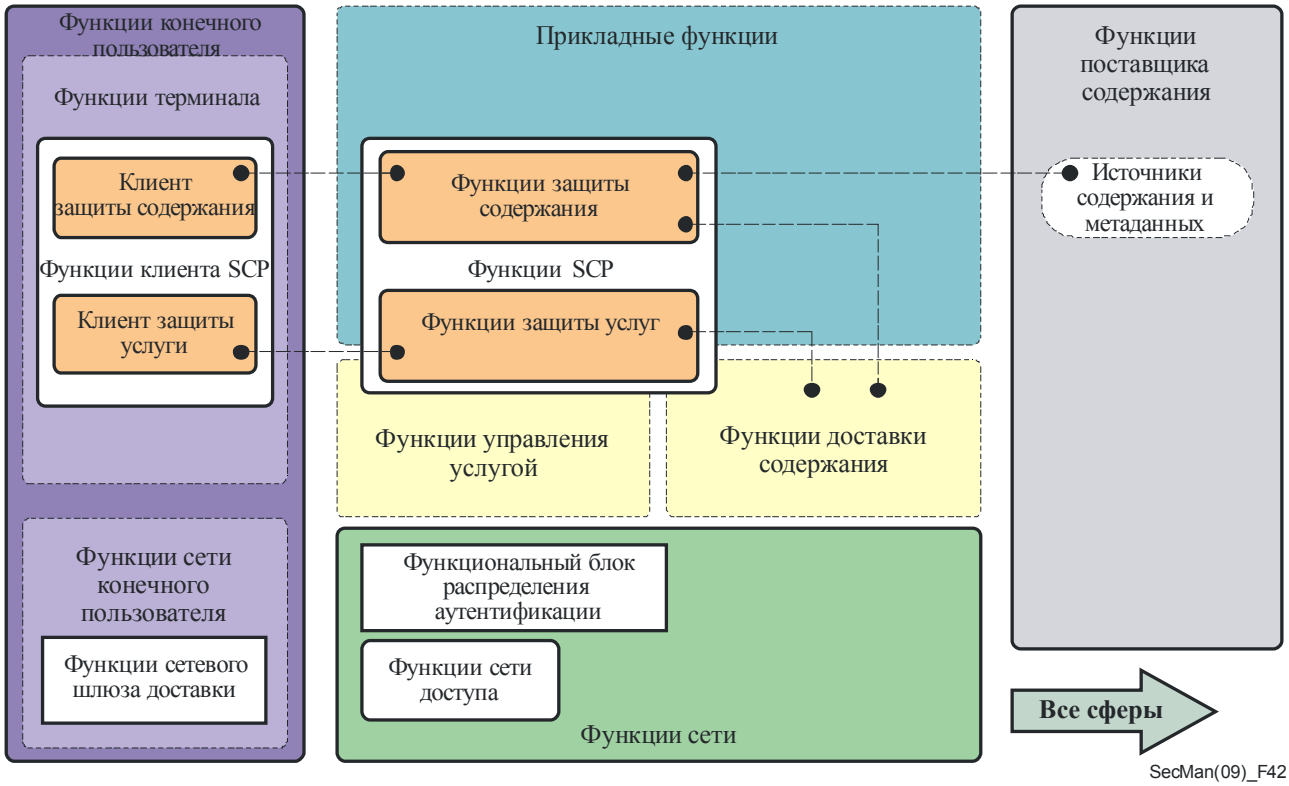


Рисунок 42 – Общая архитектура безопасности для IPTV

9.2.1 Механизмы для защиты контента IPTV

Механизмы для защиты, которые могут использоваться для защиты контента, включают в себя:

- шифрование контента;
- нанесение водяных знаков, т. е. использование стеганографии для изменения определенных функций контента, при этом это изменение нелегко обнаружить;
- идентификация отслеживания контента и информация для облегчения расследований несанкционированного доступа и использования контента;
- маркировка контента, например, использование меток, позволяющих обеспечить определенный уровень управления конечным пользователем доступом к неподходящему контенту; и
- преобразование для защиты, которое позволяет промежуточным сетевым узлам преобразовывать мультимедийный контент в иной формат или качество без дешифрования, тем самым сохраняя сквозную безопасность.

9.2.2 Механизмы для защиты услуги IPTV

Механизмы для защиты услуги включают в себя:

- 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
- контроль за доступом, в частности, для обеспечения того, что к контенту, загруженному клиентом на сервер, может иметь доступ только авторизованный поставщик услуг.

9.2.3 Защита информации абонента

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

9.3 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 в себя конфиденциальность передаваемых данных, аутентификацию и сохранность информации. 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 T.36, *Возможности безопасности для использования с терминалами факсимильной передачи 3-ей группы*, где определены два независимых технических решения, которые могут использоваться для шифрования документов при обмене. Одним из определенных решений является использование алгоритма криптографии *Райвеста-Шамира-Адлемана* (RSA); другой метод использует комбинацию *Управления ключами Готторна* (HKM) и *Шифра факсимильных передач Готторна* (HFX). К указанным услугам безопасности относятся:

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

Комбинация систем *Управления ключами Готторна* (HKM) и *Шифра факсимильных передач Готторна* (HFX) дает следующие возможности для безопасной передачи данных между объектами:

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

9.4 Веб-услуги

Веб-технологии, включая архитектуры, ориентированные на услуги (SOA), широко применяются, так как они дают разработчикам 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. Важны механизмы аутентификации и единая регистрация во всей сети путём однократного ввода пароля (SSO) и, так как веб-услуги применяются к подвижным сетям, также важно учитывать механизмы безопасности, необходимые для подвижных веб-услуг.

Экономия за счет массового производства побудила поставщиков компьютерного оборудования разработать продукты с функциональными возможностями с высокой степенью обобщенности, так что они могут использоваться в максимально широком спектре ситуаций. Эти продукты имеют максимально возможное преимущество доступа к данным и рабочему программному обеспечению, так что они могут использоваться в максимально возможном спектре применений, 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 отделом информационных систем, людскими ресурсами, юридическим отделом и финансовым отделом. Исполнение политики может осуществляться при помощи экстранета, почты, WAN и систем дистанционного доступа – платформ, по своей природе внедряющих либеральную политику безопасности. Существующей практикой является управление конфигурацией каждого пункта обеспечения исполнения политики отдельно с целью максимально точного проведения политики безопасности. Следовательно, план изменения политики безопасности будет дорогостоящим и ненадежным. Также трудно, вероятно, даже невозможно, фактически получить общий обзор мер безопасности по всему предприятию для обеспечения исполнения политики. В то же время существует растущее давление на корпоративные и правительственные органы со стороны потребителей, акционеров и регуляторных органов с требованиями продемонстрировать "примеры передового опыта" по защите информационных ресурсов предприятия и его потребителей.

По этой причине необходим общий язык для описания политики безопасности. Если такой язык внедрить на предприятии, то он 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.

9.4.1 Язык разметки, предусматривающий защиту данных

В Рекомендации МСЭ-Т X.1141 определяется язык разметки, предусматривающий защиту данных (SAML 2.0). SAML является структурой на основе XML для обмена информацией о безопасности. Эта информация безопасности выражается в виде утверждений о предмете, где предмет – это объект в некотором домене безопасности. Одно утверждение может содержать несколько различных внешних утверждений об аутентификации, авторизации и атрибутах.

Утверждения SAML обычно делаются о *предмете*. Обычно существует несколько *поставщиков услуг*, которые могут использовать утверждения о предмете с целью контроля за доступом и предоставления специализированных услуг, и соответственно они становятся доверяющими сторонами подтверждающей стороны, которая называется *поставщиком идентичности*.

В МСЭ-Т X.1141 определены три разных типа утверждений, которые могут быть созданы органом SAML. Все определенные SAML утверждения связаны с предметом. Тремя типами утверждения, определенными в МСЭ-Т X.1141, являются:

- аутентификация: Предмет утверждения был утвержден определенным способом в определенное время;

- атрибут: Предмет утверждения связан с предоставляемыми атрибутами; и
- решение об авторизации: Запрос на то, чтобы было дано или отклонено разрешение на доступ предмета утверждения к определенному ресурсу.

В МСЭ-Т X.1141 также определен протокол, при помощи которого клиенты могут запросить утверждения у органов SAML и получить от них ответ. Этот протокол, состоящий из запроса на основе XML форматов сообщений ответа, 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 одной единой регистрации во всей сети путём однократного ввода пароля (SSO) браузеров и других клиентских устройств. На Рисунке 43 показан основной шаблон для получения SSO.

Рисунок 43 – Основной шаблон для получения SSO

9.4.2 Расширяемый язык разметки контроля доступа

Расширяемый язык разметки контроля доступа (XACML) является словарем XML для выражения правил контроля за доступом. Контроль за доступом состоит из решения задачи, следует ли удовлетворить запрос на доступ к запрашиваемому к ресурсу, и принудительного применения этого решения. В Рекомендации МСЭ-Т X.1142 определяется базовый XACML, включая синтаксис языка, модели, контекст с моделью языка политики, правила синтаксиса и обработки. Для улучшения в безопасности обмена правилами на основе XACML, в МСЭ-Т X.1142 также определен профиль цифровой подписи XACML XML для данных безопасности. Профиль конфиденциальности определен, чтобы предоставить руководящие указания для средств реализации. XACML подходит для разных условий применения.

9.5 Услуги на основе меток

В настоящее время широко распространены метки идентификации, включая метки 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 критичной и/или личной информации.

Для приложений, где используются метки, или которые опираются на идентификацию на основе меток в приложениях, которые применяют 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, подлежащей личной идентификации (PII), было сосредоточено на протоколах аутентификации между меткой идентификатора и терминалом идентификатора. 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 *Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров* исследуются угрозы PII в условиях на основе отношений бизнеса и потребителя (B2C), в которых приложения используют идентификацию на основе меток. Это определяет требования для защиты PII в таких условиях и создает базовую структуру защиты PII на основе определенного пользователем профиля правил PII.

Приложения отношений бизнеса и потребителя (B2C), использующие идентификацию на основе меток, могут быть систематизированы по трем типам:

a) *Пользователь устройства, как потребитель*: В услуге доставки информационного содержания потребитель получает информацию при помощи устройства для чтения, которое у него/нее есть. В этом типе услуги большинство поставщиков услуг приложений могут предполагать, что у потребителя есть подвижный терминал, оборудованный устройством для чтения. На Рисунке 44 показана основная модель данного типа применения. Она состоит из двух основных сетевых операций: распознавание идентификатора и получение содержания. Распознавание идентификатора является процедурой перевода или изменения идентификатора в адрес. Подвижный терминал со считывающим устройством сначала изменяет ID идентификатора, после его получения от метки при помощи услуги каталогизации, а затем осуществляет получение содержания.

Рисунок 44 – Основная модель применения B2C при помощи идентификации на основе меток

b) *Пользователь метки ID, как потребитель*: Типичный пример данного применения B2C при помощи идентификации на основе меток имеет дело с управлением доступом и/или аутентификацией, например, проверкой входа, паспортом, лицензией или службой постпродажного управления. В этом типе применения устройства для чтения относятся к типу фиксированного терминала и/или типу подвижного терминала. Потребителям может не понадобиться их собственное устройство для чтения.

c) *Потребитель как пользователь и метки ID и устройства*: В услуге получения информации о продукте потребитель также становится пользователем меток после приобретения продукта с меткой после изучения содержания информации о продукте на его/ее подвижном терминале. Другими словами, можно рассмотреть услугу, относящуюся к здравоохранению, которая запускается картой пациента, позволяющей наносить метки ID. В данном применении существует много типов

потребителей, которые могут быть пользователями меток ID, например, пациент, врач, медицинская сестра. Пользователь метки ID может просматривать записи в его/ее медицинской карте, позволяющей наносить метки ID, при помощи устройства для чтения на подвижном терминале.

Для приложений B2C, которые используют идентификацию на основе меток, существует два главных риска нарушения PII:

- Утечка информации, связанной с идентификатором: в данном примере атакующий может прочесть информацию с метки ID, а пользователь помеченного продукта не будет знать об этом. Сначала атакующий считывает идентификатор с метки ID, которую несет пользователь. Затем он/она преобразует идентификатор и запрашивает от услуги каталогизации данные о местоположении информации. Наконец, атакующий запрашивает информацию, соответствующую метке ID.
- Утечка данных исторического контекста: Атакующий может извлечь данные пользователя (например, предпочтения, обычаи, область интереса и пр.) из данных исторического контекста, связанных с меткой 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 метки ID*: Пользователь метки ID должен уметь управлять или обновлять PII, связанный с его/ее меткой ID в сети. Таким образом, пользователь метки ID может определить, какой PII следует удалить или оставить в приложении.
- *Аутентификация для пользователя метки ID и/или пользователя устройства*: Для проведения процедур аутентификации для пользователя метки ID необходим сервер приложений, и сервер приложений при необходимости может обеспечить процедуру аутентификации для пользователя устройства. Некоторым приложениям, использующим идентификацию на основе метки, не обязательно аутентифицировать пользователя.
- *Контроль за доступом к PII пользователя метки ID в сервере приложений*: Для контроля за доступом к важной информации, связанной с PII пользователя метки ID необходим сервер приложений.
- *Конфиденциальность данных информации, связанной с меткой ID*: Для сохранения конфиденциальности данных необходим сервер приложений, чтобы гарантировать, что информация, относящаяся к метке ID, не могла быть прочитана неавторизованными пользователями.
- *Согласие на сбор устройством данных журнала событий пользователя*: Сервер приложений может обеспечить процедуру согласия для сбора на устройстве данных журнала событий, относящихся к пользователю, 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 метки, например, приобретение продукта с меткой. На Рисунке 45 показан общий поток услуг PPS приложения, использующего идентификацию на основе метки.

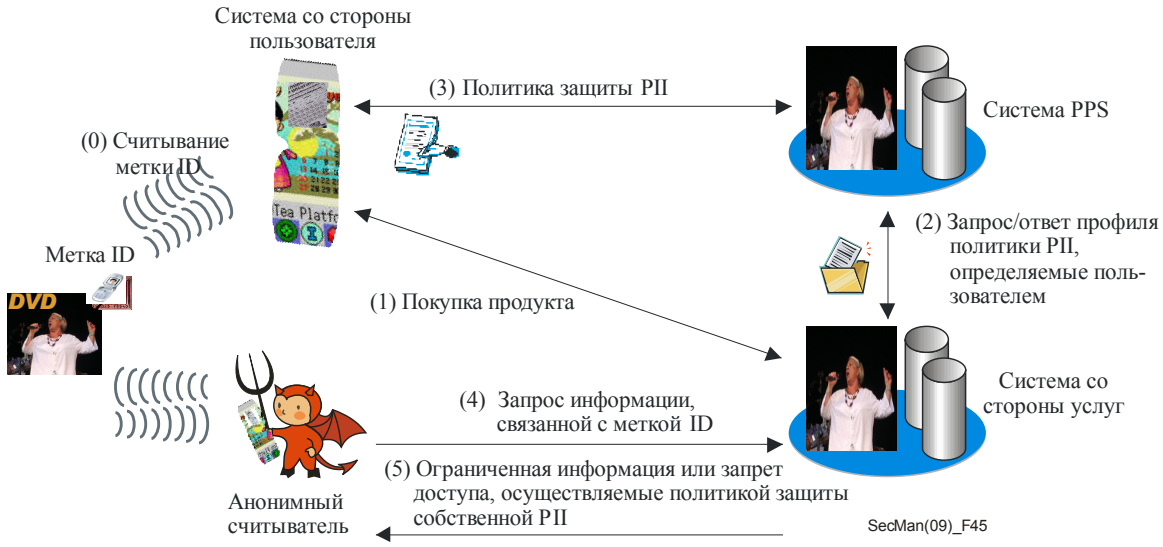


Рисунок 45 – Поток для услуги общей услуги защиты PII (PPS)

1) Потребитель считывает идентификатор продукта с меткой 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 метки ID.
3) Приложение, использующее идентификацию на основе меток, затем запросы у системы PPS определенного пользователем профиля политики PII, который соответствует определенному пользователем профилю PII для приложения.
4) Система PPS получает пользовательскую политику безопасности PII для данного приложения.
5) Любой может запросить информацию, связанную с этой меткой ID, у обслуживающей системы.
6) Запрашивающий может изучить всю представленную обслуживающей системой информацию, если запрашивающий является пользователем метки ID. В противном случае запрашивающий или не может получить доступ к любой информации или может получить только ограниченную информацию.

10. Противостояние общим сетевым угрозам

10 Противостояние 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 небольшим 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.

10.1 Противостояние спаму

Спам, т. е. незатребованная, нежелательная электронная почта, широко известна, как главная проблема для пользователей сети и поставщиков сети и услуг. Спам мешает законным действиям, занимает ширину полосы и циклы обработки, в крайних случаях он приводит к отклонению атак услуг сетей массовой рассылки. Для противостояния спаму с разной степенью эффективности применяются как юридические, так и технические меры. Ни одна мера противостояния спаму не эффективна сама по себе и, учитывая быстроту и изобретательность спамеров, даже комбинация мер часто эффективна только в пределах снижения уровня спама. Примеры использованных мер включают в себя: регулирование; технические меры, включая фильтры спама; международное сотрудничество; и обучение пользователей и поставщиков интернет-услуг.

Работа МСЭ-Т по противостоянию спаму в основном сосредоточена на технических аспектах проблемы, так что, в данном разделе, мы сосредоточимся на технических средствах для противостояния и развитию и применению технологий противодействия спаму.

10.1.1 Технические стратегии в деле противостояния спаму

В Рекомендации МСЭ-Т X.1231 *Технические стратегии в деле противостояния спаму*, 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 противостоянию 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 трех уровням. Взаимосвязи между стратегиями показаны на Рисунке 46. Эта модель указывает, что существует высокая степень взаимосвязи между стратегиями, но что вопросы затрат могут помешать использованию всех стратегий в индивидуальных случаях. Также необходима ориентация на потребителя в соответствии с определенным сценарием применения.

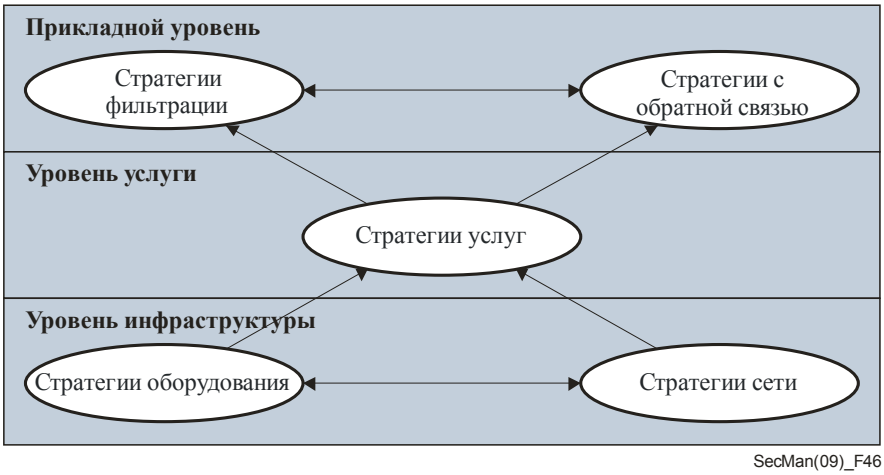


Рисунок 46 – Общая модель противостояния спаму

10.1.2 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 противостоянии спаму в электронной почте. МСЭ-Т X.1240 *Технологии, используемые в борьбе со спамом в электронной почте*, адресована пользователям, которые желают создать технические решения для противостояния спаму в электронной почте. В ней определены основные концепции, характеристики, эффекты и технические вопросы, связанные с противостоянием спаму в электронной почте. Также в ней указаны существующие технические решения и соответствующие действия организаций по разработке стандартов и других групп, работающих над противостоянием спаму в электронной почте.

В Рекомендации МСЭ-Т X.1241 *Техническая основа противодействия спаму, рассылаемому по электронной почте*, описана рекомендованная структура домена обработки для борьбы со спамом и определены функциональные возможности основных модулей в домене. Основа создает механизм, при помощи которого различные серверы электронной почты могут делиться информацией о спаме в электронной почте. Она направлена на содействие большому сотрудничеству между поставщиками услуг в борьбе со спамом. В частности она содержит основу для создания методики связи для оповещения об обнаруженном спаме. Другой документ, Дополнение к *серии МСЭ-Т X.1240 – Противостояние спаму и соответствующим угрозам,* рассматривает международные форумы, где обсуждался спам и включает тематическое исследование.

Рисунок 47 – Общая структура домена обработки для борьбы со спамом

На Рисунке 47 показаны процессы структуры 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 утвердить и уточнить правила. Также существует функция разрешения любых противоречий в правилах.

10.1.3 IP-мультимедийный спам

В Рекомендации МСЭ-Т X.1244 *Общие аспекты противостояния спаму в мультимедийных IP-приложениях* определены основные концепции, характеристики и технические вопросы, связанные с противостоянием 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 при противостоянии такому спаму. Некоторые технологии, разработанные для управления спамом в электронной почте, также могут использоваться при противостоянии спаму в IP-мультимедийных приложениях. В МСЭ-Т X.1244 анализируются традиционные механизмы противостояния спаму и обсуждается их применимость к противостоянию спаму в IP-мультимедийных приложениях.

Технологии борьбы со спамом для IP-мультимедийного спама могут применяться в соответствии с определенными характеристиками спама. В Таблице 7 приведена классификация, применяемая в МСЭ-Т X.1244.

Таблица 7 – 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

10.1.4 Спам в службе коротких сообщений (СМС)

В Рекомендации МСЭ-Т X.1242 *Система фильтрации спама в услуге передачи коротких сообщений (СМС) на основе определяемых пользователем правил* определяются структура и функции системы фильтрации спама в СМС вместе с управлением услугами пользователем, протоколами связи и основными функциональными требованиями терминалов с функциями СМС. Определены методы, при помощи которых пользователи могут управлять (запрашивать, удалять и восстанавливать) отфильтрованные короткие сообщения. Фильтрация может основываться на таких характеристиках, как адрес, телефонный номер, время или содержание. Требования для терминального программного обеспечения для поддержки фильтрации спама в СМС представлены в дополнении к МСЭ-Т X.1242.

10.2 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 программное обеспечение и другое заведомо ложное программное обеспечение, т. е. программное обеспечение, которое осуществляет несанкционированные действия, также создает значительный риск. Если организации и частные лица внедряют ряд упреждающих мер против этих угроз, среди которых брандмауэры, антивирусные меры и меры борьбы со шпионским программным обеспечением, 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 надежности, которые они предпринимают, и требуют, чтобы поставщики услуг делали еще больше, чтобы помочь пользователям добиться безопасного и надежного пользования интернетом.

Рекомендация МСЭ-Т X.1207 *Руководство для поставщиков услуг электросвязи по оценке рисков шпионских программ и потенциально нежелательного программного обеспечения* 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 надежного использования персонального компьютера и интернета.

МСЭ-Т X.1207 дает четкие руководящие указания поставщикам услуг по безопасному управлению рисками, применению надежных 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 оконечных пользователей. В несамостоятельном дополнении приведены ссылки на дополнительные материалы по ресурсам.

10.3 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 программой безопасности с хорошим управлением обычно централизованно управляют обновлением, принудительно обновляя системы оконечного пользователя. И наоборот, обновление личных систем, например, домашних компьютеров, и обновления в небольших организациях обычно происходит достаточно бессистемно.

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

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

11. Будущее стандартизации безопасности ИКТ

11 Будущее стандартизации безопасности ИКТ

В течение более 30 лет МСЭ-Т участвовал в развитии стандартов ИКТ. В последнее время эта работа 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 сети. 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 увеличения уверенности пользователя в действиях в он-лайн среде.

Если заглянуть в будущее, то сети электросвязи и компьютерные сети будут продолжать сближаться. Сети последующих поколений и услуги 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.

191 Государство-Член и более 551 участника Сектора МСЭ будут продолжать реагировать на эти проблемы, не переставая создавать технические Рекомендации и руководящие указания по безопасности в насыщенной программе работ, которая основывается на потребностях членов и организационных структурах, созданных на Всемирной ассамблее по стандартизации электросвязи 2008 года. Когда это возможно, во избежание дублирования попыток и фокусирования на ресурсах, МСЭ-Т будет сотрудничать с другими организациями по разработке стандартов для получения гармонизированных и максимально эффективных и оперативных решений.

12. Источники дополнительной информации

12 Источник дополнительной информации

В этом Руководству 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.

12.1 Обзор работы 17-й ИК

В качестве первого шага на домашней странице 17-й ИК представлены ссылки на информацию о работе 17-й ИК, включая руководства и презентации, обзор разрабатываемых Рекомендаций и основной персонал. 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.

12.2 Сборник по безопасности

Этот Сборник содержит информацию о Рекомендациях МСЭ, соответствующей 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 применение функций, относящихся к безопасности интересов и потребностей;
- 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.

12.3 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 ISO/IEC, ATIS, ENISA, ETSI, IEEE, IETF, OASIS, 3GPP и 3GPP2.

Как и Сборник, Дорожная карта состоит из пяти частей, и большинство информации напрямую доступно в режиме он-лайн:

- Часть 1: *Организации по разработке стандартов ИКТ и их работа*, которая содержит информацию о структуре Дорожной карты и о каждой перечисленной организации по разработке стандартов. В Части 1 также представлены ссылки на существующие словари по безопасности;
- Часть 2: *Утвержденные стандарты безопасности ИКТ*, которая содержит базу данных с поисковой машиной утвержденных стандартов безопасности с прямыми ссылками на большинство стандартов;
- Часть 3: *Разрабатываемые стандарты безопасности*;
- Часть 4: *Потребности в будущем и предложенные новые стандарты безопасности*; и
- Часть 5: *Примеры передового опыта по безопасности*.

12.4 Руководящие указания по внедрению безопасности

В Дополнении 3 к серии Рекомендаций МСЭ-Т X.800–X.849 *Дополнение к руководящим указаниям для внедрения системы и сети безопасности*, 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 ресурса; угрозы, уязвимости и ухудшения; и 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.

12.5 Дополнительная информация по управлению каталогом, аутентификацией и определением идентичности

Более подробная информация о серии Рекомендаций МСЭ-Т X.500, санкционированный источник информации, содержится в самой серии Рекомендаций МСЭ-Т X.500. Дополнительная руководящая информация и Руководящие указания для реализующего объекта содержится по адресу www.x500standard.com. По следующим ссылкам можно найти дополнительную информацию:

http://www.x500standard.com/index.php?n=X509.X509ProtectingDirectory содержит информацию об аутентификации пользователя;

http://www.x500standard.com/index.php?n=X500.AccessControl предоставляет больше информации об управлении доступом; и

http://www.x500standard.com/index.php?n=X500.DataPrivacyProtection предлагает более подробное описание функций конфиденциальности данных X.500.

Приложение А – Определения в области безопасности

Приложение А
Определения в области безопасности

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

Термин (англ.)	Термин	Определение	Ссылка
access control	Контроль за 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.	X.800 J.170
access control list	Список для контроля за доступом	Список объектов, имеющих полномочия на получение доступа к ресурсу, и их прав доступа.	X.800
access control policy	Правила контроля за доступом	Набор правил, которые определяют условия, при которых доступ может иметь место.	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.	X.800
accountability	Отчетность	Свойство, гарантирующее, что действия объекта могут отслеживаться с однозначной привязкой к конкретному объекту.	X.800
algorithm	Алгоритм	Математический процесс, который может использоваться для скремблирования и дескремблирования потока данных.	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.	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).	X.400
Attribute Authority (AA)	Орган по присвоению атрибутов	1. Орган, который назначает полномочия путем выдачи сертификатов атрибутов. 2. Объект, которому один или несколько объектов доверяют создание и подпись сертификатов атрибутов. Примечание – Орган сертификации (ОС) может быть также органом по присвоению атрибутов.	X.509 X.842
attribute certificate	Сертификат атрибута	Структура данных, имеющая цифровую подпись органа по присвоению атрибутов, которая связывает некоторые значения атрибутов с идентификационной информацией о держателе этого атрибута.	X.509
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.	X.811

Термин (англ.)	Термин	Определение	Ссылка
		2. Обеспечение уверенности в заявленной идентификации объекта. 3. См. Аутентификация происхождения 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 людьми-пользователями приложений. Примечание – Данный термин был определен для разъяснения того, что рассматривается более широкая сфера аутентификации, по сравнению с аутентификацией одноранговых объектов из Рекомендации МККТТ X.800. 5. Процесс проверки идентификационной информации, предъявленной одним объектом другому объекту. 6. Процесс, предназначенный для предоставления возможности системе проводить достоверную проверку идентификации стороны.	X.811 X.800 X.217 J.170 J.93
authentication exchange	Обмен данными аутентификации	1. Механизм, предназначенный для идентификации объекта посредством обмена информацией. 2. Последовательность одной или нескольких передач информации обмена данными аутентификации в целях осуществления аутентификации.	X.800 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 (строгая аутентификация).	M.3016.2
authority	Орган	Объект, ответственный за выдачу сертификатов. Определены два типа органов: орган сертификации, который выдает сертификаты открытых ключей, и орган по присвоению атрибутов, который выдает сертификаты атрибутов.	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 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.	X.800 H.235 J.170
availability	Готовность	Свойство быть доступным и годным к эксплуатации по запросу имеющего полномочия объекта.	X.800
capability	Возможность	Маркер, который используется в качестве идентификатора для ресурса, обозначающего, что владение им дает права доступа к данному ресурсу.	X.800
certificate	Сертификат	Набор относящихся к обеспечению 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.	H.235

Термин (англ.)	Термин	Определение	Ссылка
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.	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.	X.509 Q.817
Certification Authority (CA)	Орган сертификации	1. Орган, которому одним или более пользователями доверено создавать и распределять сертификаты открытых ключей. Орган сертификации 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.	X.509 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.	X.800
cleartext	Незашифрованный текст	Открытые данные, семантическое содержание которых доступно.	X.800
confidentiality	Конфиденциальность	Свойство, которое служит для предотвращения раскрытия информации объектами или процессами, не имеющими разрешения на это.	X.800
confidentiality service	Услуга обеспечения конфиденциальности	Услуга обеспечения конфиденциальности предоставляет 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.	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).	X.800 J.170 J.93
cryptographic algorithm	Криптографический алгоритм	Математическая функция, которая вычисляет результат по одному или нескольким входным значениям.	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.	X.509 Q.815

Термин (англ.)	Термин	Определение	Ссылка
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.	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.	X.509
data integrity	Целостность данных	Показатель того, что данные не были изменены или разрушены несанкционированным образом.	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.	X.800 X.811
decipherment	Дешифрование	Инверсия соответствующего обратимого шифрования.	X.800
decryption	Дешифрация	См. Дешифрование.	X.800
delegation	Делегирование	Передача полномочия от одного объекта, который владеет данным полномочием, другому объекту.	X.509
denial of service	Отказ в обслуживании	Недопущение санкционированного доступа к ресурсам или задержка выполнения операций, критических по времени.	X.800
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.	X.800 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 справочника, соответствующая Рекомендации МСЭ-Т X.500.	X.843
eavesdropping	Перехват информации	Нарушение конфиденциальности путем слежения за связью.	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.	X.800 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).	J.170 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).	X.800

Термин (англ.)	Термин	Определение	Ссылка
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.	X.842 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.	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 защитные оболочки и маркеры безопасности применяются вместе с методами секретных ключей.	X.813
forgery	Фальсификация	Объект фабрикует информацию и заявляет, что такая информация была получена от другого объекта или направлена другому объекту.	M.3016.0
hash function	Хэш-функция	Функция (математическая), которая отображает значения из крупного (возможно очень крупного) набора значений в меньший диапазон значений.	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).	X.814
integrity	Целостность	Показатель того, что данные не были изменены несанкционированным образом. (См. также Целостность данных)	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.	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".	X.800
IPCablecom	Система IPCablecom	Проект МСЭ-Т, включающий архитектуру и серию рекомендаций, который обеспечивает возможность доставки реально временных услуг по сетям кабельного телевидения с использованием кабельных модемов.	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.	J.170
Key	Ключ	1. Последовательность символов, которые управляют операциями шифрования и дешифрования. 2. Математическая величина, введенная в выбранный криптографический алгоритм.	X.800 J.170
key exchange	Обмен ключами	Обмен между объектами открытыми ключами, которые должны использоваться для кодирования связи между этими объектами.	J.170

Термин (англ.)	Термин	Определение	Ссылка
key management	Управление ключами	Создание, хранение, рассылка, удаление, архивирование и применение ключей в соответствии со стратегией обеспечения безопасности.	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.	X.1151
masquerade	Подмена	Предпринимаемая объектом попытка представить себя другим объектом.	X.800
mutual authentication	Взаимная аутентификация	Обеспечение идентификации обоих администраторов доступа.	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 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.	J.170 H.235 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.	X.800
passive threat	Пассивная угроза	Угроза несанкционированного раскрытия содержания информации без изменения состояния системы.	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 полученный совместно используемое секретное значение пользователя применяются в целях аутентификации пользователя.	X.800 H.530
physical security	Физическая безопасность	Меры, предпринимаемые для обеспечения физической защиты ресурсов от умышленных и случайных угроз.	X.800
principal	Администратор доступа	Объект, идентификация которого может быть аутентифицирована.	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.	X.800 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.	X.509 X.810 J.170
privilege	Полномочие	Атрибут или свойство, назначенное объекту соответствующим органом.	X.509
Privilege Management Infrastructure (PMI)	Инфраструктура управления полномочиями (PMI)	Инфраструктура, способная поддерживать управление полномочиями при поддержке комплексной услуги авторизации и при взаимодействии с инфраструктурой открытых ключей.	X.509

Термин (англ.)	Термин	Определение	Ссылка
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, подлежащих отправке владельцу ключа.	X.509 X.810 J.170
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 органа сертификации. 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 цифровой подписью.	X.509 H.235 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 (PPK). 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.	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.	X.509
relying party	Доверяющая сторона	Пользователь или агент, который при принятии решения полагается на данные сертификата.	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).	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.	X.800 M.3016.0 X.402
revocation list certificate	Сертификат из списка аннулированных	Сертификат безопасности, который указан в списке сертификатов безопасности как аннулированный.	X.810
secret key	Секретный ключ	Ключ, используемый с асимметричным криптографическим алгоритмом. Обладание секретным ключом ограничено (обычно двумя объектами).	X.810
security	Безопасность	Термин "безопасность" используется в смысле минимизации не незащищенности активов и ресурсов. Активом является что-либо представляющее ценность. Незащищенность - это любое слабое место, которое может использоваться для нарушения работы системы или содержащееся в ней информации. Какая-либо угроза является потенциальным нарушением безопасности.	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.	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.	X.800
security audit trail	Данные проверки безопасности	Данные, которые собраны и могут быть использованы для содействия проведению проверки безопасности.	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 серии Рекомендаций МСЭ-Т X.800 принят во избежание терминологического несоответствия с Рекомендацией МСЭ-Т X.509.	X.810
security domain	Домен безопасности	1. Совокупность пользователей и систем, подчиняющихся общей стратегии обеспечения безопасности. 2. Набор ресурсов, подчиняющихся одной стратегии обеспечения безопасности.	X.841 X.411
security information (SI)	Информация о безопасности (ИБ)	Информация, необходимая для реализации услуг обеспечения безопасности.	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 контроля за доступом и т. д.; управление данными проверки безопасности и сигналами нарушения безопасности.	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.	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).	X.509 X.800
security service	Услуга безопасности	Услуга, предоставляемая каким-либо уровнем открытых систем связи, которая гарантирует достаточную защиту систем или процессов передачи данных.	X.800
security threat (threat)	Угроза безопасности (угроза)	Потенциальное нарушение безопасности.	X.800
security token	Маркер безопасности	Набор данных, передаваемых между объектами связи, 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.	X.509
shared secret	Коллективное секретное значение	Относится к ключу системы защиты для криптографических алгоритмов; может быть получено исходя из пароля.	H.530
signature	Подпись	См. Цифровая подпись.	X.800

Термин (англ.)	Термин	Определение	Ссылка
simple authentication	Простая аутентификация	Аутентификация посредством соглашений о простых паролях.	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.	X.509
spam	Спам	Незатребованная и нежелательная электронная почта	H.235
spoofing	Спуфинг	Имитация законного ресурса или пользователя.	X.509
strong authentication	Строгая аутентификация	Аутентификация с помощью криптографически полученных полномочий.	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.	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.	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.	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.	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).	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	Несанкционированный доступ	Объект пытается осуществить доступ к данным в нарушение действующей стратегии обеспечения безопасности.	M.3016.0
user authentication	Аутентификация пользователя	Установление доказательства идентификации пользователя-человека или прикладного процесса.	M.3016.0
verifier	Верификатор	Является объектом, требующим аутентификации, или представляет его. Верификатор включает в себя функции, необходимые для осуществления обменов в целях аутентификации.	X.811
vulnerability	Уязвимость	Любое слабое место, которое может быть использовано для нарушения системы или информации, которая в ней содержится.	X.800
X.509 certificate	Сертификат X.509	Спецификация сертификата открытого ключа, разработанная как часть каталога стандартов МСЭ-Т X.500.	J.170

Приложение B – Акронимы и сокращения, использованные в этом Руководстве

Приложение B
Акронимы и сокращения, использованные в этом Руководстве

Сокращение	Расшифровка	Определение
ACI	Access Control Information	Информация контроля за 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	Орган сертификации. Доверенная организация, которая принимает приложения сертификатов от объектов, аутентифицирует приложения, выдает сертификат и осуществляет ведение информации о статусе сертификатов
CDMA	Code Division Multiple Access	Многостанционный доступ с кодовым разделением
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
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	Пропускной пункт
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	Факсимильный шифр Hawthorne

HKM	Hawthorne Key Management algorithm	Алгоритм управления ключами Hawthorne
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
ICT	Information and Communication Technology	Информационно-коммуникационные технологии
ID	Identifier	Идентификатор
IdM	Identity Management	Управление определением идентичности
IEC	International Electrotechnical Commission	Международная электротехническая комиссия
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	Мгновенный обмен сообщениями
IMS	IP Multimedia Subsystem	Подсистема передачи мультимедийных данных по IP-сетям
IMT-2000	International Mobile Telecommunications 2000	Международная подвижная электросвязь 2000
IP	Internet Protocol	Интернет-протокол
IPSec	Internet Protocol Security	Безопасность Протокола интернет
IPTV	Internet Protocol TeleVision	IP телевидение
IPX	Internet Packet Exchange	Обмен Протоколами интернет
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	Сектора стандартизации электросвязи Международного союза электросвязи (МСЭ-Т)
LAN	Local Area Network	Локальная вычислительная сеть
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
MTA	Message Transfer Agent (In messaging) Media Terminal adapter (In cable technology)	Агент передачи сообщения (при передачи 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
P2P	Peer-to-peer	Одноранговый
PC	Personal Computer	Персональный компьютер

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
RBAC	Role-Based Access Control	Контроль за доступом по ролевому признаку
RFID	Radio Frequency Identification	Радиочастотная идентификация
RSA	Rivest, Shamir and Adleman (public-key algorithm)	Алгоритм Ривеста, Шамира и Адлмана (алгоритм шифрования с открытыми ключами)
RTP	Real time protocol	Протокол реального времени
SAML	Security Assertion Markup Language	Язык разметки, предусматривающий защиту данных
SG	Study Group	Исследовательская комиссия
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 во всей сети путем однократного ввода пароля
TCP/IP	Transmission Control Protocol/Internet Protocol	Протокол управления передачей /Интернет-протокол
TLS	Transport Layer Security	Безопасность транспортного уровня
TMN	Telecommunication Management Network	Сеть управления электросвязью
UE	User Equipment	Оборудование пользователя
UICC	Universal Integrated Circuit Card	Международная смарт-карта
USN	Ubiquitous Sensor Network	Повсеместная сеть датчиков
VoIP	Voice over IP	Передача голоса по IP
VPN	Virtual Private Network	Виртуальная частная сеть

WAN	Wide Area Network	Территориально-распределительная сеть
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 обязанностей, но ИК17, основным направлением которой является безопасность, была назначена ведущей исследовательской комиссией по безопасности. В Таблице 8 представлены описания роли исследовательских комиссий, в вопросах, связанных с проблемой безопасности, и список соответствующих обязанностей ведущих исследовательских комиссий.

Таблица 8 – 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 изменению 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	Кодирования, 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, указанные в этом Руководстве

Приложение D
Рекомендаций по безопасности, указанные в этом Руководстве

В 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 он-лайн по адресу: www.itu.int/rec/T-REC/en. Рекомендации МСЭ-Т по вопросам безопасности доступны через Часть 2 (База данных) путеводителя по стандартам безопасности (www.itu.int/МСЭ-T/studygroups/com17/ict/index.html).

Рекомендация	Название	Эквивалентный документ
E.408	Требования к безопасности сетей электросвязи	
E.409	Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи	
G.827	Параметры и цели функции готовности для сквозных международных цифровых трактов с постоянной скоростью передачи	
G.1000	Электросвязь. Качество обслуживания: Структура и определения	
G.1030	Оценка сквозного качества в IP сетях для приложений передачи данных	
G.1050	Модель сети для оценки качества передачи мультимедиа по Протоколу интернет	
G.1081	Точки контроля качественных показателей для IPTV	
H.235.0	H.323 Безопасность: Инфраструктура защиты в мультимедийных системах серии H (H.323 и других, основанных на H.245)	
H.235.1	H.323 Безопасность: Базовый профиль безопасности	
H.235.2	H.323 Безопасность: Профиль безопасности с подписью	
H.235.3	H.323 Безопасность: Гибридный профиль безопасности	
H.235.4	H.323 Безопасность: Защита соединения с прямой и селективной маршрутизацией	
H.235.5	H.323 Безопасность: Структура для надежной аутентификации в RAS с использованием слабо зашифрованных совместных секретных ключей	
H.235.6	Профиль шифрования речи с управлением внутренним ключом H.235/H.245	
H.Imp235	Руководство по реализации для H.235 V3: "Безопасность и шифрование для серии H (H.323 и другие мультимедийнеы терминалы на базе H.245)"	
H.323	Мультимедийные системы связи на основе пакетов	
H.350	Архитектура служб каталогов для мультимедийной конференцсвязи	
H.460.17	Применение сигнальных линий связи H.225.0 в качестве транспорта для сообщений H.323 RAS,	
H.460.18	Передача сигнализации H.323 через трансляторы сетевых адресов и брандмауэры	
H.460.19	Передача медиасигналов H.323 через трансляторы сетевых адресов и брандмауэры	

H.510	Подвижность для мультимедийных систем и услуг H.323	
H.530	Симметричные процедуры обеспечения безопасности для подвижной связи H.323 в H.510	
J.160	Структура архитектуры для предоставления критичных по времени услуг по сетям кабельного телевидения с использованием кабельных модемов	
J.170	Спецификация обеспечения безопасности IPCablecom	
J.360	IPCablecom2 Структура архитектуры – Главный документ	
M.3010	Принципы сети управления электросвязью	
M.3016.0	Безопасность для плоскости административного управления: обзор	
M.3016.1	Безопасность для плоскости административного управления: требования по безопасности	
M.3016.2	Безопасность для плоскости управления: услуги по обеспечению безопасности	
M.3016.3	Безопасность для плоскости управления: механизм обеспечения безопасности	
M.3016.4	Безопасность для уровня управления: проформа структуры	
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	
M.3210.1	Услуги управления СУЭ для управления обеспечением безопасности сетей IMT-2000	
Q.816	Услуги СУЭ на основе CORBA	
Q.834.3	Описание UML для требований интерфейса управления широкополосных пассивных оптических сетей	
Q.834.4	Спецификация интерфейса CORBA для широкополосных пассивных оптических сетей, основанная на требованиях интерфейса UML	
Q.1701	Концепция для сетей IMT-2000	
Q.1702	Долговременный прогноз для сетевых аспектов для систем после IMT-2000	
Q.1703	Концепция услуг и функций сети для сетевых аспектов систем после IMT-2000	
Q.1741.1	Ссылки на IMT-2000 для версии 1999 года, эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN	3GPP
Q.1742.1	Ссылки на IMT-2000 для версии 4, эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN	3GPP2
T.4	Стандартизация факсимильных терминалов Группы 3 для документальной электросвязи	
T.36	Возможности обеспечения безопасности при использовании факсимильных терминалов Группы 3	
T.37	Процедуры передачи факсимильных данных путем хранения и передачи по интернету	
T.38	Процедуры для передачи факсимильных данных Группы 3 в реальном времени по IP-сетям	
T.563	Характеристики терминалов для факсимильной аппаратуры Группы 4	
X.500	Справочник: обзор понятий, моделей и услуг	ИСО/МЭК 9594-1
X.501	Справочник: модели	ИСО/МЭК 9594-2
X.509	Справочник: структуры сертификатов открытых ключей и атрибутов	ИСО/МЭК 9594-8
X.511	Справочник: Абстрактное определение услуги	ИСО/МЭК 9594-3
X.518	Справочник: Процедуры для распределенных операций	ИСО/МЭК 9594-4
X.519	Справочник: Спецификация протокола	ИСО/МЭК 9594-5
X.520	Справочник: Отдельные типы атрибутов	ИСО/МЭК 9594-6
X.521	Справочник: отдельные классы объектов	ИСО/МЭК 9594-7
X.525	Справочник: Репликация	ИСО/МЭК 9594-9

X.530	Справочник: Использование управления системами для управления каталогом	ИСО/МЭК 9594-10
X.711	Общий протокол управления информацией: спецификация	ИСО/МЭК 9596-1
X.736	Управление системами: функция оповещения о нарушении безопасности	ИСО/МЭК 10164-7
X.740	Управление системами: Функция предоставления данных проверки безопасности	ИСО/МЭК 10164-8
X.741	Управление системами: объекты и атрибуты для контроля за доступом	ИСО/МЭК 10164-9
X.780	Руководству СУЭ для определения объектов, управляемых CORBA	
X.780.1	Руководящие указания по СУЭ для определения интерфейсов крупномодульных объектов, управляемых при помощи CORBA	
X.780.2	Руководящие указания по СУЭ для определения ориентированных на услугу объектов, управляемых при помощи CORBA и передовых объектов	
X.781	Требования и руководящие указания по проформам Деклараций соответствия внедрения, связанных с системами на основе CORBA	
X.790	Функция исправления неполадок для приложений МСЭ-Т	
X.800	Архитектура обеспечения безопасности в среде взаимодействия открытых систем для приложений МККТТ	ИСО/МЭК 7498-2
X.802	Модель обеспечения безопасности низших уровней	ИСО/МЭК TR 13594
X.803	Модель обеспечения безопасности высших уровней	ИСО/МЭК 10745
X.805	Архитектура безопасности для систем, обеспечивающих связь между оконечными пунктами	ИСО/МЭК 18028-2
X.810	Инфраструктура обеспечения безопасности открытых систем: Обзор	ИСО/МЭК 10181-1
X.811	Инфраструктура обеспечения безопасности открытых систем: основа аутентификации	ИСО/МЭК 10181-2
X.812	Инфраструктура обеспечения безопасности открытых систем: основа контроля за доступом	ИСО/МЭК 10181-3
X.813	Инфраструктура обеспечения безопасности открытых систем: основа обеспечения неотрекаемости	ИСО/МЭК 10181-4
X.814	Инфраструктура обеспечения безопасности открытых систем: основа обеспечения конфиденциальности	ИСО/МЭК 10181-5
X.815	Инфраструктура обеспечения безопасности открытых систем: основа обеспечения целостности	ИСО/МЭК 10181-6
X.816	Инфраструктура обеспечения безопасности открытых систем: основа проверки безопасности и сигналов нарушения безопасности	ИСО/МЭК 10181-7
X.830	Типичные высшие уровни обеспечения безопасности: обзор, модели и нотация	ИСО/МЭК 11586-1
X.831	Типичные высшие уровни обеспечения безопасности: определение услуги, обеспечиваемой элементом услуги обмена данными о безопасности (SESE)	ИСО/МЭК 11586-2
X.832	Типичные высшие уровни обеспечения безопасности: определение протокола элемента услуги обмена данными о безопасности (SESE)	ИСО/МЭК 11586-3
X.833	Типичные высшие уровни обеспечения безопасности: спецификация синтаксиса защиты перехода	ИСО/МЭК 11586-4
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
X.835	Типичные высшие уровни обеспечения безопасности: проформа PICS защиты синтаксиса перехода	ИСО/МЭК 11586-6
X.841	Информационные технологии – Информационные объекты, относящиеся к обеспечению безопасности, для контроля за доступом	ИСО/МЭК 15816
X.842	Информационные технологии – Руководящие принципы для использования услуг пользующейся доверием третьей стороны и управления ими	ИСО/МЭК TR 14516
X.843	Информационные технологии – Спецификации услуг TTP для поддержки применения цифровых подписей	ИСО/МЭК 15945
X.Доп3 к X.800–X.849	Дополнение по руководящим указаниям для внедрения системы и безопасности сети	

X.1031	Роли конечных пользователей и сетей электросвязи в рамках архитектуры безопасности	
X.1034	Руководящие указания по расширяемому протоколу аутентификации, основанному на аутентификации и управлении ключами в сети передачи данных	
X.1035	Протокол обмена ключами (PAK) с аутентификацией по паролю	
X.1036	Структура для создания, хранения, распространения и выполнения правил для обеспечения безопасности сети	
X.1051	Методы обеспечения безопасности – Руководство по управлению информационной безопасностью для организаций электросвязи, основанное на ИСО/МЭК 27002	ИСО/МЭК 27011
X.1055	Управление рисками и руководство по профилям рисков для организаций электросвязи	
X.1056	Руководящие указания для организаций электросвязи по управлению инцидентами в области безопасности и и	
X.1081	Основа для спецификации аспектов защиты и безопасности телебиометрии	
X.1082	Телебиометрия, связанная с психологией человека	ИСО/МЭК 80000-14
X.1083	Биометрия – протокол сетевого взаимодействия BioAPI	ИСО/МЭК 24708
X.1084	Механизм телебиометрической системы – Часть 1: Общий протокол биометрической аутентификации и профили модели системы для систем электросвязи	
X.1086	Процедуры телебиометрической защиты – Часть 1: Руководство по техническим и организационным мерам противодействия для безопасности биометрических данных	
X.1088	Структура цифрового телебиометрического ключа (TDK) – Структура для генерирования и защиты цифрового телебиометрического ключа	
X.1089	Инфраструктура телебиометрической аутентификации (TAI)	
X.1111	Концепция технологий безопасности для домашней сети	
X.1112	Профиль сертификата устройства для домашней сети	
X.1113	Руководство по механизмам аутентификации пользователя для услуг домашней сети	
X.1114	Основы санкционирования для домашней сети	
X.1121	Концепция технологий безопасности для подвижной связи между конечными пунктами	
X.1122	Руководящие указания по созданию защищенных систем подвижной связи на основе инфраструктуры открытого ключа (PKI)	
X.1123	Различные услуги безопасности для подвижной передачи данных между конечными пунктами	
X.1124	Архитектура аутентификации архитектура для подвижной связи между конечными пунктами	
X.1125	Система коррелированного реагирования в подвижной передачи данных между конечными пунктами	
X.1141	Язык разметки, предусматривающий защиту данных (SAML 2.0)	OASIS SAML 2.0
X.1142	Расширяемый язык разметки контроля доступа (XACML 2.0)	OASIS XACML 2.0
X.1143	Архитектура безопасности для защиты сообщений в подвижных веб-услугах	
X.1151	Руководство по протоколу аутентификации на базе секретного пароля с обменом ключами	
X.1152	Методы безопасной передачи данных между конечными пунктами с использованием услуг доверенной третьей стороны	
X.1161	Концепция защиты одноранговой связи	

X.1162	Архитектура безопасности и работы для одноранговых сетей	
X.1171	Угрозы и требования для защиты персональной идентификационной информации в приложениях, использующих идентификацию на базе меток	
X.1191	Функциональные требования и архитектура аспектов безопасности IPTV	
X.1205	Обзор кибербезопасности	
X.1206	Независимая от поставщика концепция автоматического уведомления об информации по безопасности и распространение обновлений	
X.1207	Руководство для поставщиков услуг электросвязи по оценке рисков шпионских программ и потенциально нежелательного программного обеспечения	
X.1231	Технические стратегии в деле противостояния спаму	
X.1240	Технологии, используемые в борьбе со спамом в электронной почте	
X.1241	Технические основы противодействия спаму в электронной почте	
X.1242	Система фильтрации спама в службе коротких сообщений (СМС), основанная на правилах, определенных пользователем	
X.1244	Общие аспекты противостояния спаму в мультимедийных IP-приложениях	
X.1250	Основные возможности для расширенного глобального управления идентичностью и взаимодействием	
X.1251	Структура для управления цифровой идентичностью со стороны пользователя	
X.1303	Общий протокол оповещения (CAP 1.1)	OASIS CAP v1.1
X.Sup6	Серия МСЭ-Т X.1240 – Дополнение по вопросам противостояния спаму и связанным с ним угрозам	
X.Sup7	Серия МСЭ-Т X.1250 – Дополнение по обзору управления идентичностью контексте кибербезопасности	
Y.2001	Общий обзор СПП	
Y.2701	Требования к безопасности для СПП, релиз 1	
Y.2720	Основы управления идентичностью в СПП	
	Другие публикации	
	Технологии внешних установок для сетей общего пользования	
	Применение компьютеров и микропроцессоров для создания, установки и защиты кабелей электросвязи	

Отпечатано в Швейцарии
Женева, 2010 г.